Alcatel·Lucent Enterprise

Access Guardian and BYOD in AOS Release 8.1.1

Configuration Guide through Use Cases

Alcatel-Lucent, 26801 West Agoura Road, Calabasas, CA 91301, USA
+1(818) 880-3500

Contents

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

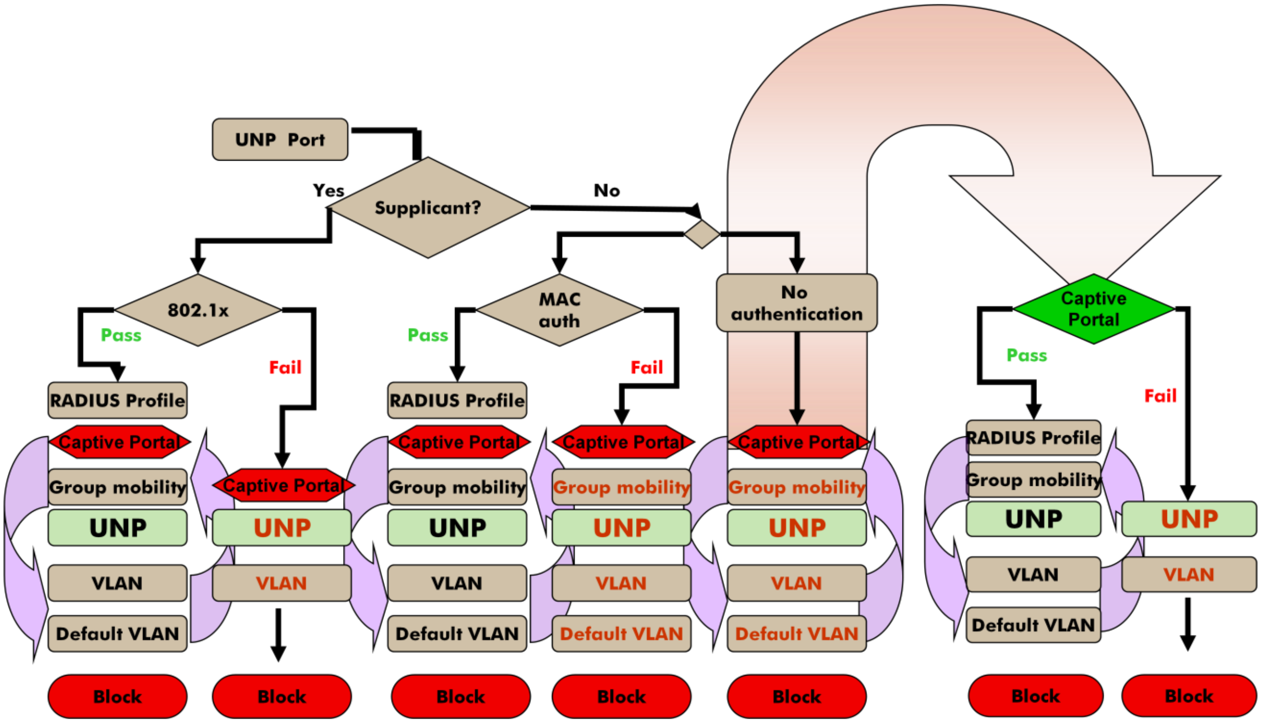
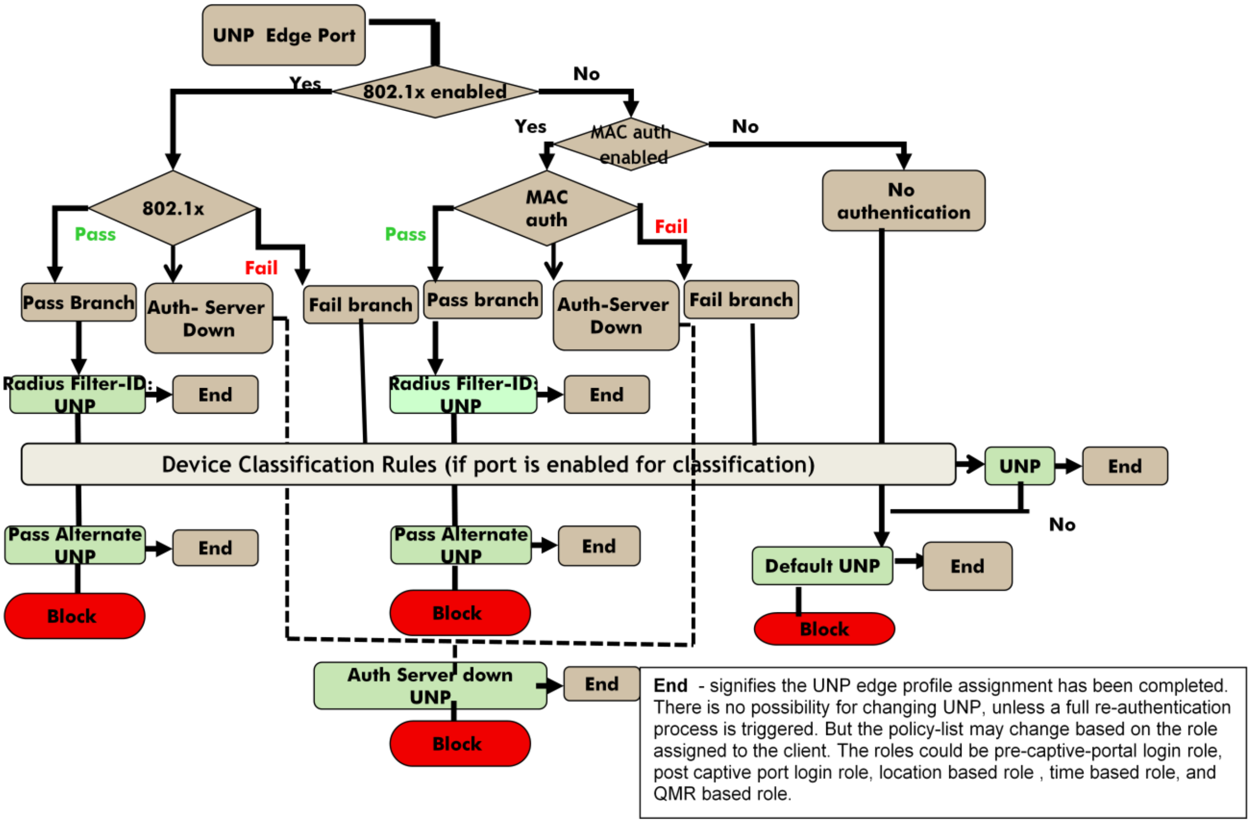


Figure 2. Access Guardian in AOS 8.1.1 Workflow



End - signifies the UNP edge profile assignment has been completed. There is no possibility for changing UNP, unless a full re-authentication process is triggered. But the policy-list may change based on the role assigned to the client. The roles could be pre-captive-portal login role, post captive port login role, location based role , time based role, and QMR based role.

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/lldp/DPI without changing the profile or VLAN.

5. VLAN to User Network Profile

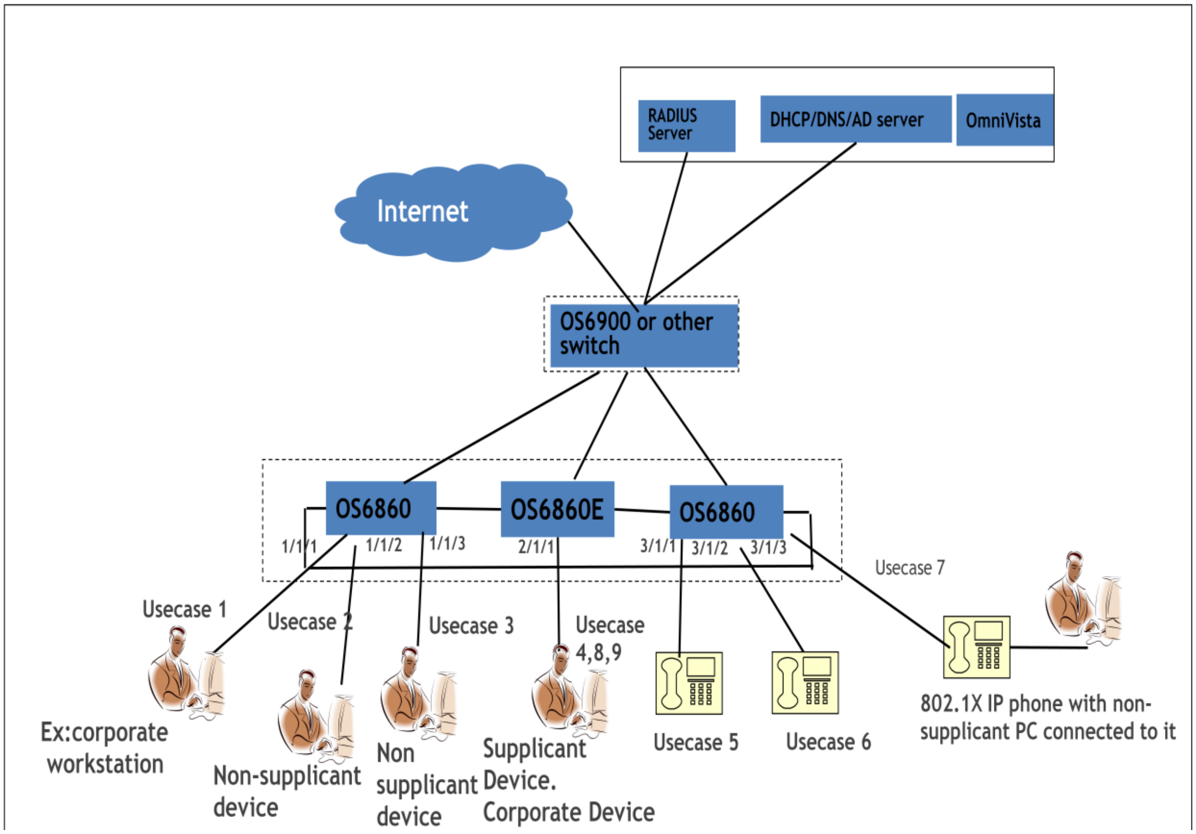
    a. In AOS 6.x, a VLAN was a property of the UNP.

    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-supplicant 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 supplicant corporate devices only.

4.5 USE CASE 4b: Supplicant/non-supplicant device authentication with Captive Portal

This use case covers supplicant 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 supplicant device
  - Will pass 802.1x authentication
  - The client can be assigned a UNP corporate edge-profile/VLAN.

- Corporate user with non-supplicant 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 supplicant 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-supplicant device
  - Will not trigger 802.1x authentication
  - If non-supplicant, 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 RAIDUS 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 RAIDUS 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

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

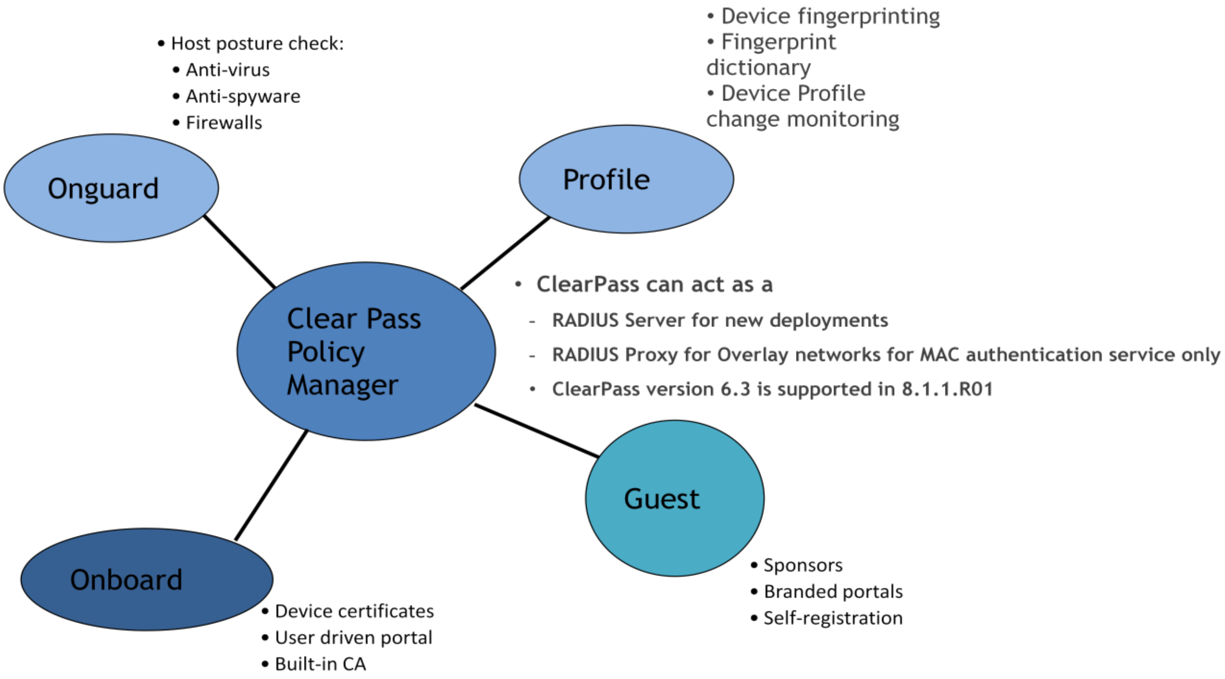
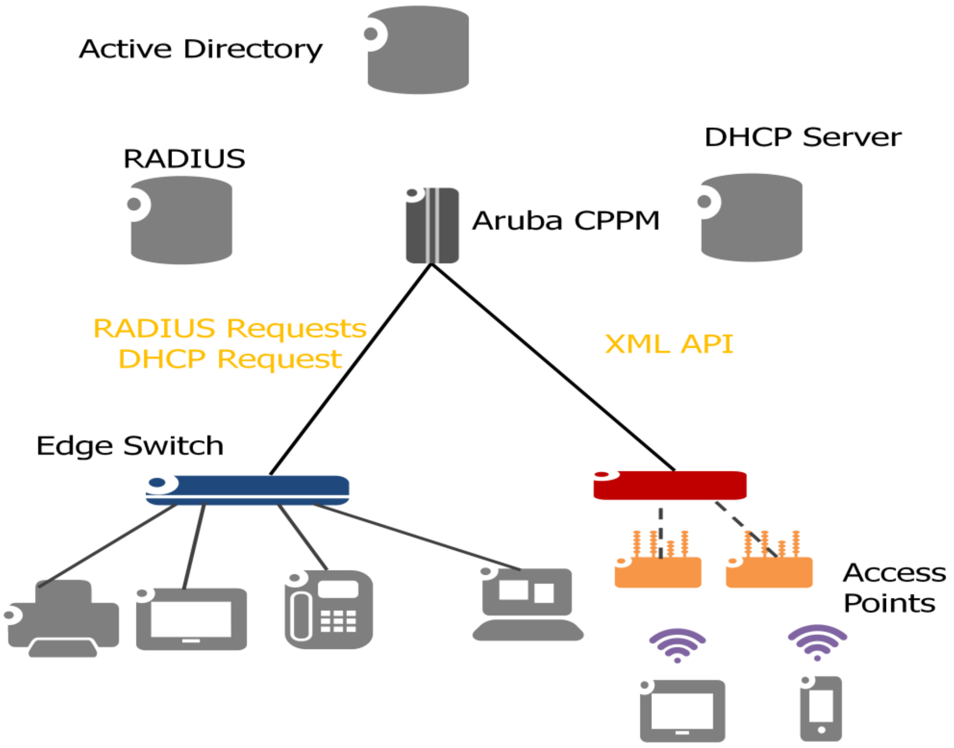


Figure 5. Components of the BYOD solution



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 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.

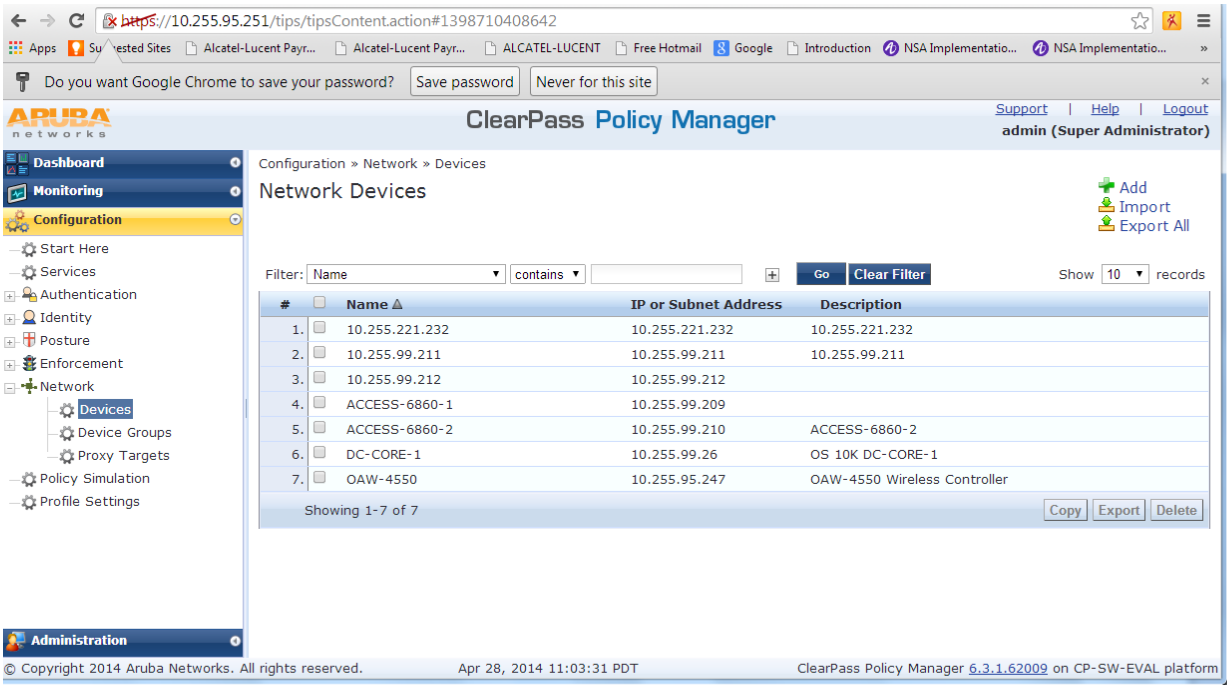
2. **Alcatel-Redirection-URL**
   - **VSA ID:** 101
   - **Description:** This attribute is used to return the URL to which the switch is required to redirect all http/https traffic arriving from the client on a port. This must be sent along with the UNP edge-profile name returned in the RADIUS Filter-id 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.



Configuration » Network » Devices

Network Devices

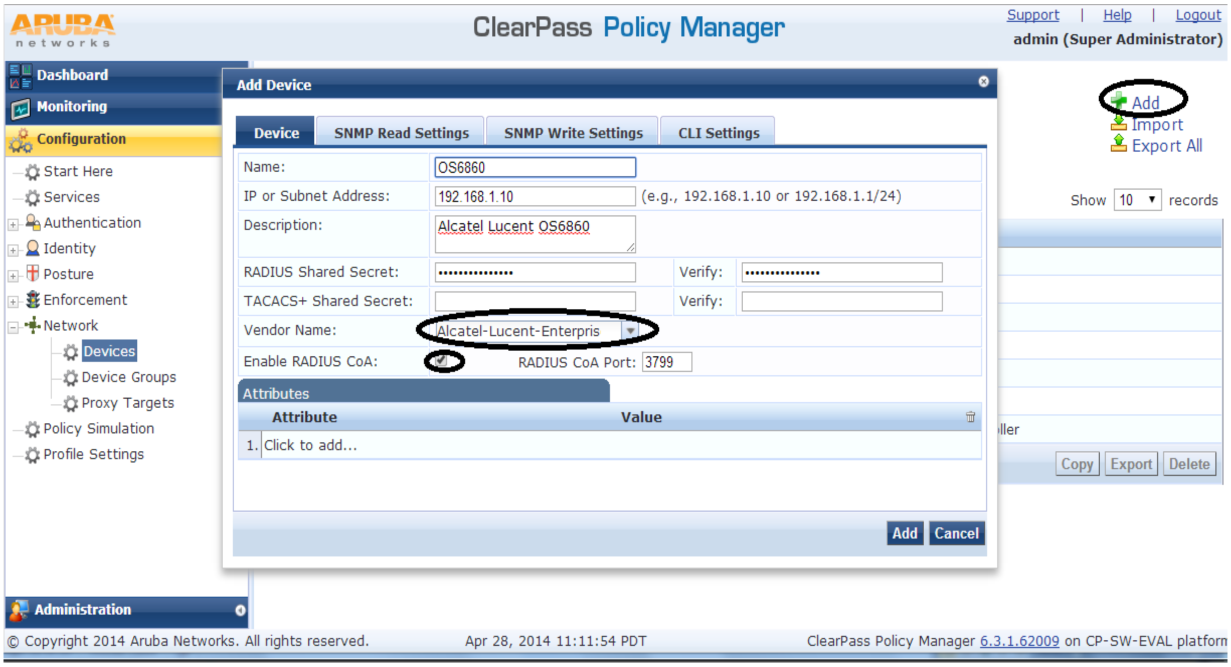
Filter: Name contains | Show 10 records

#		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

Showing 1-7 of 7

© Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 11:03:31 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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.



Add Device

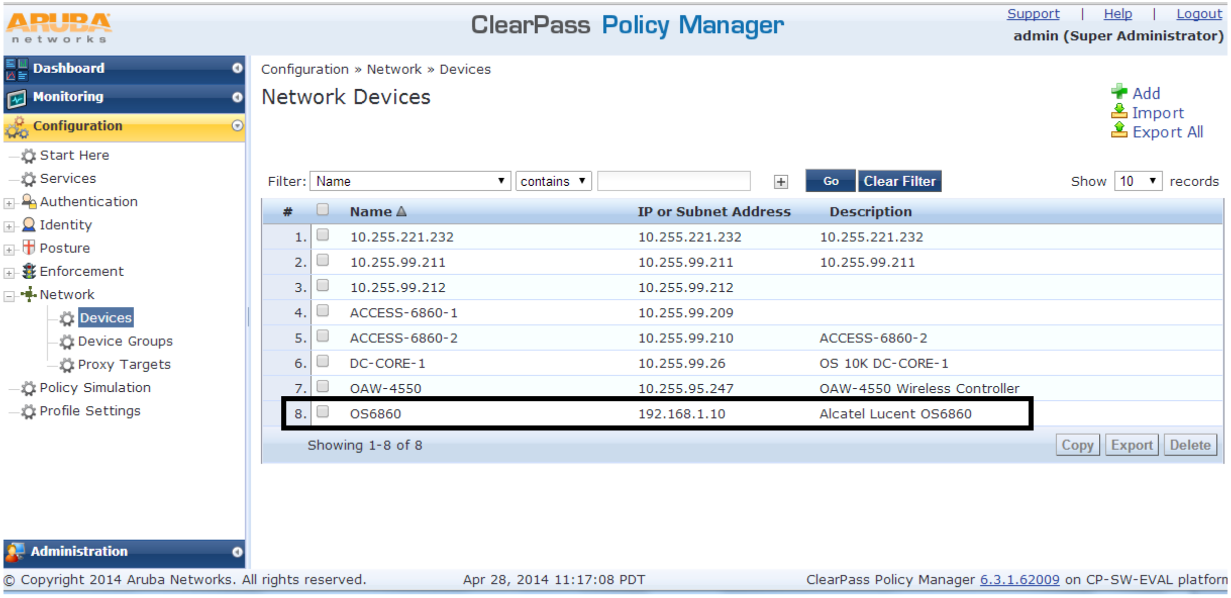
Name:	OS6860		
IP or Subnet Address:	192.168.1.10	(e.g., 192.168.1.10 or 192.168.1.1/24)	
Description:	Alcatel Lucent OS6860		
RADIUS Shared Secret:	•••••••••••••••	Verify:	•••••••••••••••
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Alcatel-Lucent-Enterpris		
Enable RADIUS CoA:	☑	RADIUS CoA Port:	3799

Attributes

	Attribute	Value
1.	Click to add...	

© Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 11:11:54 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

The device is added.



Configuration » Network » Devices

Network Devices

Filter: Name contains Show 10 records

#	□	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
8.	□	OS6860	192.168.1.10	Alcatel Lucent OS6860

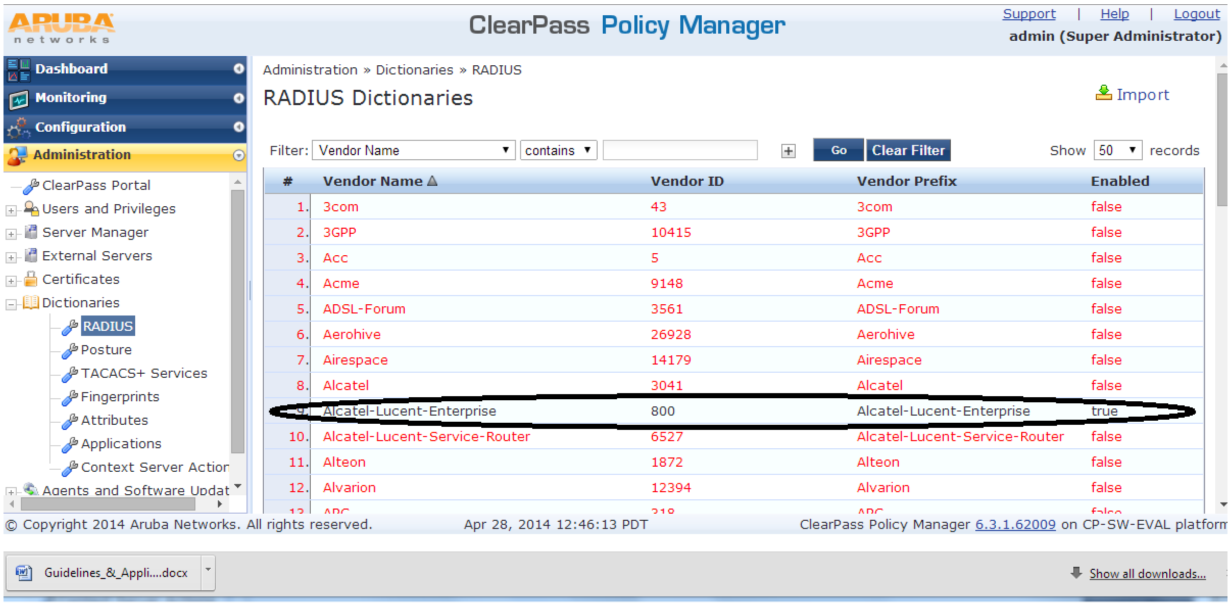
Showing 1-8 of 8

© Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 11:17:08 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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.



Administration » Dictionaries » RADIUS

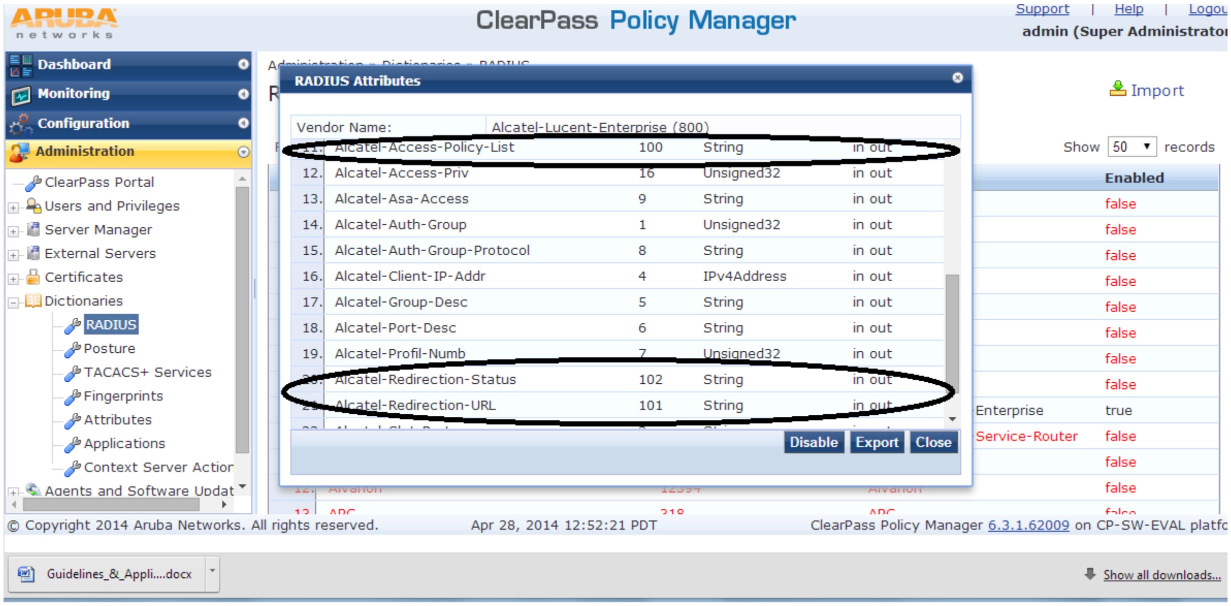
RADIUS Dictionaries

Filter: Vendor Name ▼ contains ▼ Show 50 ▼ records

#	Vendor Name	Vendor ID	Vendor Prefix	Enabled
1.	3com	43	3com	false
2.	3GPP	10415	3GPP	false
3.	Acc	5	Acc	false
4.	Acme	9148	Acme	false
5.	ADSL-Forum	3561	ADSL-Forum	false
6.	Aerohive	26928	Aerohive	false
7.	Airespace	14179	Airespace	false
8.	Alcatel	3041	Alcatel	false
9.	Alcatel-Lucent-Enterprise	800	Alcatel-Lucent-Enterprise	true
10.	Alcatel-Lucent-Service-Router	6527	Alcatel-Lucent-Service-Router	false
11.	Alteon	1872	Alteon	false
12.	Alvarion	12394	Alvarion	false

© Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 12:46:13 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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



RADIUS Attributes

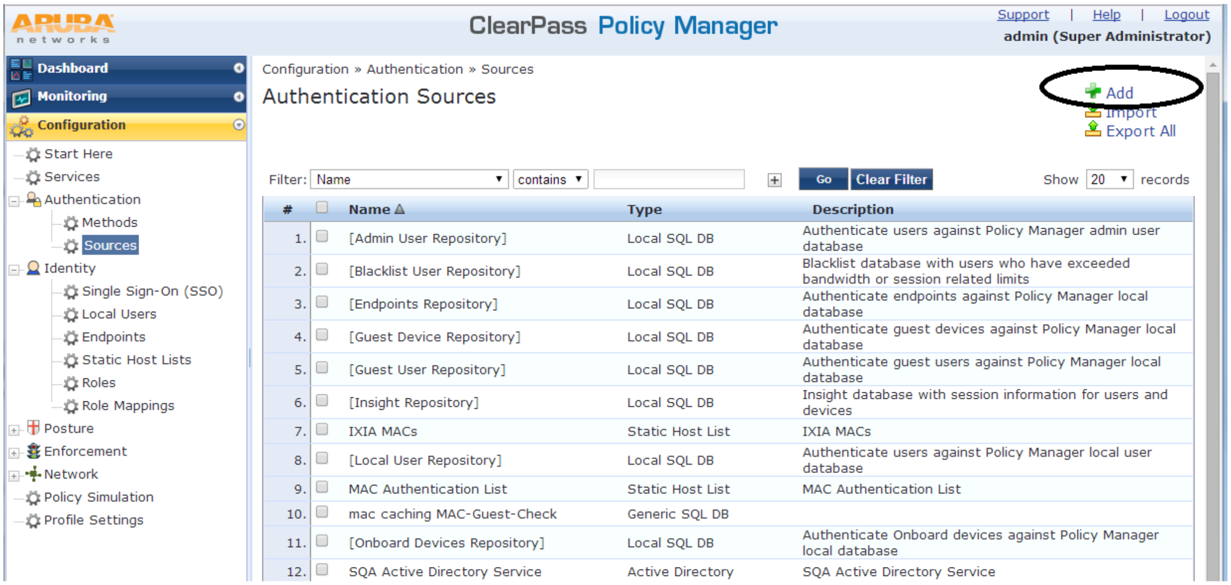
Vendor Name: Alcatel-Lucent-Enterprise (800)

11.	Alcatel-Access-Policy-List	100	String	in out
12.	Alcatel-Access-Priv	16	Unsigned32	in out
13.	Alcatel-Asa-Access	9	String	in out
14.	Alcatel-Auth-Group	1	Unsigned32	in out
15.	Alcatel-Auth-Group-Protocol	8	String	in out
16.	Alcatel-Client-IP-Addr	4	IPv4Address	in out
17.	Alcatel-Group-Desc	5	String	in out
18.	Alcatel-Port-Desc	6	String	in out
19.	Alcatel-Profil-Numb	7	Unsigned32	in out
20.	Alcatel-Redirection-Status	102	String	in out
21.	Alcatel-Redirection-URL	101	String	in out

© Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 12:52:21 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platfo

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.



admin (Super Administrator)

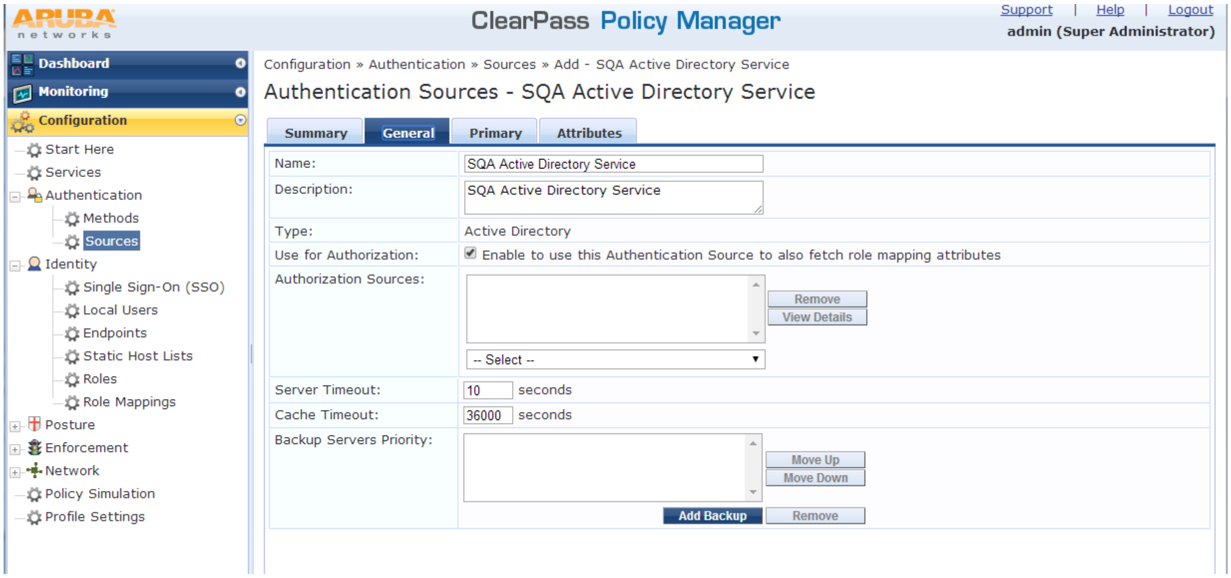
Configuration » Authentication » Sources

Authentication Sources

Filter: Name contains Show 20 records

#	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.



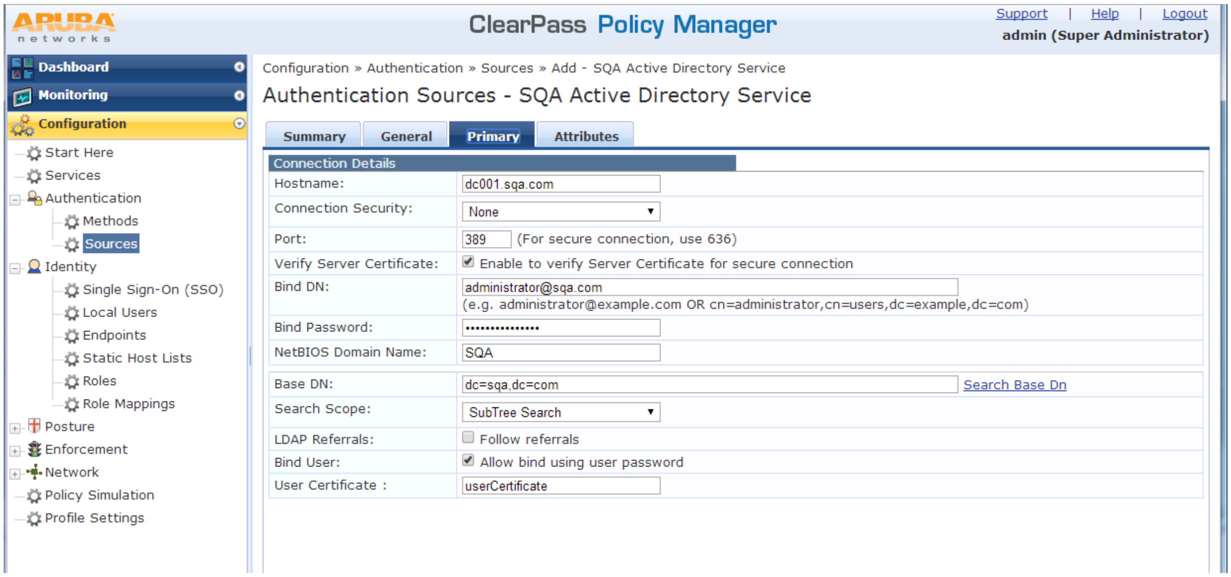
admin (Super Administrator)

Configuration » Authentication » Sources » Add - SQA Active Directory Service

Authentication Sources - SQA Active Directory Service

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:	-- Select --
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	

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



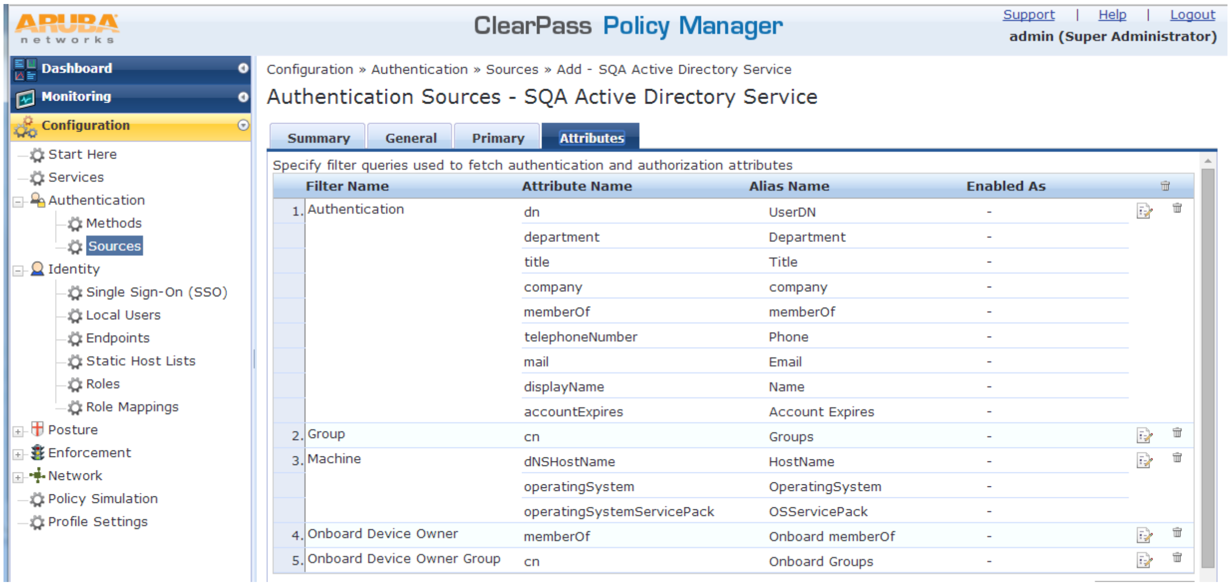
Configuration » Authentication » Sources » Add - SQA Active Directory Service

Authentication Sources - SQA Active Directory Service

Connection Details

Hostname:	dc001.sqa.com
Connection Security:	None
Port:	389 (For secure connection, use 636)
Verify Server Certificate:	☑ Enable to verify Server Certificate for secure connection
Bind DN:	administrator@sqa.com (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)
Bind Password:	•••••••••••••••
NetBIOS Domain Name:	SQA
Base DN:	dc=sqa,dc=com Search Base Dn
Search Scope:	SubTree Search
LDAP Referrals:	☐ Follow referrals
Bind User:	☑ Allow bind using user password
User Certificate :	userCertificate

4. 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.



Configuration » Authentication » Sources » Add - SQA Active Directory Service

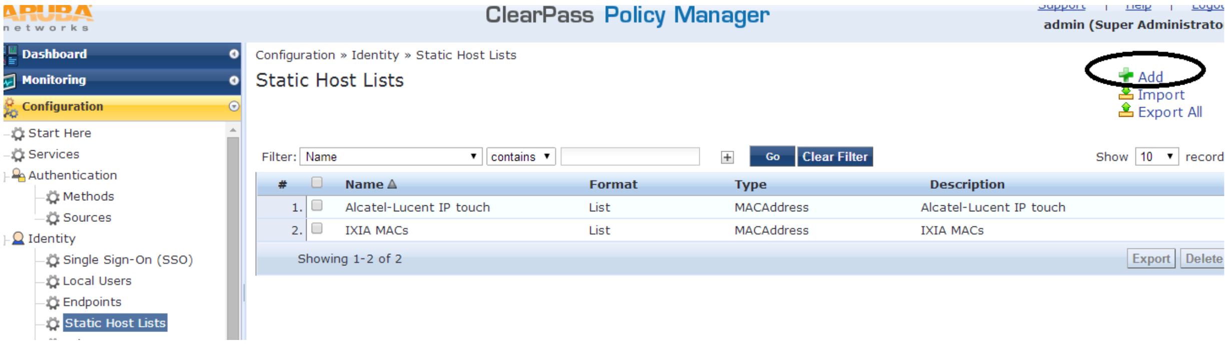
Authentication Sources - SQA Active Directory Service

Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Authentication	dn	UserDN	-
		department	Department	-
		title	Title	-
		company	company	-
		memberOf	memberOf	-
		telephoneNumber	Phone	-
		mail	Email	-
		displayName	Name	-
		accountExpires	Account Expires	-
2.	Group	cn	Groups	-
3.	Machine	dNSHostName	HostName	-
		operatingSystem	OperatingSystem	-
		operatingSystemServicePack	OSServicePack	-
4.	Onboard Device Owner	memberOf	Onboard memberOf	-
5.	Onboard Device Owner Group	cn	Onboard Groups	-

5.3.4 Configure Static Host List for IP phones/printer devices

1. 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.



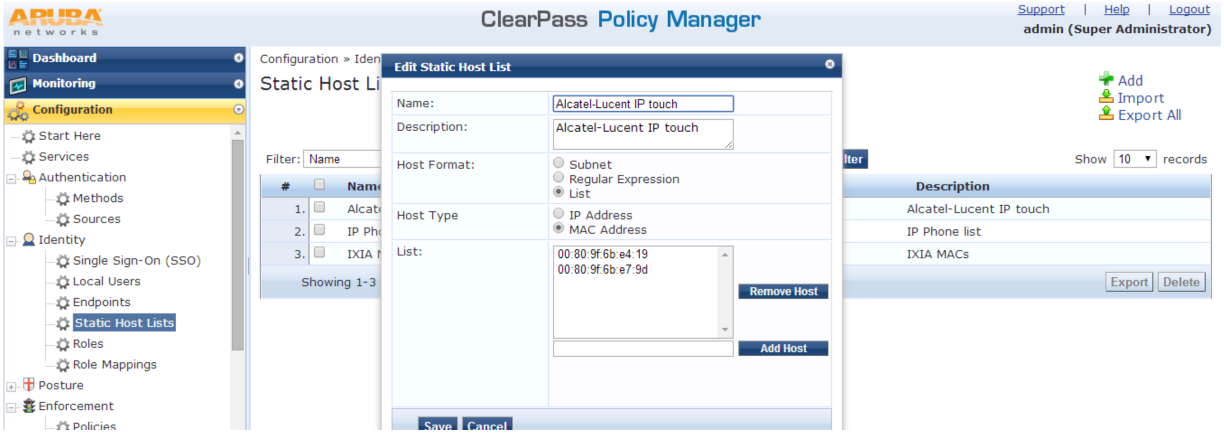
Configuration » Identity » Static Host Lists

Static Host Lists

#	Name	Format	Type	Description
1.	Alcatel-Lucent IP touch	List	MACAddress	Alcatel-Lucent IP touch
2.	IXIA MACs	List	MACAddress	IXIA MACs

Showing 1-2 of 2

2. 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.



Configuration » Iden

Static Host Li

Edit Static Host List

Name: Alcatel-Lucent IP touch

Description: Alcatel-Lucent IP touch

Host Format: ○ Subnet ○ Regular Expression ● List

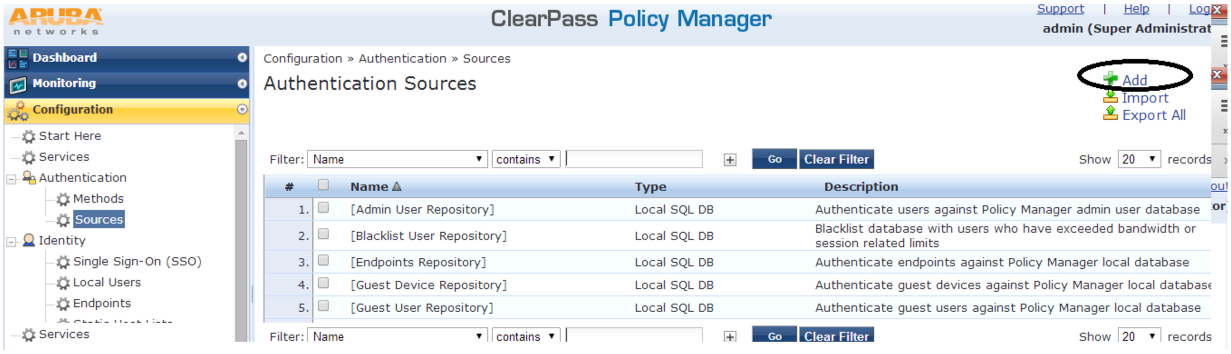
Host Type: ○ IP Address ● MAC Address

List:
00:80:9f:6b:e4:19
00:80:9f:6b:e7:9d

#	Name	Description
1.	Alcat	Alcatel-Lucent IP touch
2.	IP Ph	IP Phone list
3.	IXIA I	IXIA MACs

Showing 1-3

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

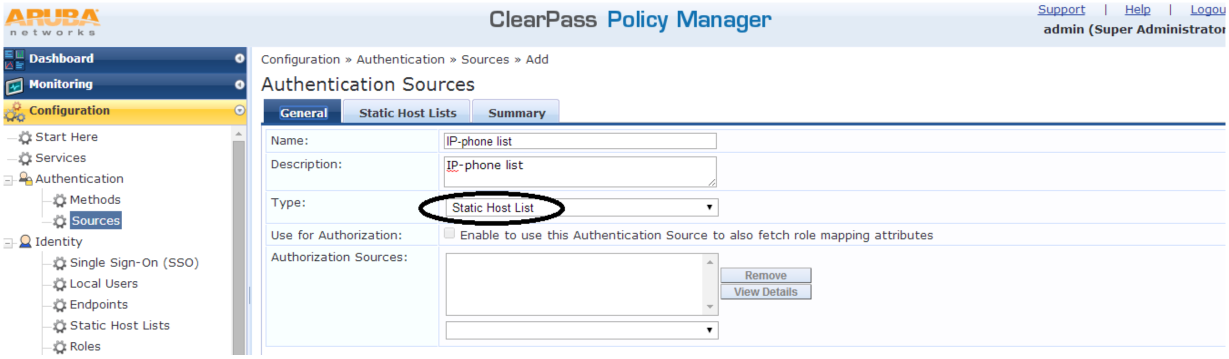


Configuration » Authentication » Sources

Authentication Sources

#	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

4. Enter a name and description and select Type to be “Static Host List”



Configuration » Authentication » Sources » Add

Authentication Sources

Name: IP-phone list

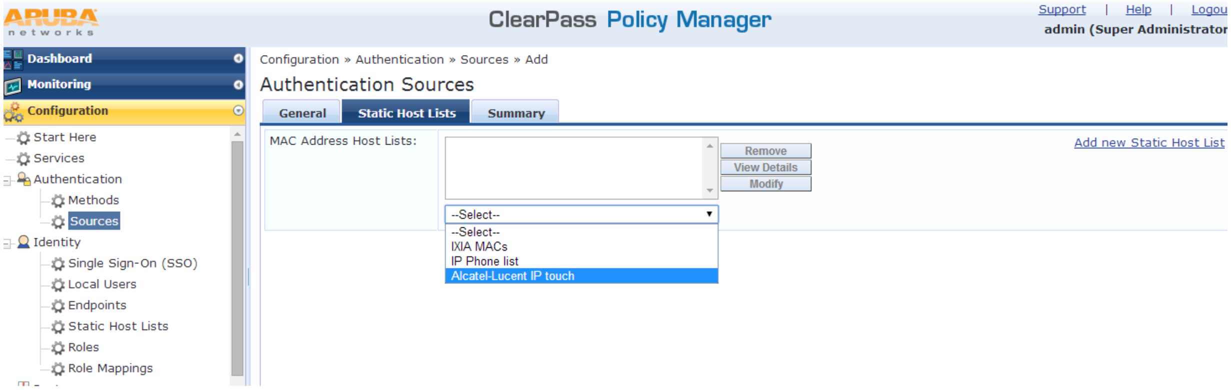
Description: IP-phone list

Type: Static Host List

Use for Authorization: ☐ Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources:

5. Select the IP phone list created



Configuration » Authentication » Sources » Add

Authentication Sources

MAC Address Host Lists:

--Select--

--Select--
IXIA MACs
IP Phone list
Alcatel-Lucent IP touch

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

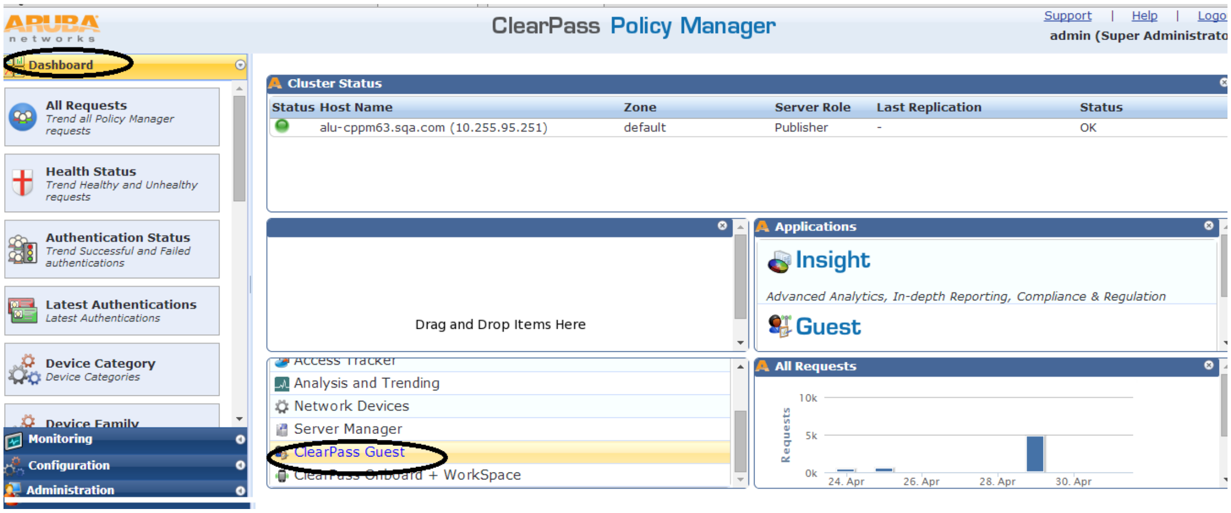
The CPPM configuration can be grouped into following three categories:

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:

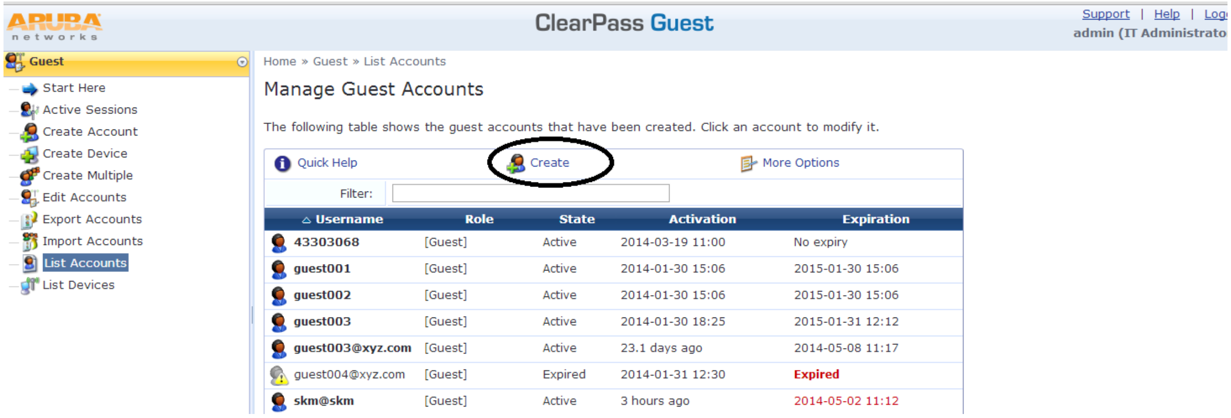
1. Go to Dashboard. Select ClearPass Guest as shown.



Cluster Status

Status	Host Name	Zone	Server Role	Last Replication	Status
●	alu-cppm63.sqa.com (10.255.95.251)	default	Publisher	-	OK

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



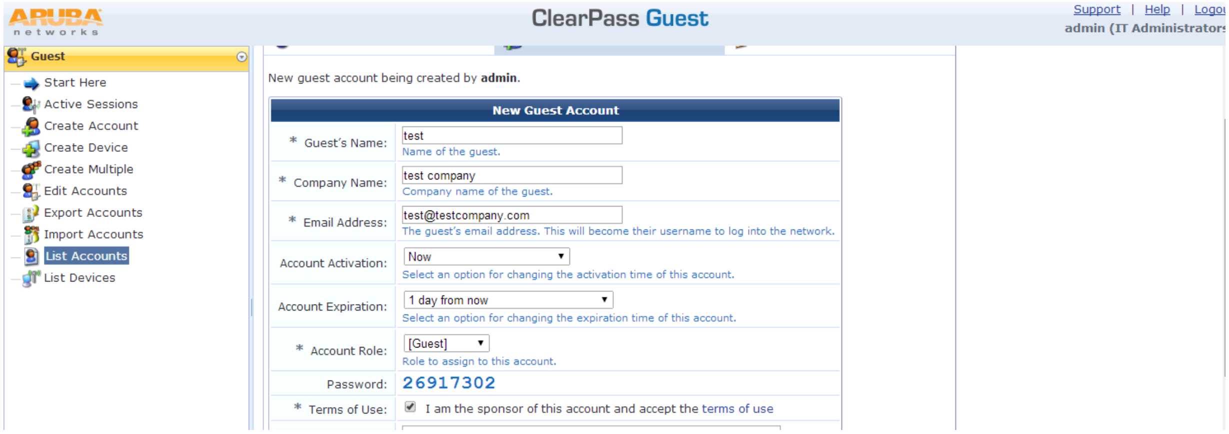
Manage Guest Accounts

The following table shows the guest accounts that have been created. Click an account to modify it.

Filter:

Username	Role	State	Activation	Expiration
43303068	[Guest]	Active	2014-03-19 11:00	No expiry
guest001	[Guest]	Active	2014-01-30 15:06	2015-01-30 15:06
guest002	[Guest]	Active	2014-01-30 15:06	2015-01-30 15:06
guest003	[Guest]	Active	2014-01-30 18:25	2015-01-31 12:12
guest003@xyz.com	[Guest]	Active	23.1 days ago	2014-05-08 11:17
guest004@xyz.com	[Guest]	Expired	2014-01-31 12:30	Expired
skm@skm	[Guest]	Active	3 hours ago	2014-05-02 11:12

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.



New guest account being created by **admin**.

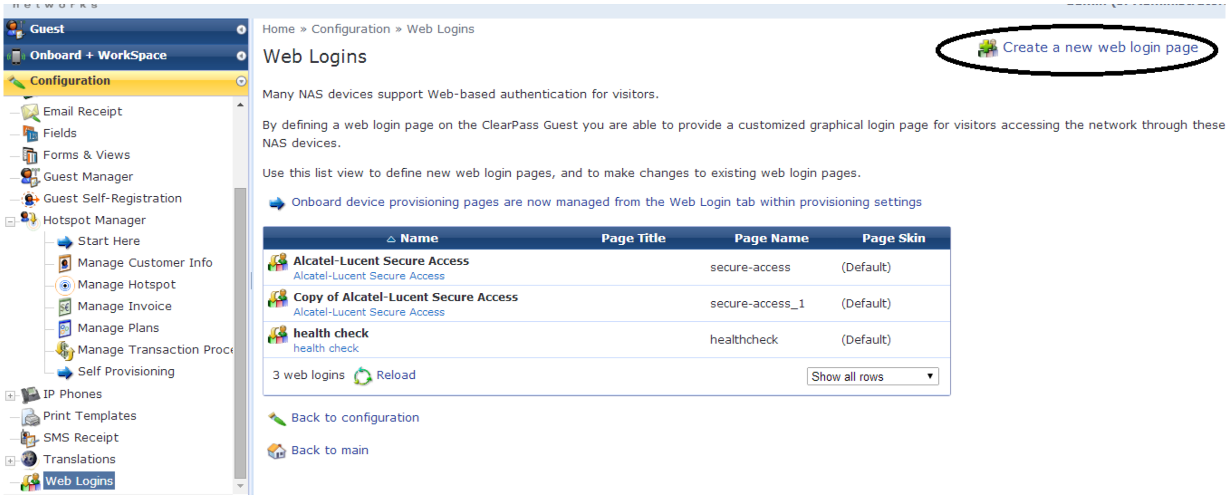
New Guest Account

* Guest's Name:	test Name of the guest.
* Company Name:	test company Company name of the guest.
* Email Address:	test@testcompany.com The guest's email address. This will become their username to log into the network.
Account Activation:	Now ▾ Select an option for changing the activation time of this account.
Account Expiration:	1 day from now ▾ Select an option for changing the expiration time of this account.
* Account Role:	[Guest] ▾ Role to assign to this account.
Password:	26917302
* Terms of Use:	☑ I am the sponsor of this account and accept the terms of use

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”.



Home » Configuration » Web Logins

Web Logins

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for visitors accessing the network through these NAS devices.

Use this list view to define new web login pages, and to make changes to existing web login pages.

Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

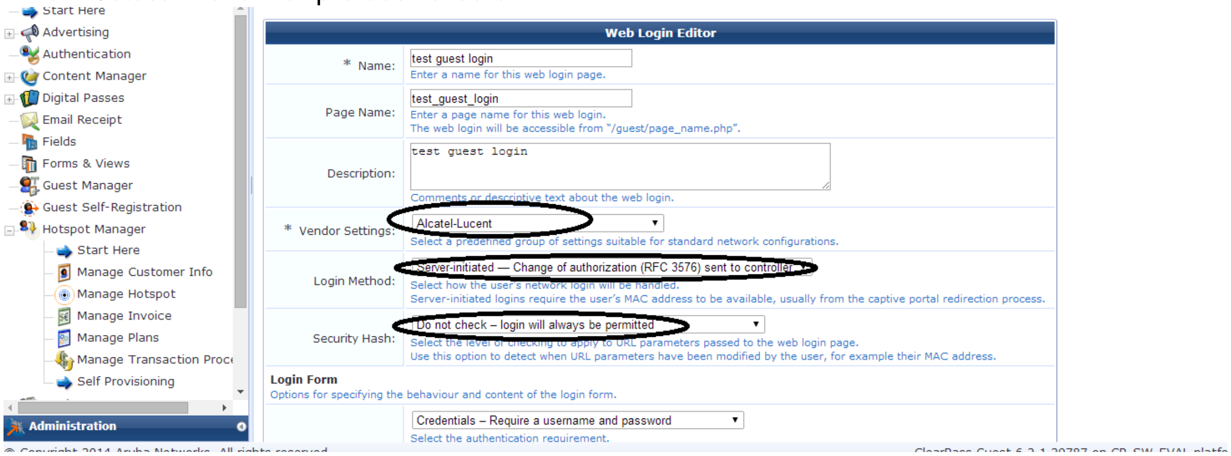
△ Name	Page Title	Page Name	Page Skin
Alcatel-Lucent Secure Access Alcatel-Lucent Secure Access		secure-access	(Default)
Copy of Alcatel-Lucent Secure Access Alcatel-Lucent Secure Access		secure-access_1	(Default)
health check health check		healthcheck	(Default)

3 web logins

Back to configuration

Back to main

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.



Web Login Editor

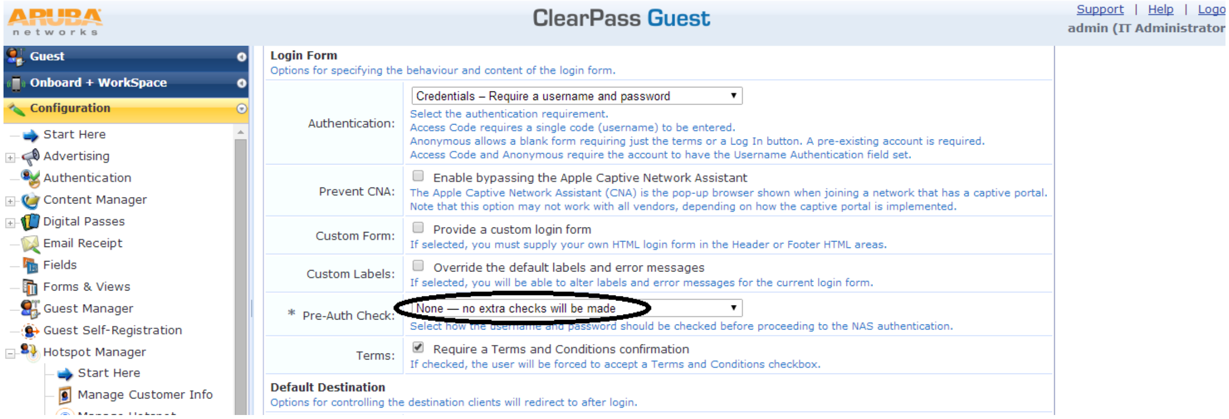
* Name:	test guest login Enter a name for this web login page.
Page Name:	test_guest_login Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	test guest login Comments or descriptive text about the web login.
* Vendor Settings:	Alcatel-Lucent Select a predefined group of settings suitable for standard network configurations.
Login Method:	Server-initiated — Change of authorization (RFC 3576) sent to controller Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
Security Hash:	Do not check – login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

Login Form
Options for specifying the behaviour and content of the login form.

	Credentials – Require a username and password Select the authentication requirement.

© Copyright 2014 Aruba Networks. All rights reserved. ClearPass Guest 6.3.1.20787 on CP-SW-EVAL platfo

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.



Login Form
Options for specifying the behaviour and content of the login form.

Authentication:	Credentials – Require a username and password ▾ Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Access Code and Anonymous require the account to have the Username Authentication field set.
Prevent CNA:	□ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	□ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	□ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	None — no extra checks will be made ▾ Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	☑ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

Default Destination
Options for controlling the destination clients will redirect to after login.

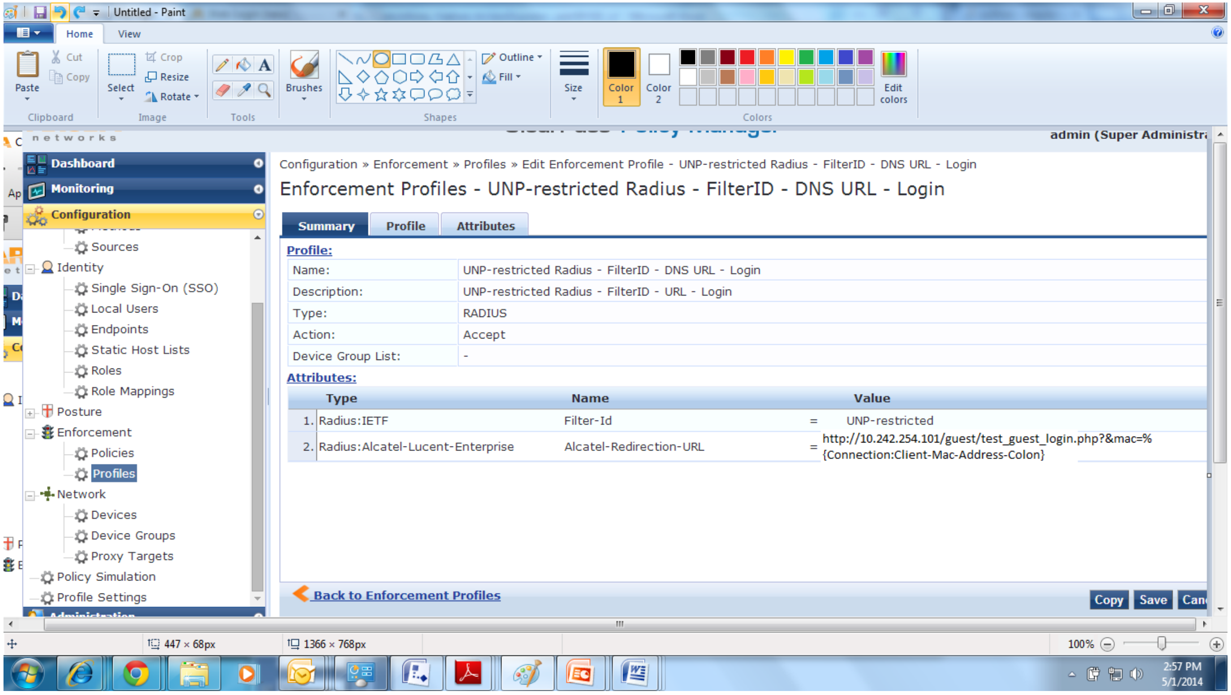
5.5.2.3 Configuring the enforcement profiles

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.



Configuration » Enforcement » Profiles » Edit Enforcement Profile - UNP-restricted Radius - FilterID - DNS URL - Login

Enforcement Profiles - UNP-restricted Radius - FilterID - DNS URL - Login

Summary | Profile | Attributes

Profile:

Name:	UNP-restricted Radius - FilterID - DNS URL - Login
Description:	UNP-restricted Radius - FilterID - URL - Login
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

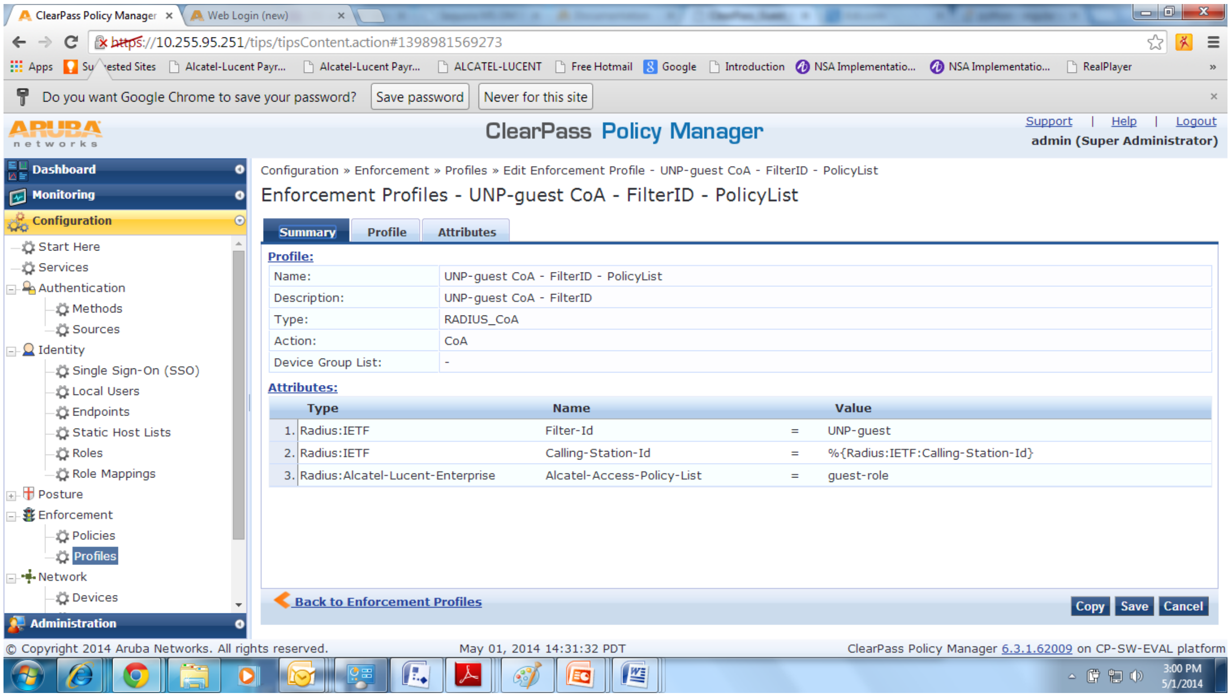
	Type	Name		Value
1.	Radius:IETF	Filter-Id	=	UNP-restricted
2.	Radius:Alcatel-Lucent-Enterprise	Alcatel-Redirection-URL	=	http://10.242.254.101/guest/test_guest_login.php?&mac=%{Connection:Client-Mac-Address-Colon}

Back to Enforcement Profiles

Copy Save Can

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.



Configuration » Enforcement » Profiles » Edit Enforcement Profile - UNP-guest CoA - FilterID - PolicyList

Enforcement Profiles - UNP-guest CoA - FilterID - PolicyList

Profile:

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

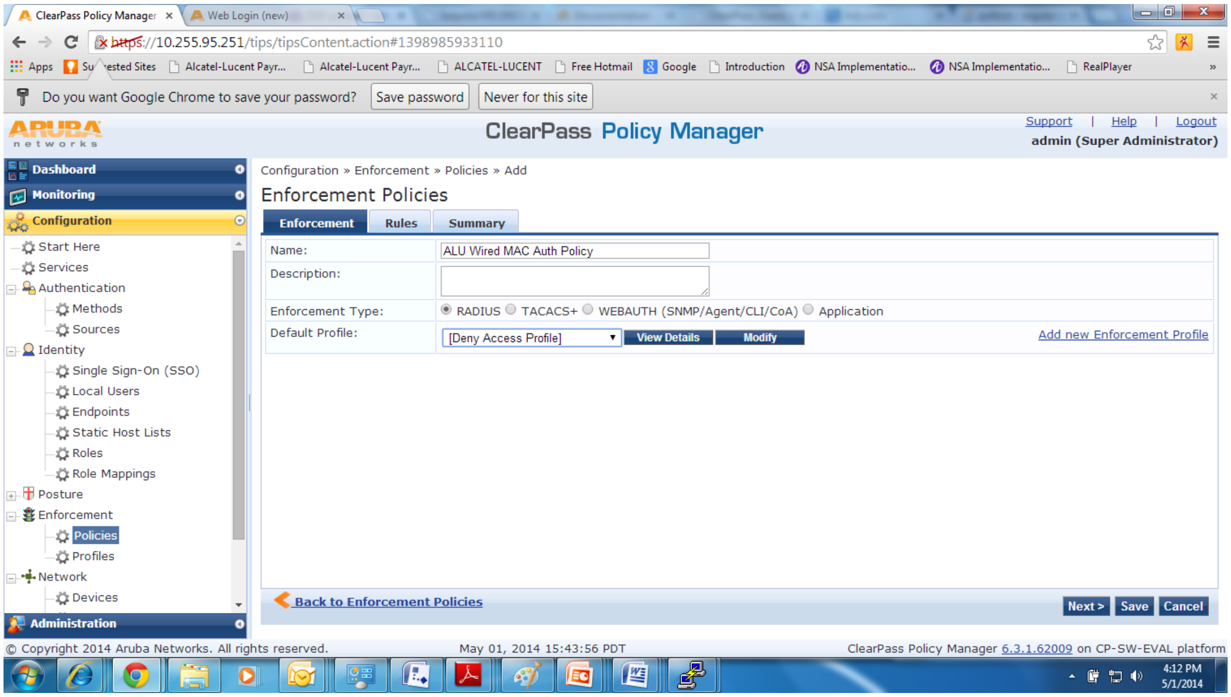
Attributes:

	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

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



Configuration » Enforcement » Policies » Add

Enforcement Policies

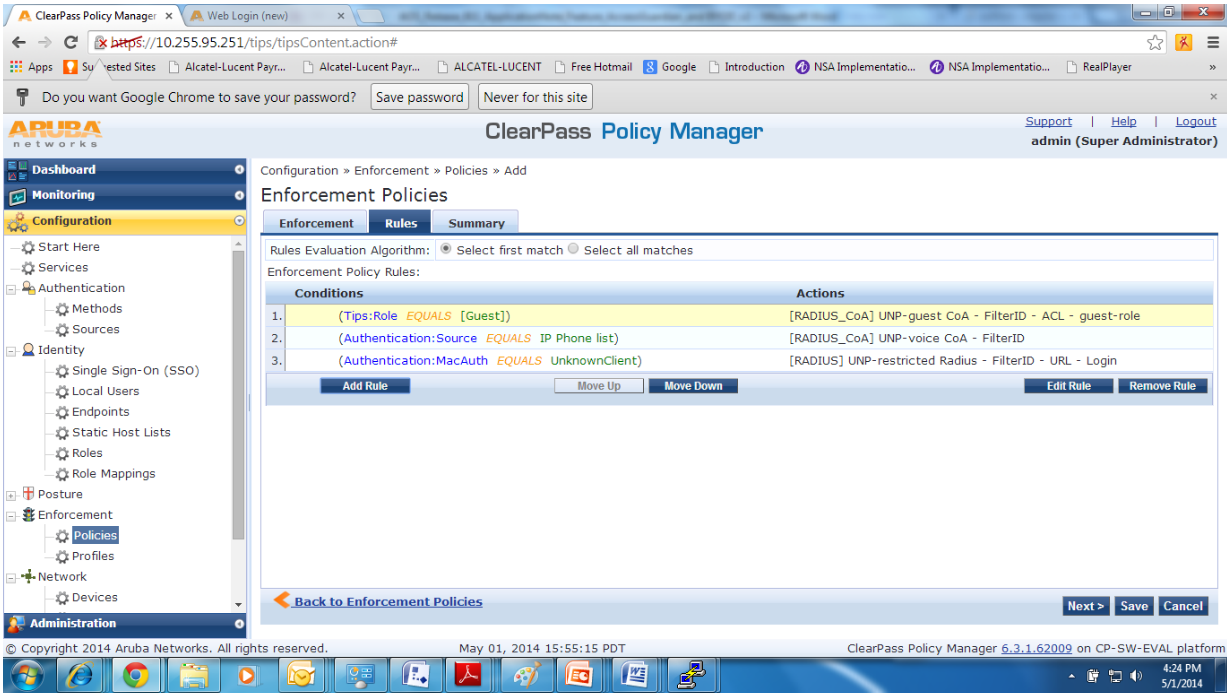
Enforcement | Rules | Summary

Name:	ALU Wired MAC Auth Policy
Description:	
Enforcement Type:	● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application
Default Profile:	[Deny Access Profile]

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



Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement | Rules | Summary

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

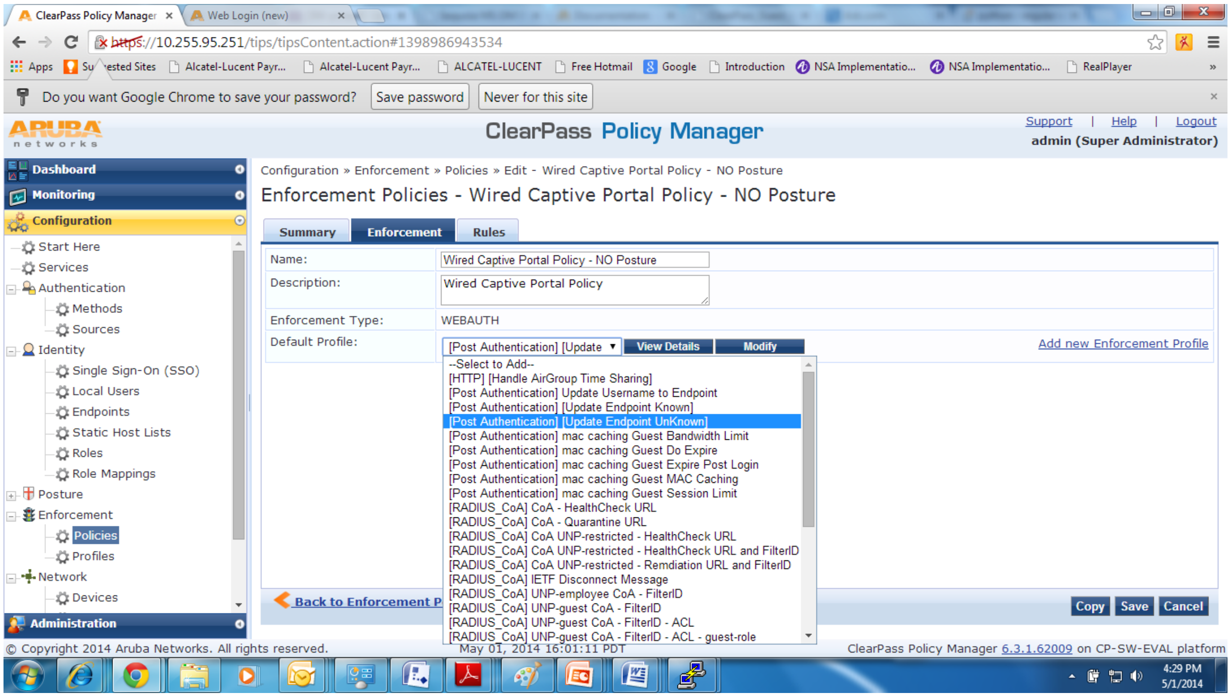
Enforcement Policy Rules:

	Conditions	Actions
1.	(Tips:Role EQUALS [Guest])	[RADIUS_CoA] UNP-guest CoA - FilterID - ACL - guest-role
2.	(Authentication:Source EQUALS IP Phone list)	[RADIUS_CoA] UNP-voice CoA - FilterID
3.	(Authentication:MacAuth EQUALS UnknownClient)	[RADIUS] UNP-restricted Radius - FilterID - URL - Login

3. Create policy for Web Authentication service:

a. Select Create a new Enforcement Policy

b. Follow the instructions for new enforcement policy creation



Configuration » Enforcement » Policies » Edit - Wired Captive Portal Policy - NO Posture

Enforcement Policies - Wired Captive Portal Policy - NO Posture

Name: Wired Captive Portal Policy - NO Posture

Description: Wired Captive Portal Policy

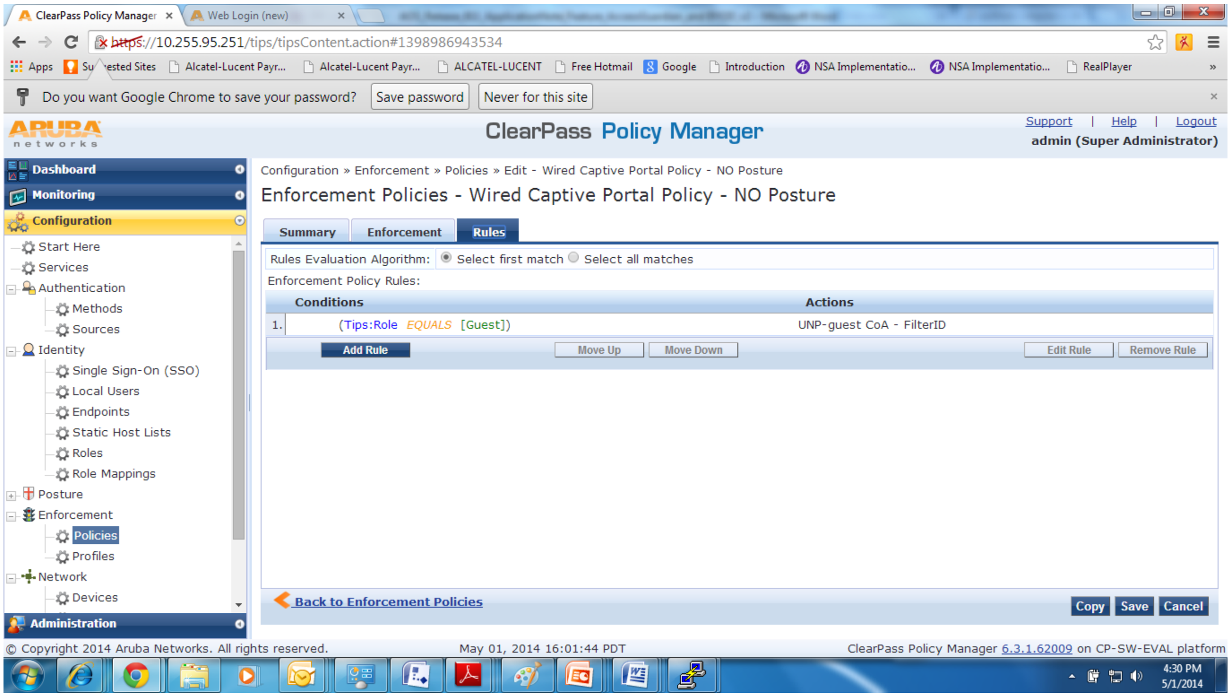
Enforcement Type: WEBAUTH

Default Profile: [Post Authentication] [Update

--Select to Add--
[HTTP] [Handle AirGroup Time Sharing]
[Post Authentication] Update Username to Endpoint
[Post Authentication] [Update Endpoint Known]
[Post Authentication] [Update Endpoint UnKnown]
[Post Authentication] mac caching Guest Bandwidth Limit
[Post Authentication] mac caching Guest Do Expire
[Post Authentication] mac caching Guest Expire Post Login
[Post Authentication] mac caching Guest MAC Caching
[Post Authentication] mac caching Guest Session Limit
[RADIUS_CoA] CoA - HealthCheck URL
[RADIUS_CoA] CoA - Quarantine URL
[RADIUS_CoA] CoA UNP-restricted - HealthCheck URL
[RADIUS_CoA] CoA UNP-restricted - HealthCheck URL and FilterID
[RADIUS_CoA] CoA UNP-restricted - Remdiation URL and FilterID
[RADIUS_CoA] IETF Disconnect Message
[RADIUS_CoA] UNP-employee CoA - FilterID
[RADIUS_CoA] UNP-guest CoA - FilterID
[RADIUS_CoA] UNP-guest CoA - FilterID - ACL
[RADIUS_CoA] UNP-guest CoA - FilterID - ACL - guest-role

c. Set attributes tab with the following rules:

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



Configuration » Enforcement » Policies » Edit - Wired Captive Portal Policy - NO Posture

Enforcement Policies - Wired Captive Portal Policy - NO Posture

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

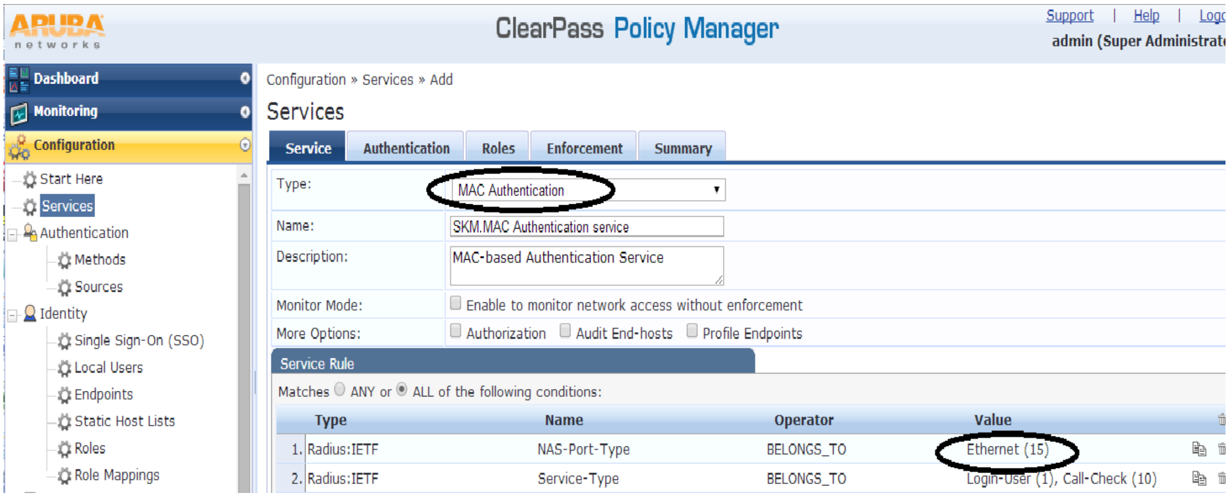
Enforcement Policy Rules:

	Conditions	Actions
1.	(Tips:Role EQUALS [Guest])	UNP-guest CoA - FilterID

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



Configuration » Services » Add

Services

Type: MAC Authentication

Name: SKM.MAC Authentication service

Description: MAC-based Authentication Service

Monitor Mode: □ Enable to monitor network access without enforcement

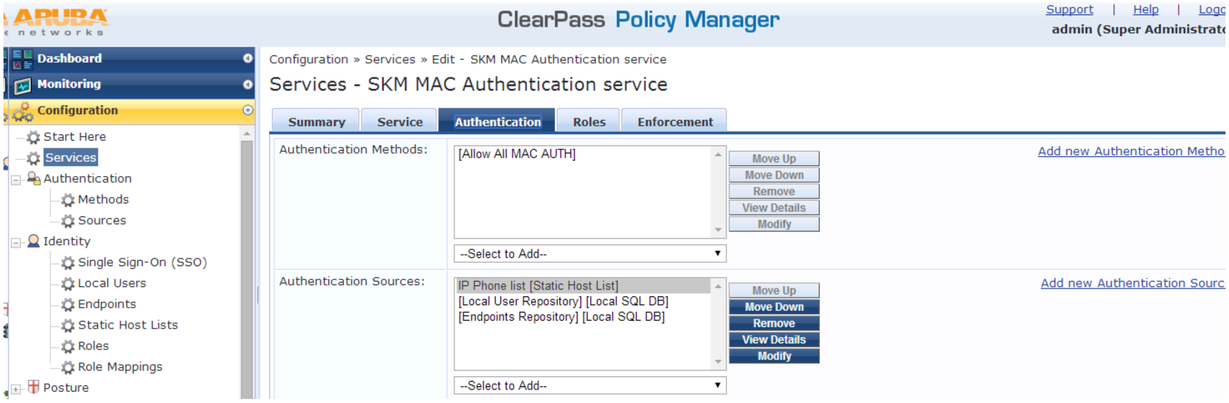
More Options: □ Authorization □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)

   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.



Configuration » Services » Edit - SKM MAC Authentication service

Services - SKM MAC Authentication service

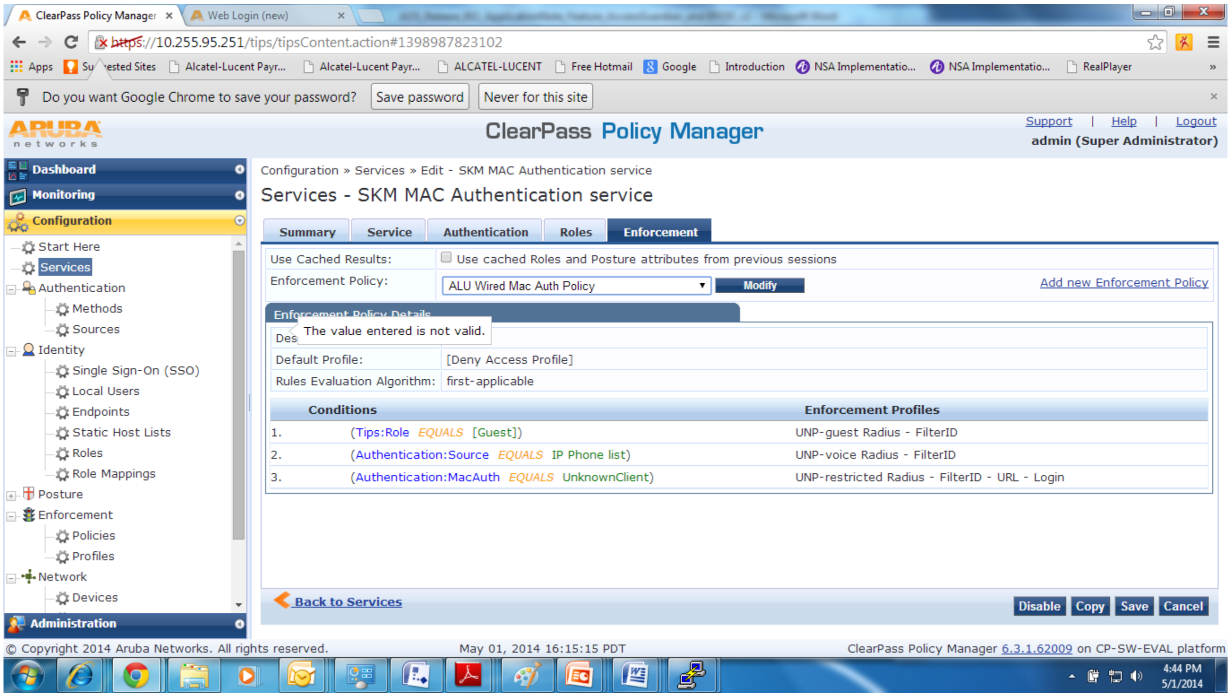
Authentication Methods: [Allow All MAC AUTH]

--Select to Add--

Authentication Sources: IP Phone list [Static Host List]
[Local User Repository] [Local SQL DB]
[Endpoints Repository] [Local SQL DB]

--Select to Add--

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



Configuration » Services » Edit - SKM MAC Authentication service

Services - SKM MAC Authentication service

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: ALU Wired Mac Auth Policy

Enforcement Policy Details

Des The value entered is not valid.

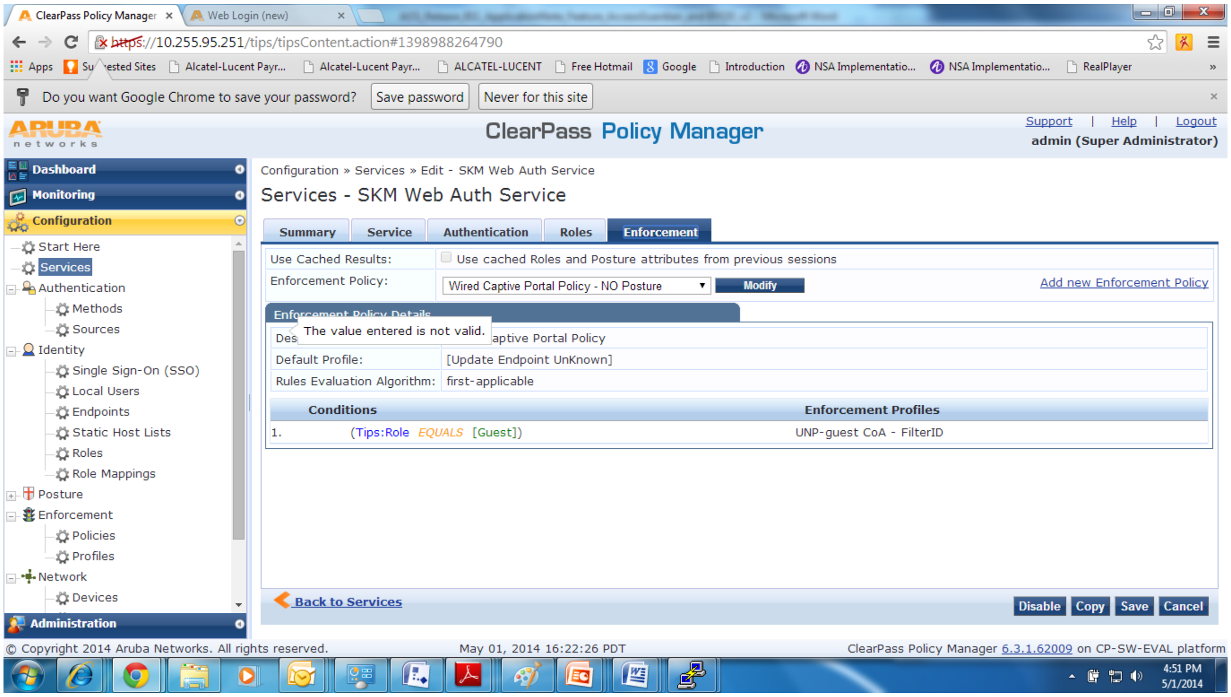
Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS [Guest])	UNP-guest Radius - FilterID
2.	(Authentication:Source EQUALS IP Phone list)	UNP-voice Radius - FilterID
3.	(Authentication:MacAuth EQUALS UnknownClient)	UNP-restricted Radius - FilterID - URL - Login

© Copyright 2014 Aruba Networks. All rights reserved. May 01, 2014 16:15:15 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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.



Configuration » Services » Edit - SKM Web Auth Service

Services - SKM Web Auth Service

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Wired Captive Portal Policy - NO Posture

Enforcement Policy Details

Des The value entered is not valid. aptive Portal Policy

Default Profile: [Update Endpoint UnKnown]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS [Guest])	UNP-guest CoA - FilterID

© Copyright 2014 Aruba Networks. All rights reserved. May 01, 2014 16:22:26 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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

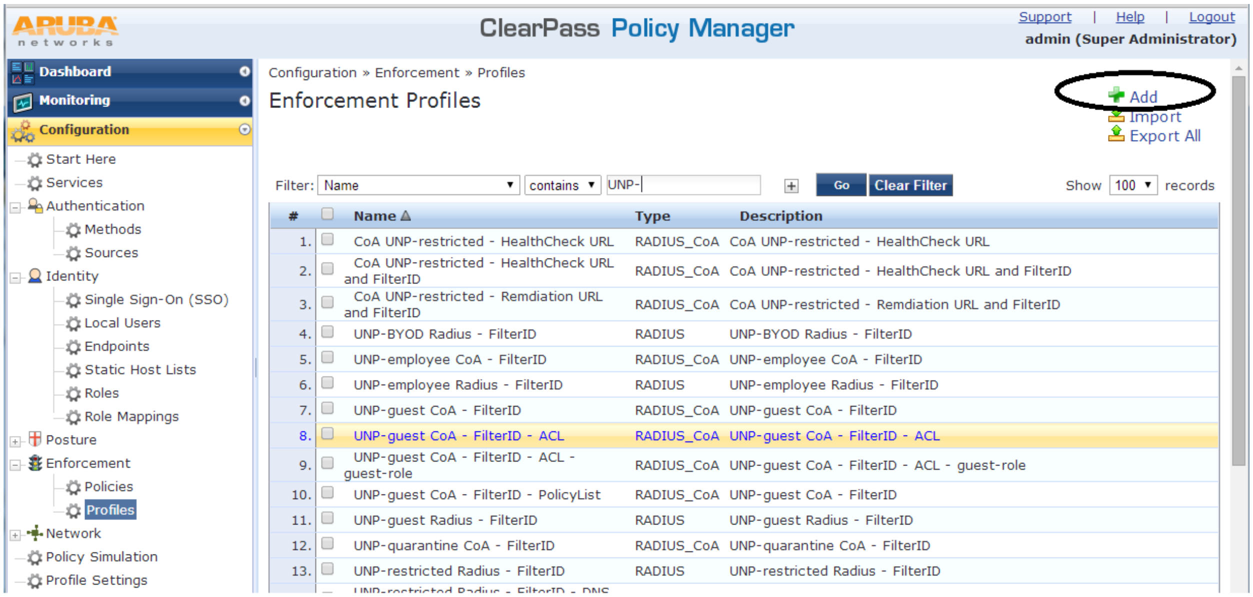
5.6.2 CPPM configuration

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.



Configuration » Enforcement » Profiles

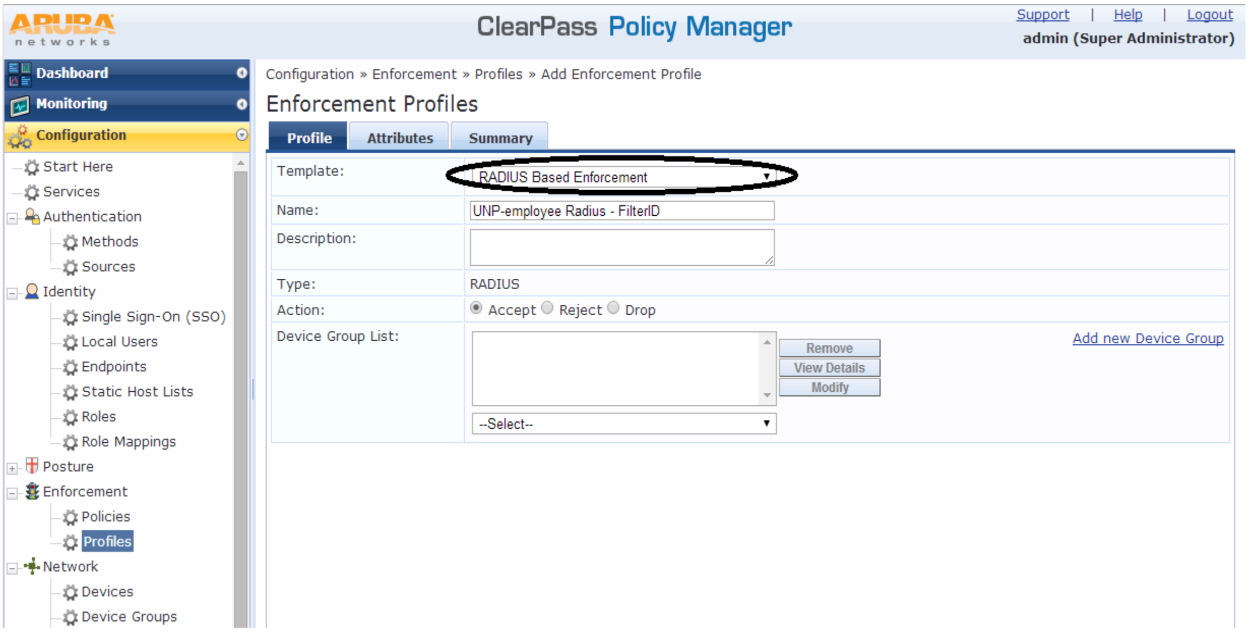
Enforcement Profiles

Filter: Name contains UNP-

Show 100 records

#		Name	Type	Description
1.	□	CoA UNP-restricted - HealthCheck URL	RADIUS_CoA	CoA UNP-restricted - HealthCheck URL
2.	□	CoA UNP-restricted - HealthCheck URL and FilterID	RADIUS_CoA	CoA UNP-restricted - HealthCheck URL and FilterID
3.	□	CoA UNP-restricted - Remdiation URL and FilterID	RADIUS_CoA	CoA UNP-restricted - Remdiation URL and FilterID
4.	□	UNP-BYOD Radius - FilterID	RADIUS	UNP-BYOD Radius - FilterID
5.	□	UNP-employee CoA - FilterID	RADIUS_CoA	UNP-employee CoA - FilterID
6.	□	UNP-employee Radius - FilterID	RADIUS	UNP-employee Radius - FilterID
7.	□	UNP-guest CoA - FilterID	RADIUS_CoA	UNP-guest CoA - FilterID
8.	□	UNP-guest CoA - FilterID - ACL	RADIUS_CoA	UNP-guest CoA - FilterID - ACL
9.	□	UNP-guest CoA - FilterID - ACL - guest-role	RADIUS_CoA	UNP-guest CoA - FilterID - ACL - guest-role
10.	□	UNP-guest CoA - FilterID - PolicyList	RADIUS_CoA	UNP-guest CoA - FilterID
11.	□	UNP-guest Radius - FilterID	RADIUS	UNP-guest Radius - FilterID
12.	□	UNP-quarantine CoA - FilterID	RADIUS_CoA	UNP-quarantine CoA - FilterID
13.	□	UNP-restricted Radius - FilterID	RADIUS	UNP-restricted Radius - FilterID
		UNP-restricted Radius - FilterID - DNS		

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

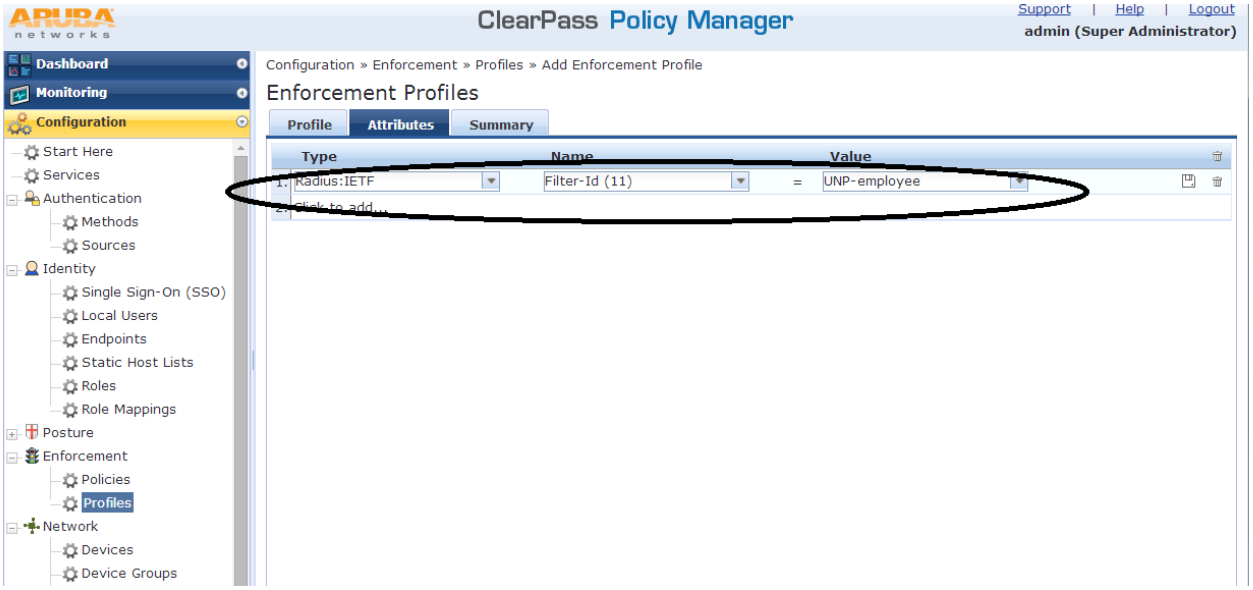


Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template:	RADIUS Based Enforcement
Name:	UNP-employee Radius - FilterID
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

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

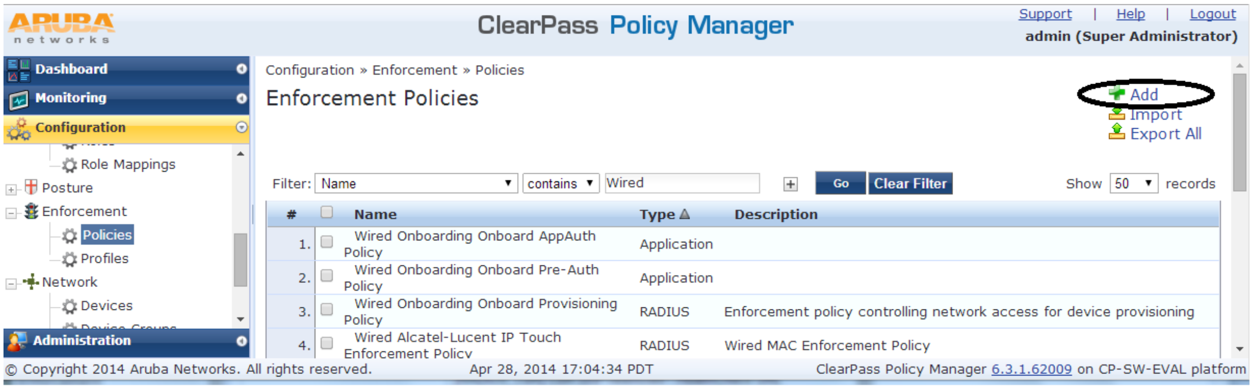
Enforcement Profiles

	Type	Name		Value
1.	Radius:IETF	Filter-Id (11)	=	UNP-employee
2.	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

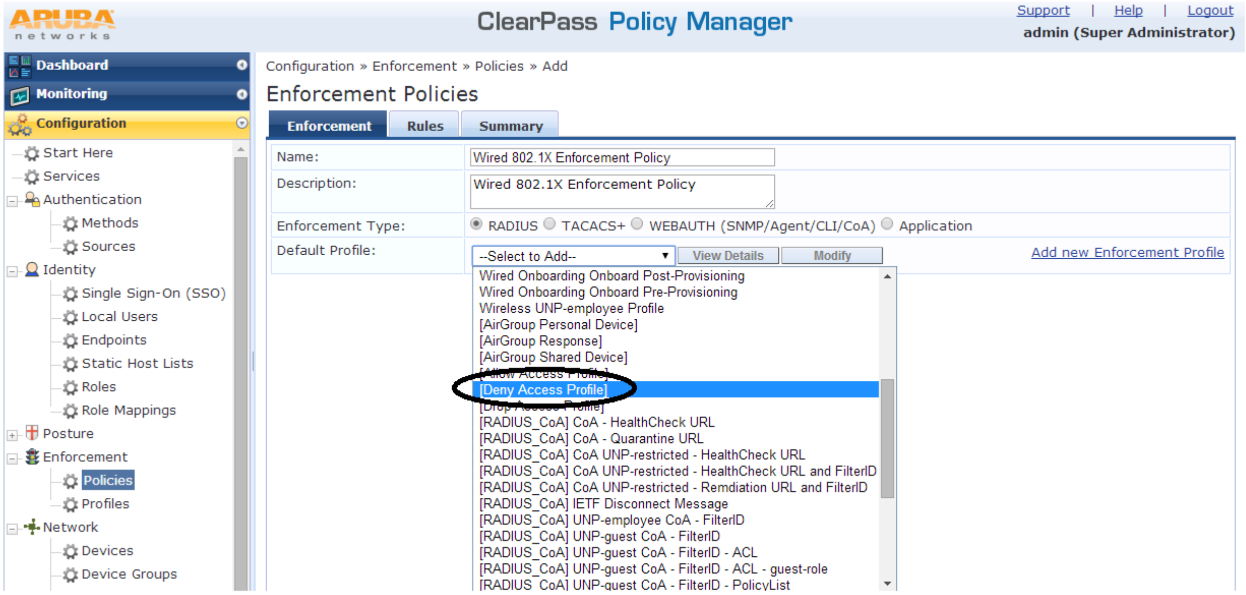
Enforcement Policies

Filter: Name ▾ contains ▾ Wired 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.



Configuration » Enforcement » Policies » Add

Enforcement Policies

Name: Wired 802.1X Enforcement Policy

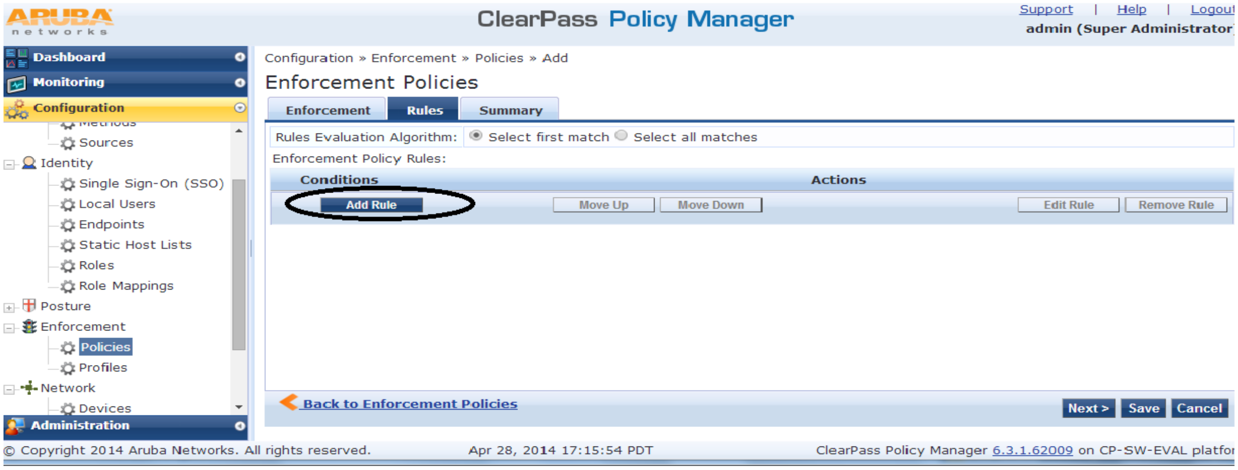
Description: Wired 802.1X Enforcement Policy

Enforcement Type: ● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application

Default Profile: --Select to Add-- View Details Modify Add new Enforcement Profile

Wired Onboarding Onboard Post-Provisioning
Wired Onboarding Onboard Pre-Provisioning
Wireless UNP-employee Profile
[AirGroup Personal Device]
[AirGroup Response]
[AirGroup Shared Device]
[Allow Access Profile]
[Deny Access Profile]
[Drop Access Profile]
[RADIUS_CoA] CoA - HealthCheck URL
[RADIUS_CoA] CoA - Quarantine URL
[RADIUS_CoA] CoA UNP-restricted - HealthCheck URL
[RADIUS_CoA] CoA UNP-restricted - HealthCheck URL and FilterID
[RADIUS_CoA] CoA UNP-restricted - Remdiation URL and FilterID
[RADIUS_CoA] IETF Disconnect Message
[RADIUS_CoA] UNP-employee CoA - FilterID
[RADIUS_CoA] UNP-guest CoA - FilterID
[RADIUS_CoA] UNP-guest CoA - FilterID - ACL
[RADIUS_CoA] UNP-guest CoA - FilterID - ACL - guest-role
[RADIUS_CoA] UNP-guest CoA - FilterID - PolicyList

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



Configuration » Enforcement » Policies » Add

Enforcement Policies

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

Enforcement Policy Rules:

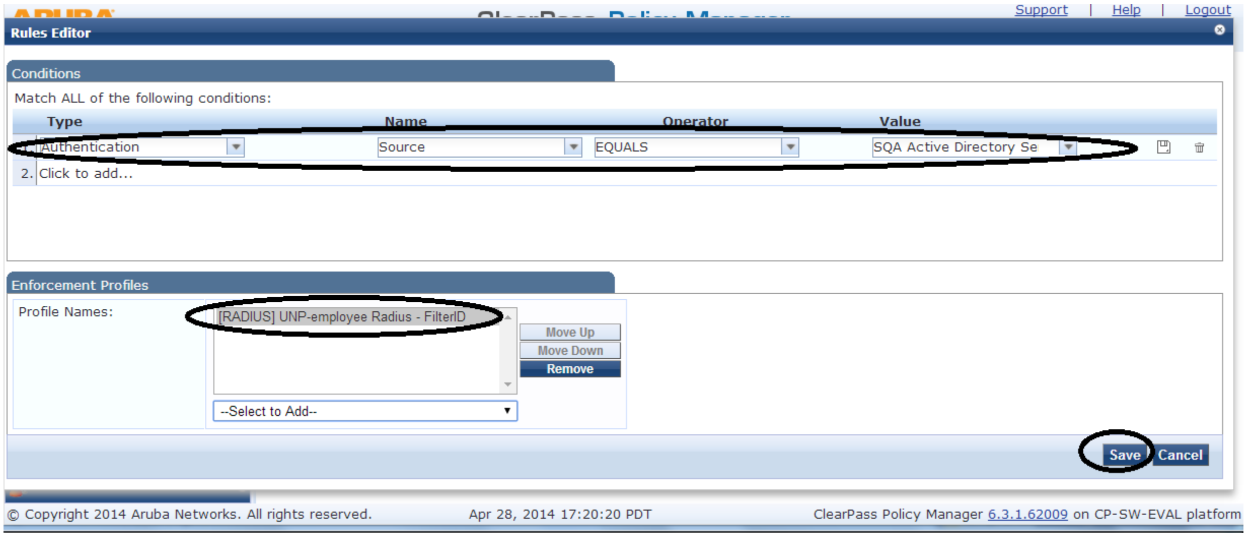
Conditions	Actions

Add Rule Move Up Move Down Edit Rule Remove Rule

Back to Enforcement Policies Next > Save Cancel

© Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 17:15:54 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platfo

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.



Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authentication	Source	EQUALS	SQA Active Directory Se
2.	Click to add...			

Enforcement Profiles

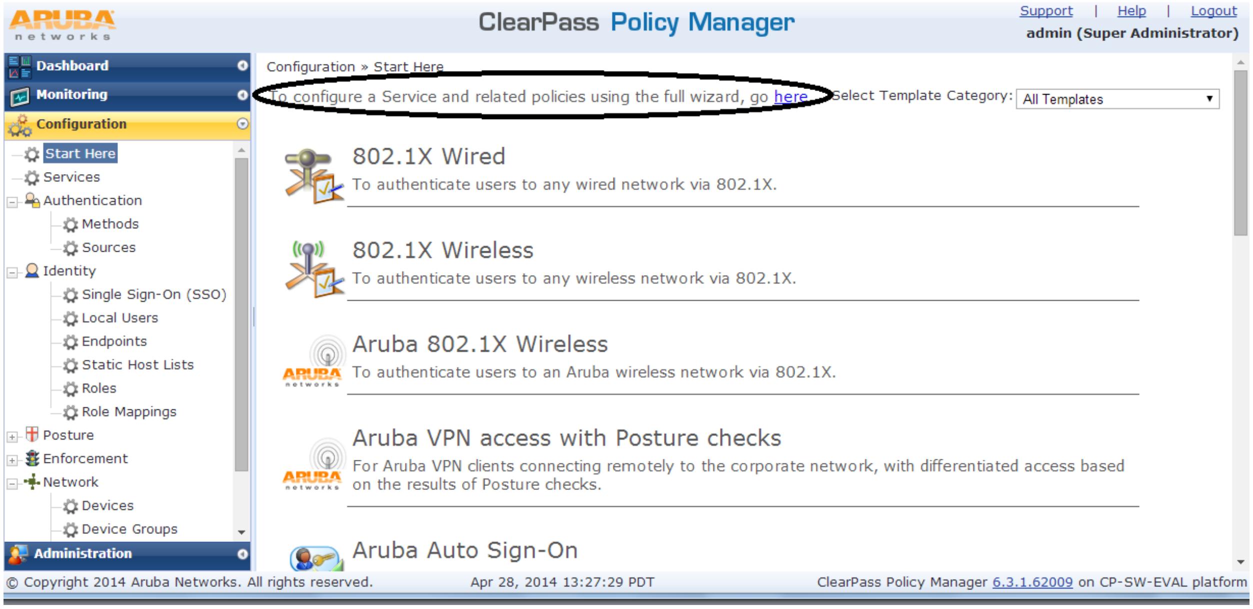
Profile Names: [RADIUS] UNP-employee Radius - FilterID

--Select to Add--

© Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 17:20:20 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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.



ClearPass Policy Manager

admin (Super Administrator)

Configuration » Start Here

To configure a Service and related policies using the full wizard, go here

Select Template Category: All Templates

802.1X Wired
To authenticate users to any wired network via 802.1X.

802.1X Wireless
To authenticate users to any wireless network via 802.1X.

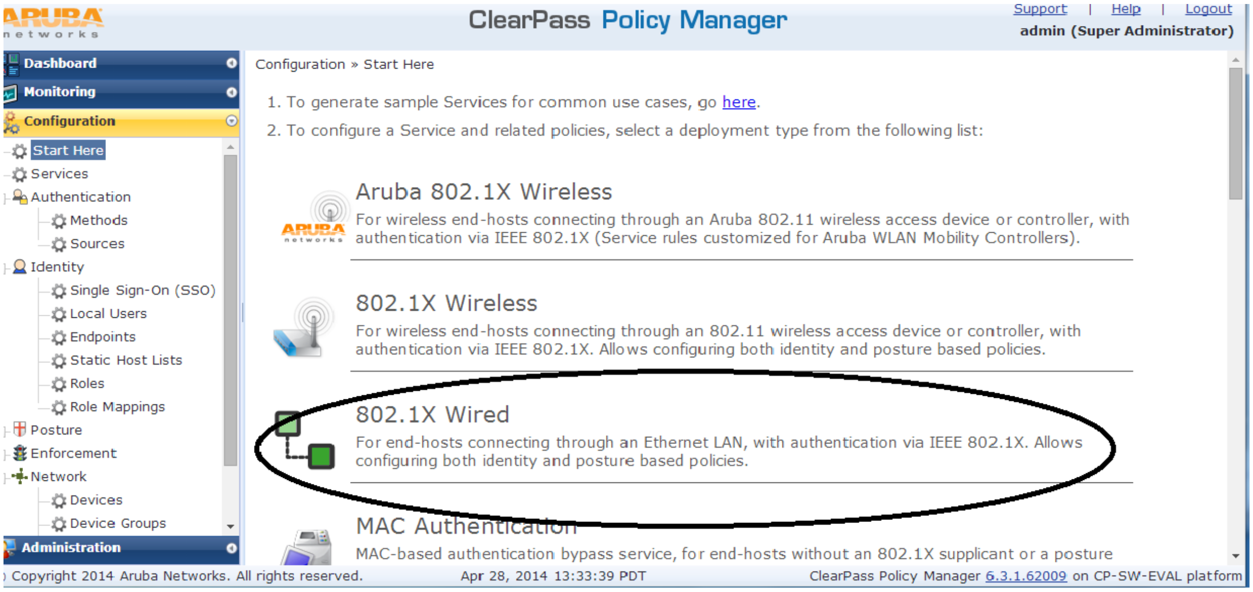
Aruba 802.1X Wireless
To authenticate users to an Aruba wireless network via 802.1X.

Aruba VPN access with Posture checks
For Aruba VPN clients connecting remotely to the corporate network, with differentiated access based on the results of Posture checks.

Aruba Auto Sign-On

© Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 13:27:29 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

2. Select the 802.1X Wired service shown below



Configuration » Start Here

1. To generate sample Services for common use cases, go here.
2. To configure a Service and related policies, select a deployment type from the following list:

Aruba 802.1X Wireless
For wireless end-hosts connecting through an Aruba 802.11 wireless access device or controller, with authentication via IEEE 802.1X (Service rules customized for Aruba WLAN Mobility Controllers).

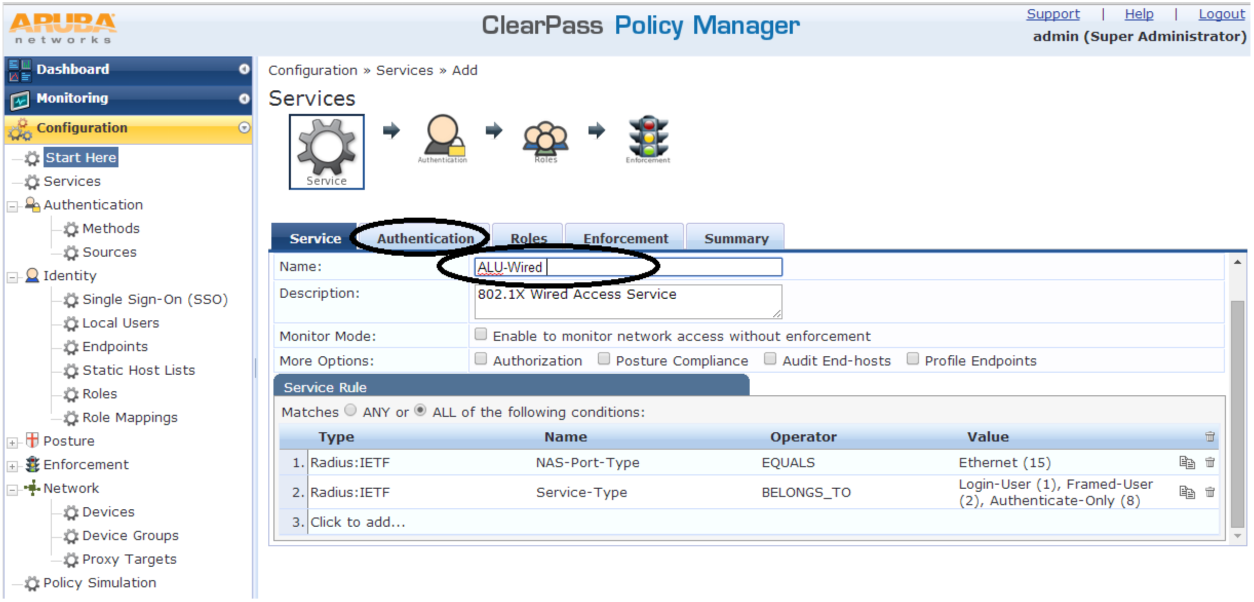
802.1X Wireless
For wireless end-hosts connecting through an 802.11 wireless access device or controller, with authentication via IEEE 802.1X. Allows configuring both identity and posture based policies.

802.1X Wired
For end-hosts connecting through an Ethernet LAN, with authentication via IEEE 802.1X. Allows configuring both identity and posture based policies.

MAC Authentication
MAC-based authentication bypass service, for end-hosts without an 802.1X supplicant or a posture

Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 13:33:39 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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.



Configuration » Services » Add

Services

Service | Authentication | Roles | Enforcement | Summary

Name: ALU-Wired

Description: 802.1X Wired Access Service

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: □ Authorization □ Posture Compliance □ Audit End-hosts □ Profile Endpoints

Service Rule

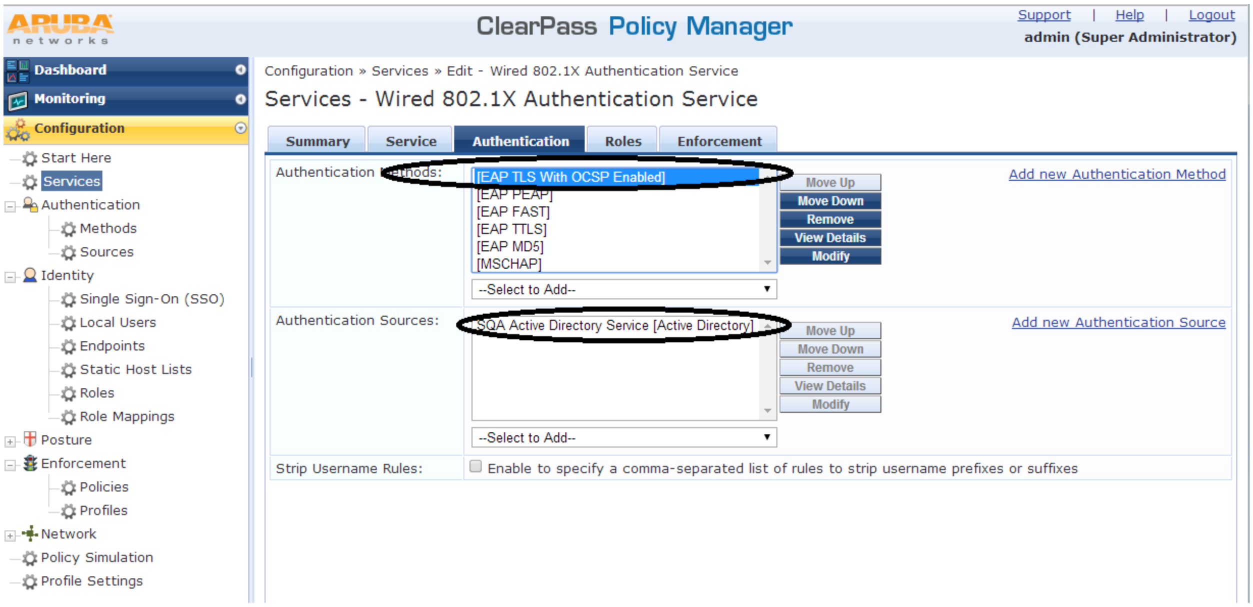
Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...			

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 OCSP Enabled” must be added to the list and moved to the topmost on the list to get the highest precedence. OCSP 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.



Configuration » Services » Edit - Wired 802.1X Authentication Service

Services - Wired 802.1X Authentication Service

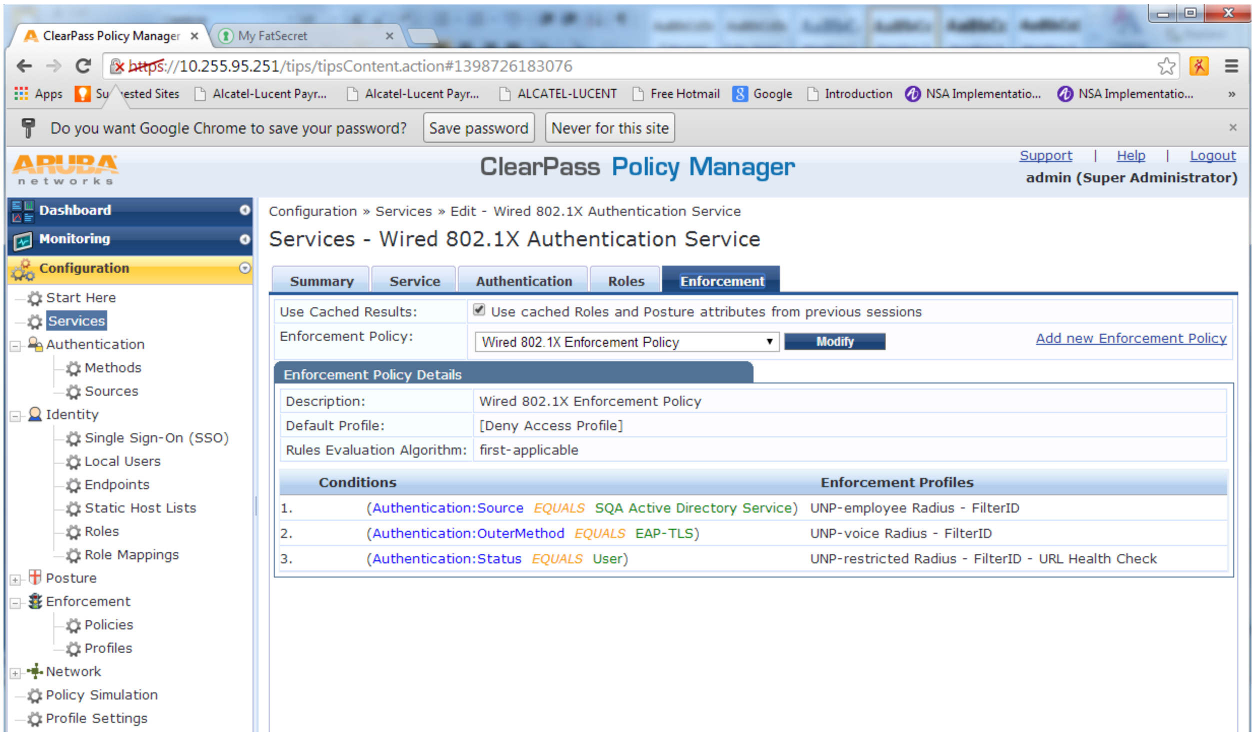
Authentication Methods:
[EAP TLS With OCSP Enabled]
[EAP PEAP]
[EAP FAST]
[EAP TTLS]
[EAP MD5]
[MSCHAP]
--Select to Add--

Authentication Sources:
SQA Active Directory Service [Active Directory]
--Select to Add--

Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

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.



Configuration » Services » Edit - Wired 802.1X Authentication Service

Services - Wired 802.1X Authentication Service

Use Cached Results: ☑ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Wired 802.1X Enforcement Policy

Enforcement Policy Details

Description:	Wired 802.1X Enforcement Policy
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authentication:Source EQUALS SQA Active Directory Service)	UNP-employee Radius - FilterID
2.	(Authentication:OuterMethod EQUALS EAP-TLS)	UNP-voice Radius - FilterID
3.	(Authentication:Status EQUALS User)	UNP-restricted Radius - FilterID - URL Health Check

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 OCSP 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:

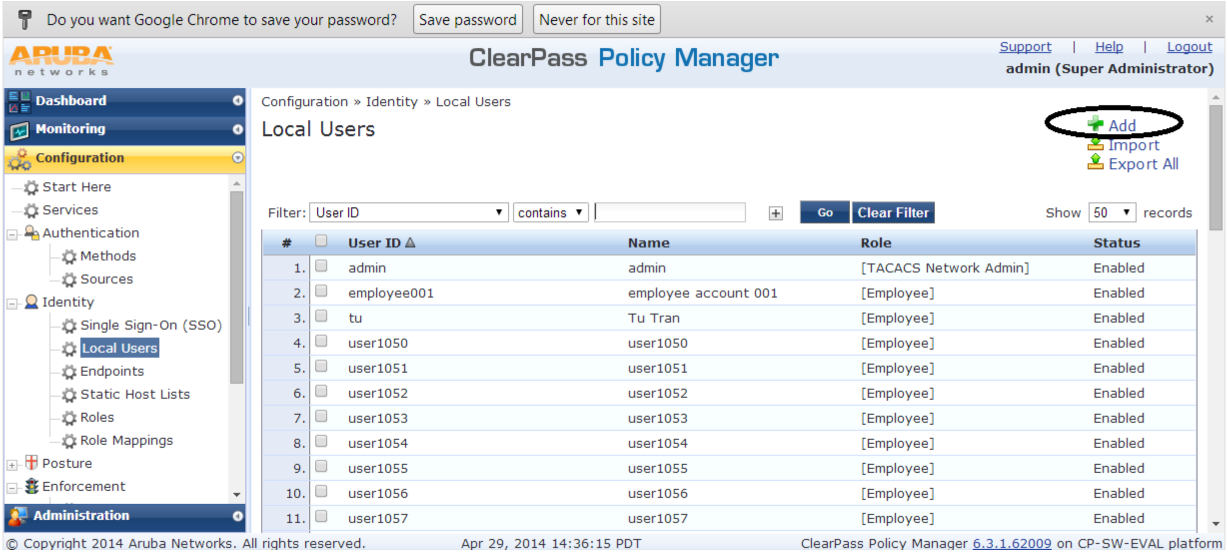
- Configure Employee Account/Onboard setting in the local database
- Configure appropriate Enforcement profiles and policies
- Configure MAC and Onboarding service
- Update the 802.1x authentication services

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.



Configuration » Identity » Local Users

Local Users

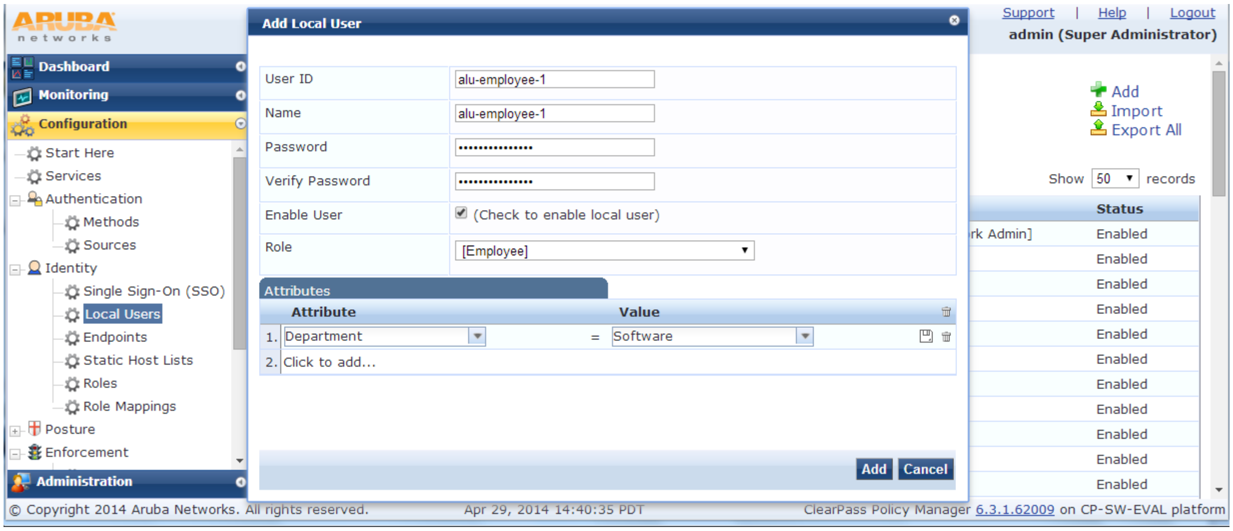
Filter: User ID contains

Show 50 records

#	☐	User ID	Name	Role	Status
1.	☐	admin	admin	[TACACS Network Admin]	Enabled
2.	☐	employee001	employee account 001	[Employee]	Enabled
3.	☐	tu	Tu Tran	[Employee]	Enabled
4.	☐	user1050	user1050	[Employee]	Enabled
5.	☐	user1051	user1051	[Employee]	Enabled
6.	☐	user1052	user1052	[Employee]	Enabled
7.	☐	user1053	user1053	[Employee]	Enabled
8.	☐	user1054	user1054	[Employee]	Enabled
9.	☐	user1055	user1055	[Employee]	Enabled
10.	☐	user1056	user1056	[Employee]	Enabled
11.	☐	user1057	user1057	[Employee]	Enabled

© Copyright 2014 Aruba Networks. All rights reserved. Apr 29, 2014 14:36:15 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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.



Add Local User

User ID	alu-employee-1
Name	alu-employee-1
Password	••••••••••••••
Verify Password	••••••••••••••
Enable User	☑ (Check to enable local user)
Role	[Employee]

Attributes

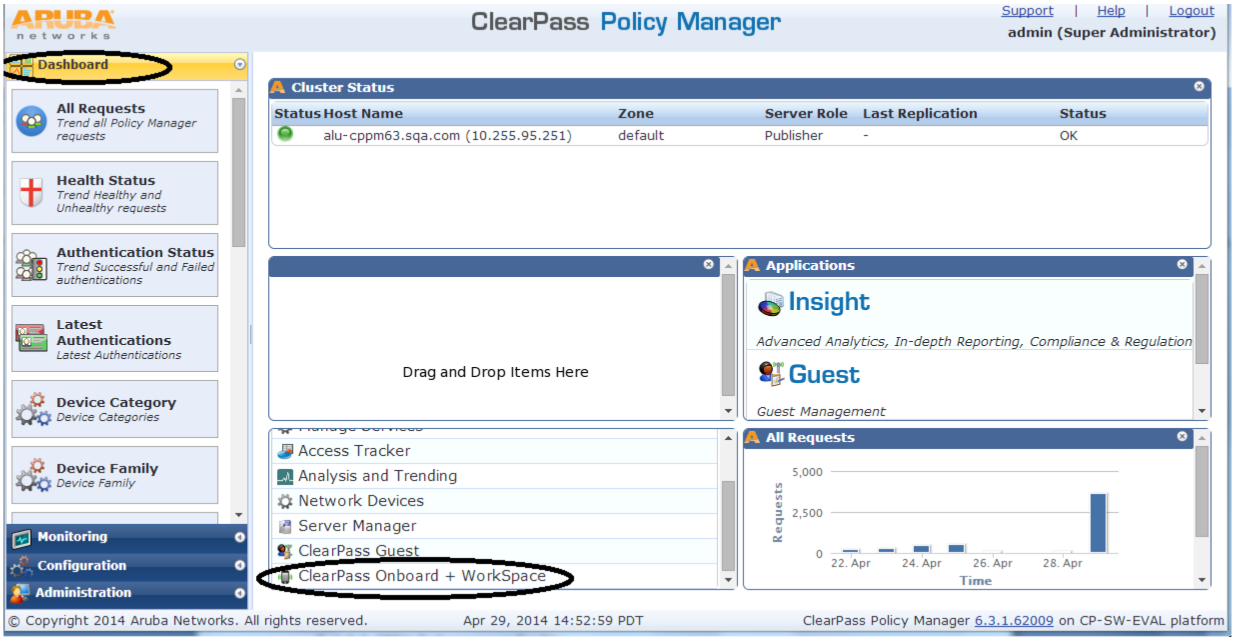
	Attribute		Value
1.	Department	=	Software
2.	Click to add...		

© Copyright 2014 Aruba Networks. All rights reserved. Apr 29, 2014 14:40:35 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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.

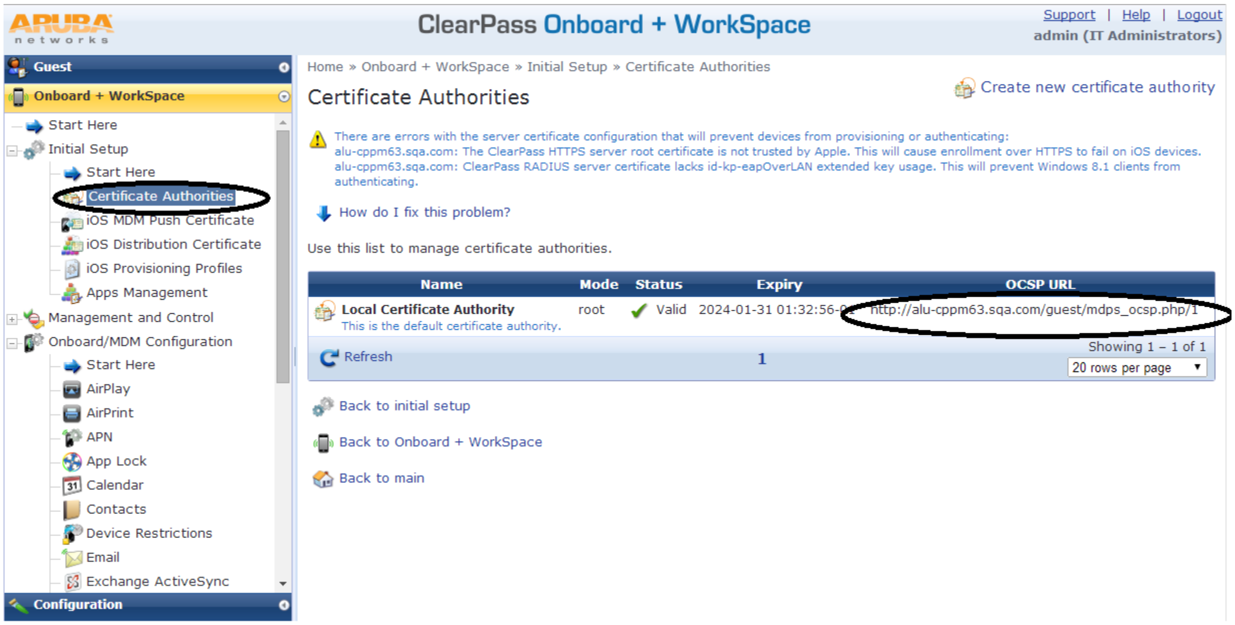
1. Go to Dashboard/QuickLinks and select “ClearPass Onboard + Workspace” tab as shown below.



Status	Host Name	Zone	Server Role	Last Replication	Status
●	alu-cppm63.sqa.com (10.255.95.251)	default	Publisher	-	OK

© Copyright 2014 Aruba Networks. All rights reserved. Apr 29, 2014 14:52:59 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

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



Certificate Authorities

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
alu-cppm63.sqa.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
alu-cppm63.sqa.com: ClearPass RADIUS server certificate lacks id-kp-eapOverLAN extended key usage. This will prevent Windows 8.1 clients from authenticating.

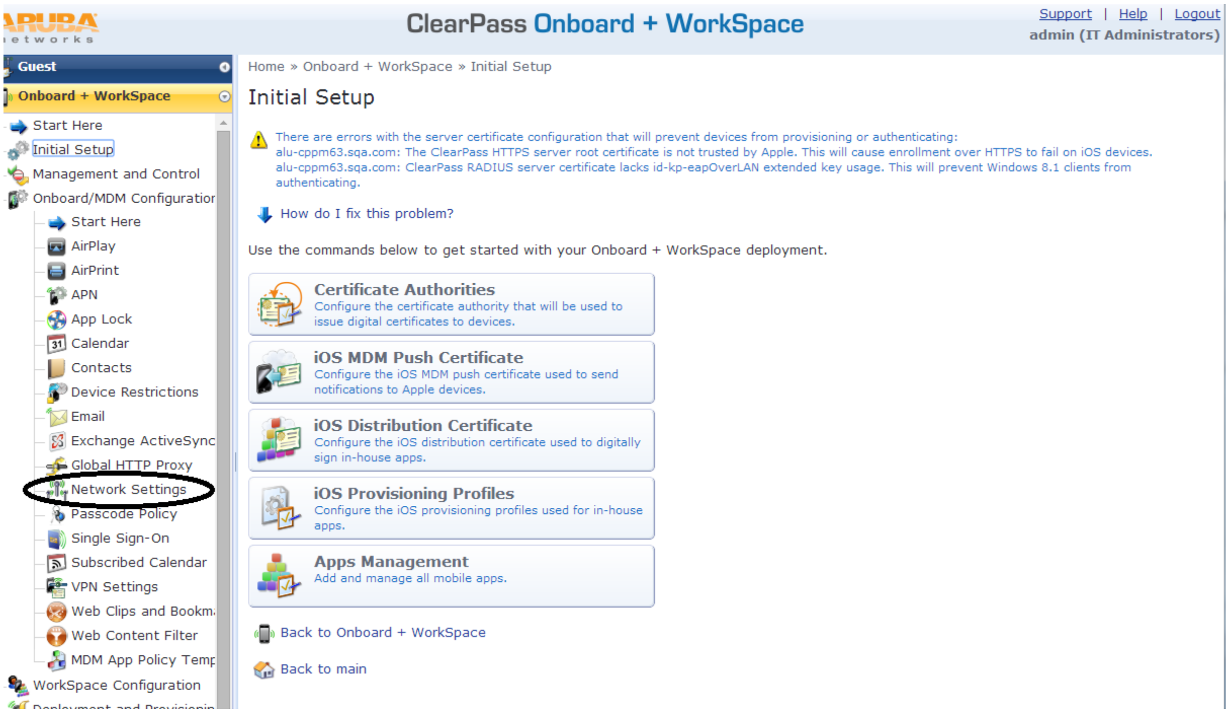
How do I fix this problem?

Use this list to manage certificate authorities.

Name	Mode	Status	Expiry	OCSP URL
Local Certificate Authority This is the default certificate authority.	root	✓ Valid	2024-01-31 01:32:56-	http://alu-cppm63.sqa.com/guest/mdps_ocsp.php/1

Showing 1 – 1 of 1
20 rows per page

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



Home » Onboard + WorkSpace » Initial Setup

Initial Setup

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
alu-cppm63.sqa.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
alu-cppm63.sqa.com: ClearPass RADIUS server certificate lacks id-kp-eapOverLAN extended key usage. This will prevent Windows 8.1 clients from authenticating.

How do I fix this problem?

Use the commands below to get started with your Onboard + WorkSpace deployment.

Certificate Authorities
Configure the certificate authority that will be used to issue digital certificates to devices.

iOS MDM Push Certificate
Configure the iOS MDM push certificate used to send notifications to Apple devices.

iOS Distribution Certificate
Configure the iOS distribution certificate used to digitally sign in-house apps.

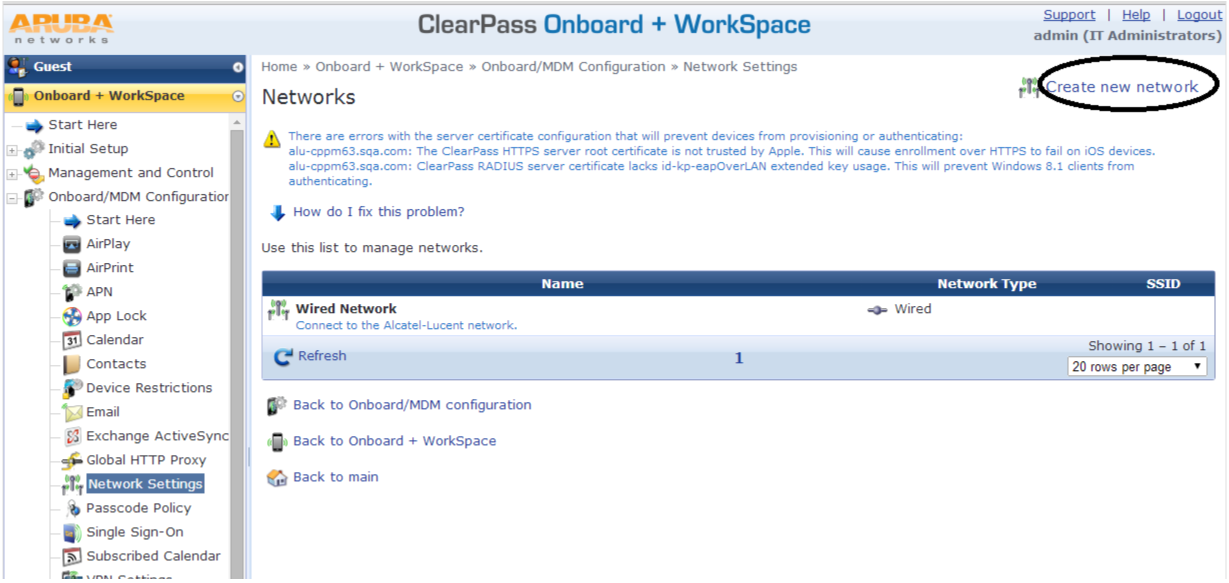
iOS Provisioning Profiles
Configure the iOS provisioning profiles used for in-house apps.

Apps Management
Add and manage all mobile apps.

Back to Onboard + WorkSpace

Back to main

4. Select Create new network as shown.



Home » Onboard + WorkSpace » Onboard/MDM Configuration » Network Settings

Networks

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
alu-cppm63.sqa.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
alu-cppm63.sqa.com: ClearPass RADIUS server certificate lacks id-kp-eapOverLAN extended key usage. This will prevent Windows 8.1 clients from authenticating.

How do I fix this problem?

Use this list to manage networks.

Name	Network Type	SSID
Wired Network Connect to the Alcatel-Lucent network.	Wired	

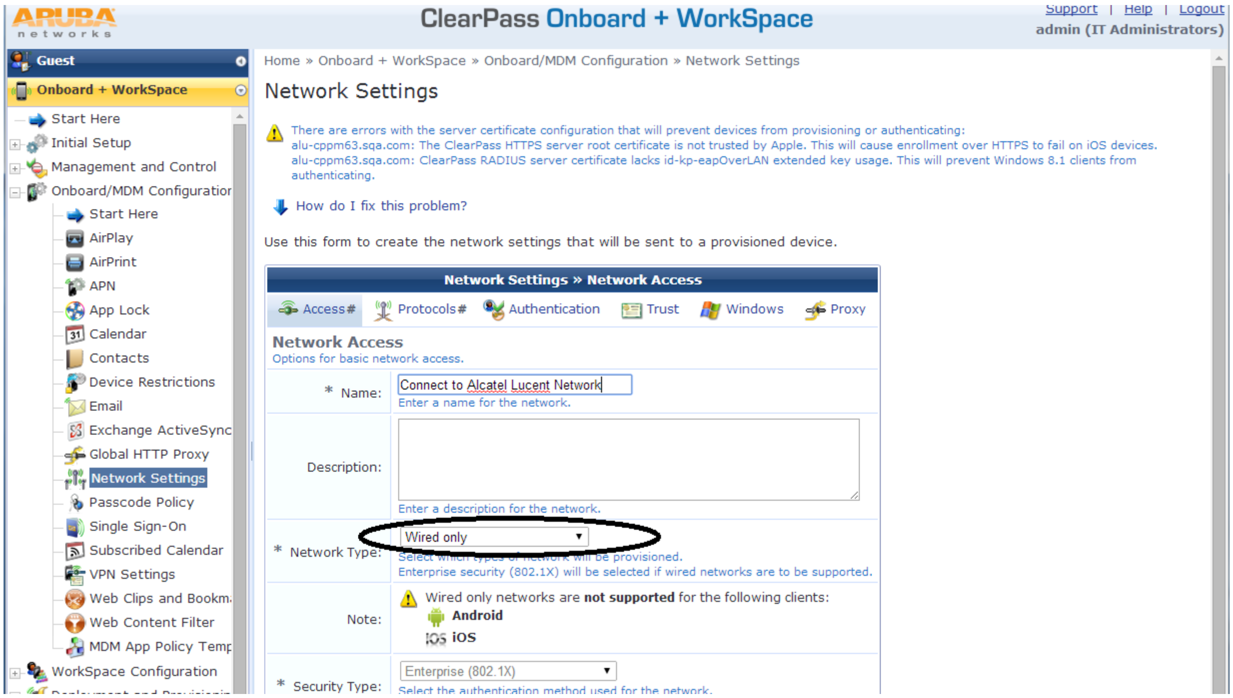
Refresh 1 Showing 1 – 1 of 1 20 rows per page

Back to Onboard/MDM configuration

Back to Onboard + WorkSpace

Back to main

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



Network Settings

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
alu-cppm63.sqa.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
alu-cppm63.sqa.com: ClearPass RADIUS server certificate lacks id-kp-eapOverLAN extended key usage. This will prevent Windows 8.1 clients from authenticating.

How do I fix this problem?

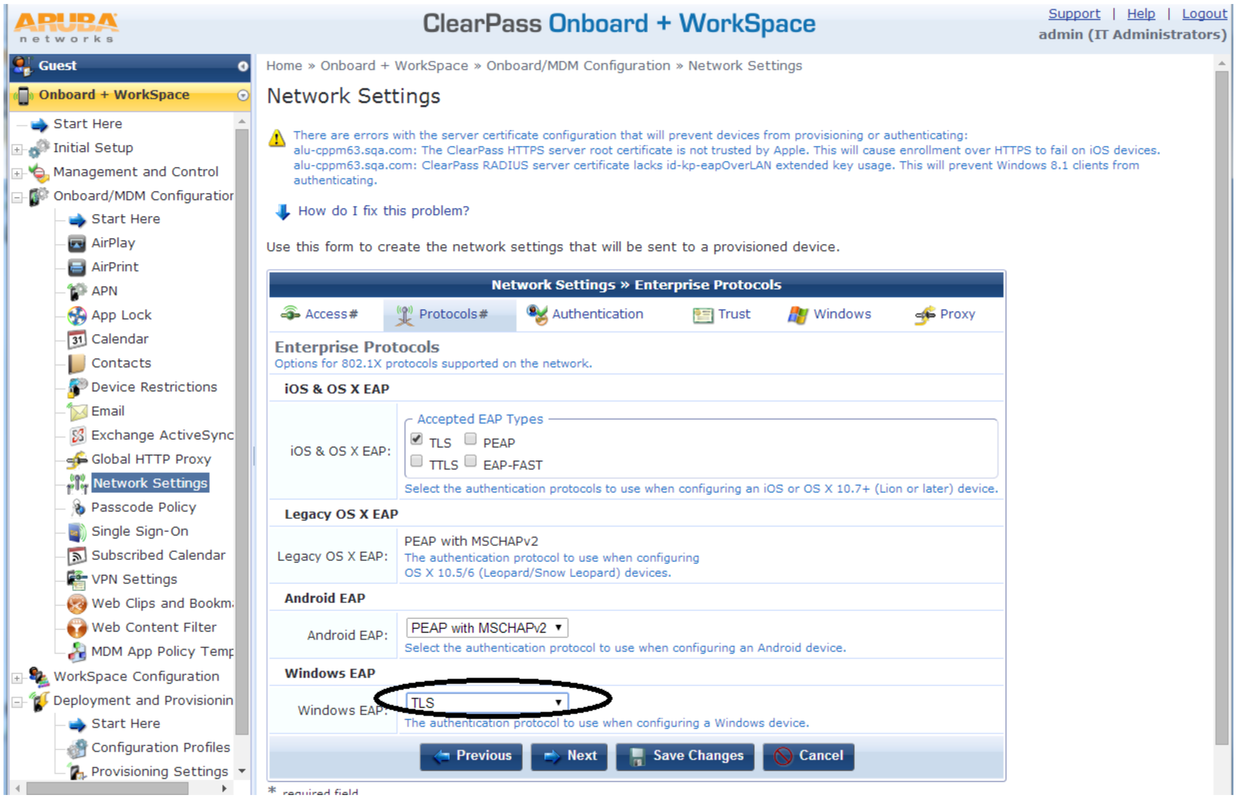
Use this form to create the network settings that will be sent to a provisioned device.

Network Settings » Network Access

Network Access
Options for basic network access.

* Name:	Connect to Alcatel Lucent Network Enter a name for the network.
Description:	Enter a description for the network.
* Network Type:	Wired only Select which types of network will be provisioned. Enterprise security (802.1X) will be selected if wired networks are to be supported.
Note:	Wired only networks are **not supported** for the following clients: **Android** **iOS**
* Security Type:	Enterprise (802.1X) Select the authentication method used for the network.

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.



Network Settings

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
alu-cppm63.sqa.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
alu-cppm63.sqa.com: ClearPass RADIUS server certificate lacks id-kp-eapOverLAN extended key usage. This will prevent Windows 8.1 clients from authenticating.

How do I fix this problem?

Use this form to create the network settings that will be sent to a provisioned device.

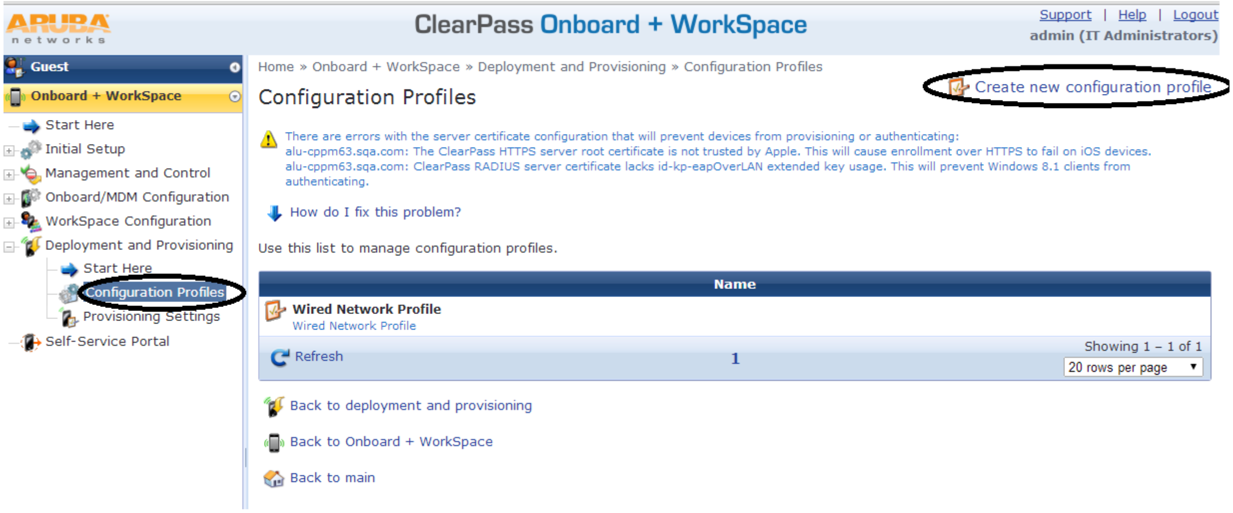
Network Settings » Enterprise Protocols

Enterprise Protocols
Options for 802.1X protocols supported on the network.

iOS & OS X EAP	
iOS & OS X EAP:	Accepted EAP Types ☑ TLS ☐ PEAP ☐ TTLS ☐ EAP-FAST Select the authentication protocols to use when configuring an iOS or OS X 10.7+ (Lion or later) device.
Legacy OS X EAP	
Legacy OS X EAP:	PEAP with MSCHAPv2 The authentication protocol to use when configuring OS X 10.5/6 (Leopard/Snow Leopard) devices.
Android EAP	
Android EAP:	PEAP with MSCHAPv2 Select the authentication protocol to use when configuring an Android device.
Windows EAP	
Windows EAP:	TLS The authentication protocol to use when configuring a Windows device.

* required field

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


ARUBA networks
ClearPass Onboard + WorkSpace
Support | Help | Logout
admin (IT Administrators)
Guest
Onboard + WorkSpace
Start Here
Initial Setup
Management and Control
Onboard/MDM Configuration
WorkSpace Configuration
Deployment and Provisioning
Start Here
Configuration Profiles
Provisioning Settings
Self-Service Portal
Home » Onboard + WorkSpace » Deployment and Provisioning » Configuration Profiles
Create new configuration profile

Configuration Profiles

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
alu-cppm63.sqa.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
alu-cppm63.sqa.com: ClearPass RADIUS server certificate lacks id-kp-eapOverLAN extended key usage. This will prevent Windows 8.1 clients from authenticating.

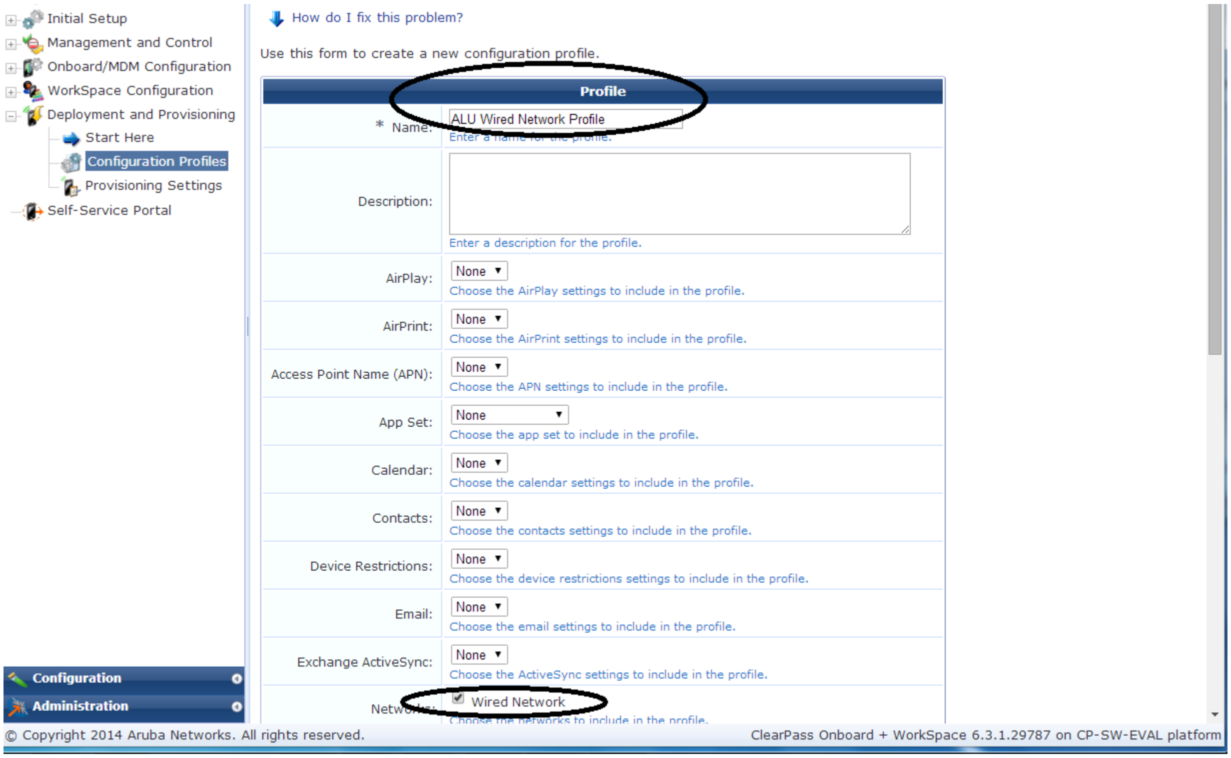
How do I fix this problem?

Use this list to manage configuration profiles.

Name
Wired Network Profile Wired Network Profile

Refresh
1
Showing 1 – 1 of 1
20 rows per page
Back to deployment and provisioning
Back to Onboard + WorkSpace
Back to main

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

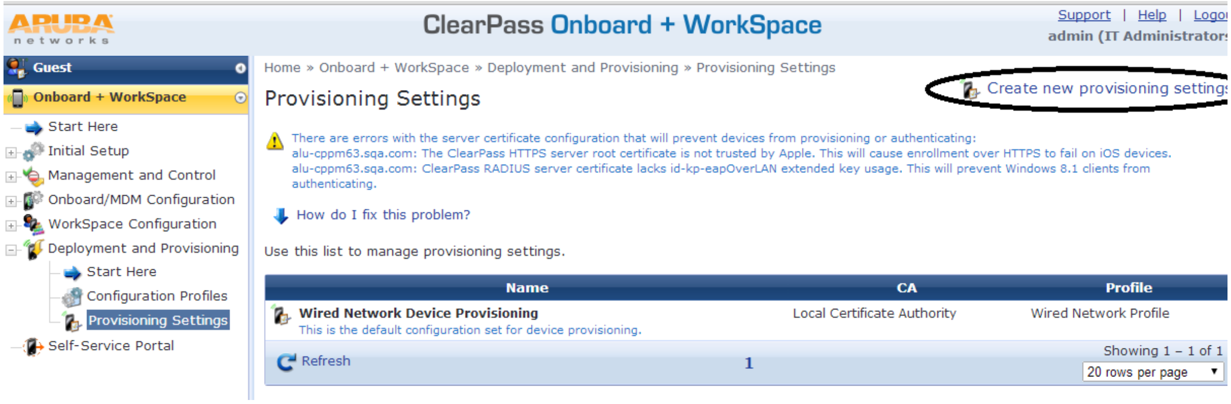


Use this form to create a new configuration profile.

Profile	
* Name:	ALU Wired Network Profile Enter a name for the profile.
Description:	Enter a description for the profile.
AirPlay:	None Choose the AirPlay settings to include in the profile.
AirPrint:	None Choose the AirPrint settings to include in the profile.
Access Point Name (APN):	None Choose the APN settings to include in the profile.
App Set:	None Choose the app set to include in the profile.
Calendar:	None Choose the calendar settings to include in the profile.
Contacts:	None Choose the contacts settings to include in the profile.
Device Restrictions:	None Choose the device restrictions settings to include in the profile.
Email:	None Choose the email settings to include in the profile.
Exchange ActiveSync:	None Choose the ActiveSync settings to include in the profile.
Networks:	☑ Wired Network Choose the networks to include in the profile.

© Copyright 2014 Aruba Networks. All rights reserved. ClearPass Onboard + WorkSpace 6.3.1.29787 on CP-SW-EVAL platform

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



ClearPass Onboard + WorkSpace

Support | Help | Logo

admin (IT Administrator

Home » Onboard + WorkSpace » Deployment and Provisioning » Provisioning Settings

Provisioning Settings

Create new provisioning setting

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
alu-cppm63.sqa.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
alu-cppm63.sqa.com: ClearPass RADIUS server certificate lacks id-kp-eapOverLAN extended key usage. This will prevent Windows 8.1 clients from authenticating.

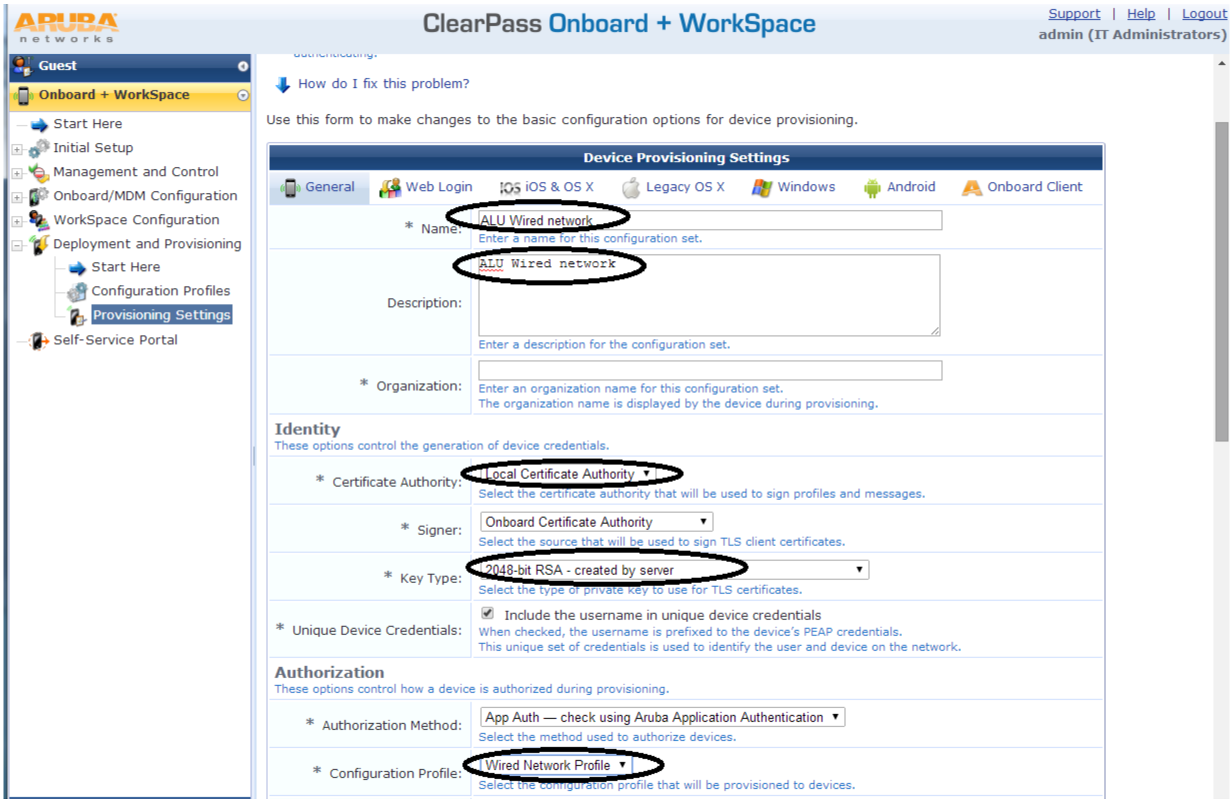
How do I fix this problem?

Use this list to manage provisioning settings.

Name	CA	Profile
Wired Network Device Provisioning This is the default configuration set for device provisioning.	Local Certificate Authority	Wired Network Profile

Refresh 1 Showing 1 – 1 of 1 20 rows per page

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”.



ClearPass Onboard + WorkSpace

Support | Help | Logout

admin (IT Administrators)

How do I fix this problem?

Use this form to make changes to the basic configuration options for device provisioning.

Device Provisioning Settings

* Name: ALU Wired network
Enter a name for this configuration set.

Description: ALU Wired network
Enter a description for the configuration set.

* Organization:
Enter an organization name for this configuration set.
The organization name is displayed by the device during provisioning.

Identity
These options control the generation of device credentials.

* Certificate Authority: Local Certificate Authority
Select the certificate authority that will be used to sign profiles and messages.

* Signer: Onboard Certificate Authority
Select the source that will be used to sign TLS client certificates.

* Key Type: 2048-bit RSA - created by server
Select the type of private key to use for TLS certificates.

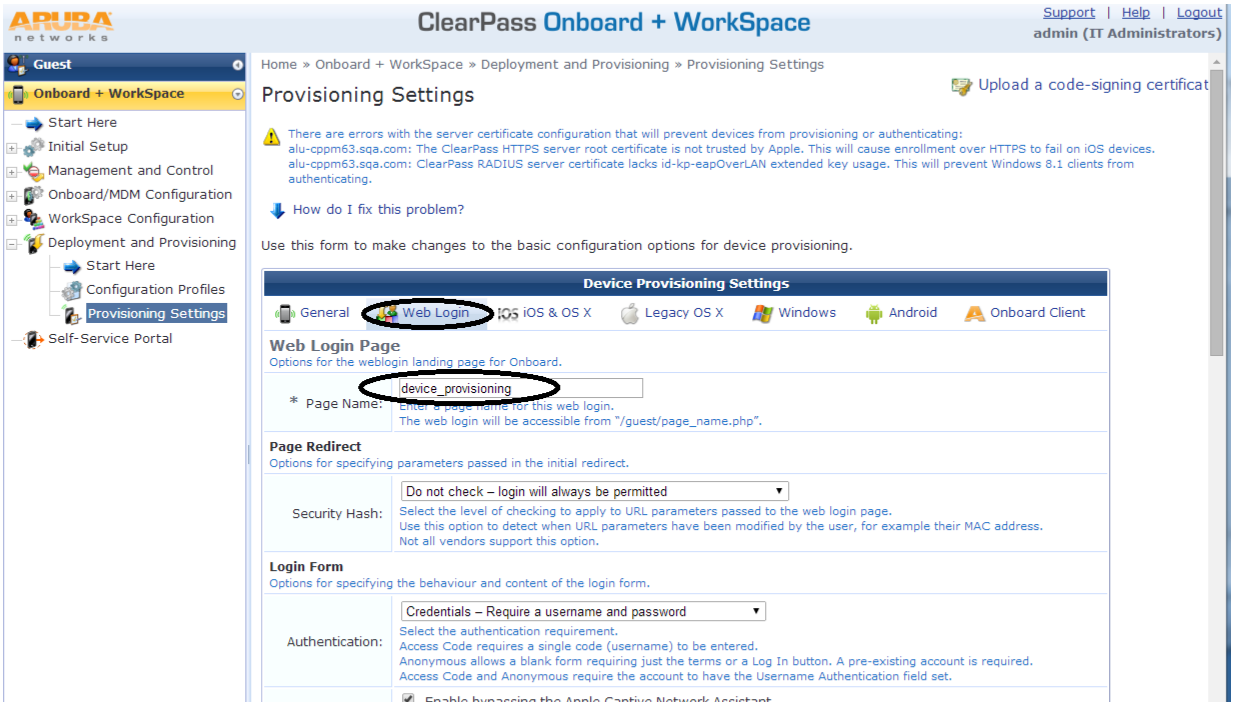
* Unique Device Credentials: ☑ Include the username in unique device credentials
When checked, the username is prefixed to the device's PEAP credentials.
This unique set of credentials is used to identify the user and device on the network.

Authorization
These options control how a device is authorized during provisioning.

* Authorization Method: App Auth — check using Aruba Application Authentication
Select the method used to authorize devices.

* Configuration Profile: Wired Network Profile
Select the configuration profile that will be provisioned to devices.

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. Accept all defaults of IOS, OSX, Windows and Android tabs.



Provisioning Settings

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
alu-cppm63.sqa.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
alu-cppm63.sqa.com: ClearPass RADIUS server certificate lacks id-kp-eapOverLAN extended key usage. This will prevent Windows 8.1 clients from authenticating.

How do I fix this problem?

Use this form to make changes to the basic configuration options for device provisioning.

Device Provisioning Settings

Web Login Page
Options for the weblogin landing page for Onboard.

* Page Name: device_provisioning
Enter a page name for this web login.
The web login will be accessible from "/guest/page_name.php".

Page Redirect
Options for specifying parameters passed in the initial redirect.

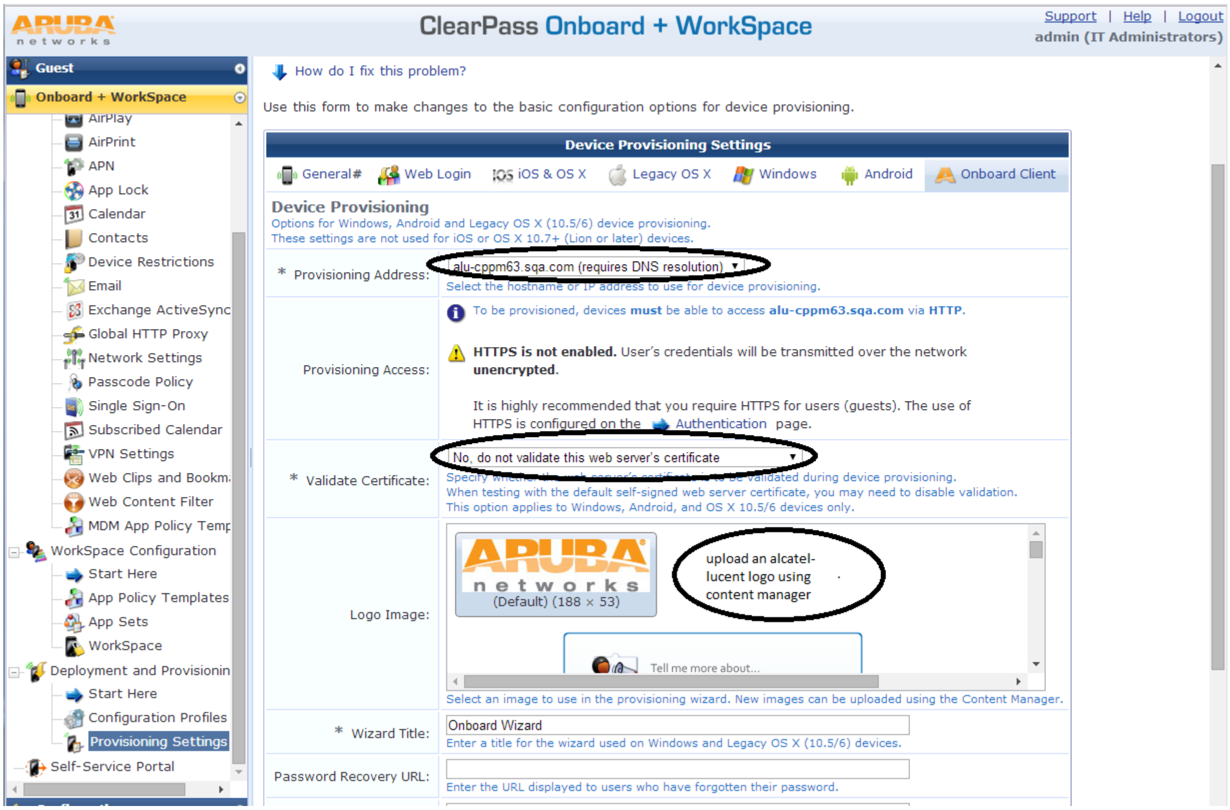
Security Hash: Do not check – login will always be permitted
Select the level of checking to apply to URL parameters passed to the web login page.
Use this option to detect when URL parameters have been modified by the user, for example their MAC address.
Not all vendors support this option.

Login Form
Options for specifying the behaviour and content of the login form.

Authentication: Credentials – Require a username and password
Select the authentication requirement.
Access Code requires a single code (username) to be entered.
Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required.
Access Code and Anonymous require the account to have the Username Authentication field set.

☑ Enable bypassing the Apple Captive Network Assistant

12. 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



How do I fix this problem?

Use this form to make changes to the basic configuration options for device provisioning.

Device Provisioning Settings

Device Provisioning
Options for Windows, Android and Legacy OS X (10.5/6) device provisioning.
These settings are not used for iOS or OS X 10.7+ (Lion or later) devices.

* Provisioning Address: alu-cppm63.sqa.com (requires DNS resolution)
Select the hostname or IP address to use for device provisioning.

Provisioning Access: To be provisioned, devices **must** be able to access **alu-cppm63.sqa.com** via **HTTP**.
HTTPS is not enabled. User's credentials will be transmitted over the network **unencrypted**.
It is highly recommended that you require HTTPS for users (guests). The use of HTTPS is configured on the Authentication page.

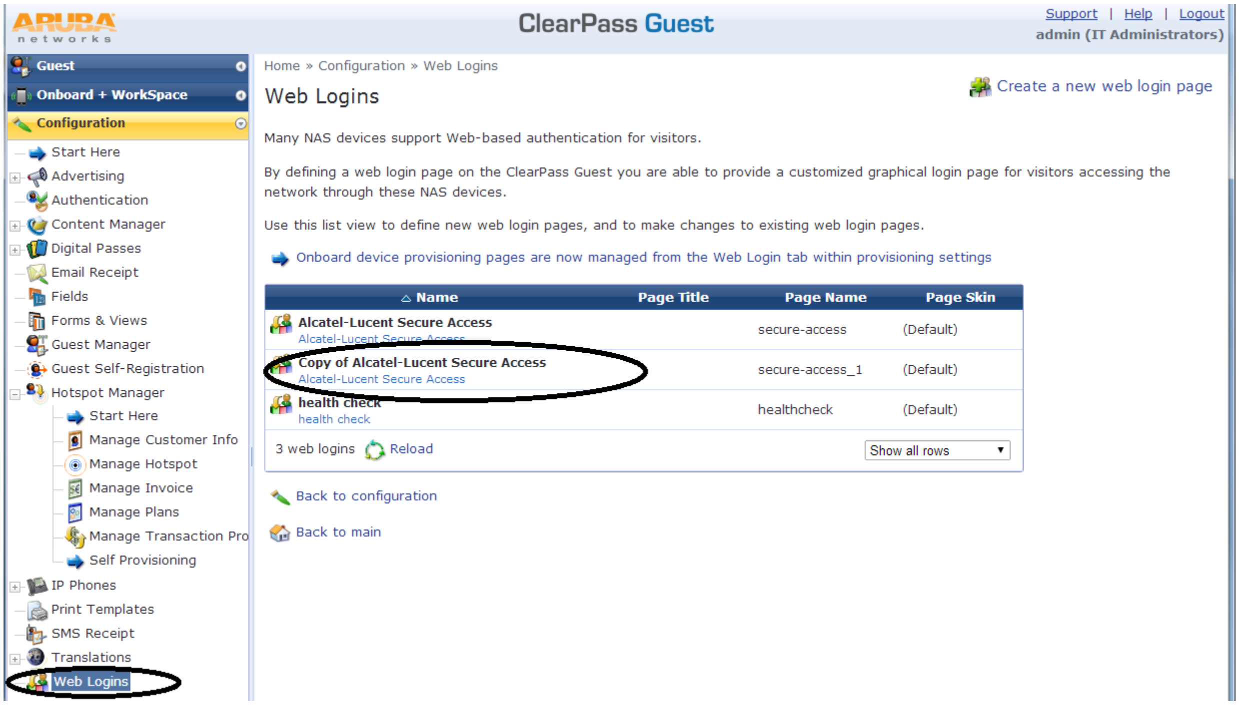
* Validate Certificate: No, do not validate this web server's certificate
Specify whether the web server's certificate is to be validated during device provisioning.
When testing with the default self-signed web server certificate, you may need to disable validation.
This option applies to Windows, Android, and OS X 10.5/6 devices only.

Logo Image: upload an alcatel-lucent logo using content manager
Select an image to use in the provisioning wizard. New images can be uploaded using the Content Manager.

* Wizard Title: Onboard Wizard
Enter a title for the wizard used on Windows and Legacy OS X (10.5/6) devices.

Password Recovery URL:
Enter the URL displayed to users who have forgotten their password.

13. 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.



Web Logins

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for visitors accessing the network through these NAS devices.

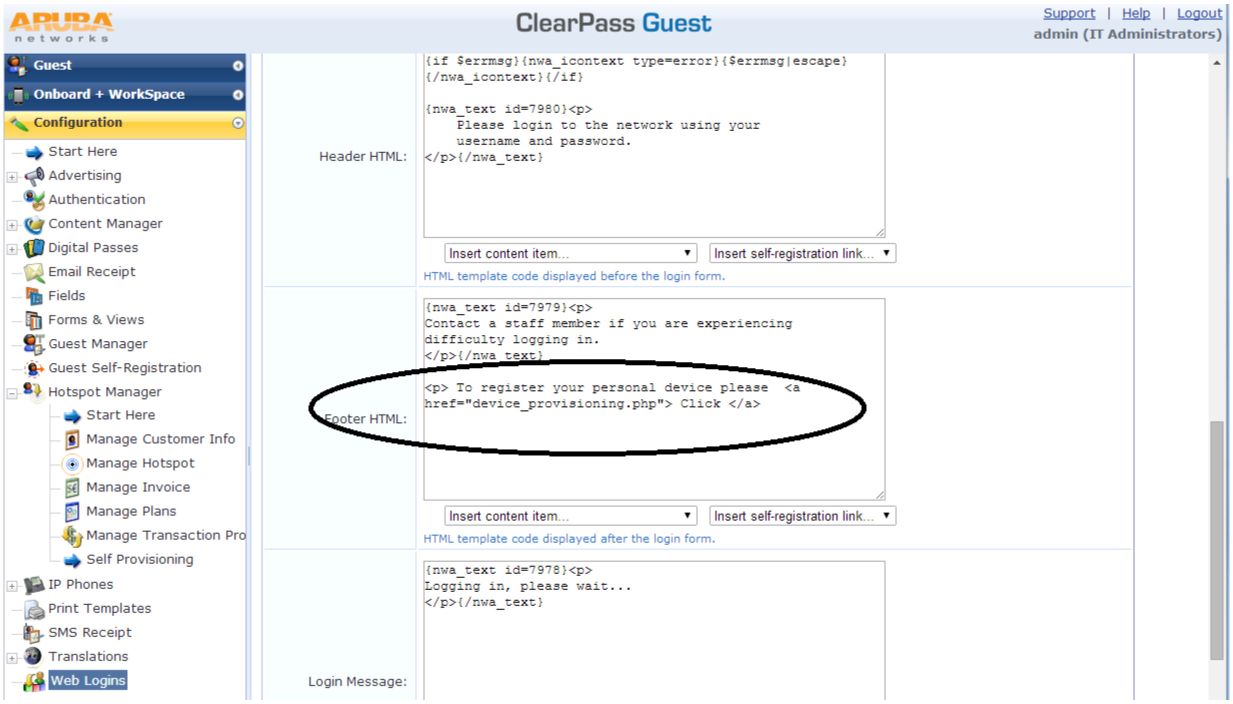
Use this list view to define new web login pages, and to make changes to existing web login pages.

Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

△ Name	Page Title	Page Name	Page Skin
Alcatel-Lucent Secure Access Alcatel-Lucent Secure Access		secure-access	(Default)
Copy of Alcatel-Lucent Secure Access Alcatel-Lucent Secure Access		secure-access_1	(Default)
health check health check		healthcheck	(Default)

3 web logins

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.



Header HTML:

```
{if $errmsg}{nwa_icontext type=error}{$errmsg|escape}
{/nwa_icontext}{/if}

{nwa_text id=7980}<p>
    Please login to the network using your
    username and password.
</p>{/nwa_text}
```

HTML template code displayed before the login form.

Footer HTML:

```
{nwa_text id=7979}<p>
Contact a staff member if you are experiencing
difficulty logging in.
</p>{/nwa_text}

<p> To register your personal device please  <a
href="device_provisioning.php"> Click </a>
```

HTML template code displayed after the login form.

Login Message:

```
{nwa_text id=7978}<p>
Logging in, please wait...
</p>{/nwa_text}
```

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:

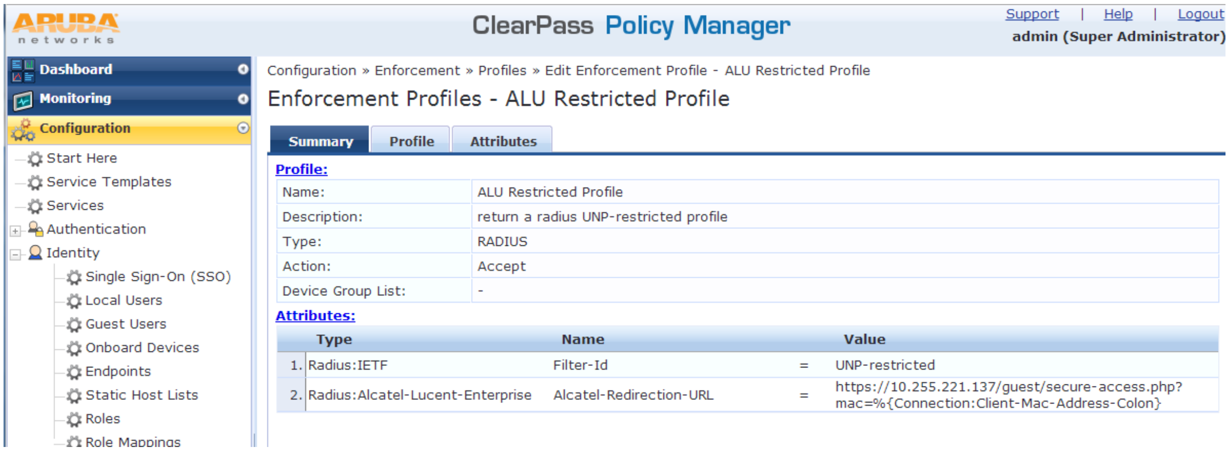
1. Restricted profile, which returns UNP-restricted to put the device with limited access and redirection
2. [Allow All Access] profile to communicate to the internal Onboard module
3. BYOD profile, which returns UNP-byod to the device post onboard provisioning

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}



Enforcement Profiles - ALU Restricted Profile

Profile:

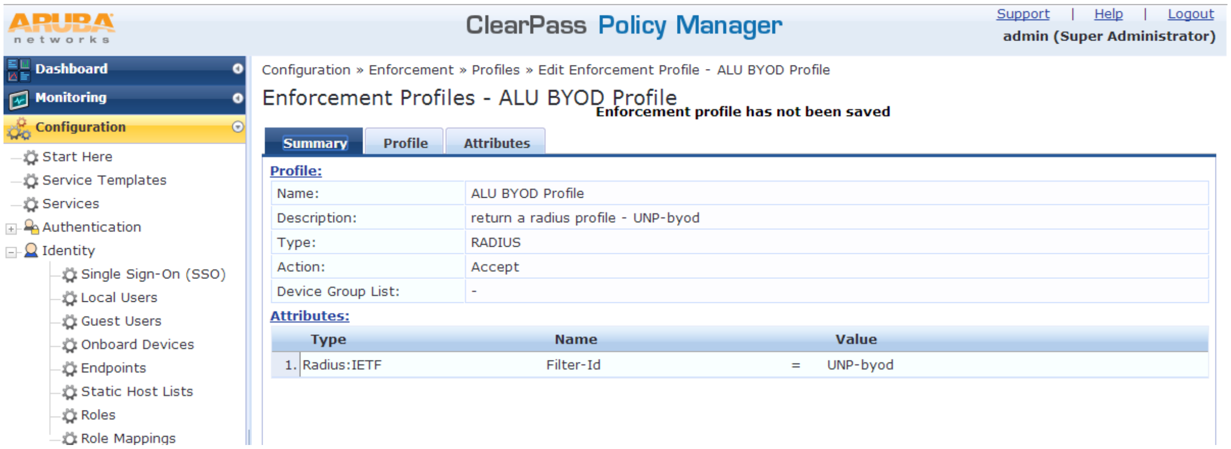
Name:	ALU Restricted Profile
Description:	return a radius UNP-restricted profile
Type:	RADIUS
Action:	Accept
Device Group List:	-

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.



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

Enforcement Profiles - ALU BYOD Profile

Enforcement profile has not been saved

Profile:

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

Attributes:

	Type	Name		Value
1.	Radius:IETF	Filter-Id	=	UNP-byod

5.7.2.4 Creating enforcement policy

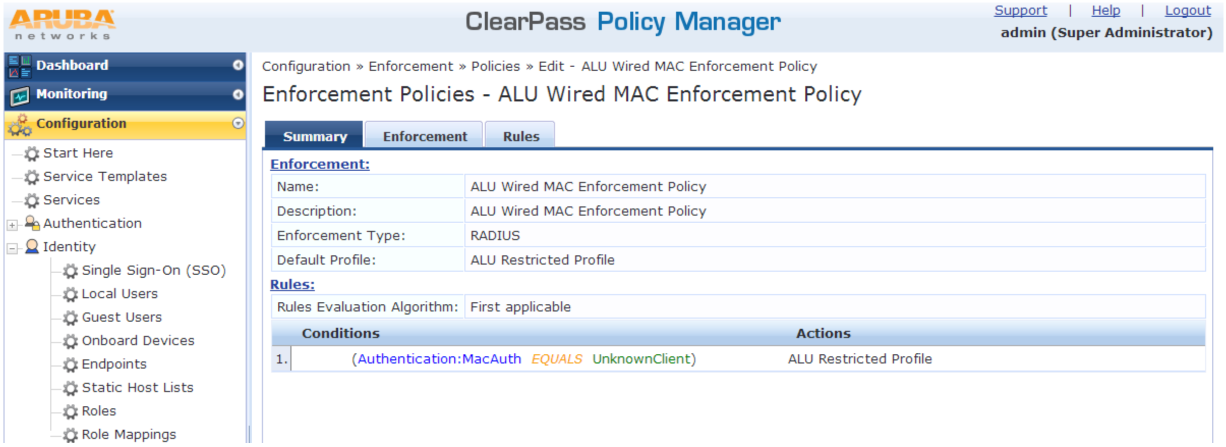
Every service is associated with an enforcement policy. Enforcement policy is configured to return different enforcement profiles based on a set of rules defined. For the Onboarding use case, there are three services that come into play:

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



Configuration » Enforcement » Policies » Edit - ALU Wired MAC Enforcement Policy

Enforcement Policies - ALU Wired MAC Enforcement Policy

Enforcement:

Name:	ALU Wired MAC Enforcement Policy
Description:	ALU Wired MAC Enforcement Policy
Enforcement Type:	RADIUS
Default Profile:	ALU Restricted Profile

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Authentication:MacAuth EQUALS UnknownClient)	ALU Restricted Profile

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:

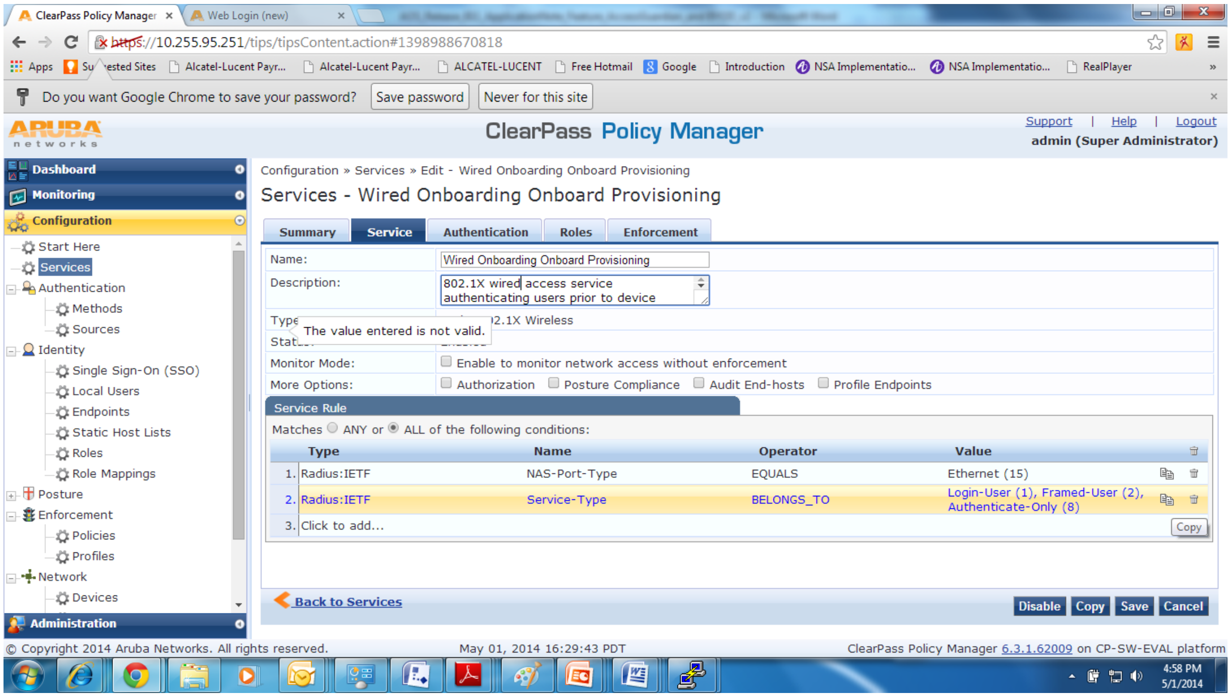
- MAC Authentication service for pre-onboard

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:

1. Go to Configuration/Services and select Create a New Service



Configuration » Services » Edit - Wired Onboarding Onboard Provisioning

Services - Wired Onboarding Onboard Provisioning

Name: Wired Onboarding Onboard Provisioning

Description: 802.1X wired access service authenticating users prior to device

Type: 802.1X Wireless

The value entered is not valid.

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: □ Authorization □ Posture Compliance □ Audit End-hosts □ Profile Endpoints

Service Rule

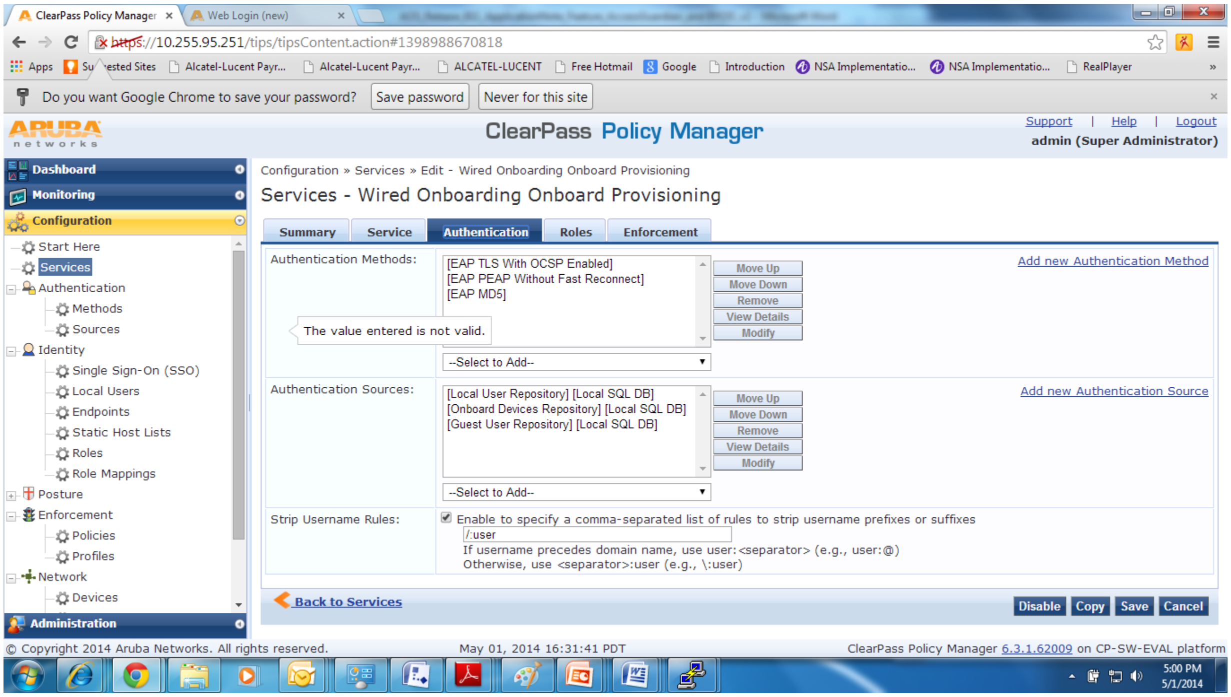
Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...			

© Copyright 2014 Aruba Networks. All rights reserved. May 01, 2014 16:29:43 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

4:58 PM 5/1/2014

2. Select the following authentication methods and sources as shown



Configuration » Services » Edit - Wired Onboarding Onboard Provisioning

Services - Wired Onboarding Onboard Provisioning

Authentication Methods:
[EAP TLS With OCSP Enabled]
[EAP PEAP Without Fast Reconnect]
[EAP MD5]

The value entered is not valid.

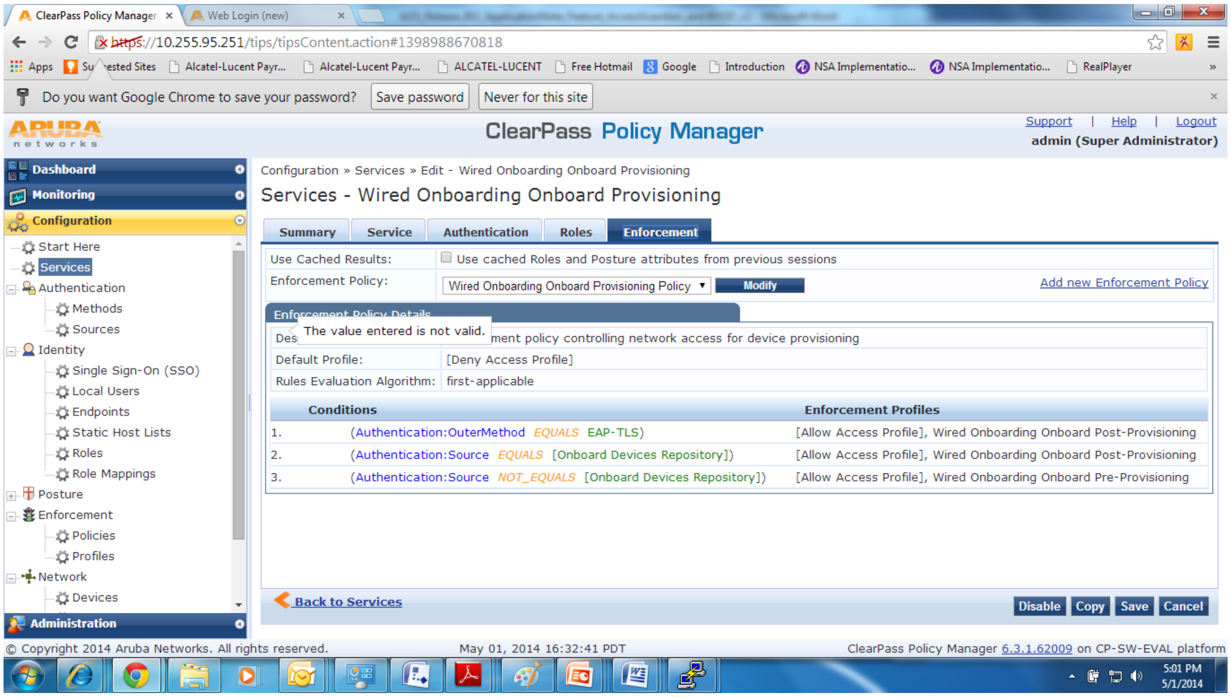
Authentication Sources:
[Local User Repository] [Local SQL DB]
[Onboard Devices Repository] [Local SQL DB]
[Guest User Repository] [Local SQL DB]

Strip Username Rules: ☑ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes
/:user
If username precedes domain name, use user:<separator> (e.g., user:@)
Otherwise, use <separator>:user (e.g., \:user)

© Copyright 2014 Aruba Networks. All rights reserved. May 01, 2014 16:31:41 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

5:00 PM 5/1/2014

3. Set the enforcement policy that was previously created.



Configuration » Services » Edit - Wired Onboarding Onboard Provisioning

Services - Wired Onboarding Onboard Provisioning

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Wired Onboarding Onboard Provisioning Policy

Enforcement Policy Details

Des The value entered is not valid. ment policy controlling network access for device provisioning

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Authentication:OuterMethod EQUALS EAP-TLS)	[Allow Access Profile], Wired Onboarding Onboard Post-Provisioning
2.	(Authentication:Source EQUALS [Onboard Devices Repository])	[Allow Access Profile], Wired Onboarding Onboard Post-Provisioning
3.	(Authentication:Source NOT_EQUALS [Onboard Devices Repository])	[Allow Access Profile], Wired Onboarding Onboard Pre-Provisioning

© Copyright 2014 Aruba Networks. All rights reserved. May 01, 2014 16:32:41 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

- 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 perfom a one-time check at login to ensure compliance. Once the browser page used for authentication is closed, the dissolvable agent is removed.

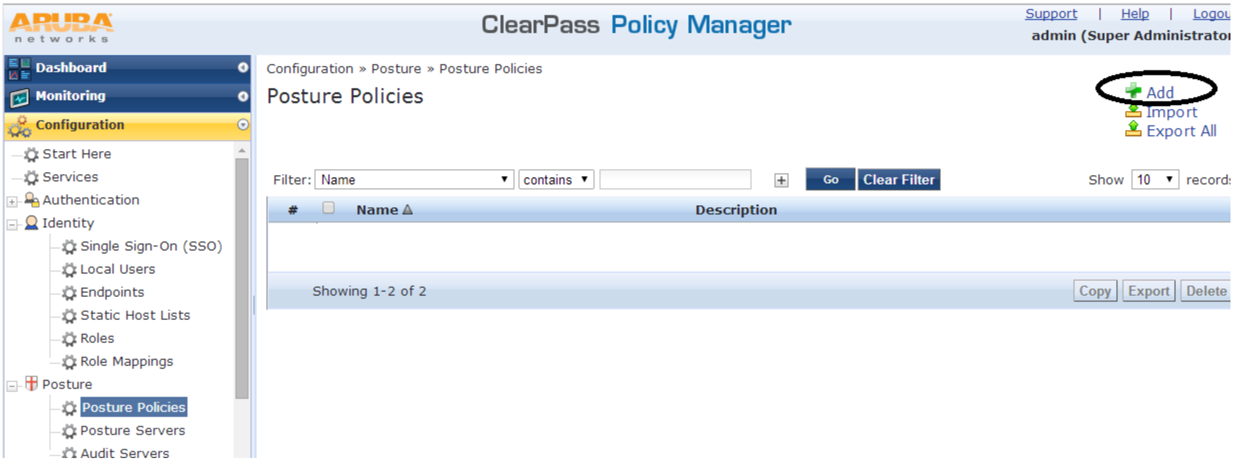
If unhealthy, the endpoints receive a message about the status and the message can include reasons for remediation, links to helpful URLs and the switch authenticating the user puts the client in a restricted mode with instructions to redirect the http traffic to the remediation URL.

5.8.1 Enabling BYOD USECASE 1 - Guest Access with Posture

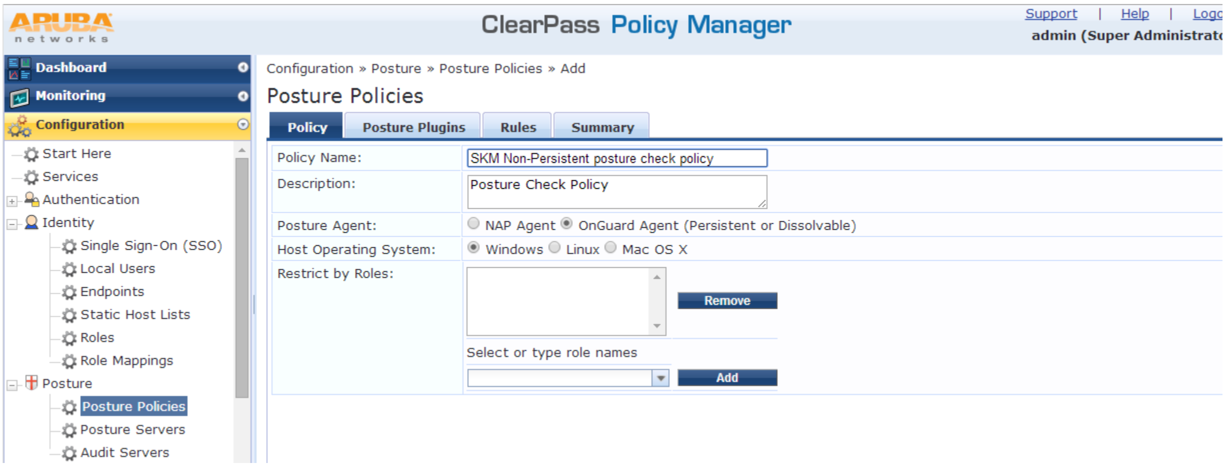
This use case can be enhanced to support Posture by taking the following steps:

5.8.1.1 Configuring the OnGuard Module on the CPPM

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

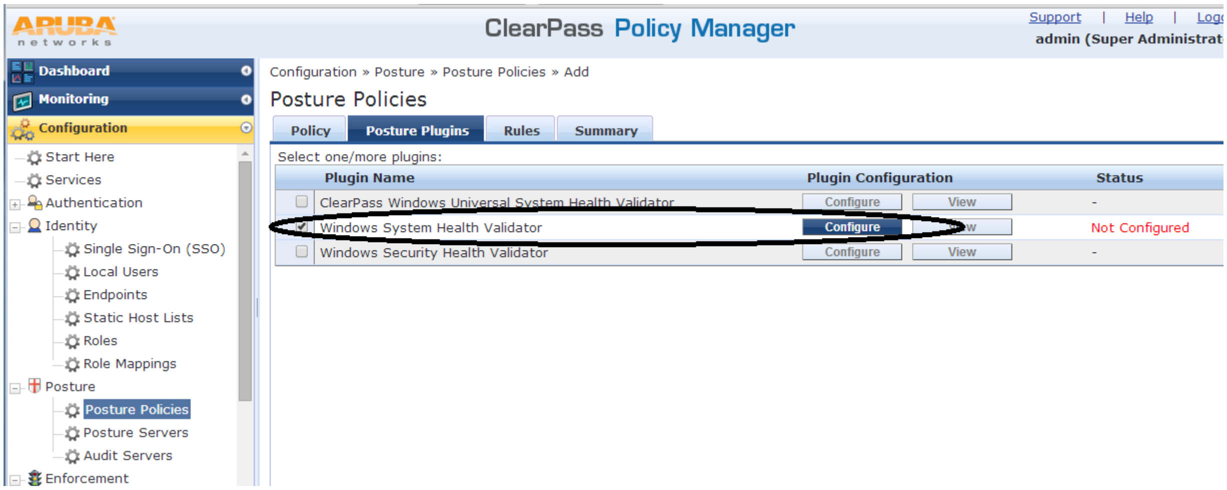


2. In the Policy tab, update the Policy Name and Description. Choose the client types to validate. The example shows a health check for Windows clients only.



Policy Name:	SKM Non-Persistent posture check policy
Description:	Posture Check Policy
Posture Agent:	○ NAP Agent ● OnGuard Agent (Persistent or Dissolvable)
Host Operating System:	● Windows ○ Linux ○ Mac OS X
Restrict by Roles:	

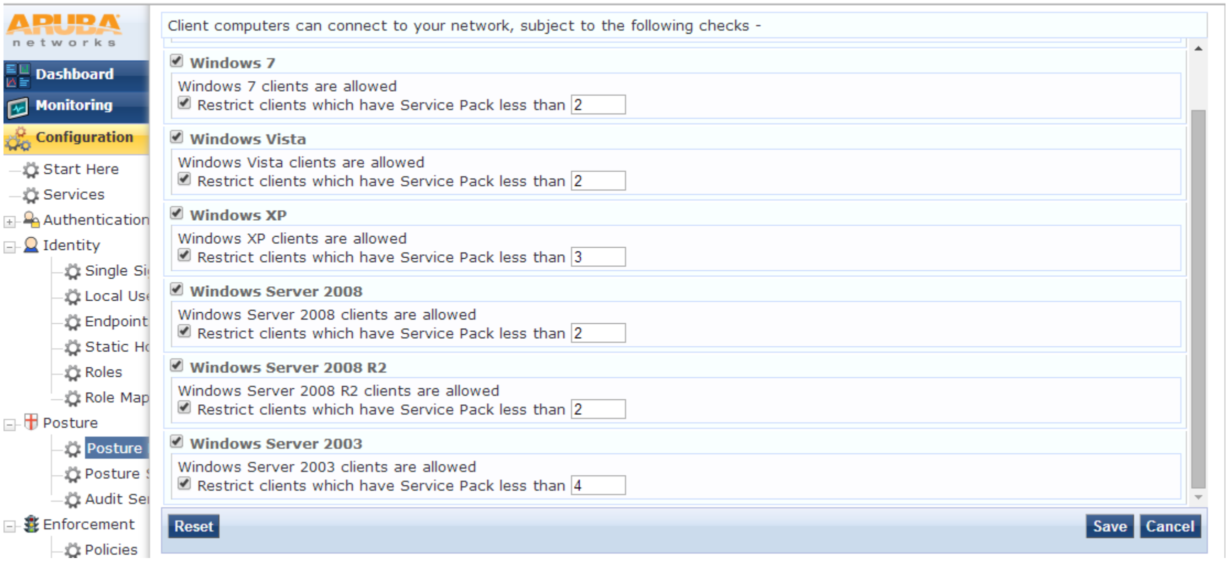
3. In the Posture Plugins tab, select "Windows System Health Validator" and "Configure".



Select one/more plugins:

	Plugin Name	Plugin Configuration		Status
☐	ClearPass Windows Universal System Health Validator	Configure	View	-
☑	Windows System Health Validator	Configure	View	Not Configured
☐	Windows Security Health Validator	Configure	View	-

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



Client computers can connect to your network, subject to the following checks -

☑ Windows 7
Windows 7 clients are allowed
☑ Restrict clients which have Service Pack less than 2

☑ Windows Vista
Windows Vista clients are allowed
☑ Restrict clients which have Service Pack less than 2

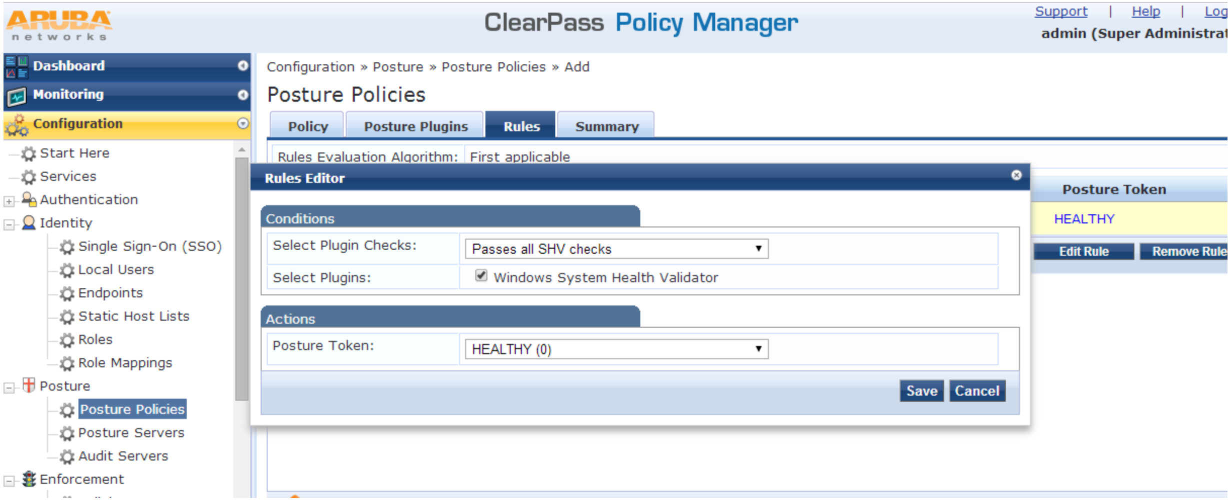
☑ Windows XP
Windows XP clients are allowed
☑ Restrict clients which have Service Pack less than 3

☑ Windows Server 2008
Windows Server 2008 clients are allowed
☑ Restrict clients which have Service Pack less than 2

☑ Windows Server 2008 R2
Windows Server 2008 R2 clients are allowed
☑ Restrict clients which have Service Pack less than 2

☑ Windows Server 2003
Windows Server 2003 clients are allowed
☑ Restrict clients which have Service Pack less than 4

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.

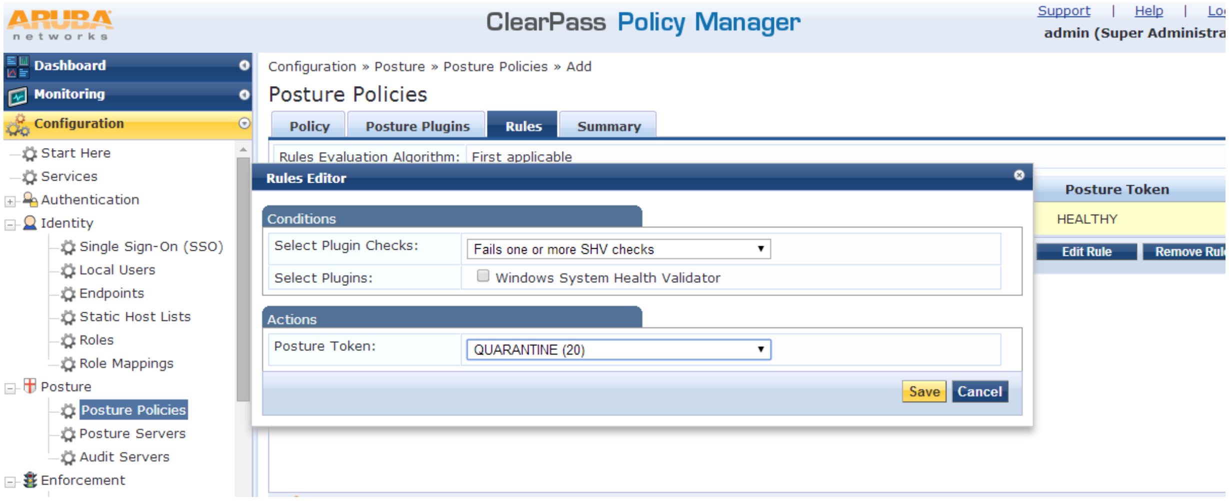


Rules Evaluation Algorithm: First applicable

Conditions
Select Plugin Checks: Passes all SHV checks
Select Plugins: ☑ Windows System Health Validator

Actions
Posture Token: HEALTHY (0)

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.

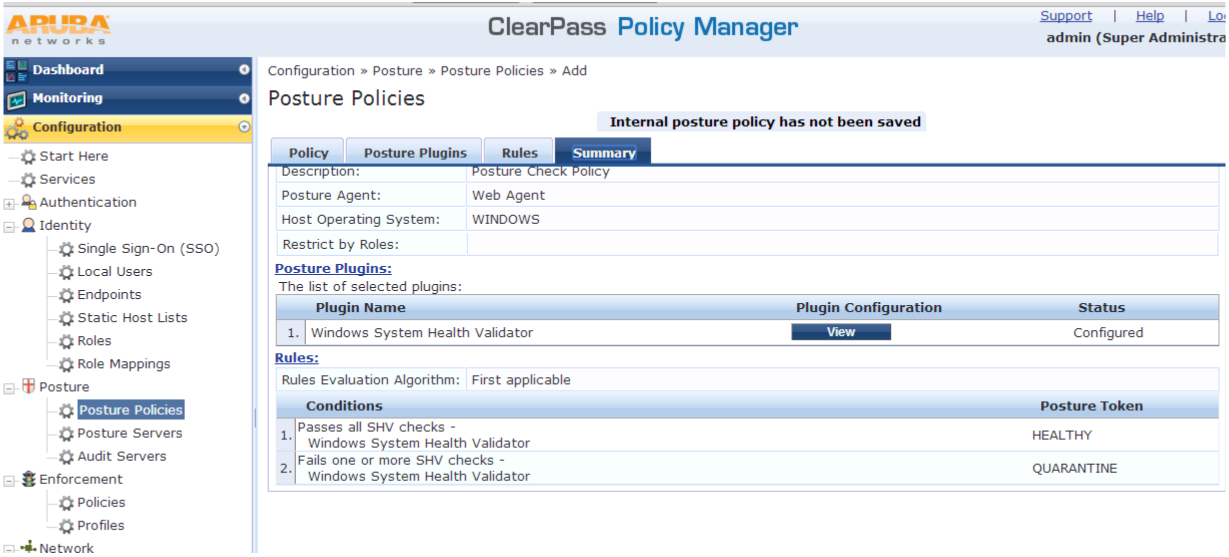


Rules Evaluation Algorithm: First applicable

Conditions
Select Plugin Checks: Fails one or more SHV checks
Select Plugins: ☐ Windows System Health Validator

Actions
Posture Token: QUARANTINE (20)

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



Internal posture policy has not been saved

Description:	Posture Check Policy
Posture Agent:	Web Agent
Host Operating System:	WINDOWS
Restrict by Roles:	

Posture Plugins:

The list of selected plugins:

	Plugin Name	Plugin Configuration	Status
1.	Windows System Health Validator	View	Configured

Rules:

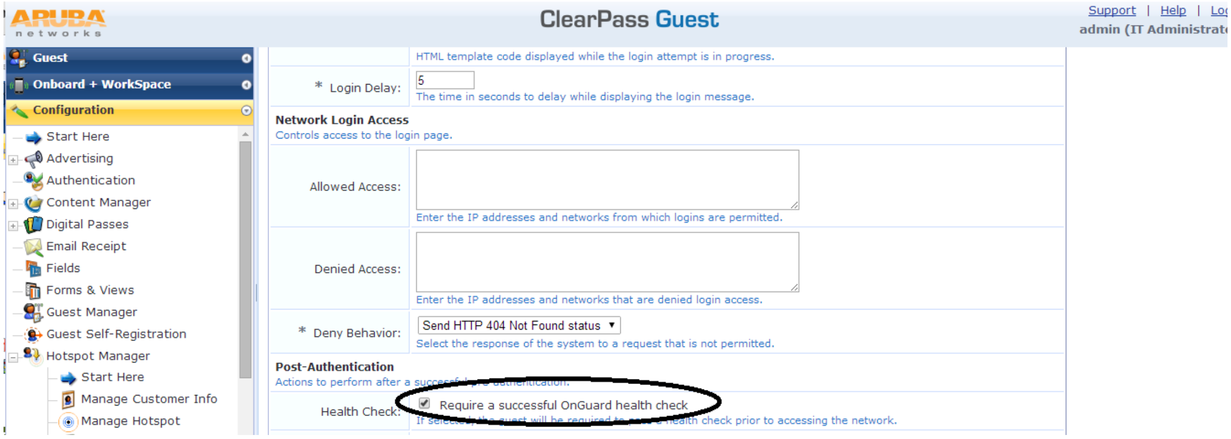
Rules Evaluation Algorithm: First applicable

	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.



HTML template code displayed while the login attempt is in progress.

* Login Delay: 5
The time in seconds to delay while displaying the login message.

Network Login Access
Controls access to the login page.

Allowed Access:
Enter the IP addresses and networks from which logins are permitted.

Denied Access:
Enter the IP addresses and networks that are denied login access.

* Deny Behavior: Send HTTP 404 Not Found status
Select the response of the system to a request that is not permitted.

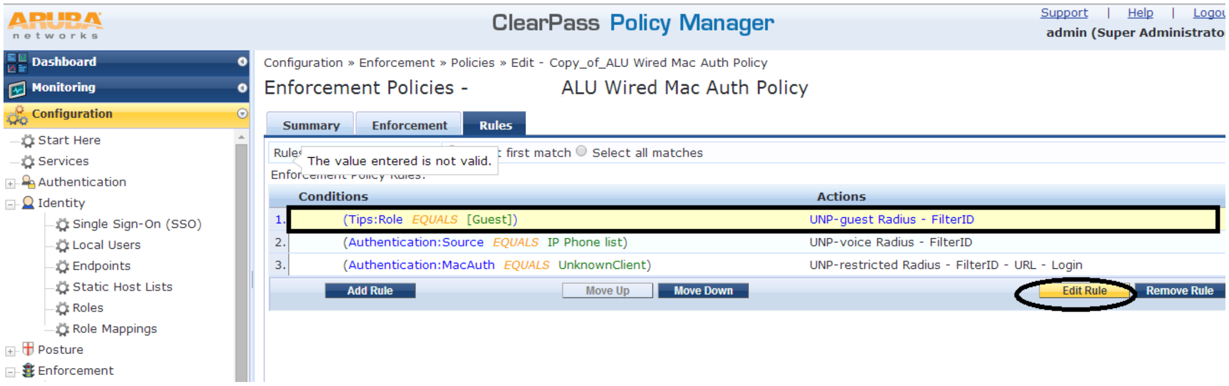
Post-Authentication
Actions to perform after a successful pre-authentication.

Health Check: ☑ Require a successful OnGuard health check
If selected, the guest will be required to pass a health check prior to accessing 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.



Configuration » Enforcement » Policies » Edit - Copy_of_ALU Wired Mac Auth Policy

Enforcement Policies - ALU Wired Mac Auth Policy

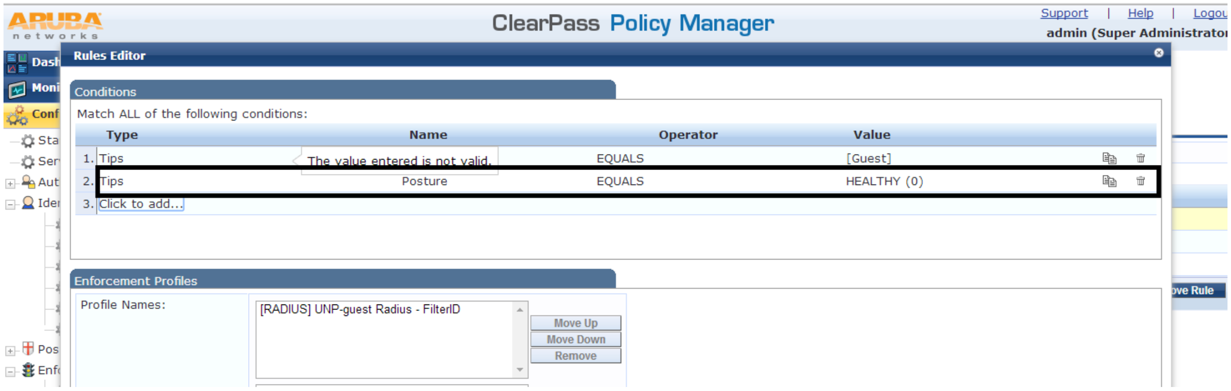
Rule… first match ○ Select all matches

The value entered is not valid.

Enforcement Policy Rules:

	Conditions	Actions
1.	(Tips:Role EQUALS [Guest])	UNP-guest Radius - FilterID
2.	(Authentication:Source EQUALS IP Phone list)	UNP-voice Radius - FilterID
3.	(Authentication:MacAuth EQUALS UnknownClient)	UNP-restricted Radius - FilterID - URL - Login

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



Rules Editor

Conditions

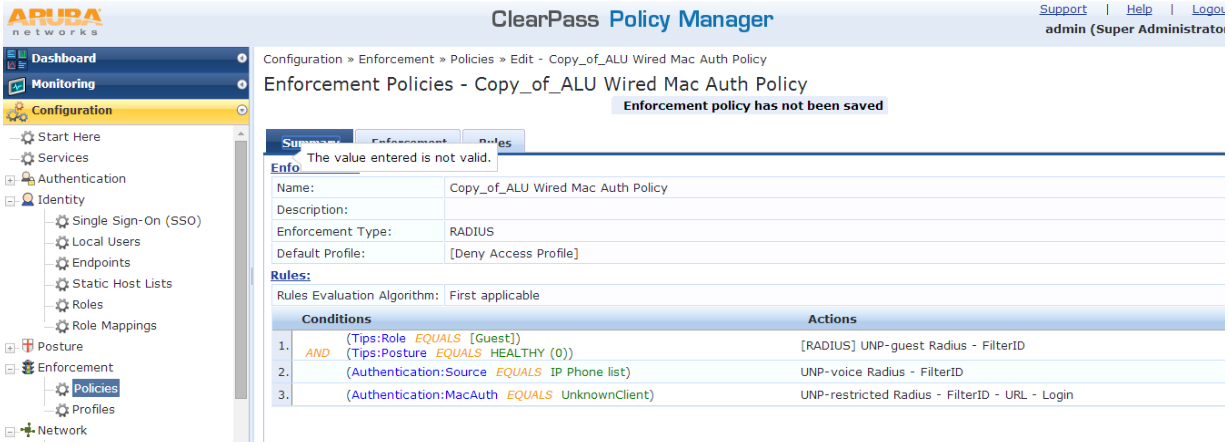
Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Tips	The value entered is not valid.	EQUALS	[Guest]
2.	Tips	Posture	EQUALS	HEALTHY (0)
3.	Click to add...			

Enforcement Profiles

Profile Names: [RADIUS] UNP-guest Radius - FilterID

3. The modified Enforcement Policy should be as follows



Configuration » Enforcement » Policies » Edit - Copy_of_ALU Wired Mac Auth Policy

Enforcement Policies - Copy_of_ALU Wired Mac Auth Policy

Enforcement policy has not been saved

The value entered is not valid.

Enfo…

Name:	Copy_of_ALU Wired Mac Auth Policy
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

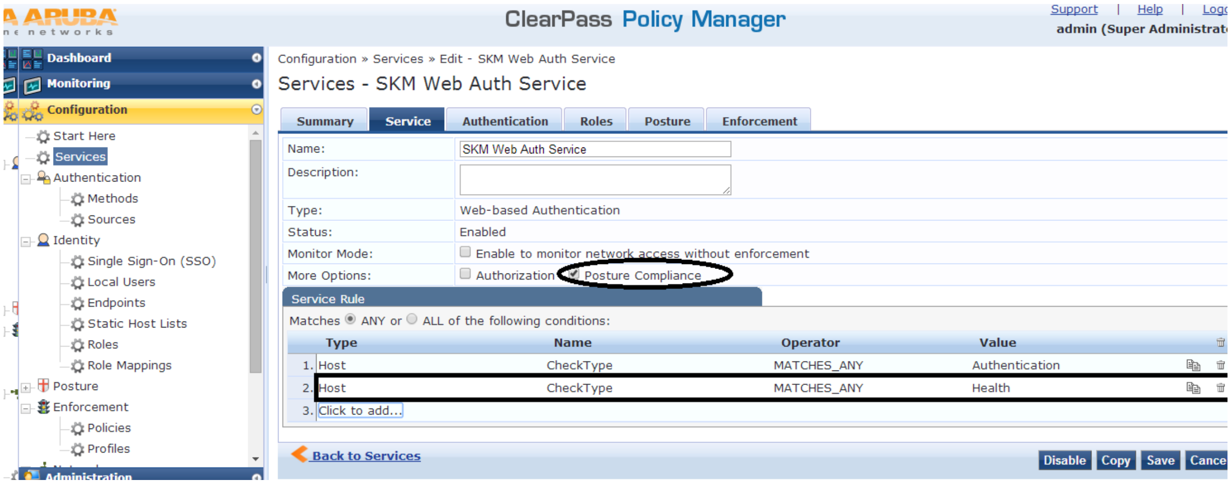
Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS [Guest]) AND (Tips:Posture EQUALS HEALTHY (0))	[RADIUS] UNP-guest Radius - FilterID
2.	(Authentication:Source EQUALS IP Phone list)	UNP-voice Radius - FilterID
3.	(Authentication:MacAuth EQUALS UnknownClient)	UNP-restricted Radius - FilterID - URL - Login

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.



Configuration » Services » Edit - SKM Web Auth Service

Services - SKM Web Auth Service

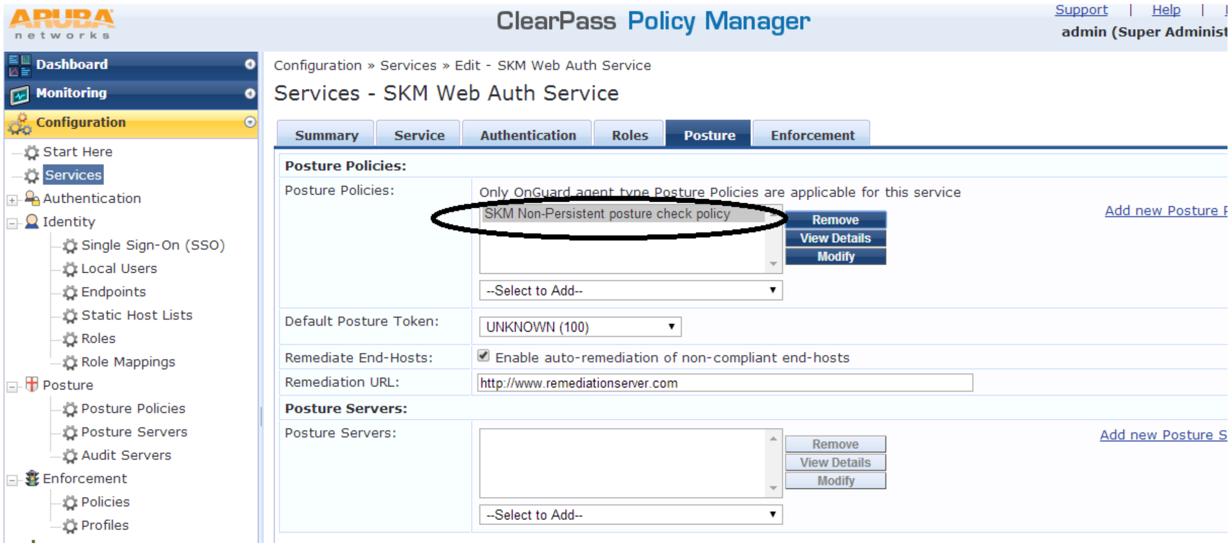
Name:	SKM Web Auth Service
Description:	
Type:	Web-based Authentication
Status:	Enabled
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization ☑ Posture Compliance

Service Rule

Matches ● ANY or ○ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Host	CheckType	MATCHES_ANY	Authentication
2.	Host	CheckType	MATCHES_ANY	Health
3.	Click to add...			

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



Configuration » Services » Edit - SKM Web Auth Service

Services - SKM Web Auth Service

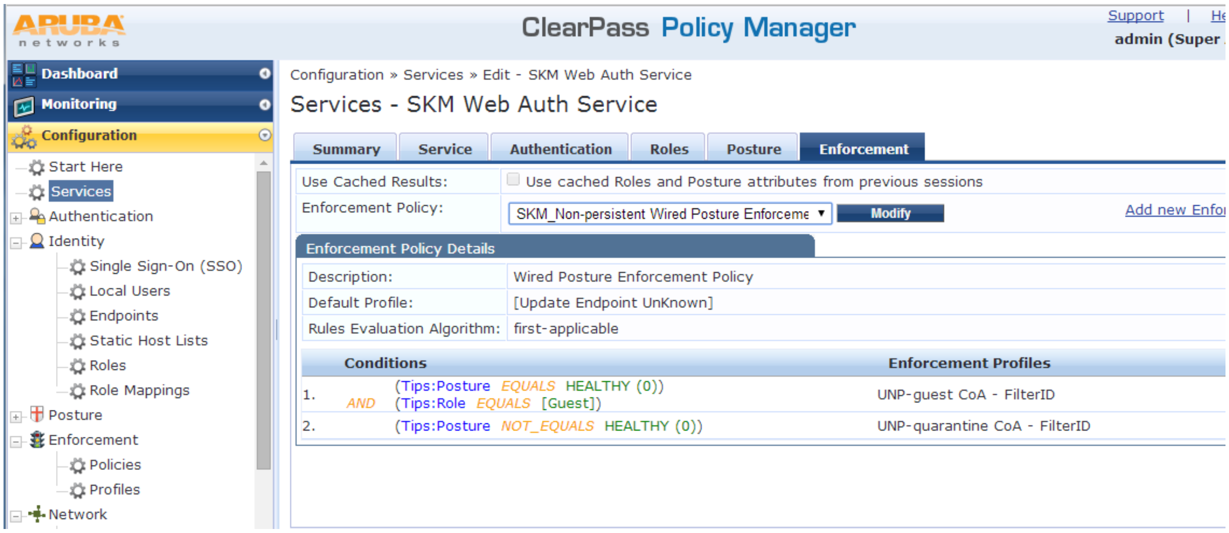
Posture Policies:

Posture Policies:	Only OnGuard agent type Posture Policies are applicable for this service SKM Non-Persistent posture check policy --Select to Add--
Default Posture Token:	UNKNOWN (100)
Remediate End-Hosts:	☑ Enable auto-remediation of non-compliant end-hosts
Remediation URL:	http://www.remediationserver.com

Posture Servers:

Posture Servers:	--Select to Add--

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



Configuration » Services » Edit - SKM Web Auth Service

Services - SKM Web Auth Service

Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	SKM_Non-persistent Wired Posture Enforceme ▾

Enforcement Policy Details

Description:	Wired Posture Enforcement Policy
Default Profile:	[Update Endpoint UnKnown]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Posture EQUALS HEALTHY (0)) AND (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:

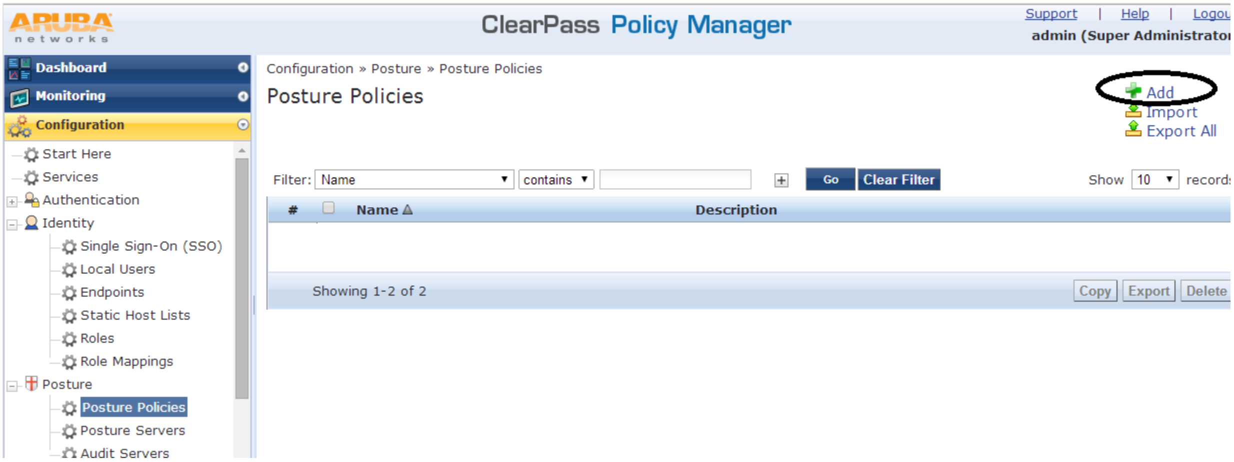
1. The client connects to a UNP edge port enabled for MAC authentication.
2. The switch sends a RADIUS MAC authentication request to the CPPM.
3. Since the client is UNKNOWN, the MAC authentication service will send a RADIUS response with:
    a. Filter-Id equals UNP-restricted
    b. Redirection URL 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.

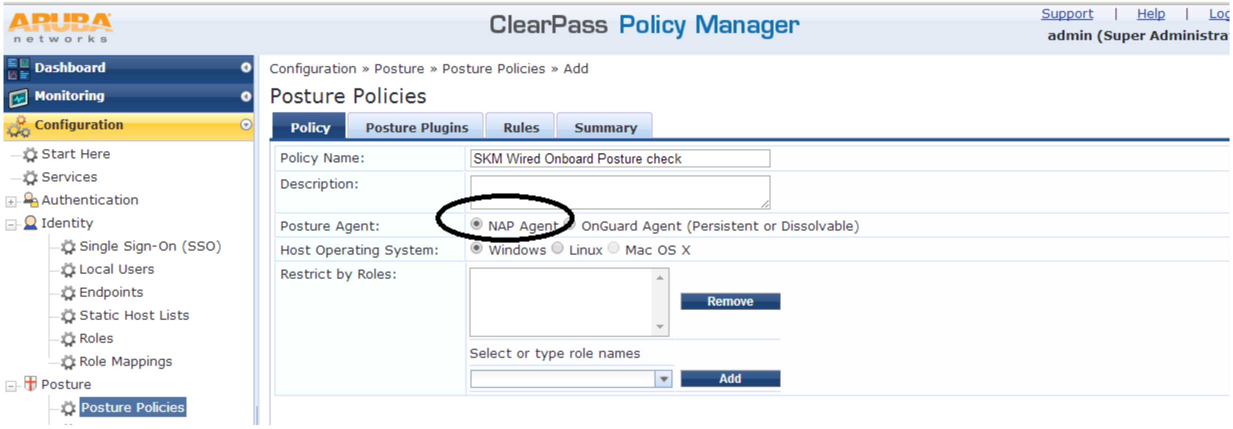


Filter: Name ▾ contains ▾ Show 10 ▾ record

#	☐	Name ▲	Description

Showing 1-2 of 2

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.



Policy Name: SKM Wired Onboard Posture check

Description:

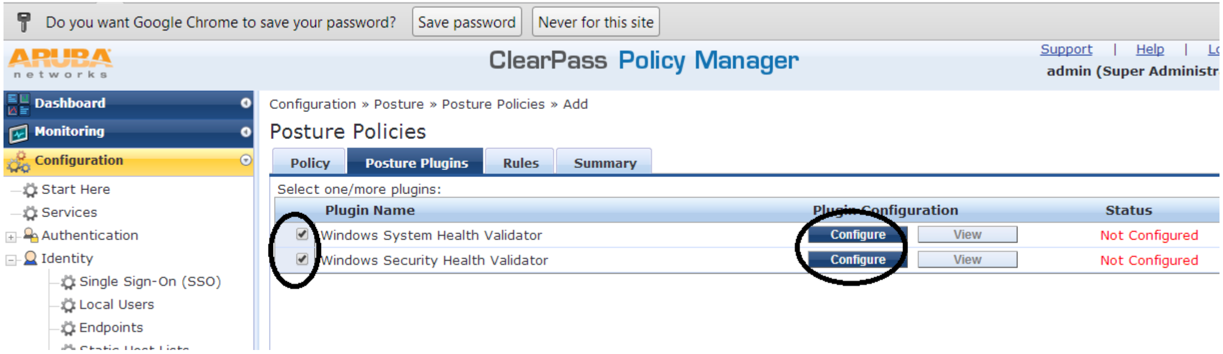
Posture Agent: ● NAP Agent ○ OnGuard Agent (Persistent or Dissolvable)

Host Operating System: ● Windows ○ Linux ○ Mac OS X

Restrict by Roles:

Select or type role names

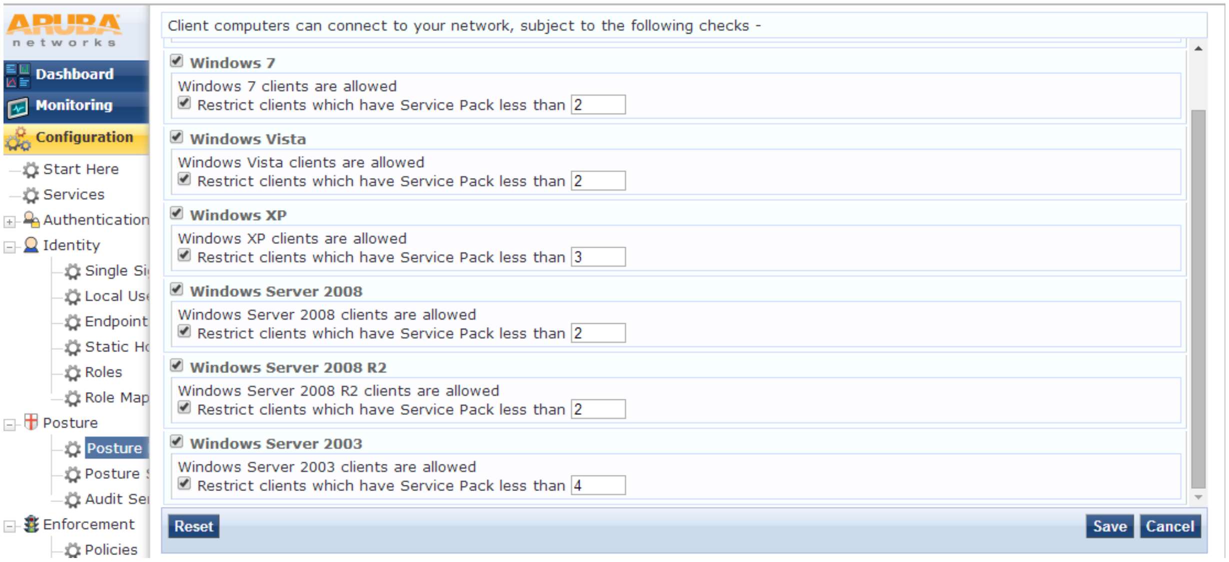
3. In the Posture Plugins tab, select "Windows System Health Check" and "Windows Security Health Validator". Configure each one as required.



Select one/more plugins:

	Plugin Name	Plugin Configuration		Status
☑	Windows System Health Validator	Configure	View	Not Configured
☑	Windows Security Health Validator	Configure	View	Not Configured

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



Client computers can connect to your network, subject to the following checks -

☑ Windows 7
Windows 7 clients are allowed
☑ Restrict clients which have Service Pack less than 2

☑ Windows Vista
Windows Vista clients are allowed
☑ Restrict clients which have Service Pack less than 2

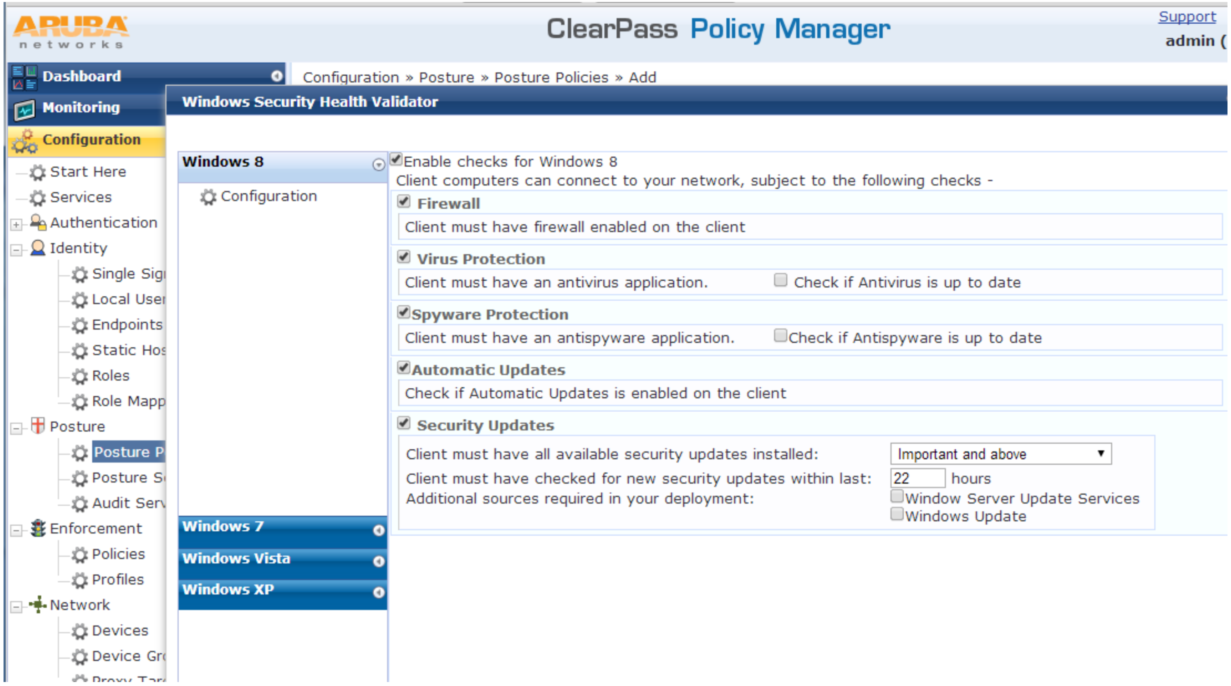
☑ Windows XP
Windows XP clients are allowed
☑ Restrict clients which have Service Pack less than 3

☑ Windows Server 2008
Windows Server 2008 clients are allowed
☑ Restrict clients which have Service Pack less than 2

☑ Windows Server 2008 R2
Windows Server 2008 R2 clients are allowed
☑ Restrict clients which have Service Pack less than 2

☑ Windows Server 2003
Windows Server 2003 clients are allowed
☑ Restrict clients which have Service Pack less than 4

5. 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.



Configuration » Posture » Posture Policies » Add

Windows Security Health Validator

☑ Enable checks for Windows 8
Client computers can connect to your network, subject to the following checks -

☑ Firewall
Client must have firewall enabled on the client

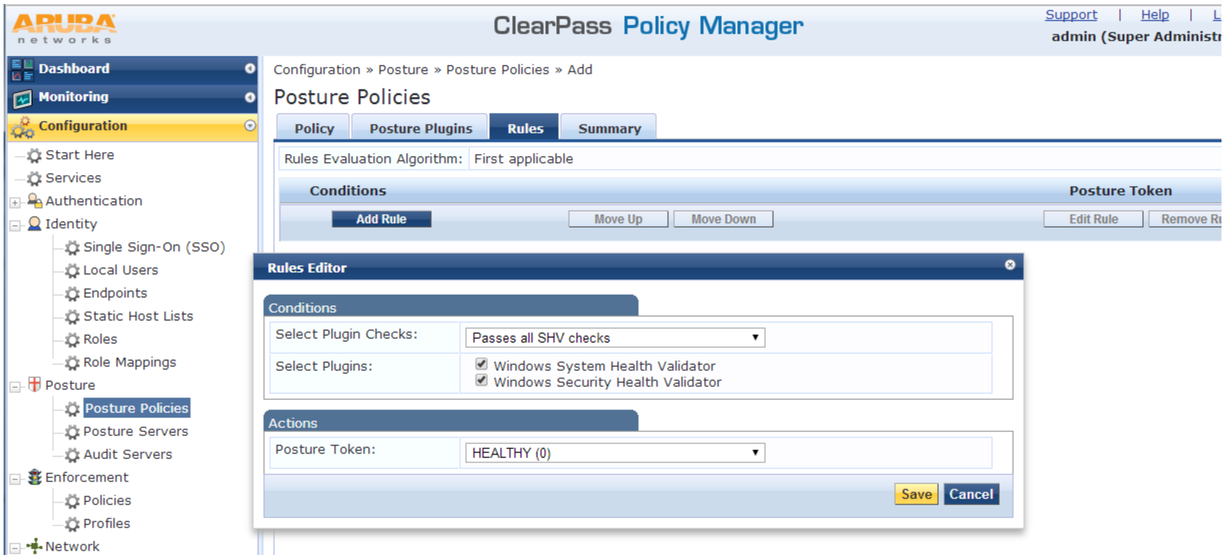
☑ Virus Protection
Client must have an antivirus application. ☐ Check if Antivirus is up to date

☑ Spyware Protection
Client must have an antispyware application. ☐ Check if Antispyware is up to date

☑ Automatic Updates
Check if Automatic Updates is enabled on the client

☑ Security Updates
Client must have all available security updates installed: Important and above
Client must have checked for new security updates within last: 22 hours
Additional sources required in your deployment: ☐ Window Server Update Services ☐ Windows Update

6. 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.



Configuration » Posture » Posture Policies » Add

Posture Policies

Rules Evaluation Algorithm: First applicable

Conditions	Posture Token

Rules Editor

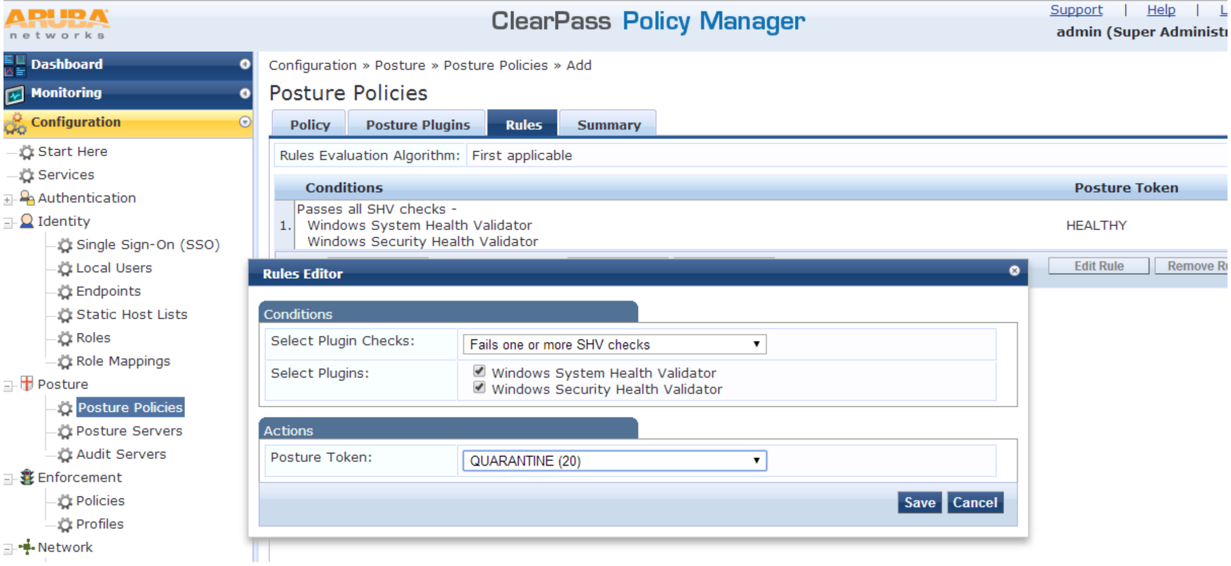
Conditions

Select Plugin Checks:	Passes all SHV checks
Select Plugins:	☑ Windows System Health Validator ☑ Windows Security Health Validator

Actions

Posture Token:	HEALTHY (0)

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.



Configuration » Posture » Posture Policies » Add

Posture Policies

Rules Evaluation Algorithm: First applicable

	Conditions	Posture Token
1.	Passes all SHV checks - Windows System Health Validator Windows Security Health Validator	HEALTHY

Rules Editor

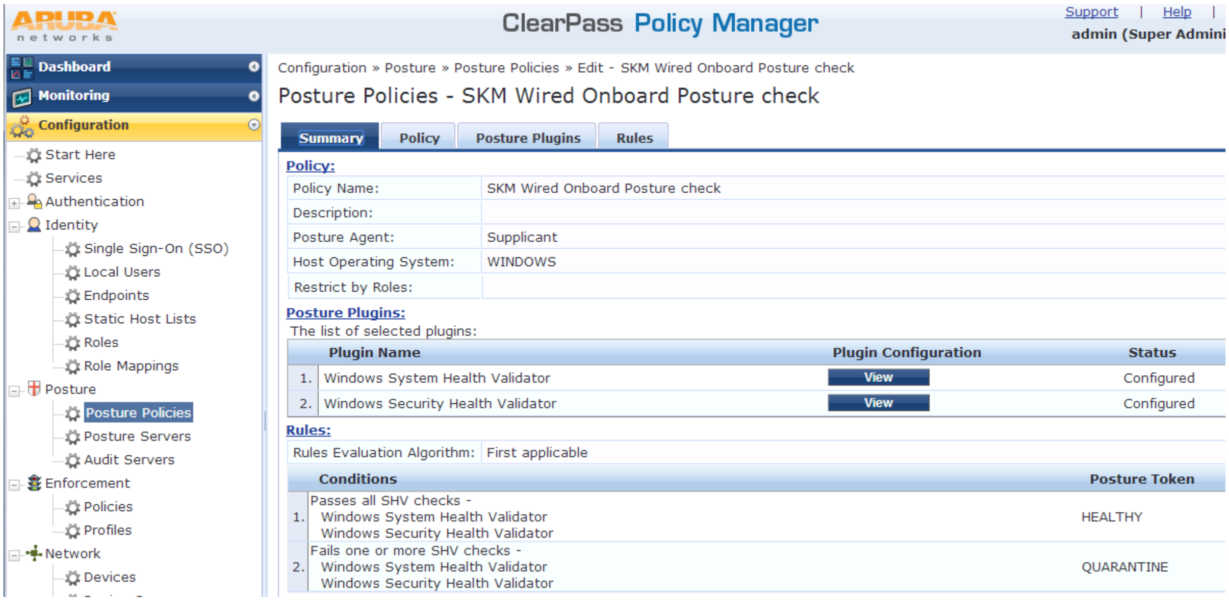
Conditions

Select Plugin Checks:	Fails one or more SHV checks
Select Plugins:	☑ Windows System Health Validator ☑ Windows Security Health Validator

Actions

Posture Token:	QUARANTINE (20)

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



Configuration » Posture » Posture Policies » Edit - SKM Wired Onboard Posture check

Posture Policies - SKM Wired Onboard Posture check

Policy:

Policy Name:	SKM Wired Onboard Posture check
Description:	
Posture Agent:	Supplicant
Host Operating System:	WINDOWS
Restrict by Roles:	

Posture Plugins:

The list of selected plugins:

	Plugin Name	Plugin Configuration	Status
1.	Windows System Health Validator	View	Configured
2.	Windows Security Health Validator	View	Configured

Rules:

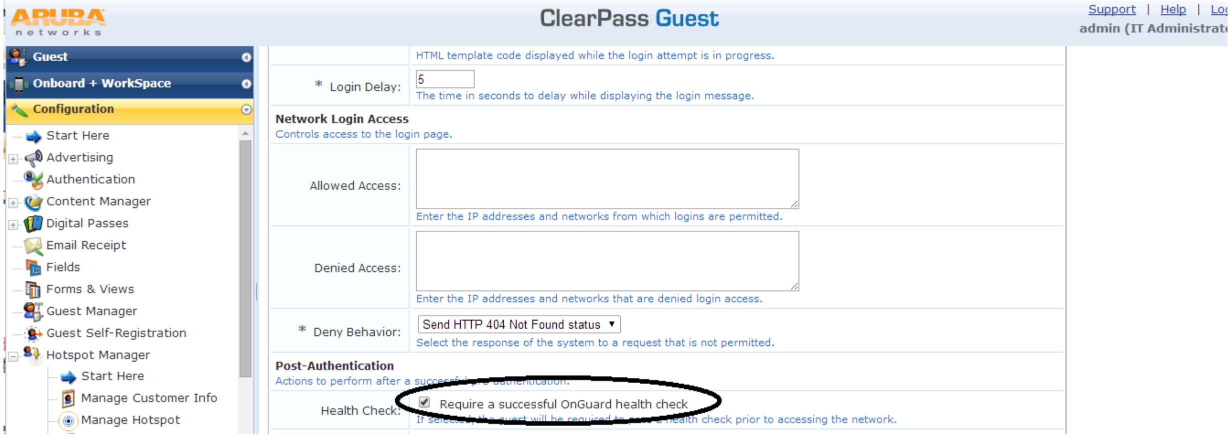
Rules Evaluation Algorithm: First applicable

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

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.



HTML template code displayed while the login attempt is in progress.

* Login Delay:	5 The time in seconds to delay while displaying the login message.

Network Login Access
Controls access to the login page.

Allowed Access:	Enter the IP addresses and networks from which logins are permitted.
Denied Access:	Enter the IP addresses and networks that are denied login access.
* Deny Behavior:	Send HTTP 404 Not Found status ▾ Select the response of the system to a request that is not permitted.

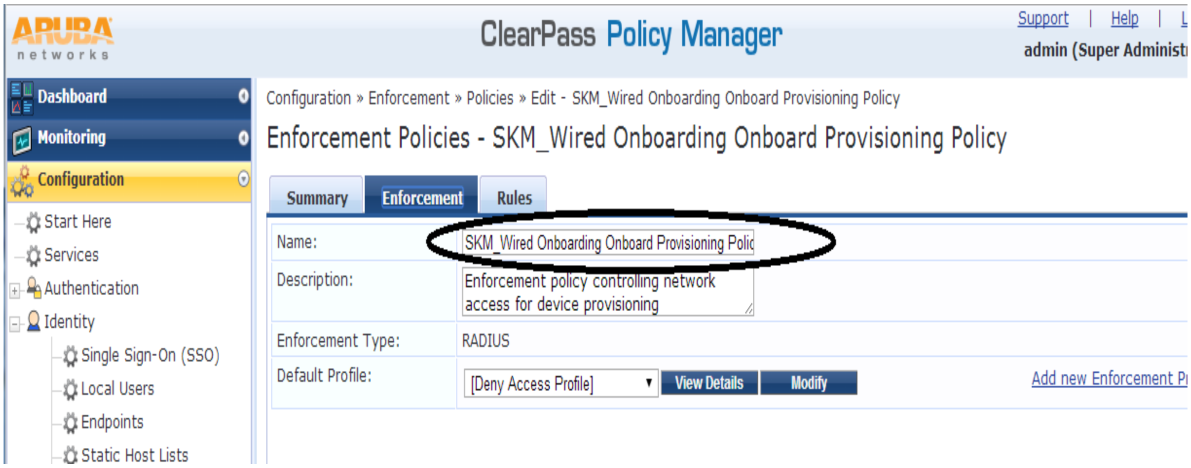
Post-Authentication
Actions to perform after a successful pre-authentication.

Health Check:	☑ Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.

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

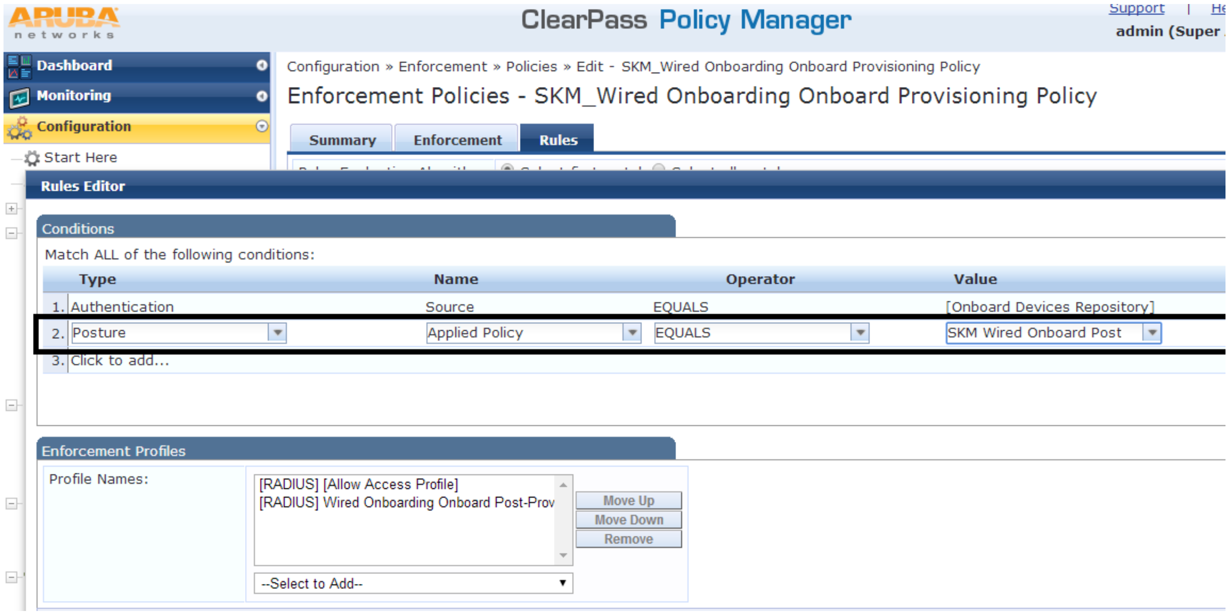
1. Go to Configuration/Enforcement/Policies and select SKM Wired Onboard Enforcement Policy. Add a rule to check for healthy state of the Client. Select the rule and select Edit.



Configuration » Enforcement » Policies » Edit - SKM_Wired Onboarding Onboard Provisioning Policy

Enforcement Policies - SKM_Wired Onboarding Onboard Provisioning Policy

Name:	SKM_Wired Onboarding Onboard Provisioning Polic
Description:	Enforcement policy controlling network access for device provisioning
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]



Configuration » Enforcement » Policies » Edit - SKM_Wired Onboarding Onboard Provisioning Policy

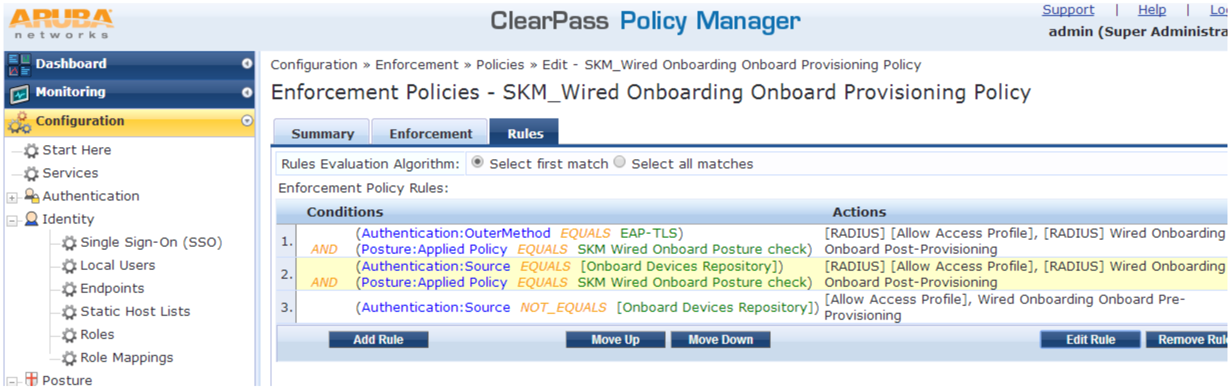
Enforcement Policies - SKM_Wired Onboarding Onboard Provisioning Policy

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authentication	Source	EQUALS	[Onboard Devices Repository]
2.	Posture	Applied Policy	EQUALS	SKM Wired Onboard Post
3.	Click to add...			

Profile Names:
[RADIUS] [Allow Access Profile]
[RADIUS] Wired Onboarding Onboard Post-Prov
--Select to Add--

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



Configuration » Enforcement » Policies » Edit - SKM_Wired Onboarding Onboard Provisioning Policy

Enforcement Policies - SKM_Wired Onboarding Onboard Provisioning Policy

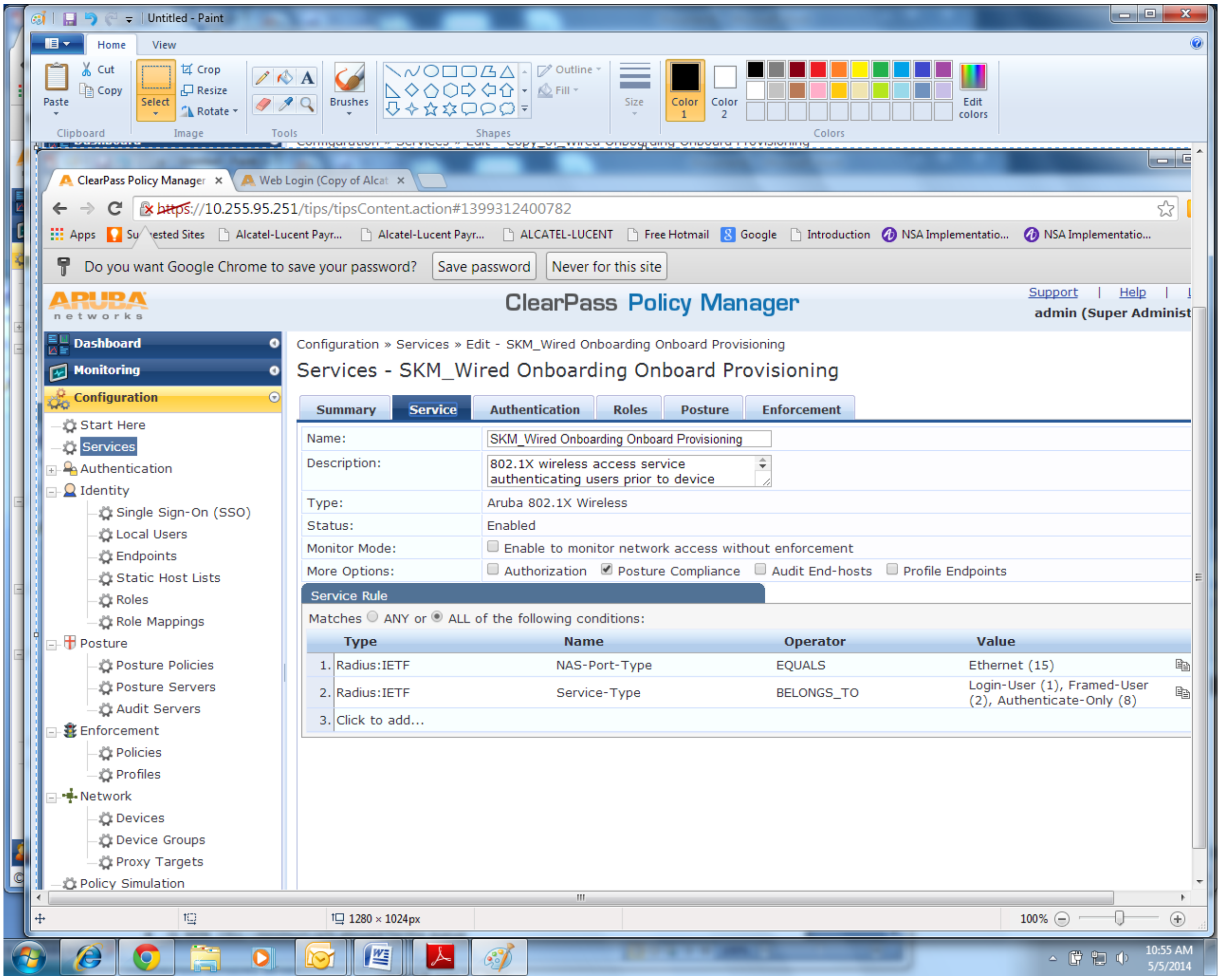
Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Enforcement Policy Rules:

	Conditions	Actions
1.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Posture:Applied Policy EQUALS SKM Wired Onboard Posture check)	[RADIUS] [Allow Access Profile], [RADIUS] Wired Onboarding Onboard Post-Provisioning
2.	(Authentication:Source EQUALS [Onboard Devices Repository]) AND (Posture:Applied Policy EQUALS SKM Wired Onboard Posture check)	[RADIUS] [Allow Access Profile], [RADIUS] Wired Onboarding Onboard Post-Provisioning
3.	(Authentication:Source NOT_EQUALS [Onboard Devices Repository])	[Allow Access Profile], Wired Onboarding Onboard Pre-Provisioning

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.



Configuration » Services » Edit - SKM_Wired Onboarding Onboard Provisioning

Services - SKM_Wired Onboarding Onboard Provisioning

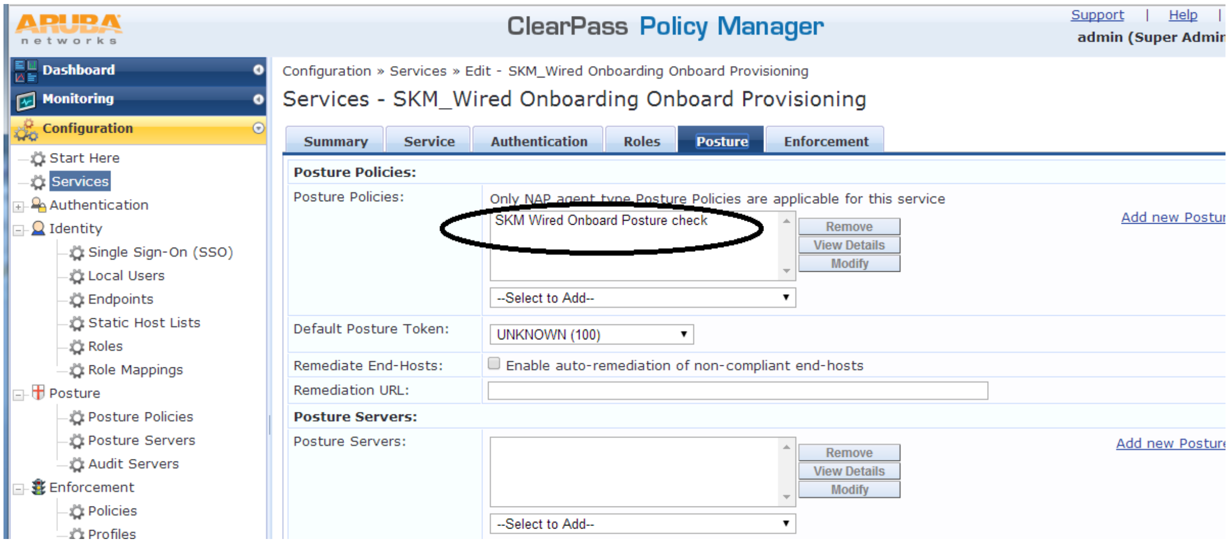
Name:	SKM_Wired Onboarding Onboard Provisioning
Description:	802.1X wireless access service authenticating users prior to device
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization ☑ Posture Compliance □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...			

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.



Configuration » Services » Edit - SKM_Wired Onboarding Onboard Provisioning

Services - SKM_Wired Onboarding Onboard Provisioning

Posture Policies:

Posture Policies: Only NAP agent type Posture Policies are applicable for this service

SKM Wired Onboard Posture check

--Select to Add--

Default Posture Token: UNKNOWN (100)

Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts

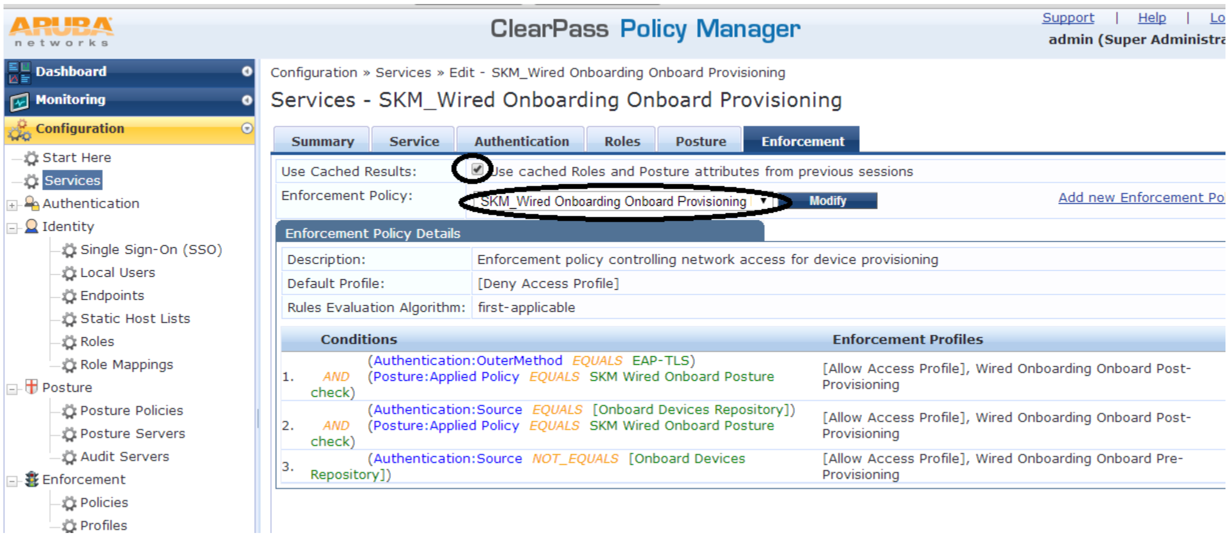
Remediation URL:

Posture Servers:

Posture Servers:

--Select to Add--

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



Configuration » Services » Edit - SKM_Wired Onboarding Onboard Provisioning

Services - SKM_Wired Onboarding Onboard Provisioning

Use Cached Results: ☑ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: SKM_Wired Onboarding Onboard Provisioning

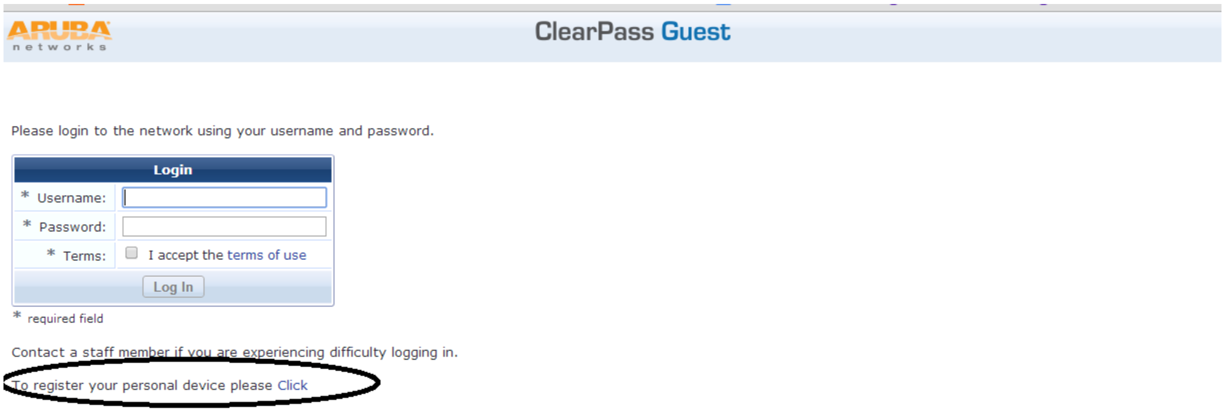
Enforcement Policy Details

Description:	Enforcement policy controlling network access for device provisioning
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Posture:Applied Policy EQUALS SKM Wired Onboard Posture check)	[Allow Access Profile], Wired Onboarding Onboard Post-Provisioning
2.	(Authentication:Source EQUALS [Onboard Devices Repository]) AND (Posture:Applied Policy EQUALS SKM Wired Onboard Posture check)	[Allow Access Profile], Wired Onboarding Onboard Post-Provisioning
3.	(Authentication:Source NOT_EQUALS [Onboard Devices Repository])	[Allow Access Profile], Wired Onboarding Onboard Pre-Provisioning

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-supplicant 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.



Please login to the network using your username and password.

Login	
* Username:	
* Password:	
* Terms:	□ I accept the terms of use

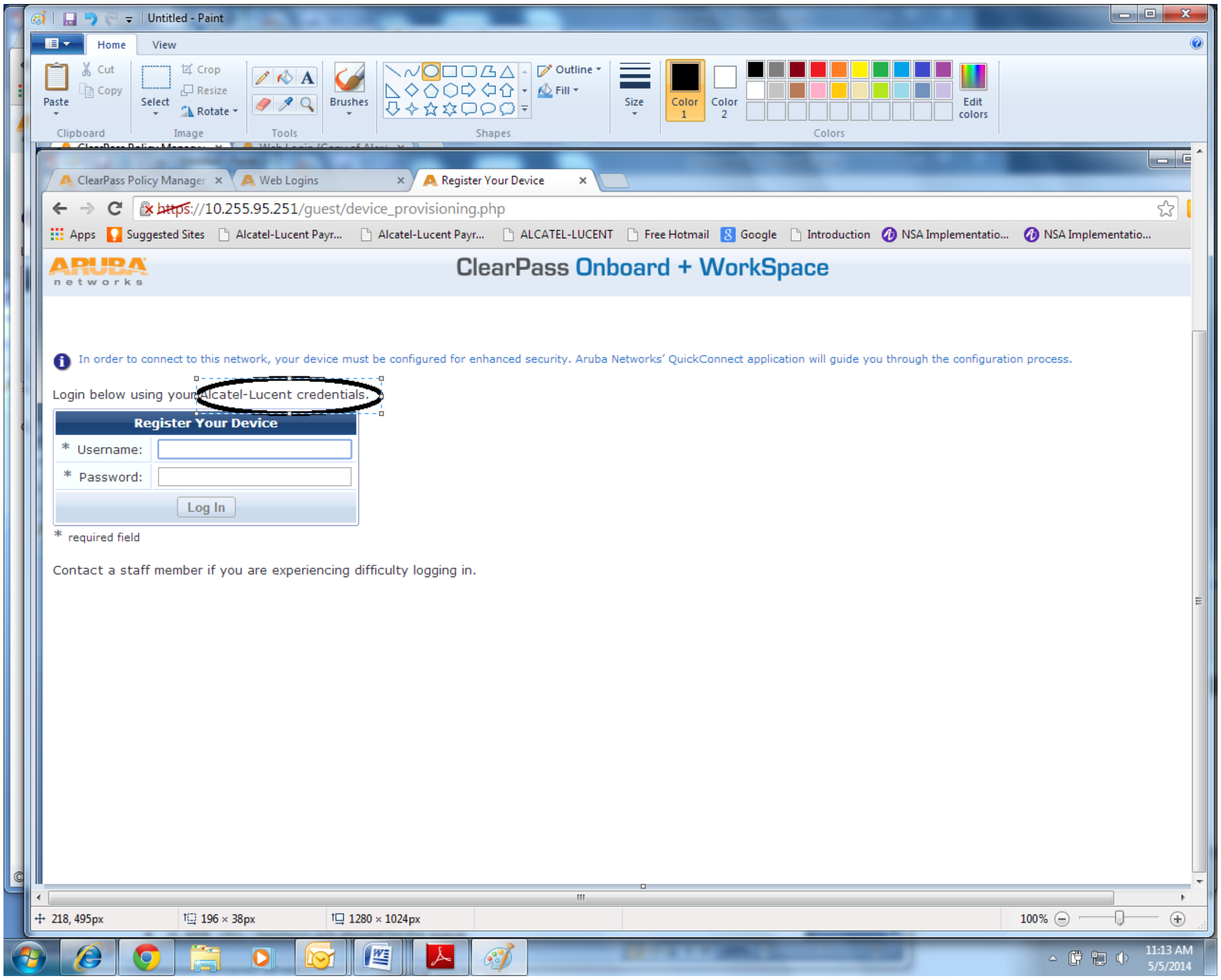
Log In

* required field

Contact a staff member if you are experiencing difficulty logging in.

To register your personal device please Click

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



In order to connect to this network, your device must be configured for enhanced security. Aruba Networks' QuickConnect application will guide you through the configuration process.

Login below using your Alcatel-Lucent credentials.

Register Your Device	
* Username:	
* Password:	

Log In

* required field

Contact a staff member if you are experiencing difficulty logging in.

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