

Access Guardian and BYOD in AOS Release 8.1.1

Configuration Guide through Use Cases

Copyright © 2014 by Alcatel-Lucent All rights reserved Alcatel-Lucent, 26801 West Agoura Road, Calabasas, CA 91301, USA +1(818) 880-3500

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

Contents

1	Ove	Overview4				
2	Intro	Introduction4				
3	Acce	Access Guardian in AOS 8.1.1				
	3.1	Acce	ess Guardian Benefits5			
	3.2	Acce	ess Guardian Terminology5			
	3.3	Acce	ess Guardian in AOS 8.1.1 vs Access Guardian in AOS 6.x8			
4	4 Access Guardian Use Cases					
	4.1	USE	CASE 1: Classification only (no authentication)			
	4.2	USE	CASE 2: Only Captive Portal authentication (no MAC/802.1x)			
	4.3	USE	CASE 3: MAC authentication and/or Captive Portal			
	4.4	USE	CASE 4a: Supplicant authentication only			
	4.5	USE	CASE 4b: Supplicant/non-supplicant device authentication with Captive Portal			
		20				
	4.6	USE	CASE 5/6: Supplicant IP phone/non-supplicant, Network Policy TLV - tagged			
	enable	enabled on switch (single device on port)23				
	4.7	USE	CASE 7: Multiple devices per UNP port. Supplicant IP phone connected to			
	switch with non-supplicant laptop connected to IP phone (multiple devices per port) \dots 25					
4.8 USE CASE 8/9: 802.1x bypass MAC auth (with b		USE	CASE 8/9: 802.1x bypass MAC auth (with blacklist/or whitelist)			
	4.9	USE	CASE 10: Post-authentication role assignment (QMR, Location- and Time-based			
	Roles) 30					
	4.9.	1	QMR			
	4.9.	2	Time policy			
	4.9.3		Location policy			
5	Access Guardian BYOD with CPPM Integration32					
	5.1	Use	Case Summary			
	5.2	Pre-	Requisite Switch Configuration			
	5.3	Pre-	Requisite CPPM Configuration			
	5.3.1		Configure the AOS switches on CPPM for which CPPM is acting as the \ensuremath{Policy}			
	Manager		RADIUS server			
	5.3.2		Update CPPM with latest Alcatel-Lucent Enterprise Dictionary			
	5.3.	3	Configure CPPM to use an external AD server as an authentication source 39			
	5.3.4		Configure Static Host List for IP phones/printer devices			
	5.4	AOS	switch and CPPM integration points			

	5.4.1	Edge-profile, access policy list and redirection URL handling	43
5	.5 BYC	DD USE CASE 1: Guest access	44
	5.5.1	Switch configuration	44
	5.5.2	CPPM configuration	45
5	.6 BYC	DD USE CASE 2: Unified authentication of IT-issued device	54
	5.6.1	Switch configuration	54
5.6.2		CPPM configuration	55
5	.7 BYC	DD USE CASE 3: Device onboarding with non-IT devices	62
	5.7.1	Switch configuration	62
	5.7.2	CPPM configuration	63
5	.8 BYC	DD USE CASE 4: Guest Access/BYOD Access with Posture Check	76
	5.8.1	Enabling BYOD USECASE 1 - Guest Access with Posture	76
	5.8.2	Enabling BYOD USECASE 3 - Onboard with Posture	82
6	Glossary		91

1 Overview

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

2 Introduction

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

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

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

3 Access Guardian in AOS 8.1.1

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

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

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

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

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

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

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

3.1 Access Guardian Benefits

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

3.2 Access Guardian Terminology

AAA Profile: AAA profiles define a specific AAA configuration that can be applied at the port level

(overrides the global AAA configuration) and are used to define the mapping of RADIUS servers

needed for 802.1x, MAC authentication and accounting. An AAA profile is a grouping of all the

properties required for authentication, authorization, accounting and can be applied on a per-port or

per-LAG basis. It includes the following configuration parameters:

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

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

The Captive Portal profile includes the following configuration parameters:

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

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

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

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

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

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

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

Edge-template: UNP edge-port templates define a specific port configuration to simplify and easily replicate the same configuration across multiple ports.

The edge-template can be assigned to a single port or a link-aggregation. The edge-template includes the following configuration parameters:

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

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

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

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

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

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

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

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

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

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







Figure 2. Access Guardian in AOS 8.1.1 Workflow

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

- 1. Triggering of the authentication/classification
 - a. In AOS 6.x, a port should first be identified as a mobile port and then 802.1x port to have the Access Guardian function enabled on the port. A port identified as mobile/802.1x port is automatically enabled for 802.1x authentication, MAC authentication and Group Mobility classification.
 - b. In AOS 8.x, a port should first be identified as a UNP edge-port. A port identified as a UNP edge-port has to be explicitly enabled for 802.1x authentication, MAC authentication and/or classification. This provides the user with the control to choose the process to be enabled on the port 802.1x or MAC authentication or both or classification only, etc.
- 2. Captive Portal authentication
 - a. In AOS 6.x implementation, the Captive Portal authentication is triggered from classification policies. The result of Captive Portal authentication is an "aaa User Network Profile" that may result in a new VLAN for the client. This requires the client to move from the temporary VLAN in which the Captive Portal was initiated to a new VLAN. This requires the DHCP address to be released and renewed.

- b. In AOS 8.x implementation, the Captive Portal authentication is triggered from a UNP edge-profile. Captive Portal enable/disable control is a property of the UNP edge-profile that is returned after the primary authentication and/or classification stage. The Captive Portal authentication does not result in a new UNP/VLAN. Instead the client remains in the same UNP/VLAN but can be associated with a post Captive Portal policy list that is different from the default policy list of the UNP profile. There is <u>no VLAN change</u> 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 edgeprofile 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

 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
 - $\circ~$ The traffic is redirected to the internal Captive Portal server. The Captive Portal server name is resolved using DNS.
 - \circ $\;$ Client is presented with internal Captive Portal login page
 - $_{\odot}$ $\,$ User enters the credentials, which are authenticated against the configured RADIUS $_{\rm server}$

- 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 edgeprofile 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 <u>not</u> 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 device-authentication 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

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 edgeprofile 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 device-authentication 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.

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 edgeprofile 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 corporatevoice

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

Ildp network-policy 1 application voice vlan 40 l2-priority 6

Ildp 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.
- \circ 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.

Create the required UNP edge-profiles
 unp edge-profile corporate
 unp edge-profile guest
 unp edge-profile corporate-voice

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

P 27 of 91

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

12. Enable MAC authentication/802.1x on the edge-template. Pass alternate UNP edgeprofile 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** corporatevoice

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

Ildp port 3/1/1-2 Ildpdu TX-AND-RX

Ildp network-policy 1 application voice vlan 40 l2-priority 6 Ildp 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. alloweap 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

Revision: 1.1, 08/01/2014

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

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

P 29 of 91

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 edgeprofile 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 <u>www.remediate.com</u>

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 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.

								· · · · · · · · · · · · · · · · · · ·
P Do you want Google Chrom	e to save you	r password?	Save password	Never for the	nis site			×
networks			Clear	Pass P	olicy Manag	er	<u>Su</u> a	pport <u>Help</u> <u>Logout</u> dmin (Super Administrator)
Dashboard	Configur	ation » Networ	k » Devices					
Monitoring	 Netwo 	ork Device	es					📌 Add
Configuration	0							Export All
🔅 Start Here								
🗘 Services	Filter:	Name	▼ c	ontains 🔻		+ Go Clear	Filter	Show 10 🔻 records
Authentication	#	🕘 Name 🛦			IP or Subnet Add	ress Descriptio	n	
J 😡 Identity	1.	10.255.22	1.232		10.255.221.232	10.255.221.2	32	
T Posture	2.	10.255.99	.211		10.255.99.211	10.255.99.21	.1	
Network	3.	10.255.99	.212		10.255.99.212			
- Devices	4.	ACCESS-	5860-1		10.255.99.209			
Device Groups	5.	ACCESS-6	6860-2		10.255.99.210	ACCESS-686	0-2	
🛱 Proxy Targets	6.	DC-CORE-	1		10.255.99.26	OS 10K DC-C	ORE-1	
🗘 Policy Simulation	7.	OAW-455	D		10.255.95.247	OAW-4550 V	/ireless Controller	
🛱 Profile Settings	s	howing 1-7 of	7					Copy Export Delete
	Dis.							

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.

ARUBA		ClearPass F	olicy Ma	ana	ager	Support Help Logout admin (Super Administrator)
Dashboard	Add Device					•
Monitoring						Add
Configuration	Device SNMP Read S	ettings SNMP Write Sett	ings CLI S	Setti	ngs	Import Export All
- 🛱 Start Here	Name:	OS6860				
- 🛱 Services	IP or Subnet Address:	192.168.1.10	(e.g., 192.	168	.1.10 or 192.168.1.1/24)	Show 10 v records
🖅 🗣 Authentication 🐨 🧕 Identity	Description:	Alcatel Lucent OS6860	2			
🛞 🖶 Posture	RADIUS Shared Secret:		Verify	y:		
🖅 💐 Enforcement	TACACS+ Shared Secret:		Verify	y:		
🖃 📫 Network	Vendor Name:	Alcatel-Lucent-Enterpris				
- 🗘 Devices	Enable RADIUS CoA:	RADIUS COA PO	ort: 3799			
Device Groups	Attributes					
Policy Simulation	Attribute		Value			il ller
- 🛱 Profile Settings	1. Click to add					Copy Export Delete
					Add Canc	el
	-					
Administration	0					
© Copyright 2014 Aruba Netwo	orks. All rights reserved.	Apr 28, 2014 11:11:54	PDT		ClearPass Policy Manage	er 6.3.1.62009 on CP-SW-EVAL platfor

The device is added.

APURA networks			Cle	arPass	Support Help Logout admin (Super Administrator)			
Dashboard	Configu	uratio	on » Network » Devices					
Monitoring	 Netw 	vorl	< Devices					Add 🚽
Configuration	0							Export All
🖧 Start Here								
- 🛱 Services	Filter:	Nar	ne 🔻	contains 🔻		+	Go Clear Filter	Show 10 🔻 records
🕀 🐴 Authentication	#		Name 🛦		IP or Subnet Add	dress	Description	
🗄 🧕 Identity	1.		10.255.221.232		10.255.221.232		10.255.221.232	
💮 📅 Posture	2.		10.255.99.211		10.255.99.211		10.255.99.211	
	3.		10.255.99.212		10.255.99.212			
Devices	4.		ACCESS-6860-1		10.255.99.209			
Device Groups	5.		ACCESS-6860-2		10.255.99.210		ACCESS-6860-2	
🛱 Proxy Targets	6.		DC-CORE-1		10.255.99.26		OS 10K DC-CORE-1	
- 🛱 Policy Simulation	7.		OAW-4550		10.255.95.247		OAW-4550 Wireless Controller	
- 🎝 Profile Settings	8.		OS6860		192.168.1.10		Alcatel Lucent OS6860	
	i i	Shov	ving 1-8 of 8					Copy Export Delete
Administration	0							
© Copyright 2014 Aruba Networks	. All rights r	reser	ved. Apr 28	, 2014 11:17	:08 PDT		ClearPass Policy Manager 6.3.1.62	009 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.

networks		ClearPass	Policy Manage	er	Support Help Logout admin (Super Administrator)
Dashboard 0	Adminis	tration » Dictionaries » RADIUS			
Monitoring 0	RADI	US Dictionaries			🐣 Import
Configuration 0					
Administration 📀	Filter:	Vendor Name Contains		🛨 Go Clear Filter	Show 50 🔻 records
- A ClearPass Portal	#	Vendor Name 🛆	Vendor ID	Vendor Prefix	Enabled
🖫 육 Users and Privileges	1.	3com	43	3com	false
🕀 🖉 Server Manager	2.	3GPP	10415	3GPP	false
庄 🕼 External Servers	з.	Acc	5	Acc	false
🗄 📒 Certificates	4.	Acme	9148	Acme	false
🖃 🛄 Dictionaries	5.	ADSL-Forum	3561	ADSL-Forum	false
RADIUS	6.	Aerohive	26928	Aerohive	false
- JP Posture	7.	Airespace	14179	Airespace	false
ACACS+ Services	8.	Alcatel	3041	Alcatel	false
Attributor	C I	Alcatel-Lucent-Enterprise	800	Alcatel-Lucent-Ente	erprise true
Applications	10.	Alcatel-Lucent-Service-Router	6527	Alcatel-Lucent-Serv	vice-Router false
Context Server Action	11.	Alteon	1872	Alteon	false
🗐 🔦 Agents and Software Updat *	12.	Alvarion	12394	Alvarion	false
© Copyright 2014 Aruba Networks. A	ul rights i	Apr 28, 2014 12:40	5:13 PDT	ClearPass Policy Manager 6.	5100 3.1.62009 on CP-SW-EVAL platform
Guidelines_&_Applidocx					Show all downloads

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

ARURA		ClearPas	s Policy	Manager		<u>Support</u> admin (Su	<u>Help</u> <u>Logou</u> uper Administrato
Dashboard O Monitoring O	Advision to a Distinguistic Strategy RADIUS Attributes	ice BADUIC	_	_	8		🐣 Import
Configuration 0	Vendor Name:	Alcatel-Lucer	It-Enterprise (8	00)			
Administration 📀	F Alcatel-Access	-Policy-List	100	String	in out	Show	w 50 🔻 records
ClearPass Portal	12. Alcatel-Access	-Priv	16	Unsigned32	in out		Enabled
Users and Privileges	13. Alcatel-Asa-Ac	cess	9	String	in out		false
F P Server Manager	14. Alcatel-Auth-G	roup	1	Unsigned32	in out		false
🖅 🕼 External Servers	15. Alcatel-Auth-G	roup-Protocol	8	String	in out		false
🖅 💾 Certificates	16. Alcatel-Client-I	P-Addr	4	IPv4Address	in out		false
🖃 🛄 Dictionaries	17. Alcatel-Group-D	Desc	5	String	in out	-	false
- Ja RADIUS	18. Alcatel-Port-De	sc	6	String	in out	-	false
- 🌽 Posture	19. Alcatel-Profil-N	umb	7	Unsigned32	in out		false
- PTACACS+ Services	Alcatel-Redirec	tion-Status	102	String	in out		false
- Je Fingerprints	Alcatel-Redirec	tion-URL	101	String	in out	Enterprise	true
- Attributes		· · · ·				Service-Router	false
- Applications				Di	sable Export Close	bernee notes	false
Context Server Action	10911 12100011111		1200		221059010101		false
Adents and software obdat	12 ADC		210	18	ADC		falco
© Copyright 2014 Aruba Networks. A	All rights reserved.	Apr 28, 2014 12	52:21 PDT		ClearPass Policy Mana	ger <u>6.3.1.62009</u> on	CP-SW-EVAL platfo
Guidelines_&_Applidocx						4	Show all downloads

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.

API PA networks			Cle	arPass	Policy Manag	er		Support Help Logour admin (Super Administrator
Dashboard O	Configu	iratio	n » Authentication » Sou	rces				\sim
Monitoring O	Auth	ent	tication Sources					🔶 🛉 Add
Configuration 💿								Export All
🋱 Start Here								
- 🛱 Services	Filter:	Nar	ne 🔻	contains •		+	Go Clear Filter	Show 20 🔻 records
Authentication	#		Name 🛦		Туре		Description	
A Methods Sources	1.		[Admin User Repository]		Local SQL DB		Authenticate users against f database	Policy Manager admin user
Q Identity	2.		[Blacklist User Repositor	y]	Local SQL DB		Blacklist database with user bandwidth or session related	s who have exceeded I limits
- 🛱 Single Sign-On (SSO) - 🛱 Local Users	з.		[Endpoints Repository]		Local SQL DB		Authenticate endpoints agai database	nst Policy Manager local
- C Endpoints	4.		[Guest Device Repositor	y]	Local SQL DB		Authenticate guest devices database	against Policy Manager local
- 🛱 Static Host Lists	5.		[Guest User Repository]		Local SQL DB		Authenticate guest users ag database	ainst Policy Manager local
Role Mappings	6.		[Insight Repository]		Local SQL DB		Insight database with session devices	n information for users and
🕞 📅 Posture	7.		IXIA MACs		Static Host List		IXIA MACs	
Enforcement	8.		[Local User Repository]		Local SQL DB		Authenticate users against database	Policy Manager local user
Protection Simulation	9.		MAC Authentication List		Static Host List		MAC Authentication List	
The Profile Settings	10.		mac caching MAC-Gues	t-Check	Generic SQL DB			
	11.		[Onboard Devices Repos	sitory]	Local SQL DB		Authenticate Onboard devic local database	es against Policy Manager
	12.		SQA Active Directory Se	ervice	Active Directory		SQA Active Directory Servic	e

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

APLPA networks	ClearPass Policy Manager admin (Super Admin								
Dashboard O Monitoring O Configuration O	Configuration » Authentication Authentication Sou	on » Sources » Add - SQA Active Directory Service Irces - SQA Active Directory Service Primary Attributes							
	Name: Description:	SQA Active Directory Service SQA Active Directory Service							
	Type: Use for Authorization: Authorization Sources:	Active Directory Enable to use this Authentication Source to also fetch role mapping attri Remove View Details - Select	butes						
	Server Timeout: Cache Timeout: Backup Servers Priority:	10 seconds 36000 seconds Move Up Move Up Move Up Move Down Add Backup Remove							

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

APLPA networks		ClearPass Policy Manager	Support Help Logout admin (Super Administrator)					
Dashboard O	Configuration » Authenticati	on » Sources » Add - SQA Active Directory Service						
Monitoring O	Authentication Sou	rces - SOA Active Directory Service						
Configuration O	Summary General	Primary Attributes						
— 🛱 Start Here	Connection Details							
- 🛱 Services	Hostname:	dc001.sqa.com						
Authentication	Connection Security:	None						
	Port: 389 (For secure connection, use 636)							
- Q Identity	Verify Server Certificate:	Enable to verify Server Certificate for secure connection	on					
- C Single Sign-On (SSO)	Bind DN: (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)							
Endpoints	Bind Password:							
Static Host Lists	NetBIOS Domain Name:	SQA						
🛱 Roles	Base DN:	dc=sqa,dc=com	Search Base Dn					
Role Mappings	Search Scope:	SubTree Search 🔻						
Posture	LDAP Referrals:	Follow referrals						
Enforcement	Bind User:	Allow bind using user password						
	User Certificate :	userCertificate						
- Crofile Settings								

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.

networks	C	Support admin (Sup	Help !	Logo trate		
Dashboard 0	Configuration » Authentication » 9	Sources » Add - SQA Active Director	y Service			
Monitoring 0	Authentication Source	s - SOA Active Director	v Service			
Configuration O	Summary General Pri	imary Attributes				
- 🛱 Start Here	Specify filter queries used to fet	sh authentication and authorization	attributes			
— 🛱 Services	Filter Name	Attribute Name	Alias Name	Enabled As	Ť	t
Authentication	1. Authentication	dn	UserDN	-	Dr.	Û
- i Methods	Contraction of the Science of the Sc	department	Department	-		
		title	Title	-		
Single Sign-On (SSO)		company	company			
Local Users		memberOf	memberOf			
Endpoints		telephoneNumber	Phone	14		
Static Host Lists		mail	Email	6		
- 🛱 Roles		displayName	Name	12		
🛱 Role Mappings		accountExpires	Account Expires	15		
🖅 📅 Posture	2. Group	cn	Groups	5	1	Ť
🕀 🖀 Enforcement	3. Machine	dNSHostName	HostName		1	Ť
+ •••• Network		operatingSystem	OperatingSystem	÷		
- Q Policy Simulation		operatingSystemServicePack	OSServicePack			
- U Proille Settings	4. Onboard Device Owner	memberOf	Onboard memberOf	-	D.	Ť
	5. Onboard Device Owner Grou	ιρ cn	Onboard Groups	12	2	T

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.

networks	Clea	rPass Policy N	Nanager	admi	in (Super Administrato
🛓 Dashboard 🕢 Monitoring	 Configuration » Identity » Static Host Lists Static Host Lists 				Add
Configuration					Export All
Authentication	Filter: Name Contains	Format	Go Clear Filter Type MACAddress	Description	Show 10 record
- ☆ Sources - ♀ Identity - ☆ Single Sign-On (SSO)	2. IXIA MACS Showing 1-2 of 2	List	MACAddress	IXIA MACs	Export Delete
- 🛱 Local Users - 🛱 Endpoints - 🏹 Static Host Lists					

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.

ARIDA networks			Cle	arPass Policy Manag	ger	Support Help Logout admin (Super Administrator)		
Dashboard	• Configuratio	on » Iden	Edit Static Host List		0			
Monitoring	Static H	lost Li					Tana Add	
Configuration	0		Name:	Alcatel-Lucent IP touch	J		Export All	
- 🛱 Start Here	*		Description:	Alcatel-Lucent IP touch				
- 🛱 Services	Filter: Nar	me	Host Format:	Subset	Iter		Show 10 Trecords	
Authentication	# 🗉	Name	noseronide	Regular Expression Ist		Description		
- i Methods	1. 🗖	Alcate	Host Type	IP Address		Alcatel-Lucent IP touch	1	
- It Sources	2. 🔲	IP Pho	nose nype	MAC Address		IP Phone list		
Single Sign-On (SSO)	3. 🗆	IXIA I	List:	00:80:9f:6b:e4:19		IXIA MACs		
Construction of the set of t	Show	wing 1-3		00:80:9f:6b:e7:9d	Remove Host		Export Delete	
🗄 📅 Posture		_						
🖃 🐉 Enforcement		_						
2 Policies			Save Cancel					

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

networks		ClearPa	iss Policy Manager		Support Help LogX admin (Super Administrat
Dashboard Monitoring Configuration	 Configuratio Authent 	n » Authentication » Sources cication Sources			Add
- ☆ Start Here - ☆ Services - ♣ Authentication	Filter: Nan	ne ▼ [contains ▼]	Type	Go Clear Filter Description	Show 20 • records
- 🛱 Methods	1.	[Admin User Repository]	Local SQL DB	Authenticate users agains	t Policy Manager admin user database or
Q Identity	2. 🔲	[Blacklist User Repository]	Local SQL DB	Blacklist database with us session related limits	ers who have exceeded bandwidth or
🖧 Single Sign-On (SSO)	3. 🗐	[Endpoints Repository]	Local SQL DB	Authenticate endpoints ag	gainst Policy Manager local database
- 🛱 Local Users	4. 🗐	[Guest Device Repository]	Local SQL DB	Authenticate guest device	es against Policy Manager local database
- 🛱 Endpoints	5. 🗆	[Guest User Repository]	Local SQL DB	Authenticate guest users	against Policy Manager local database
- & Services	Filter: Nan	ne 🔹 🔽	· · · ·	Go Clear Filter	Show 20 Trecords

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

APUPA networks		ClearPass Policy Manager					
Dashboard	Configuration » Authentica	tion » Sources » Add					
Monitoring	 Authentication So 	ources					
🖧 Configuration	General Static Hos	t Lists Summary					
—🛱 Start Here	Name:	IP-phone list					
- 🎝 Services - 🔒 Authentication	Description:	IP-phone list					
- 🛱 Methods - 🛱 Sources	Type:	Static Host List	•				
- Q Identity	Use for Authorization:	Enable to use this Auther	tication Source to also fetch role mapping attributes				
Gingle Sign-On (SSO) Gold Users Gold U	Authorization Sources:		View Details				

5. Select the IP phone list created

networks		ClearPass Policy Man	nager	Support Help Logou admin (Super Administrator
Dashboard O	Configuration » Authentication »	Sources » Add		
Monitoring O	Authentication Source	es		
🖧 Configuration 📀	General Static Host Lists	Summary		
→ Start Here → Services → Authentication → Methods → Gources ↓ Cocal Users → Endpoints → Static Host Lists → Roles → Roles → Role Mappings	MAC Address Host Lists:	Select	Remove View Details Modify	Add new Static Host List

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
- 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 edgeports

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.

ARURA	ClearPass Policy Manager						
Dashboard							
All Requests Trend all Policy Manager requests	Status Host Name alu-cppm63.sqa.com (10.255.95.251)	Zone default	Server Role Last Replication Publisher -	Status OK			
Health Status Trend Healthy and Unhealthy requests Authentication Status Trend Successful and Failed authentications			• Applications	٥ <u>۲</u>			
Latest Authentications Latest Authentications	Drag and Drop Items Here		Advanced Analytics, In-depth Reportin	ng, Compliance & Regulation			
Device Category Device Categories	Access Tracker		All Requests	0			
Device Family Monitoring	Server Manager ClearPass Guest		sk				
Configuration	Clean ass Onboard + WorkSpace		• 0k - 24. Apr 25. Apr 28.	Apr 30. Apr			

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

ARUBA networks			Support Help Log admin (IT Administrato					
🕵 Guest	Home » Guest » List Acco	Home » Guest » List Accounts						
- 🛶 Start Here - 🛃 Active Sessions - 🧟 Create Account - 🛃 Create Device - 💕 Create Multiple	Manage Guest A The following table shows Quick Help	the guest accounds	ints that have Create	been created. Click an a	ccount to modify it. More Options			
- State Accounts	Filter:	Polo	State	Activation	Expiration			
- mport Accounts	43303068	[Guest]	Active	2014-03-19 11:00	No expiry			
List Accounts	guest001	[Guest]	Active	2014-01-30 15:06	2015-01-30 15:06			
- 🚮 List Devices	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.

APLEA networks		ClearPass Guest	Support Help Logo admin (IT Administrator
🛐 Guest	0	· ·	
— 🛶 Start Here	New guest account bei	ing created by admin .	
- 🔐 Active Sessions		New Guest Account	
- 🧟 Create Account - 🛃 Create Device	* Guest's Name:	test Name of the guest.	
- 🚰 Create Multiple - 🧕 Edit Accounts	* Company Name:	test company Company name of the guest.	
Export Accounts Tripport Accounts	* Email Address:	test@testcompany.com The guest's email address. This will become their username to log into the network.	
- SList Accounts	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".



- 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.

Advertising		Web Login Editor			
Authentication Content Manager	* Name:	test guest login Enter a name for this web login page.			
Digital Passes Email Receipt	Page Name:	test_guest_login Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".			
elds yrms & Views uest Manager	Description:	test guest login Comments or descriptive text about the web login.			
lotspot Manager	* Vendor Settings:	Alcatel-Lucent Select a presented group of settings suitable for standard network configurations.			
Manage Customer Info	Login Method:	Sever-initiated — Change of authorization (RFC 3576) sent to controller Select how the user's network form will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.			
- 🛃 Manage Invoice - 🛐 Manage Plans - 🍪 Manage Transaction Proce	Security Hash:	Do not check – login will always be permitted Select the level of checking to appy to UKL 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.			
Self Provisioning	L ogin Form Options for specifying the	behaviour and content of the login form.			
ministration O		Credentials – Require a username and password Select the authentication requirement.			

- 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.

APURA networks		Support Help Logo admin (IT Administrator	
🗣 Guest	• Login Form Options for specifying the	behaviour and content of the login form.	
Configuration Configuration Start Here	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 the terms or a Loo In button. A pre-existing account is required.	
 	Prevent CNA:	Access Code and Anonymous require the account to have the Username Authentication field set. 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 pottal is implemented.	
🖭 🎁 Digital Passes — 💭 Email Receipt	Custom Form:	Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.	
- 🌇 Fields - 🛅 Forms & Views	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.	
- 🕵 Guest Manager	* Pre-Auth Check:	INone — no extra checks will be made	
Hotspot Manager	Terms:	Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.	
Manage Customer Info	Default Destination Options for controlling the		

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.

Home View					0
Paste Cut Seject Crop	Image: Weight of the second	 △ · Ø Outline * ↔ ▲ Fill * ○ ▼ 	Size	Edit colors	
Clipboard Image Tools	Sha	les	Co	lors	
C networks					admin (Super Administri
Dashboard O	Configuration » Enforcement	t » Profiles » Edit E	inforcement Profile - UNP-restricte	ad Radius - FilterID - DNS URL - Login	
Ap 🕢 Monitoring 🛛 🔍 🛛	Enforcement Profi	es - UNP-res	stricted Radius - Filter	ID - DNS URL - Login	
Configuration 📀	Summary Profile	Attributes			
- Ö Sources	Profile:	Thereades			
et 🔄 🚨 Identity	Name:	UNP-restricted	Radius - FilterID - DNS URL - Logi	n	
Single Sign-On (SSO)	Description:	UNP-restricted	Radius - FilterID - URL - Login		
- 🛱 Local Users	Type:	RADIUS	-		11
- 🛱 Endpoints	Action:	Accept			
Ci Static Host Lists	Device Group List:	-			
- 🛱 Roles	Attributes:				
I Role Mappings	Туре		Name	Value	
	1. Radius:IETF		Filter-Id	= UNP-restricted	
El Senforcement	2. Radius: Alcatel-Lucer	t-Enterprise	Alcatel-Redirection-URL	_ http://10.242.254.101/guest/test_gues	_login.php?&mac=%
- O Policies				{Connection:Client-Mac-Address-Color	0
- Promes					0
Devices					
Device Groups					
Proxy Targets					
EPolicy Simulation					
- O Profile Settings	Kack to Enforcement	t Profiles			Copy Save Can
A Administration					
+ 10 447 × 68px	1 1366 × 768px				100% 🕞 👘 🗇
		K			△ (* * (*)) 2:57 PM 5/1/2014

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.

🔼 ClearPass Policy Manager 🗙 🛕 Web L	ogin (new) ×	Supervised into	A deleases of the	Proc. Statelly, 1	Branch A. Latter	
← → C 🕼 https://10.255.95.25	1/tips/tipsContent.action#139	8981569273				☆ 🕺 🔳
🗰 Apps 🚺 Su rested Sites 🕒 Alcatel-Luc	ent Payr 📋 Alcatel-Lucent Payr	ALCATEL-LUC	ENT 🕒 Free Hotmail <u>8</u> Google 🕒 Ir	ntroduction 🥢	NSA Implementatio 🕢 NSA Implemen	ntatio 🗋 RealPlayer »
P Do you want Google Chrome to s	save your password? Save pa	ssword Never	for this site			×
networks		Cle	arPass Policy Manag	ger		Support Help Logout admin (Super Administrator)
Dashboard	Configuration » Enforceme	nt » Profiles » <mark>E</mark> di	t Enforcement Profile - UNP-guest C	CoA - FilterID	- PolicyList	
Monitoring (Enforcement Prof	les - UNP-o	juest CoA - FilterID - Po	olicyList		
Configuration	Summary Profile	Attributes				
- 🗘 Start Here	Profile:					
- 🛱 Services	Name:	UNP-guest C	oA - FilterID - PolicyList			
🖃 육 Authentication	Description:	UNP-quest C	oA - FilterID			
- 🎝 Methods	Type:	RADIUS COA				
- 🛱 Sources	Action:	CoA				
🖃 🚨 Identity	Device Group List:					
_O Single Sign-On (SSO)	Ashibuta as					
- 🛱 Local Users	Attributes:					
- C Endpoints	Type		Name		value	
Static Host Lists	1. Radius:IETF		Filter-Id	-	UNP-guest	
- Q Roles	2. Radius:IETF		Calling-Station-Id	=	%{Radius:IETF:Calling-Station-:	id}
- 💭 Role Mappings	3. Radius: Alcatel-Luce	nt-Enterprise	Alcatel-Access-Policy-List		guest-role	
🗄 🖶 Posture						
Enforcement						
- Q Policies						
- Q Profiles						
- Q Devices	Back to Enforcement	nt Profiles				Copy Save Cancel
🚰 Administration 🛛 🔹	o -					
Copyright 2014 Aruba Networks. All	rights reserved.	May 01, 2	014 14:31:32 PDT		ClearPass Policy Manager 6.	3.1.62009 on CP-SW-EVAL platform
	0 🞯 🤤 🔅	• 🔼 6	1 6 6			▲ 🛱 🔁 Φ) 3:00 PM 5/1/2014

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

🔨 ClearPass Policy Manager 🛛 🔺 🛕 Web Login (r	new) ×	A	-	-	C. Santas, Santa	a a second	
← → C & https://10.255.95.251/tip	s/tipsContent.ac	tion#139898593	3110				☆ 🕺 🔳
🗰 Apps 🚺 Su 🔤 ested Sites 📄 Alcatel-Lucent Pa	ayr 🗋 Alcatel-Lu	icent Payr 🗋 ALi	CATEL-LUCENT	ree Hotmail 🔣 Goo	gle 🗋 Introduction	🕢 NSA Implementatio	🕖 NSA Implementatio 🕒 RealPlayer »
P Do you want Google Chrome to save y	your password?	Save password	Never for this sit	e			×
APUPA networks			ClearPas	s Policy N	/lanager		<u>Support</u> <u>Help</u> <u>Logout</u> admin (Super Administrator)
Dashboard O C	Configuration » Er	nforcement » Polic	ies » Add				
Monitoring O	Enforcemen	t Policies					
Sconfiguration 📀	Enforcement	Rules Sur	nmary				
🖧 Start Here 🔨	Name:	ALU	Wired MAC Auth Pol	icv			
- 🛱 Services	Description:						
- 🛱 Methods	Enforcement Ty	pe: ® RA	DIUS O TACACS+	WEBAUTH (SN	IMP/Agent/CLI/Co	A) 🔍 Application	
🖓 Sources	Default Profile:	De	v Access Profile]	View Det	ails Modify		Add new Enforcement Profile
- Single Sign-On (SSO) - C Local Users - C Endpoints - C Static Host Lists - C Roles - C Roles							
The Posture							
Senforcement Control Senforcement Control Senforcement Control Senforcement Se							
Network	-	1					
- Devices	S Back to En	orcement Polici	<u>es</u>				Next > Save Cancel
Administration 0							
© Copyright 2014 Aruba Networks. All rights	reserved.	M	ay 01, 2014 15:43	:56 PDT		ClearPass P	olicy Manager 6.3.1.62009 on CP-SW-EVAL platform
			- 🧭 🛽	3 🖉	2		▲ 📴 👘 👘 4:12 PM 5/1/2014

- 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

🖊 ClearPass Policy Manager 🗙 🛕 Web Login	n (new) ×	10. Applications frames, in configuration and \$2000 in	
← → C (bttps://10.255.95.251/t	ips/tipsContent.action#		☆ 🕺 ≡
🗰 Apps 🚺 Su rested Sites 🕒 Alcatel-Lucent	Payr 🗋 Alcatel-Lucent Payr 🗋	ALCATEL-LUCENT 🗋 Free Hotmail <u>8</u> Google 🗅 Intro	oduction 🧿 NSA Implementatio 🗿 NSA Implementatio 🕒 RealPlayer 🛛 🔹 👋
P Do you want Google Chrome to save	e your password? Save passwor	rd Never for this site	×
networks		ClearPass Policy Manage	EP Support Help Logout admin (Super Administrator)
Dashboard 0	Configuration » Enforcement » P	olicies » Add	
Monitoring O	Enforcement Policies		
Configuration O	Enforcement Rules S	Summary	
- 🗘 Start Here	Rules Evaluation Algorithm: Enforcement Policy Rules:	Select first match 🔍 Select all matches	
Authentication	Conditions		Actions
- Q Methods	1. (Tips:Role EQUALS	[Guest])	[RADIUS_CoA] UNP-guest CoA - FilterID - ACL - guest-role
Q Sources	2. (Authentication:Sou	urce EQUALS IP Phone list)	[RADIUS_CoA] UNP-voice CoA - FilterID
Grade Sign On (SCO)	3. (Authentication:Ma	cAuth EQUALS UnknownClient)	[RADIUS] UNP-restricted Radius - FilterID - URL - Login
- 🛱 Local Users	Add Rule	Move Up Move Down	Edit Rule Remove Rule
- 🛱 Endpoints			
- 🛱 Static Host Lists			
- 🛱 Roles			
- 🎝 Role Mappings			
H 🕂 Posture			
Enforcement			
- Olicies			
Q Profiles			
- W Devices	Seck to Enforcement Pol	icies	Next > Save Cancel
👫 Administration 🛛 🗿			
© Copyright 2014 Aruba Networks. All righ	nts reserved.	May 01, 2014 15:55:15 PDT	ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform
			▲ 🛱 🗂 🕩 4:24 PM 5/1/2014

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

- 0 X A ClearPass Policy Manager × 🗛 Web Login (new) × ← → C 🕼 https://10.255.95.251/tips/tipsContent.action#1398986943534 값 🕺 🔳 🔢 Apps 🚺 Sy 🔶 ested Sites 🖒 Alcatel-Lucent Payr... 🖒 Alcatel-Lucent Payr... 🖒 ALCATEL-LUCENT 🖒 Free Hotmail 找 Google 🖒 Introduction 🤣 NSA Implementatio... RealPlayer 📍 Do you want Google Chrome to save your password? Save password 🛛 Never for this site Support | Help | Logout APUPA networks **ClearPass Policy Manager** admin (Super Administrator) Dashboard 0 Configuration » Enforcement » Policies » Edit - Wired Captive Portal Policy - NO Posture Enforcement Policies - Wired Captive Portal Policy - NO Posture Monitoring 0 Configuration Summary Enforcen ent Rules 🛱 Start Here Name Wired Captive Portal Policy - NO Posture Services Description: Wired Captive Portal Policy Authentication 🛱 Methods Enforcement Type: WEBAUTH Sources Default Profile: Add new Enforcement Profile [Post Authentication] [Update
 View Details Q Identity Select to Add-Single Sign-On (SSO) -Select to Add-[HTTP] [Handle AirGroup Time Sharing] [Post Authentication] Update Username to Endpoint [Post Authentication] [Update Endpoint Known] [Dect Authentication] [Update Endpoint Linformed] C Local Users C Endpoints Post Authentication || Updata Endowsk Ukkowyn|
 Post Authentication || mac caching Guest Bodwidth Limit
 Post Authentication || mac caching Guest Do Expire
 Post Authentication || mac caching Guest Do Expire
 Post Authentication || mac caching Guest MAC Caching
 RADUS Coal Coa + Net#Attoncek URL
 RADUS_Caal Coa UNP-restricted - HealthCheck URL
 RADUS_Caal Coa UNP-restricted - Readhtication URL and FilterID
 RADUS_Caal UNP-mentyree Coa - FilterID Static Host Lists C Roles 🛱 Role Mappings 🕫 🖶 Posture S Enforcement Delicies 🛱 Profiles + Network [RADIUS_COA] UNP-employee CoA - FilterID [RADIUS_COA] UNP-employee CoA - FilterID [RADIUS_COA] UNP-guest CoA - FilterID - ACL [RADIUS_COA] UNP-guest COA - FilterID - ACL Devices Back to Enforcement P Copy Save Cancel Administration 0 RADIUS CoAJ UNP-guest CoA - FilterID - ACL - guest-role May 01, 2014 16:01:11 PDT All right ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platfo oyright 2014 Aruba N ▲ 🛱 🐑 🚯 4:29 PM 5/1/2014 P 人 61
- b. Follow the instructions for new enforcement policy creation

c. Set attributes tab with the following rules:

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

A ClearPass Policy Manager × A Web Login	(new) ×	and another frame, is such as the party	to Married	
← → C & https://10.255.95.251/tip	ps/tipsContent.action#139898694353	34		☆ 🐹 🔳
🗰 Apps 🚺 Su Aested Sites 🕒 Alcatel-Lucent P	Payr 🗋 Alcatel-Lucent Payr 🗋 ALCATE	L-LUCENT 🕒 Free Hotmail 🙎 Google 🕒	Introduction 🕢 NSA Implementatio 🥢	NSA Implementatio 🗋 RealPlayer »
P Do you want Google Chrome to save	your password? Save password N	lever for this site		×
networks	(ClearPass Policy Mana	ager	<u>Support</u> <u>Help</u> <u>Logout</u> admin (Super Administrator)
Dashboard O	Configuration » Enforcement » Policies	» Edit - Wired Captive Portal Policy - N	IO Posture	
Monitoring O	Enforcement Policies - Wi	red Captive Portal Policy	- NO Posture	
Configuration 📀	Commence Enforcement David			
—☆ Start Here —☆ Services —☆ Authentication	Rules Evaluation Algorithm: Select Enforcement Policy Rules:	t first match Select all matches		
- 🗘 Methods	Conditions		Actions	
- 🛱 Sources	1. (Tips:Role EQUALS [Gues	st])	UNP-guest CoA - FilterID	
Generation G				
- 🛱 Devices 🖕	Stack to Enforcement Policies			Copy Save Cancel
🐉 Administration 🛛 🛛 🛛 🛛 💿				N
Copyright 2014 Aruba Networks. All right	ts reserved. May (01, 2014 16:01:44 PDT	ClearPass Policy	Manager 6.3.1.62009 on CP-SW-EVAL platform
🚱 🖉 🧕 🔁 📀		🛷 🗖 🖉 🛃		▲ 🛱 🗊 🖤 4:30 PM 5/1/2014

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

APURA networks		ClearPass Policy M	lanager	<u>Support</u> <u>Help</u> admin (Super Adm	<u>Log</u> c ninistrate
📲 Dashboard 🛛 🕻	Configuration » Services	» Add			
😥 Monitoring 💦 🕻	Services				
🖧 Configuration 🛛 🔅	Service Authenti	cation Roles Enforcement Summa	ry		
- 🗘 Start Here	Туре:	MAC Authentication	¥		
- Authentication	Name:	SKM.MAC Authentication service			
- 🗘 Methods	Description:	MAC-based Authentication Service	4		
- Q Identity	Monitor Mode:	Enable to monitor network access with	out enforcement		
Single Sign-On (SSO)	More Options:	Authorization Audit End-hosts	Profile Endpoints		
- Ö Local Users	Service Rule				
– 🛱 Endpoints	Matches O ANY or 🖲	ALL of the following conditions:			
— 🛱 Static Host Lists	Туре	Name	Operator	Value	Ť
- 🛱 Roles	1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)	Ba ti
– 🛱 Role Mappings	2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)	Be ti

- 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.

e networks		ClearPass Policy Manager	<u>Support</u> <u>Help</u> <u>Logc</u> admin (Super Administrate
Dashboard 0	Configuration » Services » E Services - SKM MA	fit - SKM MAC Authentication service C Authentication service	
Configuration 📀	Summary Service	Authentication Roles Enforcement	
→ Start Here → Services → Authentication → Authods → Sources → Gurces Jources	Authentication Methods:	[Allow All MAC AUTH] Move Up Move Down Remove View Details Modify Select to Add •	Add new Authentication Metho
- C Local Users - C Endpoints - C Static Host Lists - C Roles - C Roles - C Role Mappings	Authentication Sources:	IP Phone list [Static Host List] [Local User Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB] -Select to Add	Add new Authentication Sourc

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

← → C ★ → C ★ ++++ ★ ++++ ★ ++++ ★ ++++ ★ +++++ ★ ++++++ ★ +++++++ ★ ++++++++++ ★ ++++++++++++++++++++++++++++++++++++	51/tips/tipsContent.action#1398987823102	값 🕺
🗄 Apps 🚺 Su rested Sites 📋 Alcatel-Lu	ucent Payr 🗋 Alcatel-Lucent Payr 🗋 ALCATEL-LUCENT 📑 Free Hotma	ail 🙎 Google 🕒 Introduction 🥜 NSA Implementatio 🥝 NSA Implementatio 🗋 RealPlayer
P Do you want Google Chrome to	save your password? Save password Never for this site	
APURA networks	ClearPass Po	blicy Manager Support Help Logou admin (Super Administrator
Dashboard	Configuration » Services » Edit - SKM MAC Authentication se	rvice
Monitoring	 Services - SKM MAC Authentication services 	vice
S Configuration	Summary Service Authentication Roles	Enforcement
🛱 Start Here	Use Cached Results: Use cached Roles and Postu	re attributes from previous sessions
Authentication	Enforcement Policy: ALU Wired Mac Auth Policy	Modify Modify
-☆ Methods -☆ Sources -⊉ Identity -☆ Single Sign-On (SSO)	Enforcement Palicy Datails Des The value entered is not valid. Default Profile: [Deny Access Profile] Rules Evaluation Algorithm: first-applicable	
- Cocal Osers	Conditions	Enforcement Profiles
Chapter Construction	(Tips:Role EQUALS [Guest]) (Authentication:Source EQUALS IP Phone list (Authentication:MacAuth EQUALS IP Phone list	UNP-guest Radius - FilterID :) UNP-voice Radius - FilterID lient) UNP-restricted Padius - GilterID - URL - Login
🗄 🖶 Posture	S. (Addienceadon macAddi EgoAco onkilowite	
Enforcement		
- 🛱 Devices	<u>A Back to Services</u>	Disable Copy Save Cancel
Administration	0	blaure copy sure cancer
Convright 2014 Apples Networks All	rights reconved May 01, 2014 16:15:15 RDT	CloseBase Boliev Manager 6 3 1 62000 on CB-SW-SVAL platfo

- 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.

🖊 ClearPass Policy Manager 🛛 🔺 🗛 Web Log	gin (new) ×	Name II. Application from a contraction and \$500	of Manufacture	
← → C 🕼 bttps://10.255.95.251,	/tips/tipsContent.action#139	8988264790		☆ 🕺 🔳
🗰 Apps 🚺 Su rested Sites 🕒 Alcatel-Lucer	nt Payr 🗋 Alcatel-Lucent Payr	🗅 ALCATEL-LUCENT 🕒 Free Hotmail 🙎 Google 🕒 I	ntroduction 👩 NSA Implementatio 👩 NSA Impl	ementatio 🕒 RealPlayer 🛛 🔹 »
P Do you want Google Chrome to sa	we your password? Save pa	ssword Never for this site		×
networks		ClearPass Policy Mana	ger	<u>Support</u> <u>Help</u> <u>Logout</u> admin (Super Administrator)
Dashboard O	Configuration » Services »	Edit - SKM Web Auth Service		
Monitoring O	Services - SKM W	eb Auth Service		
Configuration	Summary Service	Authentication Roles Enforcement		
- 🗘 Start Here	Use Cached Results:	Use cached Boles and Posture attributes from	previous sessions	i l
- 🔅 Services	Enforcement Policy:	Wired Captive Portal Policy - NO Posture	Modify	Add new Enforcement Policy
- 🗘 Methods	Enforcement Policy Detai			
- 🛱 Sources	Des The value entered is	not valid.		
🖃 🚨 Identity	Default Profile:	[Update Endpoint UnKnown]		
- 🛱 Single Sign-On (SSO)	Rules Evaluation Algorith	n: first-applicable		
- 🛱 Local Users				
- Q Endpoints	Conditions		Enforcement Profiles	
- Q Static Host Lists	1. (Tips:Role	QUALS [Guest])	UNP-guest CoA - FilterID	
- Q Roles				
- T Role Mappings				
- Policies				
- O Profiles				
- + Network				
Devices	< Back to Services			Disable Copy Save Cancel
🚰 Administration 🛛 🛛 🛛				Inclusion Division Inclusion Inclusion
© Copyright 2014 Aruba Networks. All rig	ghts reserved.	May 01, 2014 16:22:26 PDT	ClearPass Policy Manager	r 6.3.1.62009 on CP-SW-EVAL platform
				▲ 🛱 🗂 🌒 😽 4:51 PM

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 UNPemployee

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.

ARURA			ClearPass F	Policy Ma	nager	Support Help Logout admin (Super Administrator)
Dashboard 0	Configu	urati	ion » Enforcement » Profiles			
Monitoring O	Enfo	rce	ement Profiles			Add
Configuration 📀						Export All
- 🛱 Start Here						The state of the second s
- 🛱 Services	Filter:	Na	me ▼ contains ▼ UN	IP-	+ Go Clear Filter	Show 100 Trecords
🔄 🖴 Authentication	#		Name 🛆	Туре	Description	
- 💭 Methods	1.	6	CoA UNP-restricted - HealthCheck URL	RADIUS_CoA	CoA UNP-restricted - HealthCheck URL	
Q Sources	2.		CoA UNP-restricted - HealthCheck URL and FilterID	RADIUS_CoA	CoA UNP-restricted - HealthCheck URL	and FilterID
- 🛱 Single Sign-On (SSO)	з.		CoA UNP-restricted - Remdiation URL and FilterID	RADIUS_CoA	CoA UNP-restricted - Remdiation URL a	nd FilterID
- Cal Users	4.		UNP-BYOD Radius - FilterID	RADIUS	UNP-BYOD Radius - FilterID	
Ctatic Host Lists	5.		UNP-employee CoA - FilterID	RADIUS_CoA	UNP-employee CoA - FilterID	
Poles	6.		UNP-employee Radius - FilterID	RADIUS	UNP-employee Radius - FilterID	
Role Mappings	7.		UNP-guest CoA - FilterID	RADIUS_CoA	UNP-guest CoA - FilterID	
F- TPosture	8.		UNP-guest CoA - FilterID - ACL	RADIUS_CoA	UNP-guest CoA - FilterID - ACL	
Enforcement	9.	۵	UNP-guest CoA - FilterID - ACL - guest-role	RADIUS_CoA	UNP-guest CoA - FilterID - ACL - guest	-role
- 🛱 Policies	10.		UNP-guest CoA - FilterID - PolicyList	RADIUS_CoA	UNP-guest CoA - FilterID	
- 🔅 Profiles	11.		UNP-guest Radius - FilterID	RADIUS	UNP-guest Radius - FilterID	
- · • Network	12.		UNP-quarantine CoA - FilterID	RADIUS_CoA	UNP-quarantine CoA - FilterID	
— OPOlicy Simulation — OPTOFile Settings	13.		UNP-restricted Radius - FilterID	RADIUS	UNP-restricted Radius - FilterID	

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

networks		ClearPass Policy Manager	Support Help Logout admin (Super Administrator)
Dashboard O	Configuration » Enforcemer	it » Profiles » Add Enforcement Profile	
Monitoring 0	Enforcement Profi	les	
Configuration O	Profile Attributes	Summary	
- Start Here	Template:	L RADIUS Based Enforcement	
Authentication	Name:	UNP-employee Radius - FilterID	
- 🛱 Methods	Description:		
- 🛱 Sources			
🖃 🚨 Identity	Туре:	RADIUS	
- 🛱 Single Sign-On (SSO)	Action:	🖲 Accept 🔍 Reject 🔍 Drop	
- 🛱 Local Users	Device Group List:	* Remove	Add new Device Group
- 🛱 Endpoints		View Details	
- 🛱 Static Host Lists	1	* Modify	
- 🛱 Roles		Select	
- 🛱 Role Mappings			
🛞 🖶 Posture			
🖃 💈 Enforcement			
- 🛱 Policies			
- 🗘 Profiles			
Network			
- 🛱 Devices			
- Device Groups			

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.

ARUBA networks		Clea	rPass Policy	Manager		Support Help admin (Super A	dministrator)
📲 Dashboard 🛛 🔍 0	Configuration » Enforcemer	nt » Profiles	» Add Enforcement Pro	file			
Monitoring O	Enforcement Profi	les					
Configuration 📀	Profile Attributes	Summar	1				
- 🛱 Start Here	Туре		Name		Value		宜
- 🛱 Services	1. Radius: IETF	*	Filter-Id (11)	*	= UNP-employee		() =
🖃 🗣 Authentication	Click to add						
- 🛱 Methods							
- 🛱 Sources							
🖃 🚨 Identity							
- 🛱 Single Sign-On (SSO)							
– 🛱 Local Users							
- 🛱 Endpoints							
- 🛱 Static Host Lists	1						
- 🛱 Roles							
- 🛱 Role Mappings							
🕀 🖶 Posture							
🖃 💐 Enforcement							
- 🛱 Policies							
- 🛱 Profiles							
- Network							
- 🛱 Devices							
- 🛱 Device Groups							

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.

networks				ClearPass	Policy N	lanager	Support Help Logout admin (Super Administrator)
Dashboard	0	Configu	iratio	on » Enforcement » P <mark>ol</mark> icies			
Monitoring	0	Enfo	rce	ment Policies			Add
& Configuration	O						Export All
- 🛱 Role Mappings	-						
🖽 🖶 Posture		Filter:	Nar	ne ▼ contains ▼	Wired	+ Go Clear Filter	Show 50 🔻 records
🖃 💈 Enforcement	1	#		Name	Type 🛦	Description	
- 🔅 Policies		1.		Wired Onboarding Onboard AppAuth Policy	Applicatio	n	
		2.		Wired Onboarding Onboard Pre-Auth Policy	Applicatio	n	
- Devices	+	з.		Wired Onboarding Onboard Provisioni Policy	ng RADIUS	Enforcement policy controlling netwo	rk access for device provisioning
🗿 Administration	0	4.		Wired Alcatel-Lucent IP Touch Enforcement Policy	RADIUS	Wired MAC Enforcement Policy	
© Copyright 2014 Aruba Netwo	orks. Al	l rights r	eser	ved. Apr 28, 2014 17:04	:34 PDT	ClearPass Policy Manag	er 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.

networks		ClearPass Policy Manager	Support Help Logout admin (Super Administrator)
Dashboard O	Configuration » Enforcement	t » Policies » Add	
Monitoring 0	Enforcement Polici	ies	
🔏 Configuration 📀	Enforcement Rules	Summary	
- 🛱 Start Here 🏠	Name:	Wired 802.1X Enforcement Policy	
- 🛱 Services 🖃 🗣 Authentication	Description:	Wired 802.1X Enforcement Policy	
— 🛱 Methods	Enforcement Type:	● RADIUS ◎ TACACS+ ◎ WEBAUTH (SNMP/Agent/CLI/CoA) ◎ Application	
→ Sources I dentity → C Single Sign-On (SSO) → C Local Users → C Endpoints → C Static Host Lists → C Roles → C Role Mappings → Role Mappings → Posture → Posture → Pofiles → Pofiles → Pofiles → C Porfiles → C Porfiles → C Porfiles	Default Profile:	Select to Add- View Details Modify Wired Onboarding Onboard Post-Provisioning Wired Onboarding Onboard Pre-Provisioning Wired Standard Statement Wired Onboarding Onboard Pre-Provisioning Wired Statement Wired Onboard Pre-Provisioning Wireless UNP-employee Profile [AirGroup Response] [AirGroup Response] [AirGroup Response] [AirGroup Shared Device] [Mont Access Profile [Deny Access Profile [Deny Access Profile [Diny Access Profile [AirGroup Scale Coal - HealthCheck URL [RADIUS Coal Coa - HealthCheck URL [RADIUS Coal Coa - UNP-restricted - HealthCheck URL and FilterID [RADIUS Coal (UNP-restricted - Remdiation URL and FilterID [RADIUS Coal UNP-restricted - Remdiation URL and FilterID [RADIUS Coal UNP-restricted - Remdiation URL and FilterID [RADIUS Coal UNP-restricted - FilterID [RADIUS Coal UNP-restrecoal - FilterID	Add new Enforcement Profile

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

APUPA networks		ClearPa	ass Policy Manager		Support Help Logoul admin (Super Administrator
Dashboard 0	Configuration » Enforce	ment » Policies » Ado	1		
Monitoring O	Enforcement Po	licies			
Configuration 📀	Enforcement Ru	les Summary			
Sources	Rules Evaluation Algor	ithm: 🖲 Select first	match 🔍 Select all matches		
□ Q Identity	Enforcement Policy Ru	les:			
Single Sign-On (SSO)	Conditions			Actions	
Cal Users Endpoints Static Host Lists Roles Role Mappings	Add Rule		Move Up Move Down		Edit Rule Remove Rule
🛞 🖶 Posture					
Benforcement Policies Orofiles					
Network					
Administration O	Sack to Enforcer	nent Policies			Next > Save Cancel
© Copyright 2014 Aruba Networks. A	ll rights reserved.	Apr 28, 2014	17:15:54 PDT	ClearPass Policy Manager 6.3	3.1.62009 on CP-SW-EVAL platfor

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.

ADUDA		01	D D!: B	A	Sup	port <u>Help</u>	Logout
Rules Editor							
Conditions							
Match ALL of the followi	ng conditions:						
Туре	-	Name	Oner	ator	Value		
Authentication	*	Source	EQUALS	*	SQA Active Directory Se		8 *
2. Click to add							
Enforcement Profiles							
Profile Names:	[RADIUS] UNP-	employee Radius - FilterID	Move Up Move Down Remove				
	Select to Add	- '					
						Save	Cancel
© Copyright 2014 Aruba I	Networks. All rights	reserved. Apr 2	8, 2014 17:20:20 PDT	Cle	arPass Policy Manager <u>6.3.1.62</u>	2009 on CP-SW-E	VAL platfor

5.6.2.3 Configuring an 802.1x service

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



2. Select the 802.1X Wired service shown below

Revision: 1.1, 08/01/2014



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.

APUPA networks		ClearPass Policy Mana	ager	<u>Support</u> <u>Help</u> admin (Super Adr	l <u>Logo</u> ninistrato			
Dashboard 0	Configuration » Service	s » Add						
Monitoring 0	Services							
Configuration 💿								
- 🛱 Start Here		Chenticalities EnterComment						
_ 🛱 Services	Service							
🖃 କ Authentication								
🚽 🛱 Methods	Service Authorit	igntion Bolac Enforcement Comm						
🛱 Sources	Service Authent	ication <u>Roles</u> Enforcement Summa	iry					
🖃 🧕 Identity	Name:	ALU-Wired						
- 🛱 Single Sign-On (SSO)	Description:	Description: 802.1X Wired Access Service						
- 🛱 Local Users	Monitor Mode	Eastha to manitar naturaly access with						
- 🛱 Endpoints	Monitor Mode.			(III)				
- 🗘 Static Host Lists	More Options:	Authorization Posture Compliance	Audit End-hosts	Profile Endpoints				
- 🛱 Roles	Service Rule							
Role Mappings	Matches 🔍 ANY or 🖲	ALL of the following conditions:						
🕣 🖶 Posture	Туре	Name	Operator	Value	Ű			
🖅 🔹 Enforcement	1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)	Ba 10			
🕞 📫 Network	2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	Ge t			
— 🛱 Devices	3. Click to add							
- 🛱 Device Groups								
- 🛱 Proxy Targets								
- Dr Policy Simulation								

- 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.

networks		ClearPass Policy N	/lanager	Support Help Logout admin (Super Administrator)
Dashboard 0	Configuration » Services » E	dit - Wired 802.1X Authentication S	ervice	
Monitoring 0	Services - Wired 8	02.1X Authentication S	ervice	
🖧 Configuration 📀	Summary Service	Authentication Poles Enf	orcomont	
\$ Start Here \$ Services \$ Authentication \$ Authentication \$ Authentication \$ Ources \$ Udentity \$ Single Sign-On (SSO) \$ Local Users \$ Call Users \$ C	Authentication Canods:	[EAP TLS With OCSP Enabled] [EAP PEAP] [EAP FAST] [EAP TLS] [EAP MD5] [MSCHAP] -Select to Add- SQA Active Directory Service [Active	Move Up Move Down Remove View Details Modify Directory! Move Up Move Down Remove View Details Modify	Add new Authentication Method
🖅 🖶 Posture		Select to Add	*	
	Strip Username Rules:	Enable to specify a comma-sep	arated list of rules to strip usernam	e prefixes or suffixes
- 🗘 Profile Settings				

- 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.

A ClearPass Policy Manager × My	FatSecret ×	A D P P LL P Annual Laboration	Line Line Autor	
← → C //10.255.95.2	51/tips/tipsContent.action#13	98726183076		☆ 🕅 🗧
🔢 Apps 🚺 Su Alcatel-L	ucent Payr 📋 Alcatel-Lucent Payr	🕒 ALCATEL-LUCENT 📋 Free Hotmail 🚺 Google	📋 Introduction 🕢 NSA Impleme	entatio 🕢 NSA Implementatio »
P Do you want Google Chrome to	o save your password? Save p	assword Never for this site		×
networks		ClearPass Policy Manager		Support Help Logout admin (Super Administrator)
Dashboard 0	Configuration » Services » Edi	t - Wired 802.1X Authentication Service		
Monitoring 0	Services - Wired 80	2.1X Authentication Service		
Configuration •	Summary Service	Authentication Roles Enforcement		
Saprices	Use Cached Results:	Use cached Roles and Posture attributes from	previous sessions	
Authentication	Enforcement Policy:	Wired 802.1X Enforcement Policy	Modify	Add new Enforcement Policy
- 🗘 Methods	Enforcement Policy Details	· · · · · · · · · · · · · · · · · · ·		
🛱 Sources	Description:	Wired 802 1X Enforcement Policy		
🖃 🧕 Identity	Default Profile	[Deny Access Profile]		
- 🛱 Single Sign-On (SSO)	Rules Evaluation Algorithm:	first-applicable		
- Cocal Users	Conditions		Enforcement Profiles	
Static Host Lists	1. (Authentication	Source EQUALS SQA Active Directory Service)	UNP-employee Radius - Filte	erID
- 🛱 Roles	2. (Authentication	:OuterMethod EQUALS EAP-TLS)	UNP-voice Radius - FilterID	
- 🛱 Role Mappings	3. (Authentication	:Status EQUALS User)	UNP-restricted Radius - Filte	erID - URL Health Check
🖅 📅 Posture				
Enforcement				
- 🛱 Policies				
- 🛱 Profiles				
🖳 📫 Network				
- C Policy Simulation				
— 🛱 Profile Settings				

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 nonsupplicant, 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** UNPemployee

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.

T Do you want Google Chrome	to save you	ir password? Save	password Never for this site		,
A PUPA networks			ClearPass Policy Manage	er Supp adm	ort <u>Help</u> Logout hin (Super Administrator)
Dashboard 0	Configur	ation » Identity » Lo	ical Users		
Monitoring O	Local	Users			Add 🚽
Configuration 💿					Export All
🖞 Start Here 🔶					
🗘 Services	Filter:	User ID	▼ contains ▼	+ Go Clear Filter	Show 50 🔻 records
🛛 🕰 Authentication	#	🕘 User ID 🛦	Name	Role	Status
- 🛱 Methods	1.	admin	admin	[TACACS Network Admin]	Enabled
- Q Sources	2.	employee001	employee account 0	01 [Employee]	Enabled
Single Sign-On (SSO)	3.	🗊 tu	Tu Tran	[Employee]	Enabled
- C Local Users	4.	user1050	user1050	[Employee]	Enabled
- 🛱 Endpoints	5.	user1051	user1051	[Employee]	Enabled
- 🛱 Static Host Lists	6.	user1052	user1052	[Employee]	Enabled
– 🛱 Roles	7.	user1053	user1053	[Employee]	Enabled
Role Mappings	8.	user1054	user1054	[Employee]	Enabled
- 🕀 Posture	9.	user1055	user1055	[Employee]	Enabled
📲 🖉 Enforcement	10.	user1056	user1056	[Employee]	Enabled
					10505 - 105

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.

APIPA networks	Add Local User				8	Support Help Logout admin (Super Administrator)
E Dashboard O	User ID	alu-employee	-1			
Monitoring 0	Name	alu omplovor	1			🕈 Add
Configuration	Name	ald-employee				🖄 Export All
🗕 🛱 Start Here 📩	Password					
- 🛱 Services	Verify Password					Show 50 🔻 records
- Authentication	Enable User	🕑 (Check t	o enable local user)			Status
Sources	Polo					rk Admin] Enabled
	Kole	[Employee]		•		Enabled
Single Sign-On (SSO)	Attributes					Enabled
- 🛱 Local Users	Attribute		Value		Ť	Enabled
- 🛱 Endpoints	1. Department		= Software	*	B #	Enabled
🛛 🎝 Static Host Lists	2. Click to add					Enabled
— 🛱 Roles	Parallel and an and a strength of the second second					Enabled
🛱 Role Mappings						Enabled
🖃 📅 Posture						Enabled
📄 🕄 Enforcement				Add	Concel	Enabled
Administration 🛛 🖉				Adu	cancer	Enabled 🗸
© Copyright 2014 Aruba Networks.	All rights reserved.	Apr 29, 20	14 14:40:35 PDT	ClearPass Poli	cy Manage	er 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.

ARURA networks	ClearPass	Policy Ma	nager	Support Help Logout admin (Super Administrator)
Dashboard 📀				
	A Cluster Status			8
All Requests Trend all Policy Manager	Status Host Name	Zone	Server Role Last Replication	Status
requests	alu-cppm63.sqa.com (10.255.95.251)	default	Publisher -	ОК
Health Status Trend Healthy and Unhealthy requests				
Authentication Status Trend Successful and Failed authentications		0	Applications	× *
Latest Authentications Latest Authentications	Drag and Drop Items Here		Advanced Analytics, In-depth Report	ing, Compliance & Regulation
Device Category			▼ Guest Management	-
			🔺 🧸 All Requests	S 💌
Ø Device Family	Access Tracker		5.000	
Contraction Device Family	Analysis and Trending		5,000 21	
*	🔅 Network Devices		2,500	
Monitoring 0	📲 Server Manager		See 3	
Configuration	🐒 ClearPass Guest		0 22 Apr 24 Apr 25 Apr	ar 28 Apr
	🚽 🕼 ClearPass Onboard + WorkSpace 🕥		Time	•
Administration 0				
© Copyright 2014 Aruba Networks. A	Il rights reserved. Apr 29, 2014 14:53	2:59 PDT	ClearPass Policy Manager <u>6.3.</u>	1.62009 on CP-SW-EVAL platforr

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.

networks	ClearPass Onboard + WorkSpace				<u>Support</u> <u>Help</u> <u>Logout</u> admin (IT Administrators)
Guest O Conboard + WorkSpace O Start Here	Home » Onboard + WorkSpace » Initia Certificate Authorities	Setup »	Certificate	Authorities	of Create new certificate authority
Thitial Setup Start Here Certificate Authorities Certificate Authorities Setup ioS Distribution Certificate Setup ioS Distribution Certificate Setup ioS Distribution Certificate Setup ioS Distribution Certificate	 There are errors with the server certific alu-cppm63.sqa.com: The ClearPass H alu-cppm63.sqa.com: ClearPass RADIU authenticating. How do I fix this problem? Use this list to manage certificate autors 	ate configu TPS serve S server o horities.	ration that v r root certific ertificate lac	vill prevent devices from pr zate is not trusted by Apple (s id-kp-eapOverLAN exter	rovisioning or authenticating: . This will cause enrollment over HTTPS to fail on iOS devices. ded key usage. This will prevent Windows 8.1 clients from
Apps Management	Name	Mode	Status	Expiry	OCSP URL
Management and Control	Local Certificate Authority This is the default certificate authority.	root	🖌 Valid	2024-01-31 01:32:56-0	<pre>nttp://alu-cppm63.sqa.com/guest/mdps_ocsp.php/1</pre>
- Start Here	C ⁴ Refresh			1	Showing 1 – 1 of 1 20 rows per page 🔻
– 💽 AirPlay – 📑 AirPrint	💞 Back to initial setup				
- 🌮 APN	🚛 Back to Onboard + WorkSpace				
– 👀 App Lock – 🛐 Calendar	😭 Back to main				
- 🗾 Contacts - 🌮 Device Restrictions					
_12 Email					
– 💹 Exchange ActiveSync 🛛 👻					
Configuration 0					

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

Revision: 1.1, 08/01/2014



4. Select Create new network as shown.



5. Enter a name, select "Wired" and click Next.



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

networks		Support Help Logo admin (IT Administrator					
🗣 Guest 🛛 🖡	lome » Onboard + ۱	WorkSpace » Onl	board/MDM Configuration	» Network Set	tings		
Onboard + WorkSpace 💿 👔	Vetwork Sett	ings					
	 There are errors v alu-cppm63.sqa.cc alu-cppm63.sqa.cc authenticating. How do I fix th Use this form to create 	with the server certion: The ClearPass om: ClearPass RAD is problem? ate the network	ficate configuration that will HTTPS server root certificat IUS server certificate lacks settings that will be ser	prevent devices fi is not trusted by d-kp-eapOverLAN it to a provision	rom provisioning or a Apple. This will caus I extended key usage ned device.	uthenticating: e enrollment over HT . This will prevent W	TPS to fail on iOS devices. indows 8.1 clients from
- AirPrint		Ne	etwork Settings » Ente	rprise Protoco	Is		
- 🚱 App Lock	🌲 Access#	2 Protocols#	Nuthentication	Trust	Mindows	🚓 Proxy	
- 🛐 Calendar 📙 Contacts	Enterprise Prot Options for 802.1X pr	ocols otocols supported o	on the network.		Conversion Review		
- Device Restrictions	IOS & OS X EAP						
- 🔯 Email - 🔯 Exchange ActiveSync - 🚰 Global HTTP Proxy	IOS & OS X EAP:						
Passcode Policy		Select the authent	tication protocols to use whe	n configuring an it	OS or OS X 10.7+ (Li	on or later) device.	
Single Sign-On	Legacy OS X EAP:	PEAP with MSCH The authentication OS X 10.5/6 (Leop	APv2 n protocol to use when config pard/Snow Leopard) devices	uring			
- Web Clips and Bookm.	Android EAP						
	Android EAP:	PEAP with MSC Select the authent	HAPv2 tication protocol to use when	configuring an Ar	ndroid device.		
🗄 🎭 WorkSpace Configuration	Windows EAP						
Deployment and Provisionin	Windows EAP:	TLS The authentication	protocol to use when config	uring a Windows	device.		
Configuration Profiles		reviou:	s 📄 Next 📲 Sa	ve Changes	Cancel		

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

APUPA networks	ClearPass C	nboard + WorkSpace	Support Help Logout admin (IT Administrators)
🍕 Guest 🛛 🕚	Home » Onboard + WorkSpace » Deployment	and Provisioning » Configuration Profiles	
Onboard + WorkSpace 📀	Configuration Profiles		Create new configuration profile
Start Here	There are errors with the server certificate con alu-cppm63.sqa.com: The ClearPass HTTFS sei alu-cppm63.sqa.com: ClearPass RADIUS serve authenticating. How do I fix this problem? Use this list to manage configuration profiles	figuration that will prevent devices from provisioning or authe rver root certificate is not trusted by Apple. This will cause en r certificate lacks id-kp-eapOverLAN extended key usage. Thi	nticating: rollment over HTTPS to fail on iOS devices. Is will prevent Windows 8.1 clients from
- Start Here		Name	
Provisioning Settings	Wired Network Profile		
— 🔂 Self-Service Portal	C Refresh	1	Showing 1 - 1 of 1 20 rows per page 🔻
I	₩ 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.

ice Configuration	Profile	
ent and Provisioning * Name:	ALU Wired Network Profile	
nfiguration Profiles invisioning Settings vice Portal 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 •	

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

APURA	ClearPass Onboard + W	Support Help Logo admin (IT Administrator:	
🗣 Guest 🔹 🔹	Home » Onboard + WorkSpace » Deployment and Provisioning » Pro Provisioning Settings	visioning Settings	. Create new provisioning setting:
A Start Here Start Here Management and Control Monagement and Control Monagement Configuration MorkSpace Configuration Deployment and Provisioning	 There are errors with the server certificate configuration that will preven alu-cppm53.sqa.com: The ClearPass HTTPS server root certificate is not alu-cppm53.sqa.com: ClearPass RADIUS server certificate lacks id-kp-e authenticating. How do I fix this problem? Use this list to manage provisioning settings. 	: devices from provisioning or authenticating: trusted by Apple. This will cause enrollment c pOverLAN extended key usage. This will pre	ver HTTPS to fail on iOS devices. vent Windows 8.1 clients from
Start Here Configuration Profiles	Name	CA	Profile
Provisioning Settings	Wired Network Device Provisioning This is the default configuration set for device provisioning.	Local Certificate Authority	Wired Network Profile
- 🗗 Self-Service Portal	C 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".

APUPA networks	Clea	rPass Onboard + WorkSpace	Support Help Logo admin (IT Administrator
Guest O Onboard + WorkSpace O Start Here	How do I fix this problem? Use this form to make changes	to the basic configuration options for device provisioning.	
🗄 🧬 Initial Setup		Device Provisioning Settings	
	👘 General 🚜 Web Login	🛛 😥 iOS & OS X 🛛 🗯 Legacy OS X 🛛 🎥 Windows 🛛 🏺 Android 🛛 🙏	Onboard Client
WorkSpace Configuration Jone Deployment and Provisioning	* Name:	ALU Wired network Enter a name for this configuration set.	
Start Here	Description:	ALD Wired network	
- 🙌 Ser-Service Portai	* Organization:	Enter a description for the configuration set. Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning.	
	Identity These options control the generation	on of device credentials.	
	* Certificate Authority:	□_ocal 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	e 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 <u>http://cppm-ip-address/guest/device_provisioning.php</u>. Accept all defaults of IOS, OSX, Windows and Android tabs.

Revision: 1.1, 08/01/2014



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



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.

Revision: 1.1, 08/01/2014

ARURA networks	ClearF	ass Guest			<u>Support</u> <u>Help</u> <u>Logout</u> admin (IT Administrators)
Guest O Onboard + WorkSpace O	Home » Configuration » Web Logins Web Logins			🚑 Cre	eate a new web login page
Configuration	Many NAS devices support Web-based authentica By defining a web login page on the ClearPass Gu network through these NAS devices. Use this list view to define new web login pages, Onboard device provisioning pages are now r	ation for visitors. est you are able to pr and to make changes nanaged from the We	rovide a customized g to existing web login b Login tab within pro	raphical login page fo pages. ovisioning settings	r visitors accessing the
- 🌇 Fields	ے Name	Page Title	Page Name	Page Skin	
🋅 Forms & Views 🕵 Guest Manager	Alcatel-Lucent Secure Access		secure-access	(Default)	
Guest Self-Registration	Copy of Alcatel-Lucent Secure Access Alcatel-Lucent Secure Access	\geq	secure-access_1	(Default)	
- 🋶 Start Here	health check		healthcheck	(Default)	
— 🚺 Manage Customer Info — 💿 Manage Hotspot	3 web logins 💭 Reload		S	Show all rows 🔹	
 Anage Invoice Manage Plans Manage Transaction Pro Self Provisioning IP Phones Print Templates SMS Receipt Translations Web Logins 	Back to configuration Back to main				

14. Update the Footer HTML with the following " To register your personal device please Click ". Please see below. Once this is done, save and test to see if the Onboard page is shown.



5.7.2.3 Configuring enforcement profile

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

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

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

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

5.7.2.3.1 Creating an ALU Restricted enforcement profile

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

- 1. Modify the Attributes tab as shown below to return
 - a. RADIUS Filter-Id with UNP edge-profile UNP-restricted. The Edge-profile <u>must be</u> "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}}

APURA networks	ClearPass Policy Manager			Support Help Logo admin (Super Administrato
Dashboard O Monitoring O	Configuration » Enforcement » Profiles » Edit Enforcement Profile - ALU Restricted Profile Enforcement Profiles - ALU Restricted Profile			
Configuration 📀	Summary Profile	Attributes		
	Profile:			
	Name:	ALU Restricted Profile		
	Description:	return a radius UNP-restricted profile		
	Type:	Type: RADIUS		
	Action:	Accept		
	Device Group List:			
	Attributes:			
	Туре	Name	Value	
	1. Radius:IETF	Filter-Id	= UNP-restri	icted
	2. Radius: Alcatel-Lucer	t-Enterprise Alcatel-Redirection-URL	= https://10 mac=%{C	0.255.221.137/guest/secure-access.php? connection:Client-Mac-Address-Colon}
Roles	1			

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.
networks		Clear	Pass Policy I	Vlanager	Support Help Logout admin (Super Administrator)
Dashboard O Monitoring O	Configuration » I Enforceme	Enforcement » Profiles » nt Profiles - ALU	Edit Enforcement Prof J BYOD Profile Enforcemen	ile - ALU BYOD Profile t profile has not been saved	
Configuration O	Summary	Profile Attributes			
	Profile: Name: Description: Type: Action:	ALU BYO return a RADIUS Accept	D Profile radius profile - UNP-by	od	
	Attributes: Type	List: -	Name	Value	
C Endpoints C Static Host Lists C Roles Role Mappings	1. Radius:IET	F	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

networks		ClearPass Policy Manager	admin (Super Administrator)
Dashboard O Monitoring O	Configuration » Enforcement Enforcement Policie	» Policies » Edit - ALU Wired MAC Enforcement es - ALU Wired MAC Enforcement	Policy nt Policy
Configuration O	Summary Enforcement:	Rules	
	Name: Description: Enforcement Type:	ALU Wired MAC Enforcement Policy ALU Wired MAC Enforcement Policy RADIUS	
	Default Profile: Rules:	ALU Restricted Profile	
	Conditions 1. (Authentication	First applicable :MacAuth EQUALS UnknownClient)	Actions ALU Restricted Profile
- C Static Host Lists - C Roles - C Role Mappings			

- 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



2. Select the following authentication methods and sources as shown

← → C 🕼 https://10.255.95.25	1/tips/tipsContent.action#139	8988670818	☆ 🕺 🗉
🗄 Apps 🚺 Su rested Sites 📋 Alcatel-Luc	ent Payr 📋 Alcatel-Lucent Payr	🗅 ALCATEL-LUCENT 🗋 Free Hotmail 💈 Google 🕒 Introduction 🤣 NSA Implementatio 🤣 NSA I	nplementatio 🕒 RealPlayer 🛛 🛛 🛛
P Do you want Google Chrome to s	ave your password? Save pa	ssword Never for this site	*
APURA networks		ClearPass Policy Manager	Support Help Logout admin (Super Administrator)
Dashboard	Configuration » Services »	Edit - Wired Onboarding Onboard Provisioning	
Monitoring (Services - Wired (Onboarding Onboard Provisioning	
Configuration	Summary Service	Authentication Roles Enforcement	
Start Here Services Authentication Methods Q Jources Jources Jidentity	Authentication Methods:	[EAP TLS With OCSP Enabled] Move Up [EAP PEAP Without Fast Reconnect] Move Down Remove View Details Not valid. Modify	Add new Authentication Method
- 🌣 Single Sign-On (SSO) - 🌣 Local Users - 🌣 Endpoints - 🌣 Static Host Lists - 🌣 Roles - 🔅 Role Mappings	Authentication Sources:	Select to Add-	Add new Authentication Source
Posture Enforcement OPolicies OPofiles Notwork	Strip Username Rules:	Select to Aod-	
- Devices	Back to Services		Disable Conv Save Cancel
Administration (0		Restored Barris & Barris & Barris

3. Set the enforcement policy that was previously created.

← → C 🕼 bttps://10.255.95.25	1/tips/tipsContent.action#1	398988670818	☆ 🕺 :		
🗒 Apps 🚺 Su rested Sites 📋 Alcatel-Luc	ent Payr 🗋 Alcatel-Lucent Pa	r 🗅 ALCATEL-LUCENT 🛅 Free Hotmail 🙎 Google 🕒 Introdu	uction 🕜 NSA Implementatio 🕜 NSA Implementatio 🕒 RealPlayer		
P Do you want Google Chrome to s	ave your password? Save	password Never for this site			
networks		ClearPass Policy Manager	C Support Help Logor admin (Super Administrator		
Dashboard	Configuration » Services	» Edit - Wired Onboarding Onboard Provisioning			
Monitoring (Services - Wired	Onboarding Onboard Provisioning			
Configuration	Summary Servic	e Authentication Roles Enforcement			
🖧 Start Here	Use Cached Results:	I lise cached Boles and Posture attributes from prev			
- 🔆 Services - 🕰 Authentication	Enforcement Policy:	Wired Onboarding Onboard Provisioning Policy	Add new Enforcement Policy		
- 🌣 Methods - 🔅 Sources	Enforcement Policy De Des The value entere	Enforcement Policy Details Des The value entered is not valid. ment policy controlling network access for device provisioning			
Q Identity	Default Profile:	[Deny Access Profile]			
- gr single sign-On (SSO)	Rules Evaluation Algor	ithm: first-applicable			
- T Endpoints	Conditions		Enforcement Profiles		
_ 🛱 Static Host Lists	1. (Authent	cation:OuterMethod EQUALS EAP-TLS)	[Allow Access Profile], Wired Onboarding Onboard Post-Provisioning		
- 🛱 Roles	2. (Authent	cation:Source EQUALS [Onboard Devices Repository])	[Allow Access Profile], Wired Onboarding Onboard Post-Provisioning		
- 🛱 Role Mappings	3. (Authent	cation:Source NOT_EQUALS [Onboard Devices Repository]]) [Allow Access Profile], Wired Onboarding Onboard Pre-Provisioning		
Posture					
Senforcement					
- Profiles					
-+ Network					
- 🛱 Devices	Back to Services		Disable Come Consol		
Administration	0		Disable Copy Save Caller		
Copyright 2014 Aruba Networks. All I	rights reserved.	May 01, 2014 16:32:41 PDT	ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platfo		
			5.01 DM		

• 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.

networks	ClearPass Policy Manager	<u>Support</u> <u>Help</u> Logou admin (Super Administrator
Dashboard	Configuration » Posture » Posture Policies	\sim
Monitoring	 Posture Policies 	Add 🕐
Configuration	o	🛎 Import 🏝 Export All
- 🛱 Start Here		
— 🛱 Services	Filter: Name 🔻 contains 🔻 🕂 Go Clear Filter	Show 10 🔻 record:
🕀 🔒 Authentication	# Name A Description	
🖃 🚨 Identity	w o name a beschpton	
- 🛱 Single Sign-On (SSO)		
🖓 Local Users		17
— 🛱 Endpoints	Showing 1-2 of 2	Copy Export Delete
— 🛱 Static Host Lists		
- 🛱 Roles		
🔤 🛱 Role Mappings		
🖃 🖶 Posture		
-🛱 Posture Policies		
- 🛱 Posture Servers		
Ph Audit Convora		

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.

networks		ClearPass Policy Manager	Support Help Logo admin (Super Administrato
E Dashboard O Monitoring O	Configuration » Posture » Po Posture Policies	osture Policies » Add	
Configuration	Policy Posture Plugi	ns Rules Summary	
- 🗘 Start Here	Policy Name: Description:	SKM Non-Persistent posture check policy Posture Check Policy	
∴ Addrendcation ⊇ Identity _☆ Single Sign-On (SSO)	Posture Agent: Host Operating System:	NAP Agent OnGuard Agent (Persistent or Dissolvable) Windows Linux Mac OS X	
Local Users Cal Jusers Cal Endpoints Static Host Lists Roles Cal Roles Cal Role Mappings	Restrict by Roles:	Select or type role names	
Posture Posture Policies Order Posture Servers Q Audit Servers		Add	

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

ARUBA	ClearPass Policy M	Support Help Loga admin (Super Administrat	
Dashboard G	Configuration » Posture » Posture Policies » Add		
Monitoring G	Posture Policies		
Configuration	Policy Posture Plugins Rules Summary		
- 🗘 Start Here	Select one/more plugins:		
- 🛱 Services	Plugin Name	Plugin Configuration	Status
🖅 🚘 Authentication	ClearPass Windows Universal System Health Validator	Configure View	-
🖃 🚨 Identity	Windows System Health Validator	Configure	Not Configured
- 🛱 Single Sign-On (SSO)	Windows Security Health Validator	Configure View	-
- 🛱 Local Users			
— 🛱 Endpoints			
- 🛱 Static Host Lists			
- 🛱 Roles			
- 🛱 Role Mappings			
🖃 📅 Posture			
- 🛱 Posture Policies			
- 🛱 Posture Servers			
🛱 Audit Servers			

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

networks	client computers can connect to your network, subject to the following checks	21
Dachhoard	☑ Windows 7	
Monitoring	Windows 7 clients are allowed Restrict clients which have Service Pack less than 2	
Configuration	✓ Windows Vista	
Ö Start Here	Windows Vista clients are allowed Restrict clients which have Service Pack less than 2	
Authentication	Windows XP	
Q Identity	Windows XP clients are allowed ${\ensuremath{\overline{\!\!\mathcal M\!}}}$ Restrict clients which have Service Pack less than 3	
- Dingle St	☑ Windows Server 2008	
Endpoint	Windows Server 2008 clients are allowed Restrict clients which have Service Pack less than 2	
- C Roles	☑ Windows Server 2008 R2	
- Ö Role Map	Windows Server 2008 R2 clients are allowed Restrict clients which have Service Pack less than 2	
Posture	☑ Windows Server 2003	
- O Posture :	Windows Server 2003 clients are allowed Restrict clients which have Service Pack less than 4	
Stenforcement	Reset	Save Cancel
- X Policies		

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.

networks		Support Help Log admin (Super Administrat	
Dashboard 0	Configuration » Posture »	Posture Policies » Add	
Monitoring O	Posture Policies		
🖧 Configuration 📀	Policy Posture Plu	gins Rules Summary	
- 🗘 Start Here 🄶	Rules Evaluation Algorith Rules Editor	m: First applicable	0
🖅 🗣 Authentication			Posture Token
- Q Identity	Conditions		HEALTHY
- 🛱 Single Sign-On (SSO)	Select Plugin Checks:	Passes all SHV checks	Edit Rule Remove Rule
- 🛱 Local Users - 🛱 Endpoints	Select Plugins:	Vindows System Health Validator	
- 🛱 Static Host Lists	Actions		
- 🛱 Roles - 🛱 Role Mappings	Posture Token:	HEALTHY (0)	
- 🕂 Posture			Save Cancel
-🛱 Posture Policies			
- 🛱 Posture Servers			
Audit Servers			
Enforcement			

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.

networks		<u>Support</u> <u>Help</u> <u>Lo</u> admin (Super Administra	
Dashboard O	Configuration » Posture »	Posture Policies » Add	
Monitoring O	Posture Policies		
🔏 Configuration 📀	Policy Posture Plu	gins Rules Summary	
- 🛱 Start Here 🔶	Rules Evaluation Algorith	m: First applicable	
- 🛱 Services	Rules Editor		Posture Token
- Q Identity	Conditions		HEALTHY
🛱 Single Sign-On (SSO)	Select Plugin Checks:	Fails one or more SHV checks	Edit Rule Remove Rul
- 🛱 Local Users - 🛱 Endpoints	Select Plugins:	G Windows System Health Validator	
- 🛱 Static Host Lists	Actions		
- 🛱 Roles - 🛱 Role Mappings	Posture Token:	QUARANTINE (20)	
🕞 🖶 Posture			Save Cancel
-🛱 Posture Policies			Contraction of the second s
- 🛱 Posture Servers			
- 🛱 Audit Servers			
🔄 🚦 Enforcement			

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

APLIBA networks		ClearPass Policy N	lanager	Support Help Lo admin (Super Administra
Dashboard O	Configuration » Posture » Po	sture Policies » Add		
Monitoring d	Posture Policies			
Configuration G		Internal postu	ire policy has not been saved	
- 🛱 Start Here	Policy Posture Plugin	s Rules Summary		
- n Services	Description:	Posture Check Policy		
Authentication	Posture Agent:	Web Agent		
- Q Identity	Host Operating System:	WINDOWS		
Single Sign-On (SSO)	Restrict by Roles:			
- 🛱 Local Users	Posture Plugins: The list of selected plugins	10 20		
A Static Heat Lists	Plugin Name		Plugin Configuration	Status
- Roles	1. Windows System Heal	th Validator	View	Configured
Role Mappings	Rules:	1		
Posture	Rules Evaluation Algorithm:	First applicable		
- 🛱 Posture Policies	Conditions			Posture Token
- Desture Servers	1. Passes all SHV checks - Windows System Health Validator			HEALTHY
🖃 💐 Enforcement	2. Windows System Healt	h Validator		QUARANTINE
- 🛱 Policies				
- Q Profiles				
- Metwork				

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.

networks		ClearPass Guest	Support Help Los admin (IT Administrate
🖣 Guest 🔹	0	HTML template code displayed while the login attempt is in progress.	
Onboard + WorkSpace	* Login Delay:	5	
Configuration	Network Login Access	The since in eccentre, to acity, mine supplying the regim incodeger	
🗕 🛶 Start Here 🔮	Controls access to the log	in 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.	
- S. Guest Manager	* Deny Behavior:	Send HTTP 404 Not Found status Select the response of the system to a request that is not permitted.	
Hotspot Manager	Post-Authentication Actions to perform after a	SUCCESS ¹¹ , N. USARCHIUSIUII.	
- 🚺 Manage Customer Info - 💿 Manage Hotspot	Health Check:	Require a successful OnGuard health check In Stream will be required to come intentith 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.

networks		ager Support Help Log admin (Super Administra	
Dashboard	• Configuration » Enforcement » Policies	s » Edit - Copy_of_ALU Wired Mac Auth	Policy
Monitoring	 Enforcement Policies - 	ALU Wired Mac Au	th Policy
Configuration	Cummany Enforcement Pr	ulor	
- Authentication	Rule ⁴ The value entered is not valid. Enforcemence oncy rules. Conditions	t first match 🔍 Select all matches	Actions
Single Sign-On (SSO)	1. (Tips:Role EQUALS [Gue	est])	UNP-guest Radius - FilterID
- Ö Local Users	2. (Authentication:Source	EQUALS IP Phone list)	UNP-voice Radius - FilterID
- C Endpoints	3. (Authentication:MacAuth	n EQUALS UnknownClient)	UNP-restricted Radius - FilterID - URL - Login
 	Add Rule	Move Up Move Down	n Edit Rule Remove Rule
Enforcement			

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

PA rks	Clea	arPass Policy Manager		Support Help admin (Super A
Rules Editor				
Conditions				
Match ALL of the follo	owing conditions:			
Туре	Name	Operator	Value	
1. Tips	The value entered is not valid.	EQUALS	[Guest]	Pa 8
2. Tips	Posture	EQUALS	HEALTHY (0)	B 8
3. Click to add				
Enforcement Profiles				
Profile Names:	[RADIUS] UNP-guest Radius - FilterID	Move Up		

3. The modified Enforcement Policy should be as follows



5.8.1.4 Modify the Web Authentication Service

1. Go to CPPM/Configuration/Services.

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

n e r	etworks		ClearPass Policy	Manager	<u>Support</u> admin (Su	<u>Help</u> <u>Log</u> c Jper Administrat
	Dashboard	• Configuration » Services » E	dit - SKM Web Auth Service			
	Monitoring	 Services - SKM We 	eb Auth Service			
20 4	Configuration	Summary Service	Authentication Roles Posture	Enforcement		
-	🛱 Start Here	Name:	SKM Web Auth Service			
12	Authentication	Description:				
	- 🛱 Methods	Туре:	Web-based Authentication	//		
	- g Sources	Status:	Enabled			
	Single Sign-On (SSO)	Monitor Mode:	Enable to monitor network access without enforcement			
	- CLocal Users	More Options:	🖾 Authorization 🐨 Posture Complianc			
	- C Endpoints	Service Rule				
	- Ö Static Host Lists	Matches ANY or ALL	of the following conditions:			
- 2	- Ör Roles	Туре	Name	Operator	Value	Ť
	Role Mappings	1. Host	CheckType	MATCHES_ANY	Authentication	R <u>a</u> 17
	🖶 Posture	2. Host	CheckType	MATCHES_ANY	Health	
	2 Enforcement	3. Click to add				
	- 🛱 Policies					
	🖓 Profiles	Back to Services			Disable Co	
-10	Administration	0			Disable Co	py Save Cance

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

ARUBA		ClearPass Policy Manager	<u>Support</u> <u>Help</u>] admin (Super Administ
Dashboard G	Configuration » Services » I	Edit - SKM Web Auth Service	
Monitoring 0	Services - SKM W	eb Auth Service	
Configuration 🖸	Summary Service	Authentication Roles Posture Enforcement	
- 🛱 Start Here	Posture Policies:		
Gervices Authentication	Posture Policies:	Only OnGuard agent type Posture Policies are applicable for this service	Add new Posture F
☐ Q Identity ☐ C Sign-On (SSO) ☐ C Local Users		View Details Wodify	
- 🛱 Endpoints		Select to Add	
– 🛱 Static Host Lists – 🛱 Roles	Default Posture Token:	UNKNOWN (100)	
Role Mappings	Remediate End-Hosts:	Enable auto-remediation of non-compliant end-hosts	
- 🕀 Posture	Remediation URL:	http://www.remediationserver.com	
- 🛱 Posture Policies	Posture Servers:		
	Posture Servers:	-Select to Add	Add new Posture S

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

APURA networks		ClearPass Policy Man	ager	Support H admin (Super
Dashboard O	Configuration » Services » Ed Services - SKM We	it - SKM Web Auth Service b Auth Service		
Configuration G	Summary Service	Authentication Roles Posture	Enforcement	
Start Here Services Authentication	Use Cached Results: Enforcement Policy:	Use cached Roles and Posture attribut SKM_Non-persistent Wired Posture Enforcem	tes from previous sessions ne v Modify	Add new Enfo
⊡- Q Identity	Enforcement Policy Details			
- g Single Sign-On (SSO)	Description:	Wired Posture Enforcement Policy		
- Q Local Users	Default Profile:	[Update Endpoint UnKnown]		
Static Host Lists	Rules Evaluation Algorithm:	first-applicable		
- Q Roles	Conditions		Enforcement Profiles	
Role Mappings	1. (Tips:Posture 1. AND (Tips:Role EQU	EQUALS HEALTHY (0)) JALS [Guest])	UNP-guest CoA - FilterID	
Posture Senforcement Onicies	2. (Tips:Posture	NOT_EQUALS HEALTHY (0))	UNP-quarantine CoA - Filte	rID
- Tronies				

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 UNPrestricted 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.

ARIPA networks	ClearPass Policy Manager			Support Help Logou admin (Super Administrator	
Dashboard	Configuration » Posture » Posture Po	licies			
Monitoring	Posture Policies			Add 🚽	
Configuration	<mark>o</mark>			Limport 🏝 Export All	
- 🗘 Start Here					
- 🛱 Services	Filter: Name	contains 🔻	+ Go Clear Filter	Show 10 v record:	
🖅 🗣 Authentication	# Nama A	Description	ation		
🕞 🧕 Identity	* • Name A	Descrip	1000		
- 🛱 Single Sign-On (SSO)					
— 🛱 Local Users					
— 🛱 Endpoints	Showing 1-2 of 2			Copy Export Delete	
— 🋱 Static Host Lists					
— 🛱 Roles					
- 🛱 Role Mappings					
🖃 📅 Posture					
- 🍄 Posture Policies					
- 🛱 Posture Servers					
Audit Servers					

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.

networks		ClearPass Policy Manager	Support Help Loc admin (Super Administra
Dashboard O	Configuration » Posture » Po	sture Policies » Add	
Monitoring O	Posture Policies		
Configuration 📀	Policy Posture Plugi	ns Rules Summary	
	Policy Name: Description: Posture Agent:	SKM Wired Onboard Posture check NAP Agent OnGuard Agent (Persistent or Dissolvable) Utindews Dissolvable	
Cal Users Cal Users Cal Users Cal Users	Restrict by Roles:	Select or type role names Add	

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

Do you want Google Chrome t	to save your password? Save password Never for this site	
ARURA networks	ClearPass Policy Manager	<u>Support</u> <u>Help</u> <u>Lo</u> admin (Super Administr
Dashboard C	Configuration » Posture » Posture Policies » Add	
Monitoring C	Posture Policies	
🔏 Configuration 🛛 🤆	Policy Posture Plugins Rules Summary	
— 🛱 Start Here	Select one/more plugins:	
— 🛱 Services	Plugin Name Plugin Configuration	Status
🖽 🖴 Authentication	Windows System Health Validator View	Not Configured
Identity	Windows Security Health Validator Configure View	Not Configured
Local Users		
- Ctatic Upot Lists		

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

ARUPA	Client computers can connect to your network, subject to the following checks -	
Dashboard	☑ Windows 7	
Monitoring	Windows 7 clients are allowed Restrict clients which have Service Pack less than 2	
Configuration	🗹 Windows Vista	
Start Here	Windows Vista clients are allowed Restrict clients which have Service Pack less than 2	
Authentication	🖉 Windows XP	
Identity	Windows XP clients are allowed $\overrightarrow{\!$	
- C Local Us	☑ Windows Server 2008	
- C Endpoint	Windows Server 2008 clients are allowed Restrict clients which have Service Pack less than 2	
- X Roles	☑ Windows Server 2008 R2	
Role Map	Windows Server 2008 R2 clients are allowed Restrict clients which have Service Pack less than 2	
- Ö Posture	☑ Windows Server 2003	
- Ö Posture :	Windows Server 2003 clients are allowed Restrict clients which have Service Pack less than 4	
Enforcement	Reset	Save Cancel
🖧 Policies		

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.

Deshboard Configuration » Posture » Posture Policies » Add Windows Security Health Validator Configuration Start Here Start Here Configuration Configuration Configuration Configuration Client computers can connect to your network, subject to the following checks - Client must have frewall enabled on the client Client must have an antivirus application. Check if Antivirus is up to date Client must have an antisyware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Client must have an antisypware application. Check if Antisypware is up to date Check if Antional cupdates Check if Antional cupdates Client must have an antisymport excertiny updates installed: Client must have an antisymport excertiny updates installed: Client must have an antisymport excertiny updates within last: Additional sources required in your deployment: Windows Vista Windows Vista Windows Vista Windows Vista O Device for Network Additional sources required in your deployment: Device for Network Device for	ARUBA networks		ClearPass Policy Manager	<u>Support</u> admin (
Monitoring Windows Security Health Validator Start Here Start Here Services Authentication Identity Identity Configuration Identity Identity Identity Galax Particle Single Sig Single Sig Identity Identity <th>Dashboard</th> <th> Configurat </th> <th>ion » Posture » Posture Policies » Add</th> <th></th>	Dashboard	 Configurat 	ion » Posture » Posture Policies » Add	
Configuration Start Here Services Configuration Cient computers can connect to your network, subject to the following checks - Cient computers can connect to your network, subject to the following checks - Cient computers can connect to your network, subject to the following checks - Cient computers can connect to your network, subject to the following checks - Cient computers can connect to your network, subject to the following checks - Cient must have firewall Cient must have an antivirus application. Check if Antispyware is up to date Static Hos Check if Automatic Updates Check if Automatic Updates Check if Automatic Updates Check if Automatic Updates is enabled on the client Posture Posture Oposture S Audit Services Windows Vista Windows XP Windows XP	Monitoring	Windows Security Health V	/alidator	
Image: Start Here Vindows 8 Services Client computers can connect to your network, subject to the following checks - Image: Services Client computers can connect to your network, subject to the following checks - Image: Services Client computers can connect to your network, subject to the following checks - Image: Services Configuration Image: Services Client must have firewall Image: Services Client must have firewall Image: Services Client must have an antivirus application. Image: Services Client must have an antispyware application. Image: Services Check if Antispyware is up to date Image: Services Check if Automatic Updates Image: Services Check if Automatic Updates is enabled on the client Image: Services Check if Automatic Updates is enabled on the client Image: Services Check if Automatic Updates Image: Services Client must have an available security updates installed: Image: Services Client must have checked for new security updates within last: Image: Services Vindows Vista Image: Services Vindows Vista Image: Services Vindows XP	Configuration			
 ☆ Configuration ♥ 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 ♥ Spyware Protection Client must have an antispyware application. Check if Antispyware is up to date ♥ Spyware Protection Client must have an antispyware application. Check if Antispyware is up to date ♥ Soture ♥ Posture ♥ Posture P ♥ Posture S ♥ Audit Sen ♥ Windows 7 ♥ Network ♥ Profiles ♥ Network ♥ Dicies ♥ Network ♥ Divices ♥ Network ♥ Divices ♥ Network ♥ Divices ♥ Divice Sr 	- 🛱 Start Here	Windows 8	Enable checks for Windows 8 Client computers can connect to your network, subject to the following checks -	
 Authentication Authentication Identity	- 🛱 Services	🛱 Configuration	Firewall	
 Lidentity Single Sig Local User Endpoints Static Hos Roles Roles Role Mapp Posture Posture Posture S Audit Sen Windows 7 Vinus Protection or security updates installed: Important and above < Client must have all available security updates within last: 22 hours Audit Sen Vindows 7 Windows 7 Windows 7 Windows 7 Windows 7 Vindows Vista Vindows XP Device Gr 	- Authentication		Client must have firewall enabled on the client	
Client must have an antivirus application. Check if Antivirus is up to date Client must have an antispyware application. Check if Antispyware is up to date Static Hos Client must have an antispyware application. Check if Antispyware is up to date Client must have an antispyware application. Check if Antispyware is up to date Client must have an antispyware application. Check if Antispyware is up to date Client must have an antispyware application. Check if Antispyware is up to date Check if Automatic Updates Check if Automatic Updates is enabled on the client Client must have all available security updates installed: Client must have all available security updates within last: Additional sources required in your deployment: Windows Vista Windows XIP Check if Automatic Updates Client must have all available security updates within last: Client must have checked for new security updates within last: Client must have checked for new security updates within last: Client must have all available services Windows Vista Windows XIP Client must have all available security updates within last: Client must have all available security updates within last: Client must have checked for new security updates within last: Client must have checked for new security updates within last: Client must have antispyware update Services Windows Vista Windows XP Client must have antispyware application. Client must have antispyware applicatintent application.	E- 🚨 Identity		✓ Virus Protection	
 Clocal User C Endpoints C Endpoints Static Hos Roles Role Mapp Posture Posture S Audit Sen Mindows 7 Windows Vista Windows Vista Windows XP Network Device 6n 	- 🗘 Single Sigi		Client must have an antivirus application.	
Client must have an antispyware application. Check if Antispyware is up to date Client must have an antispyware application. Check if Antispyware is up to date Check if Automatic Updates Check if Automatic Updates is enabled on the client Check if Automatic Updates is enabled on the client Check if Automatic Updates Check if Automatic Updates is enabled on the client Check if Automatic Updates Check if Automatic Updates is enabled on the client Client must have all available security updates installed: Client must have all available security updates within last: Additional sources required in your deployment: Windows Vista Windows Vista Windows XP O Devices of Check if Automatic Updates Check if Automatic Updates Check if Automatic Updates Check if Automatic Updates is enabled on the client Client must have all available security updates within last: Additional sources required in your deployment: Windows Vista Windows XP O Norther Automatic Updates Check if Automatic Updates Client must have checked for new security updates within last: Additional sources required in your deployment: Windows Update Windows Vista Windows XP O Check if Automatic Updates Check if Automatic Updates Client must have checked for new security updates within last: Additional sources required in your deployment: Windows Update Check if Automatic Updates Client must have checked for new security updates Client must have checked for new	- Q Local User		Spyware Protection	
C Static Hos C Roles C Role Mapp C Role Mapp Posture Posture S C Posture S C Posture S C Audit Sen Vindows 7 Windows Vista Windows Vista Windows XP Vindows XP O	- 🛱 Endpoints		Client must have an antispyware application. Check if Antispyware is up to date	
CRoles CRoles CRoles CRoles CRoles Check if Automatic Updates is enabled on the client Check if Automatic Updates is enabled on the client Check if Automatic Updates Check if Automatic Updates is enabled on the client Posture Posture S Audit Sen Audit Sen Vindows 7 Windows Vista Windows XP O Devices Device Gr	- Static Hos			
→ C Role Mapp → Posture → Posture → Posture P → Posture S → Audit Sen → A Audit Sen → Mindows 7 → Policies → Windows Vista → Policies → Windows XP → Devices Gr → Network	- C Roles		Check if Automatic Undates is enabled on the client	
 Posture Posture P Posture P Posture S Client must have all available security updates installed: Client must have all available security updates installed: Client must have checked for new security updates within last: Additional sources required in your deployment: Windows Vista Windows XP Windows XP 	Role Mapp			
Posture P Audit Sen	- 🕆 Posture		Security Updates	
Posture S Audit Ser Audit Ser Audit Ser Windows 7 Windows 7 Windows Vista Windows XP O Policies Audit Ser A	- 🌣 Posture P		Client must have all available security updates installed: Important and above	
Additional sources required in your deployment: Windows verver opdate services Windows 7 0 Windows 7 0 Windows Vista 0 Windows XP 0 Windows XP 0	- O Posture S		Client must have checked for new security updates within last: 22 hours	
Image: Second	- Q Audit Serv	and the second	Additional sources required in your deployment:	
Policies Windows Vista Vindows XP	Enforcement	Windows 7		
Profiles Windows XP O	- O Policies	Windows Vista		
	- O Profiles	Windows XP	b	
	- • Network			
- Xî Device Gri	- 🛱 Devices			
	- 🛱 Device Gro			

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.

APURA networks		ClearPass Policy Manager	<u>Support</u> <u>Help</u> admin (Super Admin
Dashboard	O Configuration » Posture »	Posture Policies » Add	
Monitoring	• Posture Policies		
Configuration	O Policy Posture Plu	igins Rules Summary	
- 🎝 Start Here	Rules Evaluation Algorith	nm: First applicable	
🛱 Services 🗊 କ Authentication	Conditions		Posture Token
🖃 🧟 Identity	Add Rule	Move Up Move Down	Edit Rule Remov
- 🛱 Single Sign-On (SSO)			0
- 💭 Local Users	Rules Editor		
- g Endpoints	Conditions		
- 🛱 Roles	Select Plugin Checks:	Passes all SHV checks	
🔄 🛱 Role Mappings	Select Plugins:	✓ Windows System Health Validator ✓ Windows Security Health Validator	
- 🙀 Posture Policies	Actions		
- 🗘 Posture Servers - 🛱 Audit Servers	Posture Token:	HEALTHY (0)	
Enforcement			
- 🛱 Policies			Save Cancel
- 🛱 Profiles			
🖃 📫 Network			

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.

APURA networks		ClearPass Policy Manager admin (Support Help	
Dashboard (Configuration » Posture » Posture Policies 	Posture Policies » Add	
Configuration	Policy Posture Plu	ugins Rules Summary	
- 🛱 Start Here	Rules Evaluation Algorit	nm: First applicable	
- 🛱 Services 🗄 🔓 Authentication	Conditions Passes all SHV check	S -	Posture Token
Single Sign-On (SSO)	1. Windows System He Windows Security H	alth Validator Iealth Validator	HEALTHY
- C Local Users - C Endpoints	Rules Editor		C Edit Rule Remove R
- C Roles	Select Plugin Checks:	Fails one or more SHV checks	
🎝 Role Mappings 	Select Plugins:		
- 🔅 Posture Policies - 🎇 Posture Servers	Actions		
Audit Servers	Posture Token:	QUARANTINE (20)	
- 🛱 Policies 🎝 Profiles			Save Cancel
- + Network			

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

networks	ClearPass Policy Manager			Support Help admin (Super Admin	
Dashboard O Monitoring O	Configuration » Posture » Po Posture Policies - S	sture Policies » Ed SKM Wired C	it - SKM Wired Onboard Pos Inboard Posture ch	ture check eck	
🖧 Configuration 📀	Summary Policy	Posture Plugins	Rules		
	Policy: Policy Name: Description: Posture Agent: Host Operating System: Restrict by Roles: Posture Plugins: The list of selected olugins	SKM Wired Onbo Supplicant WINDOWS	Nules		
- 🗘 Roles	Plugin Name			Plugin Configuration	Status
Role Mappings Posture Posture Policies	Windows System Hea Windows Security Hea	lth Validator alth Validator		View View	Configured Configured
Posture Servers	Rules Evaluation Algorithm	: First applicable			
Contract Servers Servers Servers Servers Contract Servers Contract Servers Contract Servers Contract Servers Servers Contract	Conditions Passes all SHV checks 1. Windows System Heal Windows Security Heal	th Validator			Posture Token HEALTHY
Network	Fails one or more SHV or 2. Windows System Heal Windows Security Hea	thecks - th Validator alth 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.

APURA networks		ClearPass Guest	Support Help Log admin (IT Administrate
鸋 Guest 🔹 🛛		HTML template code displayed while the login attempt is in progress.	
Onboard + WorkSpace O	* Login Delay:	5	
🔦 Configuration 📀	Network Login Access		
🗕 🤿 Start Here 🛕	Controls access to the log	in page.	
 Advertising Authentication Ontent Manager 	Allowed Access:		
🗉 🚺 Digital Passes		Enter the IP addresses and networks from which logins are permitted.	
— 🙀 Email Receipt — 🌆 Fields — 🛐 Forms & Views	Denied Access:		
- 🛒 Guest Manager		Enter the IP addresses and networks that are denied login access.	
- Suest Self-Registration	* 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	successfully a astrenutation.	
- 🚺 Manage Customer Info - 💿 Manage Hotspot	Health Check:	Require a successful OnGuard health check If science, the quart will be required to an enter the 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.

A n e	tworks		ClearPas	s Policy Manager	r	<u>Support</u> <u>Help</u> <u>L</u> admin (Super Administr
	Dashboard O	Configuration » Enforcemen	t » Policies » Edit - S	KM_Wired Onboarding Onboard	Provisioning Policy	
	Monitoring O	Enforcement Polic	ies - SKM_Wi	red Onboarding Onb	oard Provision	ing Policy
å	Configuration 💿	Summary Enforcem	ent Rules			
-Q	Start Here	Name:	SKM_Wired Onboar	ding Onboard Provisioning Polic		
₩	Authentication	Description:	Enforcement polic access for device	y controlling network		
- - 2	Identity	Enforcement Type:	RADIUS			
	–ଫ୍ଲ Single Sign-On (SSO) –ଫ୍ଲ Local Users	Default Profile:	[Deny Access Prof	ile] View Details	Modify	Add new Enforcement Pi
	–🛱 Endpoints					
	tworks Dashboard Monitoring Configuration I Start Here Rules Editor	Configuration » Enforce Enforcement P Summary Enfo	Clear ement » Policies » olicies - SKM rcement Rules	rPass Policy Ma Edit - SKM_Wired Onboardin I_Wired Onboardin	nager g Onboard Provision g Onboard Pr	Support I He admin (Super ng Policy rovisioning Policy
	Conditions	112				
	Type	naitions:	lame	Operat	tor	Value
	1. Authentication	So	urce	EQUALS		[Onboard Devices Repository]
	2. Posture	▼	plied Policy	▼ EQUALS	*	SKM Wired Onboard Post
8						
	Enforcement Profiles					
Ξ	Profile Names:	[RADIUS] [Allow Access Prof [RADIUS] Wired Onboarding (le] Dnboard Post-Prov	Move Up Move Down Remove		
E.		Select to Add	Ŧ			

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

networks	ClearPass Policy Manager	Support Help Lo. admin (Super Administra
Dashboard	Configuration » Enforcement » Policies » Edit - SKM_Wired Onboarding Onboard Provisioning Policy	
Monitoring	Enforcement Policies - SKM_Wired Onboarding Onboard Provisioning Poli	icy
Configuration	Summary Enforcement Pules	
- 🖧 Start Here - 🛱 Services 🗊 🗣 Authentication	Rules Evaluation Algorithm: Select first match Select all matches Enforcement Policy Rules:	
Q Identity	Conditions Actions	
Single Sign-On (SSO)	1. (Authentication:OuterMethod EQUALS EAP-TLS) [RADIUS] [Allow Access Pro AND (Posture:Applied Policy EQUALS SKM Wired Onboard Posture check) Onboard Post-Provisioning	file], [RADIUS] Wired Onboarding
- 🛱 Local Users	2. (Authentication:Source EQUALS [Onboard Devices Repository]) [RADIUS] [Allow Access Pro AND (Posture:Applied Policy EQUALS SKM Wired Onboard Posture check) Onboard Post-Provisioning	file], [RADIUS] Wired Onboarding
- 💭 Static Host Lists	3. (Authentication:Source NOT_EQUALS [Onboard Devices Repository]) [Allow Access Profile], Wire Provisioning	d Onboarding Onboard Pre-
- 🛱 Roles - 🎝 Role Mappings	Add Rule Move Up Move Down	Edit Rule Remove Rule
🖃 📅 Posture		

5.8.2.4 Modify the Wired Onboard Provisioning Service

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



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

APUPA networks		ClearPass Policy Manager	<u>Support</u> <u>Help</u> admin (Super Admin
Dashboard C	Configuration » Services » I	Edit - SKM_Wired Onboarding Onboard Provisioning	
Monitoring C	Services - SKM_W	ired Onboarding Onboard Provisioning	
👶 Configuration 🛛 🖸	Summary Service	Authentication Roles Posture Enforcement	
- 🛱 Start Here	Posture Policies:		
	Posture Policies:	Only NAP agent type Posture Policies are applicable for this service	
E Q Identity	<	SKM Wired Onboard Posture check	Add new Postu
-🛱 Single Sign-On (SSO)	200 	View Details Modify	
- Cocal Users			
		Select to Add	
Boles	Default Posture Token:	UNKNOWN (100)	
Role Mappings	Remediate End-Hosts:	Enable auto-remediation of non-compliant end-hosts	
E TPosture	Remediation URL:		
- 🛱 Posture Policies	Posture Servers:		
- 🛱 Posture Servers	Posture Servers:	Remove	Add new Postur
- 🛱 Audit Servers		View Details	
Enforcement		- Modify	
- Olicies		Select to Add	
-II Profiles			

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

ARUBA networks		ClearPass Policy Manager		<u>Support</u> <u>Help</u> <u>Lo</u> admin (Super Administra	
Dashboard O Monitoring O	Configuration » Services » Ed Services - SKM_Wi	lit - SKM_Wired Onboarding Onboard Provisioning red Onboarding Onboard Provisior	ing		
🔏 Configuration 📀	Summary Service	Authentication Roles Posture Enforce	ment		
- 🛱 Start Here	Use Cached Results:	Jse cached Roles and Posture attributes from p	evious sessions		
Authentication	Enforcement Policy:	SKM_Wired Onboarding Onboard Provisioning	Modify	Add new Enforcement Po	
🔄 🚨 Identity	Enforcement Policy Details				
Single Sign-On (SSO)	Description: Enforcement policy controlling network access for device provisioning				
- O Local Users	Default Profile: [Deny Access Profile]				
- Ctatic Leat Lista	Rules Evaluation Algorithm:	first-applicable			
- Q Roles	Conditions		Enforcement Profiles		
Role Mappings	(Authentication 1, <u>AND</u> (Posture:Applic check)	n:OuterMethod EQUALS EAP-TLS) ed Policy EQUALS SKM Wired Onboard Posture	[Allow Access Profile], Wire Provisioning	d Onboarding Onboard Post-	
— 🛱 Posture Policies — 🛱 Posture Servers	(Authentication:Source EQUALS [Onboard Devices Repository]) 2. AND (Posture:Applied Policy EQUALS SKM Wired Onboard Posture check)		[Allow Access Profile], Wire Provisioning	d Onboarding Onboard Post-	
Audit Servers	3. (Authentication 3. Repository])	3. (Authentication:Source NOT_EQUALS [Onboard Devices Repository])		d Onboarding Onboard Pre-	
– 🎝 Policies – 🎝 Profiles					

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.

APURA networks	ClearPass Guest
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.

	🥑 🛄 🌖 🖓 🗢 Untitled - P	aint		A DESCRIPTION OF TAXABLE PARTY.				×
4	Home View							۷
	Paste Copy Copy Cimboard	rop esize otate *		→ ♥ Outline ▼ ▼ ▲ Fill ▼ ▼ Size ▼	Color 2 Colors	Edit colors		
	CleanDers Dalia, Manage	N 1 N/sh Lasis /Canad	E Mart W	-	Colors			
	ClearPass Policy Manage	× 🙇 Web Logins	🗙 🙏 Register Your D	levice ×		_		
		'10.255.95.251/guest/d	evice_provisioning.php				ź	3
	🔛 Apps 🚺 Suggested Sites	Alcatel-Lucent Payr	🗋 Alcatel-Lucent Payr	ALCATEL-LUCENT	🛛 🕙 Google 🗋 Introduction	🕢 NSA Implementatio	🕖 NSA Implementatio	
	ARUBA		Clear	Pass Onboard + V	VorkSpace			
	networks							
	A In order to connect to t	his network, your device m	ist be configured for enhanced	d security, Aruba Networks' OuickC	onnect application will quide vo	u through the configuration	process.	
							5010100	
	Login below using yours	Alcatel-Lucent credentia	IS. 0					
1	Register Y	our Device						
	* Username:							
	Password:							
		gin						
	"" required field							
	Contact a staff member	if you are experiencing	difficulty logging in.					
								ш
C								_
-	<			m				•
	+ 218, 495px 1⊡ :	196 × 38px 1 □ 1	280 × 1024px			1	.00% 🕞 —— 🗍 ——	٠
6	9 🙆 👩 📜		🖭 🔼 🧭				- 🛱 🔁 🔶 🛄	3 AM /2014

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

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

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

