Integration with Aruba ClearPass

Table of Contents

Typical Connection Workflows in Enterprise Wi-Fi	1
802.1x Authentication of Enterprise Users on Enterprise Devices	1
Employee-Owned Devices	2
Guest Users	3
A Wi-Fi Policy	
Case 1: Enterprise 802.1x Authentication Using PEAP	4
CloudVision Cognitive Unified Edge Configuration	4
RADIUS Profile	5
802.1x SSID Settings	5
ClearPass Configuration	6
Arista APs as RADIUS Clients	6
Active Directory	7
Create a Service	8
Case 2: Enterprise 802.1x Authentication Using EAP-TLS	8
CloudVision Cognitive Unified Edge Configuration	9
RADIUS Settings	
Role Profiles	
Vendor Specific Attribute	11
ClearPass Configuration	12
Arista APs as RADIUS Clients	12
Active Directory	12
Certificate Authority	13
Certificate-Onboarding Portal	13
Role-Based Access Control	14
Approaches to Guest User Onboarding	
Guest User Onboarding Using Role Profiles	17
CloudVision Cognitive Unified Edge Configuration	18
ClearPass RADIUS Profile	18
Pre-Authentication Role	19
Post-Authentication Role	20
RADIUS MAC Authentication and Role-Based Control	21
ClearPass Configuration	22
Enforcement Profiles and Policies	
Web Authentication Service	
External Captive Portal with RADIUS Authentication	27
CloudVision Cognitive Unified Edge Configuration	
ClearPass Configuration	
Guest Portal Configuration	29



Guest Access Control	0
----------------------	---



Integration with Aruba ClearPass

This site will be decommissioned on October 15, 2024. All content is migrated to Arista Community Central. Visit Arista Community Central for help articles and community engagement discussions on the complete range of Arista products.

This document describes how Arista Wi-Fi works with Aruba ClearPass to onboard Wi-Fi clients and keep enterprise Wi-Fi networks secure. The first section describes the different Wi-Fi client types in an enterprise environment and the typical connection workflows for these clients. The second section defines a Wi-Fi policy based on the workflows. Subsequent sections describe how to configure Arista CloudVision Cognitive Unified Edge and ClearPass to implement the Wi-Fi policy.

Typical Connection Workflows in Enterprise Wi-Fi

A typical enterprise network offers Wi-Fi access to the following types of client devices:

- 1. **Enterprise-owned** devices (typically laptops): Assets of the enterprise that are issued typically by its IT team to its employees and are part of the domain.
- 2. **Employee-owned** (or BYOD, typically smartphones): Not assets of the enterprise, but employee-owned devices used to connect to the enterprise Wi-Fi network.
- 3. **Guest**-user devices (laptops or smartphones): Owned by visitors who might want to connect to the enterprise Wi-Fi network as guests.

Based on the device type, enterprises want to restrict or allow access to parts of their network. Consider a corporate Wi-Fi network with two SSIDs: a "Corporate" SSID for employees and a "Guest" SSID for visitors. Below are the high-level steps for how each client device type connects to this network.

802.1x Authentication of Enterprise Users on Enterprise Devices

- The employee usernames and passwords are defined in Active Directory (AD).
- The wireless MAC addresses of the enterprise-owned devices are entered in ClearPass.

Enterprises typically use 802.1x authentication with PEAP (MSCHAPv2) for onboarding of clients using enterprise-owned devices onto the intranet, i.e., the corporate VLAN.

The following figure shows the workflow.



- 1. The client sends an 802.11 Association Request for access to the corporate SSID.
- 2. The Arista access point (AP) sends an EAP Identity Request to the client, which responds with an EAP Identity Response message.
- 3. The AP then sends a RADIUS Access-Request message to ClearPass. This message identifies the security mechanism (PEAP MSCHAPv2) and the corporate intranet VLAN to which the SSID is mapped.
- 4. ClearPass generates and sends a RADIUS-Challenge to the AP. The AP sends an EAP Challenge to the client, which responds with an EAP Response.
- 5. The AP passes on the client's response to ClearPass via a RADIUS Access-Request. ClearPass queries its database to verify the response.
- 6. Once the response is verified, ClearPass sends a RADIUS Access-Accept to the AP. The AP sends an 802.11 Association Response to the client, granting it access to the network.

Employee-Owned Devices

Employee-owned devices can connect to the network using any of the following methods:



- 802.1x authentication (with any type of EAP)
- Central web authentication (similar to the External Captive Portal with RADIUS method described later)
- A hybrid solution (802.1x authentication with some web sign-in or an "Accept" click for terms and conditions).

Guest Users

Guest users connect to the "Guest" SSID. A typical process is as follows:

- 1. Guest SSIDs are typically "Open."
- 2. Visitors register at the front desk and receive a Guest-Wi-Fi PIN or password.
- 3. On connecting to the "Guest" SSID, visitors get Internet access by entering the PIN/password on a captive portal page. Alternatively, they might first connect to the "Guest" SSID, self-register, and get login credentials via email.



ClearPass supports this workflow using a standard protocol called WISPr.

As shown in the figure above, the guest user workflow consists of the following steps:

- 1. The guest Wi-Fi client connects to an SSID and attempts to access a URL on the internet.
- 2. The AP redirects the client to the portal page configured in ClearPass.
- 3. The guest user enters the username/password in the portal and submits the page to ClearPass.
- 4. Clearpass encodes the password (using the portal secret configured in CloudVision Cognitive Unified Edge) and redirects the client web browser to the AP with the username and the encoded password



included as URL arguments.

- 5. The AP decodes the password and sends a RADIUS Access-Request message to ClearPass with the username and password.
- 6. ClearPass responds with a RADIUS Access-Accept message granting guest access and the client is connected.

A Wi-Fi Policy

We can now define a Wi-Fi policy based on the workflows described above. The way to differentiate between the use cases is to define a Role for each device type.

Device Type	Description	SSID	Role Name	Authentication Method	Traffic VLAN
Enterprise-owned (MAC entered in RADIUS)	Enterprise-owned devices.	Corporate	Role-Onboard	PEAP	VLAN1
User-Owned (MAC NOT entered in RADIUS)	Employee-owned devices.	Corporate	Role-BYOD	PEAP	VLAN2
Guest	Visitor/Guest-owned devices.	Guest	Role-Guest	WISPr/802.1x	Guest VLAN

Note: The table shows three roles on a single SSID, but you can define roles across multiple SSIDs as well.

Thus, based on the device type (mapped to a Role), users can connect to different SSIDs, use different Authentication Methods, and are assigned different VLANs. This allows you to control access for each role. So, for example, once BYOD devices are mapped to a separate VLAN, their bandwidths can be capped, and they can be restricted to access only the internet and not the internal enterprise resources.

The next sections describe how you can implement this policy on Arista CloudVision Cognitive Unified Edge and ClearPass for two use cases of the Corporate SSID. The last section describes the process for the Guest SSID.

Case 1: Enterprise 802.1x Authentication Using PEAP

This section describes how to configure CloudVision Cognitive Unified Edge and ClearPass to implement the PEAP (MSCHAPv2) based 802.1x authentication workflow for Enterprise-owned devices described earlier.

CloudVision Cognitive Unified Edge Configuration

This section describes the steps to configure CloudVision Cognitive Unified Edge for 802.1x authentication of corporate users



RADIUS Profile

Under Configure > WiFi > RADIUS profile, select "Add RADIUS Server" and enter the ClearPass server details as shown in the following figure.

Wi-Fi SSID RADIUS Tunnel Interface Role Profile Radio Settings Device Settings Image: Clear Pass RADIUS Server Clear Pass RADIUS Server Clear Pass RADIUS Server Clear Pass RADIUS Server IP Address * 123.123.12.112 Authentication Port * Accounting Port * Shared Secret * 1812 11.655.251 1813 11.655.251 Image: Clear Pass Page Port *	Location	5						
ClearPass RADIUS Server RADIUS Server Name * ClearPass RADIUS Server IP Address * 123.123.12.112 Authentication Port * Accounting Port * Shared Secret * 1812 L4655351	Wi-Fi	SSID	RADIUS	Tunnel Ir	nterface	Role Profile	Radio Settings	Device Settings
ClearPass RADIUS Server RADIUS Server Name* ClearPass RADIUS Server IP Address* 123.123.12.112 Authentication Port* Accounting Port* Shared Secret* 1812 U655351 1813 U655351								
ClearPass RADIUS Server	ClearPa	ass RADI _{lame} *	US Serve	r				
IP Address * 123.123.12.112 Authentication Port * Accounting Port * Shared Secret * 1812 1813 181	ClearPass RAD	IUS Server						
IP Address * 123.12.3.12.112 Authentication Port * Accounting Port * 1812 • (1-655351) 1813 • (1-655351)								
123.123.12.112 Authentication Port * Accounting Port * Shared Secret * 1812 11-655351 1813 11-655351	IP Address *							
Authentication Port * Accounting Port * Shared Secret *	123.123.12.112	2						
1812 1 [1-65535] 1813 1 [1-65535]	Authenticatio	n Port *	Acc	ounting Po	ort *	Shared	Secret *	
	1812 🗘	[1-65535]	18	13 🗘	[1-65535]			۲

802.1x SSID Settings

Under Configure > WiFi, add a new SSID or modify an existing one to support 802.1x authentication. To do so, go to the Security tab of the SSID, select the "WPA/WPA2 Mixed Mode" option, and enable 802.1x. Select the appropriate ClearPass servers under the Primary and Secondary tabs in the RADIUS Settings. The following figure shows an example.

WiFi - SSID RADIUS Tunnel Interface	Role Profile Radio Settings Device Settings	
	Changes to this SSID will a	flect all groups and folders that use this SSID. See groups and folders using
⊕ ABC Corp	Basic Security Network	
Select Security Level for Associations		
WPA/WPA2 Mixed Mode	○ PSK	
RADIUS Settings		
Primary Secondary		
Authentication Server *	Accounting Server	
ClearPass 👻	ClearPass 👻	
Add/Edit	Add/Edit	
Retry Parameters		
Attempts *	Timeout *	
4 8 [1-10]	2 🗘 seconds [1 - 10]	
Called Station/NAS ID		
Called Station ID *	NAS ID *	%m - Access Point's Ethernet MAC
5im/Sia	Sm-Sa	%s - SSID %n - Device Name %i - Location Tag

ClearPass Configuration

Typical enterprise networks integrate the ClearPass RADIUS server with an Active Directory, although they could use ClearPass itself as a username and password store. The process below describes the Active Directory case.

Broadly, configuring ClearPass for user and client onboarding consists of the following steps:

- 1. Add Arista APs as authorized ClearPass RADIUS clients.
- 2. Point ClearPass to the Active Directory.
- 3. Create a Service that uses PEAP as the Authentication method and points ClearPass to the Arista SSID.

Each of the steps is described in detail below.

Arista APs as RADIUS Clients

Note: The steps below assume that ClearPass RADIUS has been installed in the network.

You can add Arista APs as authorized clients of ClearPass RADIUS under **Configuration > Network > Devices** in the ClearPass Policy Manager as shown below. Click **Add** and the Add Device window appears. Enter the Arista AP information in the Name, IP or Subnet Address, Description (optional), and the RADIUS

Shared Secret fields of the Add Device window. The other fields use default values.



Active Directory

Note: The steps below assume that ClearPass RADIUS has been installed in the network and is able to access the Active Directory (AD) username and password store.

You can point ClearPass to the AD under **Configuration > Authentication > Sources > Add** as shown below.

ClearPass Policy Manager						
Configuration » Authentication » Sources » Add						
Authentication Sou	irces					
General Primary	Attributes Summary					
Name:						
Description:						
Type:	Active Directory \$					
Use for Authorization:	Enable to use this Authentication Source to also fetch role mapping attributes					
Authorization Sources:	Remove View Details					
	Select +					
Server Timeout:	10 seconds					
Cache Timeout:	36000 seconds					
Backup Servers Priority:	Add Backup Remove					



Create a Service

Finally, under **Configuration > Services**, create a Service that uses PEAP-MSCHAPv2 as the authentication method and points ClearPass to the Arista SSID. Set the NAS Identifier to the Arista "Corporate" SSID.

Case 2: Enterprise 802.1x Authentication Using EAP-TLS

This section describes how to configure CloudVision Cognitive Unified Edge and ClearPass to support Enterprise 802.1x Authentication, i.e., the onboarding of users connecting to the Corporate SSID, using EAP-TLS.

Enterprise-Owned Client	Arist	ca AP C	learPass
PEAP (First attempt)			
1. PEAP-based	authentication request	Credentials	
		Success: Enterprise-owned device	MAC matches that of an "enterprise-owned" device
•		2. Redirect to ClearPass-hosted certificate portal	>
3. Insta	II EAP-TLS Certificate		
EAP-TLS (Subsequ	ent Attempts)		
EAP-TLS Authenticat	ion for Subsequent Attempts		

As shown in the preceding figure, the onboarding process broadly consists of three steps:

- 1. When an enterprise-owned client device first attempts to connect to the Corporate SSID, it does PEAPbased authentication with the RADIUS server. The RADIUS server has the client MAC address and therefore recognizes it as an enterprise-owned device.
- 2. The Arista AP redirects the client to a portal hosted on ClearPass, from where the user can install an EAP-TLS certificate on the client. (See Appendix for steps on how to install the certificate on a client.)
- 3. Once the certificate is installed on the client, subsequent connections of this client to the SSID use EAP-TLS.

A key difference between PEAP and EAP-TLS is that PEAP uses only a server-side certificate and EAP-TLS uses both server-side and client-side certificates. With the client-side certificate, EAP-TLS adds another layer of protection to the user's password. Access to a user's password is no longer enough to break into the network; the client also needs to have a valid certificate.



CloudVision Cognitive Unified Edge Configuration

Broadly, configuring CloudVision Cognitive Unified Edge to work with ClearPass consists of three steps:

- 1. Point the Arista APs to the ClearPass RADIUS server.
- 2. Define Role Profiles corresponding to the roles in the Wi-Fi policy described above.
- 3. Configure Role-Based Access Control, wherein you define the Vendor Specific Attributes (VSA) that ClearPass will use to communicate roles in the RADIUS response.

Each of the steps is described in detail below.

RADIUS Settings

 Under Configure > RADIUS, create a RADIUS object and enter the details of the ClearPass RADIUS server, including the IP address and the Shared Secret. Note: Enter the same Shared Secret in ClearPass RADIUS settings when you define Arista APs as ClearPass RADIUS clients (see the Corporate SSID: ClearPass Configuration section).

Locations							
Wi-Fi	SSID	RADIUS	Tunnel Interface	e Role Pr	ofile Radio S	ettings Device	e Settings
ClearPas	ss RADIU	S Serve	r				
ClearPass RADI	US Server						
IP Address *							
123.123.12.112							
Authentication	Port * [1-65535]	Acc 18	ounting Port *	35]	Shared Secret *	4	D

2. Add the ClearPass RADIUS server to the **SSID > Security** tab.

WiFi - SSID RADIUS Tunnel Interface	Role Profile Radio Settings Device Settings	
	Changes to this SSID will affect all groups and t	biders that use this SSID. See groups and folders using
⊕ ABC Corp	Basic Security Network	
Select Security Level for Associations		
WPA/WPA2 Mixed Mode	○ PSK	
RADIUS Settings		
Primary Secondary		
Authentication Server *	Accounting Server	
ClearPass 👻	ClearPass 👻	
Add/Edit	Add/Edit	
Retry Parameters		
Attempts *	Timeout *	
4 🗢 [1-10]	2 🗢 seconds [1 - 10]	
Called Station/NAS ID		
Called Station ID *	NAS ID *	%m - Access Point's Ethernet MAC
%m-Na	Similia	%s - SSID %n - Device Name %i - Location Tag

Role Profiles

Under **Configure > Role Profile**, add the Role Profiles shown below.

Locations		
WI-FI SSID RADIUS Tunnel I	nterface Role Profile Radio Settings	Device Settings
•		
10	10	10
Role-TLS	Role-Onboard	Role-BYOD
Profile Name : Custom-1 Inherit From SSID : No VLAN : Enabled - 10 Location : //Locations Finewall : Disabled	Profile Name : Custom-2 Inherit From SSID : No VLAN : Enabled - 20 Location : //Locations Firewall : Disabled	Profile Name : Custom-3 Inherit From SSID : No VLAN : Enabled - 30 Location : //Locations Firewall : Disabled
Bandwidth : Disabled Redirection : Disabled	Bandwidth : Disabled Redirection : Enabled	Bandwidth : Disabled Redirection : Disabled



The table below shows what you need to define within each Role Profile.

Role Name	VLAN ID	Redirection
Role-TLS	VLAN 1	Disabled
Role-Onboard	VLAN 2	 Enabled In the Redirect URL field, enter the IP/URL of the ClearPass certificate- onboarding portal where you want to redirect users. Enable HTTPS Redirection Under Websites that can be accessed before authorization, enter the IP/URL of the ClearPass certificate-onboarding portal and enter www.apple.com
Role-BYOD	VLAN 3	Disabled

This configuration supports the workflow described earlier. When an enterprise-owned client first connects to the SSID, it authenticates using PEAP and is assigned "Role-Onboard". This causes the client to be redirected to the ClearPass certificate-onboarding portal, from where it installs the EAP-TLS certificate. The next time it connects to the SSID, it uses EAP-TLS and is assigned "Role-TLS".

When a BYOD client connects to the SSID, it authenticates using PEAP and is simply put on a different VLAN.

Vendor Specific Attribute

Under **SSID > Access Control**, enable Role-Based Access Control, and enter the RADIUS Vendor-Specific Attribute (VSA) details as shown below. ClearPass uses the VSA to return a role in the RADIUS "Access Accept" message.





ClearPass Configuration

Typical enterprise networks integrate the ClearPass RADIUS server with an Active Directory, although they could use ClearPass itself as a username and password store. The process below describes the Active Directory case.

Broadly, configuring ClearPass for user and client onboarding consists of the following steps:

- 1. Add Arista APs as authorized ClearPass RADIUS clients.
- 2. Point ClearPass to the Active Directory.
- 3. Define a new Certificate Authority.
- 4. Create a Certificate-Onboarding Portal, from where the user installs the client-side certificate.
- 5. Define the Role-Based Access Control mechanism.
- 6. Create a Service tying all the above steps together and pointing ClearPass to the Arista SSID.

Each of the steps is described in detail below.

Arista APs as RADIUS Clients

Note: The steps below assume that ClearPass RADIUS has been installed in the network.

You can add Arista APs as authorized clients of ClearPass RADIUS under **Configuration > Network > Devices** in the ClearPass Policy Manager as shown below. Click **Add** and the Add Device window appears. Enter the Arista AP information in the Name, IP or Subnet Address, Description (optional), and the RADIUS Shared Secret fields of the Add Device window. The other fields use default values.

aruba	ClearPass Policy Manager	Support I they I Logond scalarst (Natural Administrator)
Benhovel Machaning Generating	Configuration + Network + Devices Network Devices	Ant
O Start Here O Services Services Services Services Services Services	Filter Name	Show 10 * recents
Comparison C	1 Add Device 0 2 0 Add Device 0 3 0 0 0 0 4 0 Name Add AP 0 5 0 0 0 0 0 6 0 0 0 0 0 0 6 0 0 0 0 0 0 0 0 7 0 Add Device 0	Copy Export Onists

Active Directory

Note: The steps below assume that ClearPass RADIUS has been installed in the network and is able to access the Active Directory (AD) username and password store.

You can point ClearPass to the AD under **Configuration > Authentication > Sources > Add** as shown below.



ClearPass Policy Manager								
Configuration » Authenticat	ion » Sources » Add							
Authentication Sou	Irces							
General Primary	Attributes Summary							
Name:								
Description:								
Type:	Active Directory \$							
Use for Authorization:	Enable to use this Authentication Source to also fetch role mapping attributes							
Authorization Sources:	Remove View Details							
	Select \$							
Server Timeout:	10 seconds							
Cache Timeout:	36000 seconds							
Backup Servers Priority:	Move Up Move Down Add Backup Remove							

Certificate Authority

Note: The steps below assume that Certificate Authority (CA) certificates have been installed in ClearPass RADIUS to support certificate-based transactions.

Go to Home > Onboard > Certificate Authorities and follow the "Create new certificate authority" wizard shown below.

😫 Guest 🛛 0	Home + Onboard + Certificate Authorities	0	
Onboard O	Certificate Authorities	Create new certificate authority	
- Start Here - 6 Certificate Authorities	Use this list to manage certificate authorities.		

This video by ClearPass explains the process.

Certificate-Onboarding Portal

The next step is to create the certificate-onboarding portal. WiFi clients will be redirected to this portal to generate and install client certificates for EAP-TLS.

To create a portal in ClearPass, you need to create a Configuration Profile followed by a Provisioning Profile. Go to **Onboard > Deployment and Provisioning > Configuration Profile** and follow the "Create new configuration profile" wizard shown below.



🐫 Guest	Home + Onboard + Deployment and Provisioning + Configuration Profiles	
Onboard	Configuration Profiles	Create new configuration profile
- 🛶 Start Here	Use this list to manage conflouration profiler	
- 6 Certificate Authorities	use ons list to manage computation profiles.	

Next, create a Provisioning Profile using the Configuration Profile.

aruba	ClearPass Onboard	Support Help Lo bhupinder.misra (IT Administrat
Guest 0	Home > Onboard > Deployment and Provisioning > Provisioning Settings Provisioning Settings	Create new provisioning settings
- 🛶 Start Here - 👩 Certificate Authorities	Use this list to manage provisioning settings.	

This video by ClearPass explains how to create Configuration and Provisioning Profiles.

Once you have created a Provisioning Profile, it will appear under **Onboard > Deployment and Provisioning > Provisioning Settings**. Click Test to see the configured portal.



You now need to redirect the "Role-Onboard" Wi-Fi users to this portal. To do so, copy the portal URL from the browser. Go to CloudVision Cognitive Unified Edge. Under **Configure > Role Profiles**, select the "Role-Onboard" profile, enable **Redirection**, and paste the URL in the **Redirect URL** field as shown below.

Locations	Search for MAC/ IP Address/User Name/ Device Name.
WI-FI SSD RADIUS Tunnel Interface Role Profile Radio Settings Device Settings	
Changes to this Role Profile will affect all SSIDs that use this I	Iole Profile.
€ Role-Onboard	
Redirection	
Redirect URL * https://ClearPass-Onboard-URL.com	

Role-Based Access Control

The ClearPass workflow to configure Role-Based Access Control consists of the following steps:

- 1. Define the Roles.
- 2. Define a Role Mapping, i.e., a set of conditions that decide which role is assigned.
- 3. Define an Enforcement Profiles, i.e., the actions used to assign roles.
- 4. Define the Enforcement Policy, i.e., the actions that trigger the role assignment.
- 5. Create a Service that ties everything together.



Each step is described in detail below.

1. Create the three Roles under Configuration > Identity > Roles as shown below.

aruba		ClearPass Policy Manager							
Dashboard Monitoring	•	Configuration » Identity » Roles Roles							
		Filter: Name ▲	Role deleted successfully Clear Filter Description						
Gingle Sign-On (SSO) GSO) Gold Users Gold Endpoints Gold Endpoints		3. Role-TLS Showing 1-3 of 3							

2. Under Identity > Role Mappings, define a Role Mapping—a set of conditions that decide which role is assigned to an authenticated client. "Role-Default" is assigned if none of the conditions is met, but this scenario will never arise in our case. Note: The group Corp-Clients (used in Condition #2 below, for the "Role-Onboard" case) is a list of wireless MAC addresses of enterprise-owned devices. You can create this group by entering the MAC addresses of enterprise-owned devices in Configuration > Identity >Static Host Lists.

Dashboard Monitoring	 Configuration >> Ide Role Mapping 	Configuration >> Identity >> Role Mappings >> Edit-Arista-CP-Roles-Mapping Role Mappings - Arista-CP- Roles-Mapping						
Configuration	Summary Polic	cy Mapping Rules						
Start Here Services Services Authentication Methods Sources Sources Single Sign-On (SSO) Cocal Users Cocal Use	Policy: Policy Name: Description: Default Role: Mapping Rules: Rules Evaluation Alg Conditions 1. (Authent 2. (Authent 3. (Authent	Arista-CP-Roles-Mapping Role-Default gorithm: First applicable Exection:OuterMethod EQUALS EAP-TLS) Exection:OuterMethod EQUALS EAP-PEAP) IETF:Calling-Station-Id BELONGS_TO_GROUP Corp-Clients) Exection:OuterMethod EQUALS EAP-PEAP)	Role Name Role-TLS Role-Onboard Role-BYOD					

 Define the three Enforcement Profiles, one for each role. Enforcement Profiles are basically actions—in our case, values that ClearPass RADIUS must return in the "Access Accept" message. You can define Enforcement Profiles under Configuration > Enforcement > Profiles. The "Role-Onboard" profile is shown below; you can similarly define the other two profiles.



aruba		ClearPass Policy Manager							
Dashboard O Monitoring O	Configuration » Enforcement » Profiles » Edit Enforcement Profile - Role-Onboard Enforcement Profiles - Role-Onboard								
Configuration O	Summary Profile	Attributes							
A Pietrious	Profile:								
- La Sources	Name:	Role-Onboard							
Single Sign-On (SSO)	Description:								
The sign of (350)	Type:	RADIUS							
The Endpoints	Action:	Accept							
- The Static Host Lists	Device Group List:	1.Arista APs							
- D Roles	Attributes:								
C Role Mappings	Туре	Name		Value					
🕞 🖶 Posture	1. Radius:Aruba	Aruba-User-Role		Role-TLS					
S Enforcement Olicies Olicies Olicies									

 To associate profiles (actions) to the roles via conditions, define the Enforcement Policy under Configuration > Enforcement > Policies as shown below. Note that the top condition here is that the user's account is disabled in the AD.

aruba	ClearPass Policy Manager						
Dashboard O Monitoring O	Configuration >> Enforcement >> Policies >> Edit - Arista-CP-Roles-Policy Enforcement Policies - Arista-CP-Roles-Policy						
🔗 Configuration 💿	Summ	ary Enforceme	nt Rules				
Methods Sources Sources Identity Gord Users Cocal Users Gord Users	Enforce Name: Descrip Enforce Default Rules: Rules E	ement: otion: ement Type: : Profile: Evaluation Algorithm	Arista-CP-F RADIUS [Deny Acco 1: First appli	oles-Policy ess Profile]			
Role Mappings	Co	nditions			Actions		
🕣 🖶 Posture	1.	(Authorization:	AD-Server:A	ccountStatus EQUALS 66050)	[Deny Access Profile]		
B Enforcement	2.	2. (Tips:Role EQUALS Role-TLS)			Role-TLS		
- 🛱 Policies	3.	(Tips:Role EQU	UALS Role-Onboard)		Role-Onboard		
Profiles	4.	(Tips:Role EQU	JALS Role-B	YOD)	Role-BYOD		

5. Finally, under **Configuration > Services**, create a Service to tie all of this together and point ClearPass to the Arista SSID. As shown below, you need to set the NAS Identifier to the Arista "Corporate" SSID.



Summary Service	Authentication	Authorization	Roles	Enforcement		
Service:						
Name:	Arista-ClearPass	-Integration				
Description:	Arista 802.1 X W	ireless Access Se	rvice			
Type:	802.1X Wireless					
Status:	Enabled					
Monitor Mode:	Disabled					
More Options:	Authorization					
Service Rule						
Match ALL of the followin	g conditions:					
Туре		Name			Operator	Value
1. Radius: IETF		NAS-Port-	Туре		EQUALS	Wireless-802.11 (19)
2. Radius: IETF		NAS-Iden	tifier		EQUALS	Corporate
Authentication:						
Authentication Methods:	1. [EAP PEAP] 2. [EAP TLS]					
Authentication Sources:	AD-Server					
Strip Username Rules:						
uthorization:						
Authorization Details:	AD-Server					
toles:						
Role Mapping Policy:	Arista-CP-Roles-	Mapping				
inforcement:						
Use Cached Results:	Disabled					
Enforcement Policy:	Arista-CP-Roles-	Policy				

Approaches to Guest User Onboarding

Arista WiFi Guest users can be onboarded using one of two approaches:

Using Role Profiles: In this approach, you configure CloudVision Cognitive Unified Edge to assign two roles: a pre-authentication role and a post-authentication role. The pre-authentication role redirects guest clients to a web-authentication portal and the post-authentication role grants access to guest users.

Using Captive Portal: In this approach, you configure a third-party hosted captive portal in CloudVision Cognitive Unified Edge, with the ClearPass web-authentication portal as its splash page. This approach is useful when you want a captive portal experience for guests—a splash page, a landing page, and/or a walled garden of sites that guests can access before authentication. Because the guest role is the only role on the Guest SSID, in this approach you can simply define a "Guest" role in ClearPass and tie it to the Arista WiFi Guest SSID; you need not define any roles in CloudVision Cognitive Unified Edge.

The next two sections describe the steps to configure CloudVision Cognitive Unified Edge and ClearPass for each approach.

Guest User Onboarding Using Role Profiles

The workflow for guest user onboarding using role profiles is shown in the figure below.





- 1. When the client first connects to the SSID, the Wi-Fi access point (AP) sends an Access Request containing the client's MAC address to ClearPass.
- 2. ClearPass responds with an Access-Accept message containing the Pre-Authentication role. The Pre-Authentication role redirects the client to the ClearPass web authentication portal.
- 3. The user enters a username and password into the portal. ClearPass authenticates these credentials and saves the client MAC address against this user (per the MAC Caching configuration).
- 4. ClearPass then sends a Change of Authorization (CoA) message containing the Post-Authentication role to the AP. The AP connects the client to the network.

CloudVision Cognitive Unified Edge Configuration

The CloudVision Cognitive Unified Edge configuration involves pointing CloudVision Cognitive Unified Edge to the ClearPass RADIUS server, defining the two roles (pre-authentication and post-authentication), and configuring role-based control on the SSID.

ClearPass RADIUS Profile

Under Configure > WiFi > RADIUS profile, select "Add RADIUS Server" and enter the ClearPass server details as shown below.



WiFi 🗸	SSID	RADIUS	Tunnel Interface	Role Profile	Radio Settings	Device Settings
😔 Primary /	Auth					
PADIUS Server Nar	me *					
Primary Auth	110					
IP Address *						
10.313150						
Authentication	Port *	Accou	nting Port *	Shared Se	ecret *	
1812 🗘 [[1-65535]	1813	\$ [1-65535]			٢

Pre-Authentication Role

The Pre-Authentication role profile enables redirection to the URL of the ClearPass web authentication portal, as shown below.

Note: You must add the web authentication portal URL, and ports 80 and 443 to the "Websites That Can Be Accessed Before Authorization" list.



-				
Locestone				
WiFi 🛨 ssid radiu	IS Tunnel Interface	Role Profile	Radio Settings	Device Settings
0				
Pre-Authentication				
Pre-Authentication		Use SSID	Settings in Absend	e .
Protie Name		of Role-S	pecific Settings	
				i
Role-Specific Settings				
VLAN				
 Firewall 				
User Bandwidth Control				
Limit the maximum upload bandwi	dth per user to			
Redirection				
Dadiract I DI				
https://loginportal.com				
HTTPS Redirection				
Certificate Information				
Common Name	Organization		Organiza	tion Unit
www.arista.com	Arista Networks		rista Ne	tworks
Websites That Can Be Accessed	Before Authorization			
loginportal.com.80.443 x				

You need to configure ClearPass to return this role in the Access-Accept message it sends to the AP.

Post-Authentication Role

The Post-Authentication role profile defines the connection settings (e.g., VLAN, Firewall rules) for successfully authenticated guest clients.

Loosions			Search for MAC/ IP Address/ User Name/ Device Name.
WiFi - SSO RADUS Turnel Interface	Role Profile Radio Settings Device Setting	28	
Post-Authentication			
Role Name *			
Post-Authentication	Use SSID Settings in Absence		
Profile Name *	of Role-Specific Settings		
Post-Auchenbolistion			
Role-Specific Settings			
VLAN			
VLANID *			
10 0 [0-4094]			
 Firewall 			
User Bandwidth Control			
Limit the maximum upload bandwidth per user to		Limit the maximum download be	ndwidth ger uwr to
and anticide an interview approach and remaining the same of		Land Contract of Contract of Contract of	
Refrection			

You need to configure ClearPass to return this role in the Change Of Authorization (CoA) message it sends to the AP.

RADIUS MAC Authentication and Role-Based Control

The steps to configure RADIUS MAC Authentication and Role-Based Control are:

- Under SSID > Access Control, enable Client Authentication > RADIUS MAC Authentication and select "Disconnect" if authentication fails. This causes the client to disconnect if authentication fails. If authentication succeeds, roles defined in the SSID are applied.
- 2. Next, under RADIUS Settings, select the ClearPass server. **Note**: Set the Calling Station ID to %m-%s (MAC Address and SSID), and the NAS ID to "%s" (only the SSID).
- 3. Finally, enable Role-Based Control on the SSID and assign the two roles via the RADIUS VSA, as shown below.



WiFi - ssid radius	Tunnel Interface	Role Pro	ofile	Radio	Settings	Device Settings	
						Changes to th	is SSID
⊖ ABC Corp Guest		Basic	Secur	ity	Network	Access Control	Capt
Disconnect Stay connected							
✓ Role Based Control							
RADIUS VSA Google OU This	s setting is not edita	ible because	e Client .	Authen	tication via G	Google Integration is di	abled.
Rule Type *	Vendor ID *			Attrib	ute ID *		
Custom RADIUS attributes VSA 🛛 🔻	14823	:	\$	1	\$		(
Operand *	Assign Role *						
Match 💌	Role Name (P	rofile Name	•				
	Search						
Bonjour Gateway	Select All						
Redirection	Arista Pos Authentic Authentic	(Test User F st ation (Post ation)	(ole)				
Blacklisting and Whitelisting of Wi	Fi (Arista Pre (Pre-Auth	-Authentica entication)	ition				

Note: For ClearPass, use Custom RADIUS Attributes, and set Vendor ID to "14823" and Attribute ID to "1".

ClearPass Configuration

The logic behind the ClearPass configuration for role-profile based access is as follows:

- If a device attempts MAC authentication via Arista Wi-Fi and ClearPass has no cached role for the device, then redirect the device to the guest login page.
- Once the user logs in to Guest, set the role to "Guest" and send CoA with the Post-Authentication user role to the AP.



• For subsequent MAC Authentication requests from the same device, assign guest access to the device.

Note:

- The guest SSID configuration described here was implemented with ClearPass version 6.6.10.106403.
- Make sure that the FQDN Certificate is installed on ClearPass before you configure it for guest logins.

To implement this, you need to define the following in ClearPass:

- 1. Enforcement Profiles
- 2. A MAC-Authentication Service
- 3. A Web-Based Authentication Service

Each of these is described in detail below.

Enforcement Profiles and Policies

Enforcement profiles define the actions used to assign roles. The ClearPass configuration needs to be such that once a user is authenticated and is part of Guest user repository, then the following three enforcement profiles are applied:

- 1. Send a RADIUS CoA with the Post-Authentication Role
- 2. Mark the endpoint as "Known endpoint" [Update Endpoint Enown]
- 3. Apply Arista MAC caching

You can define Enforcement profiles under **Configuration > Enforcement > Profiles**. The MAC Caching Enforcement Profile is shown below.

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Arista MAC Caching Enforcement Profiles - Arista MAC Caching						
Summary	Profile	Attributes				
Profile:						
Name:		Arista MAC	Arista MAC Caching			
Description:		Endpoint at	Endpoint attribute updates for Employee			
Type:		Post_Authe	Post_Authentication			
Action:						
Device Group	List:	-				
Attributes:						
Туре			Name			Value
1. Endpoint			Username		=	%{Authentication:Username}
2. Endpoint			Guest Role ID		-	%{GuestUser:Role ID}
3. Endpoint			MAC-Auth Expiry		=	%{Authorization:[Time Source]:Five Minutes DT}

Note: The MAC-Authentication Expiry is set to five minutes in the figure above, which means that a guest user reconnecting within five minutes of a successful authentication will not need to re-authenticate.

Enforcement profiles apply based on the configured conditions. As shown in the figure below, when the

client matches a web-authenticated or cached guest, apply the "Post Auth" role. If any of the conditions are not met, then the default profile, i.e. "Deny", kicks in.

Enforcement Profile	Enforcement Profiles - ARISTA_BYOD_GUEST-profile			
Summary Profile	Attributes			
Profile:				
Name:	ARISTA_BYOD_GUEST-profile			
Description:				
Type:	RADIUS			
Action:	Accept			
Device Group List:	1. asvin-group			
Attributes:				
Туре	Name		Value	
1. Radius:Aruba	Aruba-User-Role	-	ARISTA_BYOD_GUEST	
2. Radius:IETF	Session-Timeout	=	360	

Enforcement policies define the conditions that trigger the role assignment; they tie the enforcement profiles to the services. You can define Enforcement policies under **Configuration > Enforcement > Policies**. The MAC Authentication Enforcement Policy is shown below.

En	forcement Policy Details			_
De	escription:			
De	efault Profile:	[Deny Access Profile]		
Ru	ules Evaluation Algorithm:	first-applicable		
	Conditions		Enforcement Profiles	
1.	(Tips:Role MATC WebAuthenticated1)	CHES_ANY Cached-Guest1	Copy_of_[Allow Access Profile]	
2.	(Tips:Role EQUA	LS ARISTA_BYOD_GUEST)	ARISTA_BYOD_GUEST-profile	

The figure below shows a summary view of the MAC Authentication Service configuration.



Configuration » Services » Edit - Copy_of_CP2ndMethod_Asvin MAC AUTH				
Services - Copy_of	_CP2ndMethod_As	vin MAC AUTH		
Summary Service	Authentication Autho	rization Roles	Enforcement	
Service:				
Name:	Copy_of_CP2ndMethod_A	svin MAC AUTH		
Description:	MAC-based Authentication Service			
Туре:	MAC Authentication			
Status:	Enabled			
Monitor Mode:	Disabled			
More Options:	Authorization			
Service Rule				
Match ALL of the following	conditions:			
Туре	Name	Opera	tor	Value
1. Radius:IETF	NAS-Port-Type	BELONG	S_TO	Ethernet (15), Wireless-802.11 (19)
2. Connection	Client-Mac-Addres	s EQUALS		%{Radius:IETF:User-Name}
3. Radius:IETF	NAS-IP-Address	BELONG	S_TO_GROUP	asvin-group
4. Radius:IETF	NAS-Identifier	CONTAI	NS	Lab-Asvin-COA
Authentication:				
Authentication Methods:	[Allow All MAC AUTH]			
Authentication Sources:	 [Endpoints Repository] [Time Source] 			
Strip Username Rules:	-			
Authorization:				
Authorization Details:	 [Endpoints Repository] [Time Source] 			
Roles:				
Role Mapping Policy:	Copy_of_Arista-MAC-Auth			
Enforcement:				
Use Cached Results: Enabled				
Enforcement Policy:	Copy_of_2ndMethod_ARIS	FA_BYOD_GUEST		
< Back to Services				Disable Copy Save Cancel

For a first-time user, the condition shown in the figure below fails and the default role is applied.

Summary Service	Authentication Authorization	Roles Enforcement	
Role Mapping Policy:	Copy_of_Arista-MAC-Auth	Modify	Add new Role Mapping Policy
Role Mapping Policy Details			
Description:			
Default Role:	ARISTA_BYOD_GUEST		
Rules Evaluation Algorithm:	first-applicable		
Conditions	Conditions Role		
(Authentication:MacAuth EQUALS KnownClient) 1. AND (Authorization:[Time Source]:Now DT LESS_THAN % Cached-Guest1 {Endpoint:MAC-Auth Expiry})			

The steps to configure the MAC Authentication Service are as follows:

- 1. Add a new service and select "MAC Authentication" as the Type.
- 2. Configure the following two mandatory rules (rules 1 and 4 in the figure above are mandatory; the other rules are optional) of the RADIUS IETF type:
- 1. NAS-Identifier contains the SSID name, and
- 2. NAS-Port-Type belongs to "Wireless 802.11".
- 3. On the Authentication tab, select **[Allow All MAC AUTH]** under Authentication methods, and specify the **[Time Source]** and **[Endpoints Repository]** under Authentication sources, as shown in the figure above.
- 4. On the Authorization tab, add **[Time Source]** and **[Endpoints Repository]** under Authorization Details.
- 5. On the Roles tab, set the default role to the Pre-Authentication role configured in CloudVision Cognitive Unified Edge. If the condition shown in the preceding figure fails, i.e., if the device is not in the ClearPass cache, the default role is applied. Since that is the Pre-Authentication role, the device will be redirected to the guest login portal.
- 6. On the Enforcement tab, set the Default Profile to **[Deny Access Profile]** and define the conditions shown below. The Enforcement Policy ties the service to the enforcement profiles. When the condition holds true, the appropriate Enforcement Profile is applied. For example, if the role matches that of a web-authenticated, cached guest, then the guest is allowed access.

Enforcement Policy Details				
De	escription:			
De	efault Profile:	[Deny Access Profile]		
Ru	ules Evaluation Algorithm:	first-applicable		
	Conditions		Enforcement Profiles	
1.	(Tips:Role MATC WebAuthenticated1)	CHES_ANY Cached-Guest1	Copy_of_[Allow Access Profile]	
2.	(Tips:Role EQUA	ALS ARISTA_BYOD_GUEST)	ARISTA_BYOD_GUEST-profile	

Web Authentication Service

Finally, you need to configure the Web Authentication service. The figure below shows a summary view of the MAC Authentication Service configuration.



Configuration » Services » E	Configuration » Services » Edit - Copy_of_Asvin Web Auth				
Services - Copy_of	_Asvin Web A	Auth			
			Datas		
Summary Service	Authentication	Authorization	Roles	Enforcement	
Service:					
Name:	Copy_of_Asvin W	eb Auth			
Description:					
Туре:	Web-based Authe	entication			
Status:	Enabled				
Monitor Mode:	Disabled				
More Options:	Authorization				
Service Rule	Service Rule				
Match ANY of the following	g conditions:				
Туре	Name		Opera	ator	Value
1. Host	CheckTyp	e	MATCH	ES_ANY	Authentication
Authentication:					
Authentication Sources:	1. [Guest User Re 2. [Local User Re	epository] pository]			
Strip Username Rules:	-				
Authorization:					
Authorization Details:	1. [Time Source] 2. [Guest User Re	epository]			
Roles:					
Role Mapping Policy:	Copy_of_Guest R	oles for WebAuth			
Enforcement:					
Use Cached Results:	Disabled				
Enforcement Policy:	Copy_of_Asvin C	DA policy			
< Back to Services	Back to Services Disable Copy Save Cancel				

The process to configure the Web Authentication Service is the same as that of the MAC Authentication Service.

An important difference is the Enforcement Policy for web-authentication. On the Enforcement tab, define the enforcement policy as shown below. The Enforcement Policy ties the service to the enforcement profiles. When the condition holds true, the corresponding Enforcement Profiles are applied. For example, if the user is successfully authenticated, then the Post-Authentication role (PostAuth_COA in the figure below) is applied, the client is added as a "Known Endpoint" and MAC Caching is applied for subsequent connection attempts by this client.

External Captive Portal with RADIUS Authentication

The workflow for external captive portal with RADIUS authentication, i.e. guest user onboarding using a captive portal, is shown below.



Gue	st Client	Arista AP	ClearPass	RADIUS
		Australia		
1	HTTP Request for any URL	Redirect to	ClearPass-hosted captive portal	2
3	Enter username and password			
			4	Encode password using the shared secret
4	Redirect browser to AP. Include userna and encoded password	me		
	L	RADIUS Ac and passw	ccess-Request (with username ord)	-
		RADIUS Ad	ccess Accept	6

- 1. The guest Wi-Fi client connects to an SSID and attempts to access a URL on the internet.
- 2. The AP redirects the client to the ClearPass-hosted captive portal.
- 3. The guest user enters the username/password in the portal and submits the page to ClearPass.
- 4. Clearpass encodes the password (using the portal secret configured in CloudVision Cognitive Unified Edge) and redirects the client web browser to the AP with the username and the encoded password included as URL arguments.
- 5. The AP decodes the password and sends an Access-Request to ClearPass with the username and password.
- 6. ClearPass responds with an Access-Accept granting guest access and the client is connected.

CloudVision Cognitive Unified Edge Configuration

The CloudVision Cognitive Unified Edge configuration consists of two steps:

- 1. Point CloudVision Cognitive Unified Edge to the ClearPass guest captive portal.
- 2. Add the ClearPass RADIUS server to the Guest SSID.

Each step is described below.

 To point CloudVision Cognitive Unified Edge to the ClearPass guest captive portal URL, enter the captive portal URL under SSID > Captive Portal, in the Splash Page URL field as shown. The shared secret for the guest portal (different from the RADIUS shared secret) is the UAM secret and it comes from the ClearPass configuration described below.



Locations		Search for MAC/ IP Address/ U
Wi-Fi SSID RADIUS Tunnel Interface	e Role Profile Radio Settings Device Settings	
	Changes to this SSID will affect all groups and folders that use this SSID. See groups	and folders using this SSID.
€ Guest	Basic Security Network Captive Portal	
✓ Captive Portal Third-Party Hosted ▼		
With RADIUS Authentication	RADIUS Settings Shared Secret *	
https://ClearPass-GuestPortal-URL.com/		
HTTPS Redirection		
Websites that users can access before login.		

2. Add the ClearPass RADIUS server to the Guest SSID by clicking the RADIUS Settings link shown above.

ClearPass Configuration

- The guest SSID configuration described here was implemented with ClearPass version 6.6.10.106403.
- Make sure that the FQDN Certificate is installed on ClearPass before you configure it for guest logins.

Broadly, the ClearPass configuration for Guest access consists of two steps:

- 1. Configure the Guest Portal.
- 2. Create the Guest Service.

Each of these steps is described below in detail.

Guest Portal Configuration

Follow the ClearPass-recommended steps to create a guest portal under **Configuration > Pages > Guest Self-Registrations**. Select the **Advanced Editor**. Go to the **Login** section; this is the Arista-specific portion of the configuration.



🗣 Guest 🛛 0	Home » Configuration »	Home » Configuration » Pages » Guest Self-Registrations				
📳 Onboard 🛛 O	Customize Gues	Customize Guest Registration (Login)				
Configuration ·	Use this form to make changes to the guest self-registration instance Login.					
Advertising	Customize Guest Registration					
- Sea Authentication	Login Options controlling logging	In for self-registered guests.				
Start Here	Enabled:	Enable guest login to a Network Access Server				
Private Files Public Files Guest Manager Hotspot Manager Pages	* Vendor Settings:	Custom Settings Select a predefined group of settings suitable for standard network configurations.				
	* Submit URL:	http://192.0.2.254/logon?tres=success The URL of the NAS device's login form.				
	* Submit Method:	GET 0 Choose the method to use when logging into the NAS.				
	* Username Field:	username The name of the username field for the NAS device's login form.				
Forms & Views Guest Self-Registrations	* Password Field:	password The name of the password field for the NAS device's login form.				
Web Logins	* Password Encryption:	PAP with shared secret Choose the type of password encryption to use when logging into the NAS.				
Web Pages Receipts	UAM Secret:	1234567890 Enter the shared secret between the NAS device and the web login form.				
SMS Services Translations	Extra Fields:	Specify any additional field names and values to send to the NAS device as name=value pairs, one per line.				
	Username Suffix:	The suffix is automatically appended to the username before logging into the NAS.				

As shown in the figure above, the settings for this section are:

- Enabled: Select "Enable guest login to a Network Access Server".
- Vendor Settings: Select "Custom Settings".
- Submit URL: Enter "http://192.0.2.254:80/logon?res=success"
- Submit Method: Select "GET".
- Enter the username and password
- Password Encryption: Select "PAP with shared secret".
- Enter the UAM Secret you wish to use.

Guest Access Control

The ClearPass workflow to configure Guest Access Control consists of the following steps:

- 1. Create the Guest Role.
- 2. Define a Role Mapping, i.e., a set of conditions that assign the role.
- 3. Define an Enforcement Profiles, i.e., the actions used to assign roles.
- 4. Define the Enforcement Policy, i.e., the conditions that trigger the role assignment.
- 5. Create a Service that ties everything together.

Each step is described in detail below.

1. Create the "Guest" role as shown below.

Configuration * Identity	* Roles	
Roles		
Ð		
Filter: Name		Go Clear Filter
I. [Guest]		Default role for a Guest
Name:	[Guest]	
Description:	Default role for a Guest	a
Save Cancel		
	Configuration > Identity Roles Filter: Name 1. Gues Edit Role Name: Description:	Configuration * Identity * Roles Roles Filter: Name I. [Guest] Edit Role Name: Description: Default role for a Guest Save Cancel

2. Because the Guest SSID has only one role, the workflow does not require any mapping as such. Select "Guest" as the Default Role and as the Role Name for whatever condition shows up in the Role Mapping below.

aruba	ClearPass Policy Manager Configuration >> Identity >> Role Mappings >> Edit -Guest-Role-Arista Role Mappings - Guest-Role-Arista			
Dashboard Monitoring				
Configuration C	Summary Policy Mapping Rules Policy: Policy Name: Guest-Role-J Description: The roles used in Default Role: [Guest] Mapping Rules: Rules Evaluation Algorithm: First applicable	-Arista by Guest.		
	Conditions 1. (GuestUser:Role ID EQUALS 2	2)	Role Name [Guest]	

 Create an Enforcement Profile. The action shown below allows a Guest user access only for 8 hours (28800 seconds) after registration. ClearPass sends this value as a standard Session-Timeout attribute in the RADIUS "Access Accept" message.

aruba	ClearPass Policy Manager			
Dashboard O Monitoring O	Configuration > Enforcement > Profiles > Edit Enforcement Profile - Allow Access Policy for 8Hrs Enforcement Profiles - Allow Access Policy for 8Hrs			
Configuration O	Summary Profile	Attributes		
- 🔅 Start Here - 🔅 Services E 🗣 Authentication	Profile:			
	Name: Allow Access Policy for 8Hrs			
	Description: System-defined profile to allow network access			
Posture	Type: RADIUS			
⇒ ĝ Enforcement	Action: Accept			
2 Policies	Device Group List:	-		
- O Profiles	Attributes:			
Network	Туре	Name		Value
- 🛱 Policy Simulation	1. Radius:IETF	Session-Timeout	-	28800
- Q Profile Settings				



4. Define an Enforcement Policy that decides when the action (i.e., the Enforcement Profile) is triggered. Shown below is an Enforcement Policy that allows access only on weekdays.

Dashboard O	Configuration > Enforcement > Policies > Edit - Weekdays-Only			
Honitoring 0	Enforcement Policies - Weekdays-Only			
Configuration O	Summary Enforcement Rules			
🛱 Start Here 🛱 Services	Rules Evaluation Algorithm: Select first match Select all matches			
Authentication	Enforcement Policy Rules:			
Identity	Conditions (Date: Day of Week, 851 OMOS, 70, Meeday, Tuesday, Wedeesday, Thursday,	Actions		
- 🛱 Single Sign-On (SSO)	1. Friday)	Allow Access Policy for 8Hrs		
🛱 Local Users	2. (Date:Day-of-Week BELONGS_TO Saturday, Sunday)	[Deny Access Profile]		
- Q Endpoints	Add Rule Move Up Move Down			
- Q Static Host Lists				
C Role Mannings				
Posture				
- Q Posture Policies				
i Audit Servers				
- Dilcies				
i Profiles				
Network				

5. Finally, under **Configuration > Services**, create a Service to tie all of this together and point ClearPass to the Arista SSID. As shown below, define a Rule that the NAS-Identifier in the RADIUS message "CONTAINS" the value "Guest".

aruba	ClearPass Policy Manager			Support i Hele i Looput bhupinder.miara (Super Adminiatrator	
Deshiver	Configuration >> Services >> Edit >> Arista-ClearPass-Integration				
Autoring (Services - Arista-ClearPass-Guest-Integration				
🖧 Configuration	Summary Service	Authentication	Rales Enforcement		
Cartines Cartines Cartines Cartentiny Cartent	Service Name Oescription Type: Statu: Nambar Hode: Nambar Hode: Nam Options: Enclose Rule Patch ALL of the following Type: I Ladues 2017 I Ladues 2017 I Ladues 2017 Authentication Methods: Authentication Methods: Sciptions: Rate Mapping Pulley: Enforcement Use Cached Results: Enforcement	Arista-ClearPa Arista-ClearPa Anosta-ClearPa RADIS Enforcem Enabled	ss-Guest-Integration ss-Guest-Integration et (Generic) Nati-Port Type Nati-Port Type Nati-Sectifier Rory)	Operator EQUALS CONTAINS	Value Wireless 402.11 (19) Guest
	< Beck to Services				Disable Copy Serve Cancel