ARISTA

# Integration with Aruba ClearPass

## Table of Contents

# 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.

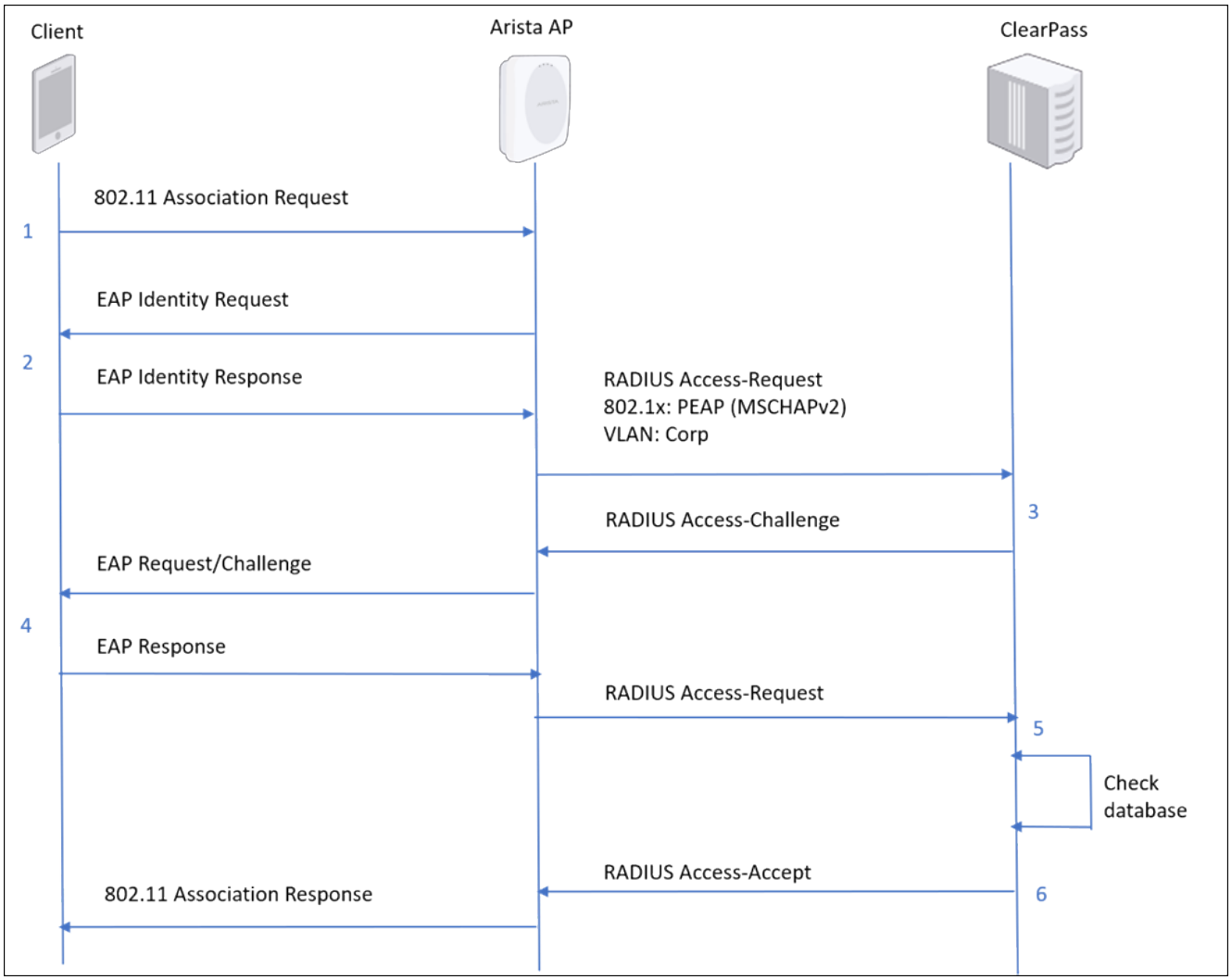
### 802.1x Authentication of Enterprise Users on Enterprise Devices

Assume that:

- 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:

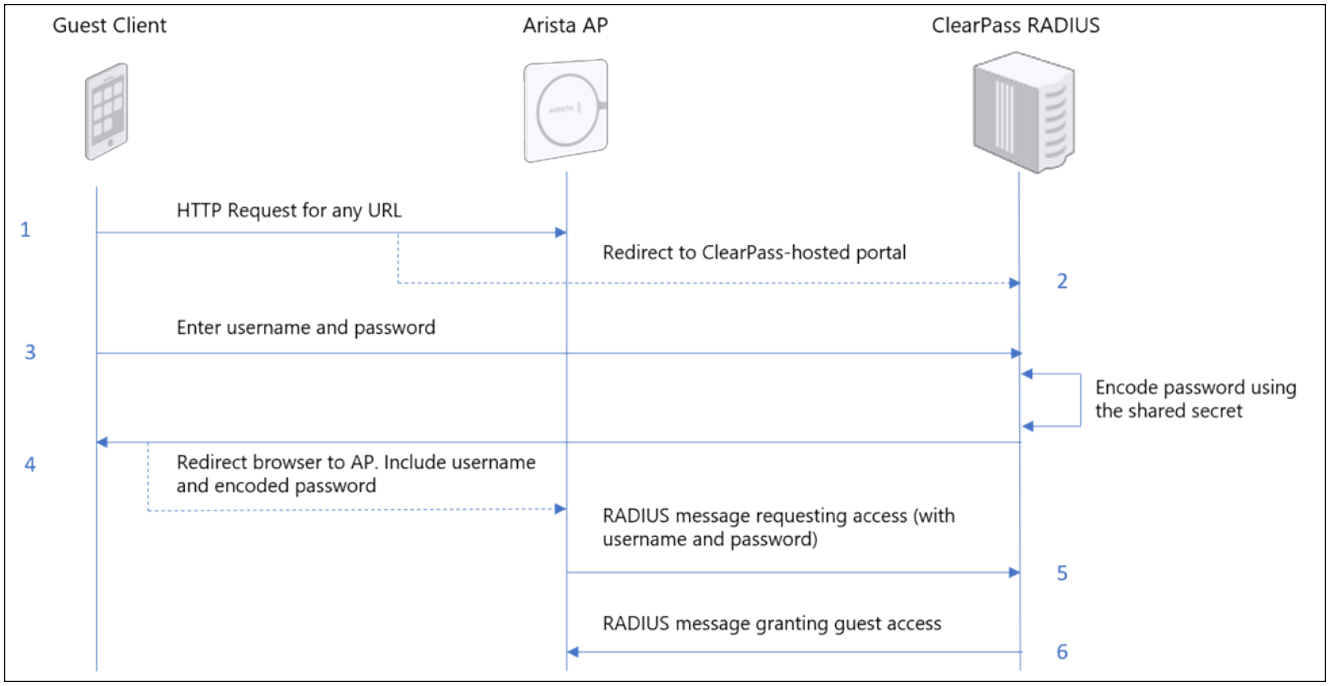
- 802.1x authentication (with any type of EAP)
- Central web authentication (similar to the External Captive Portal with RADIUS method described later)
- A hybrid solution (802.1x authentication with some web sign-in or an "Accept" click for terms and conditions).

## 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

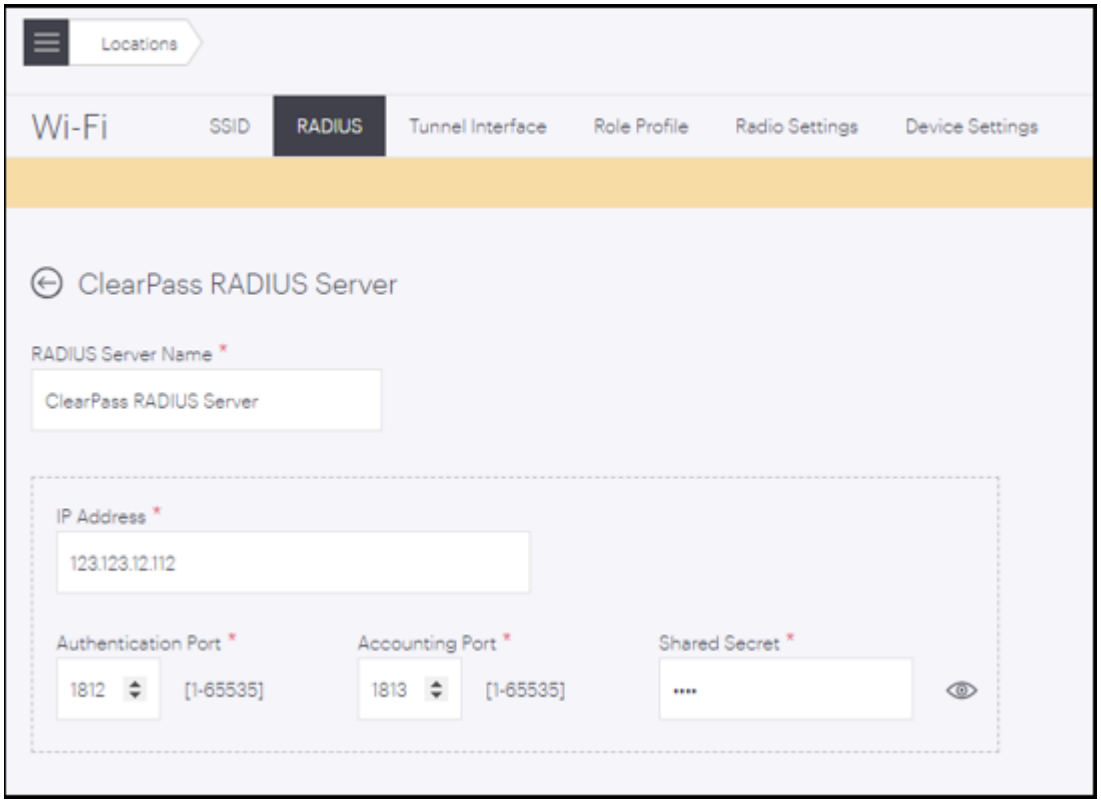
This section describes how to configure CloudVision Cognitive Unified Edge and ClearPass to implement the PEAP (MSCHAPv2) based 802.1x authentication workflow for Enterprise-owned devices described earlier.

### CloudVision Cognitive Unified Edge Configuration

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

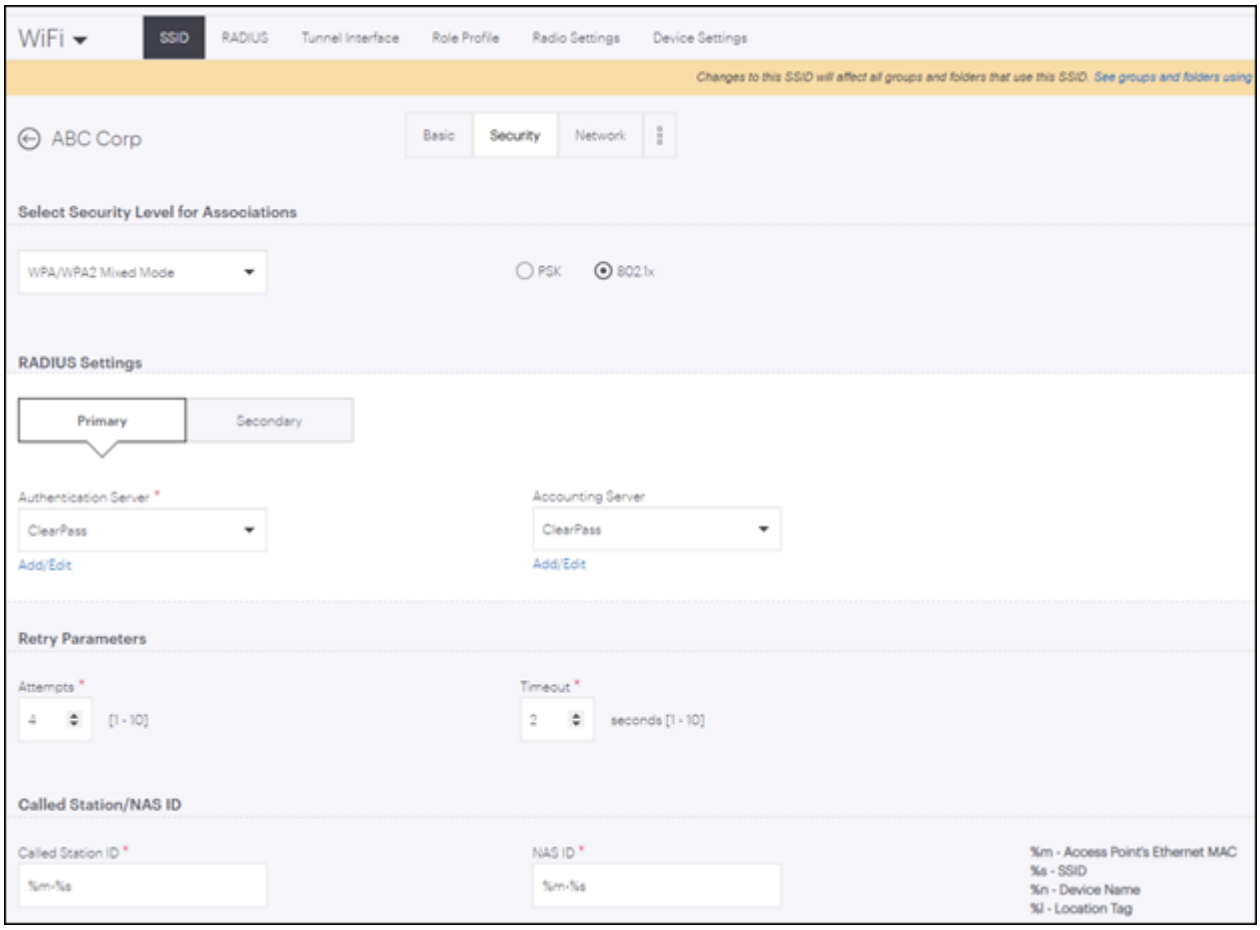
## RADIUS Profile

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




## 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.




## 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.

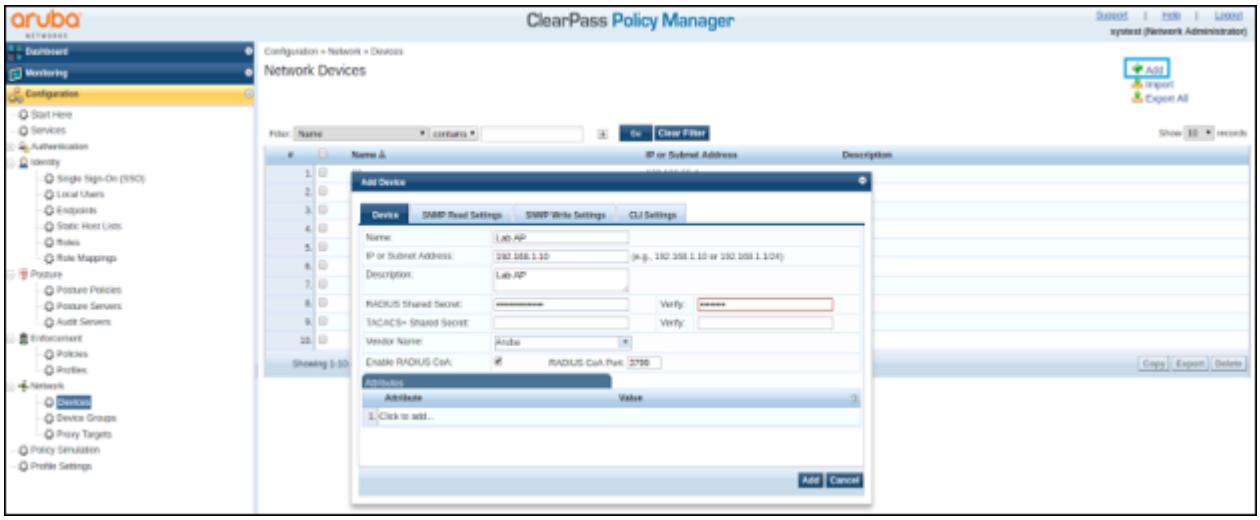
Each of the steps is described in detail below.

### 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

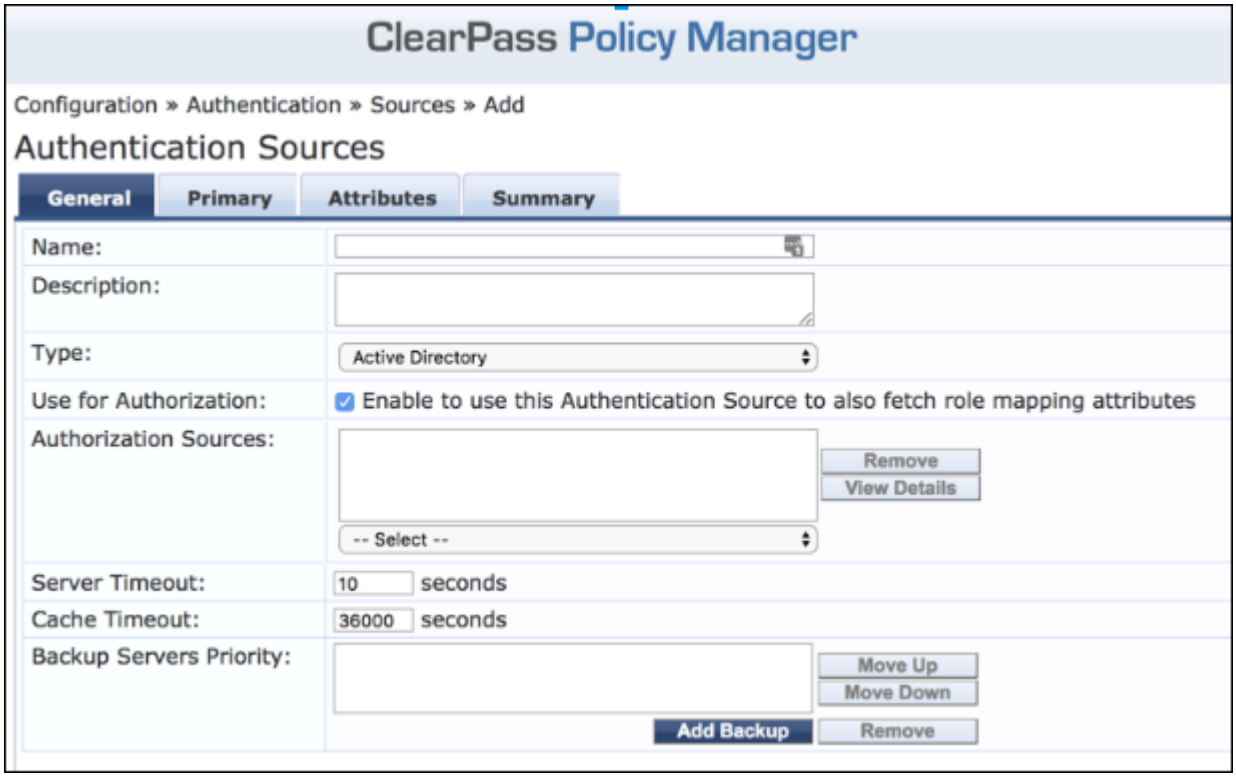
Shared Secret fields of the Add Device window. The other fields use default values.




## 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.

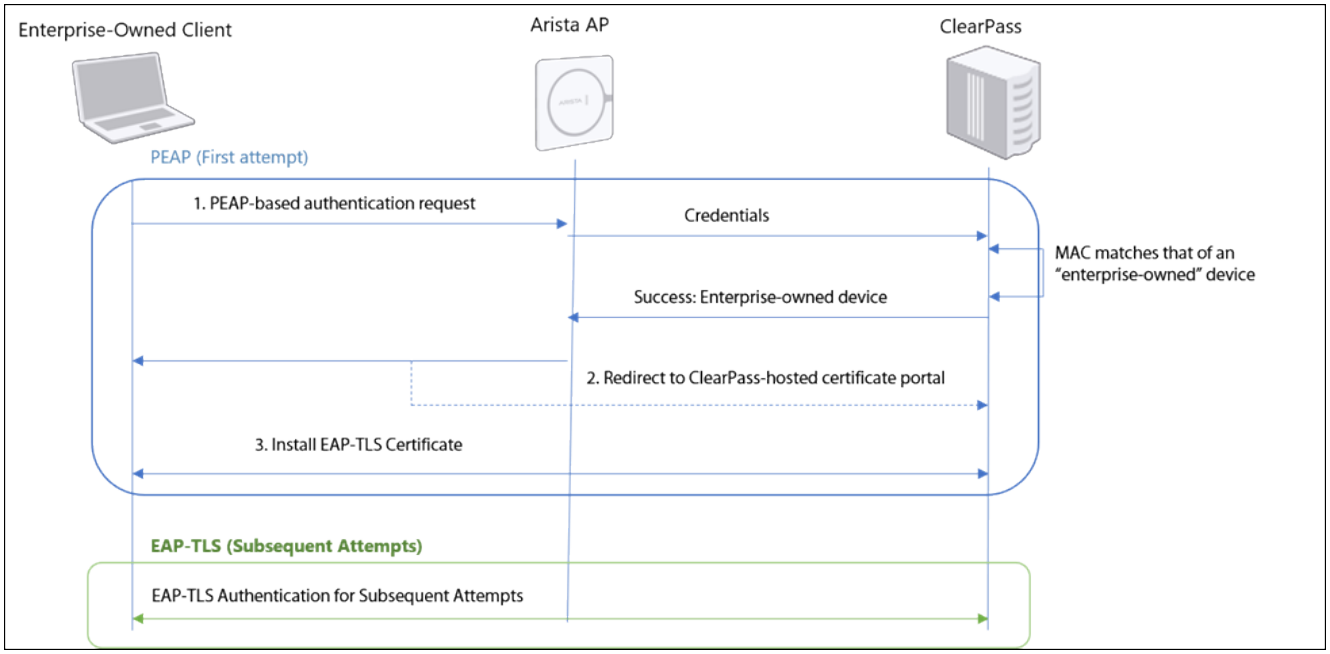


### Create a Service

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.




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 PEAP-based 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

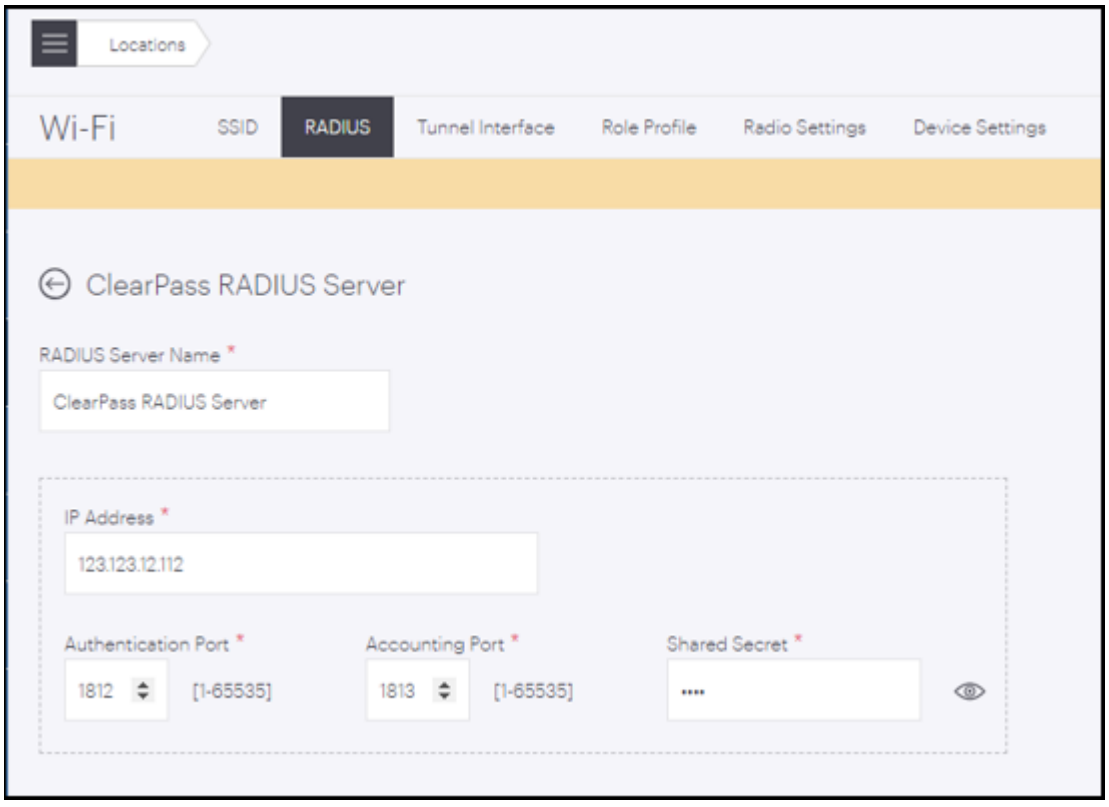
Broadly, configuring CloudVision Cognitive Unified Edge to work with ClearPass consists of three steps:

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.

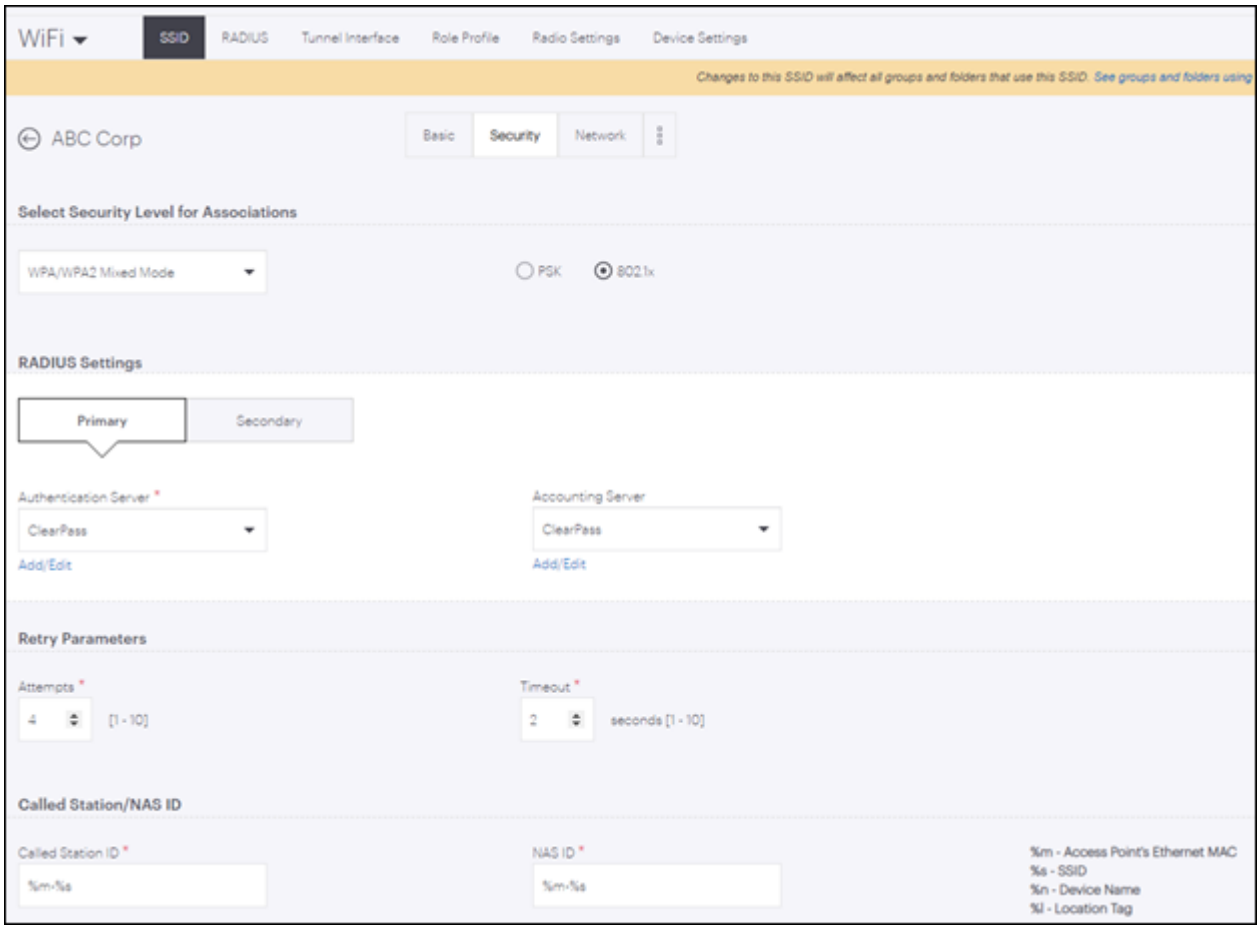
Each of the steps is described in detail below.

### RADIUS Settings

1. 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).

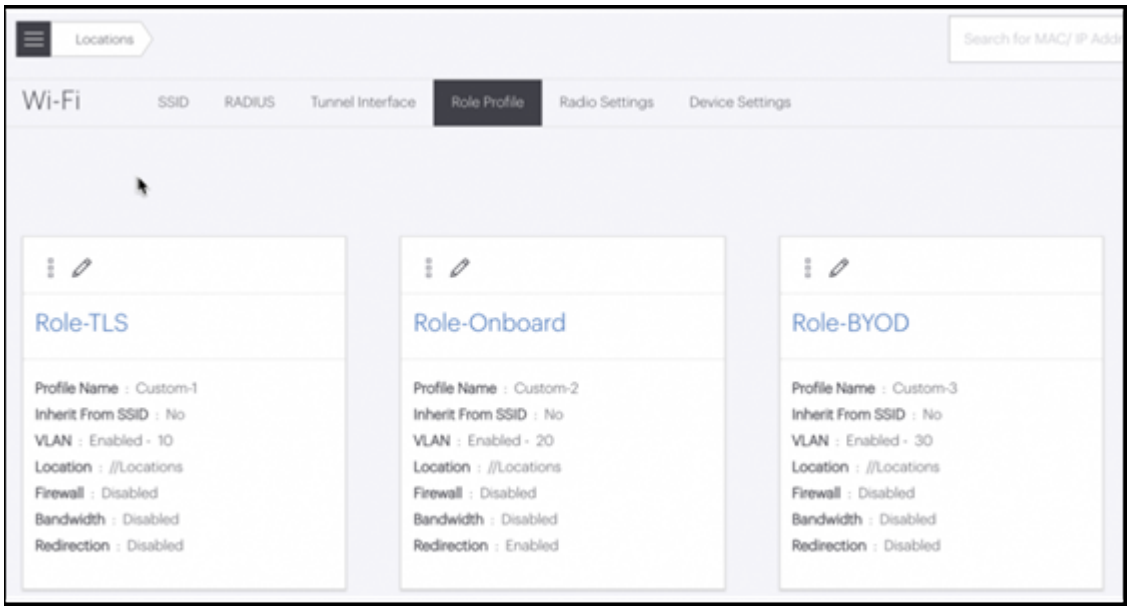



2. Add the ClearPass RADIUS server to the **SSID > Security** tab.




## Role Profiles

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



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

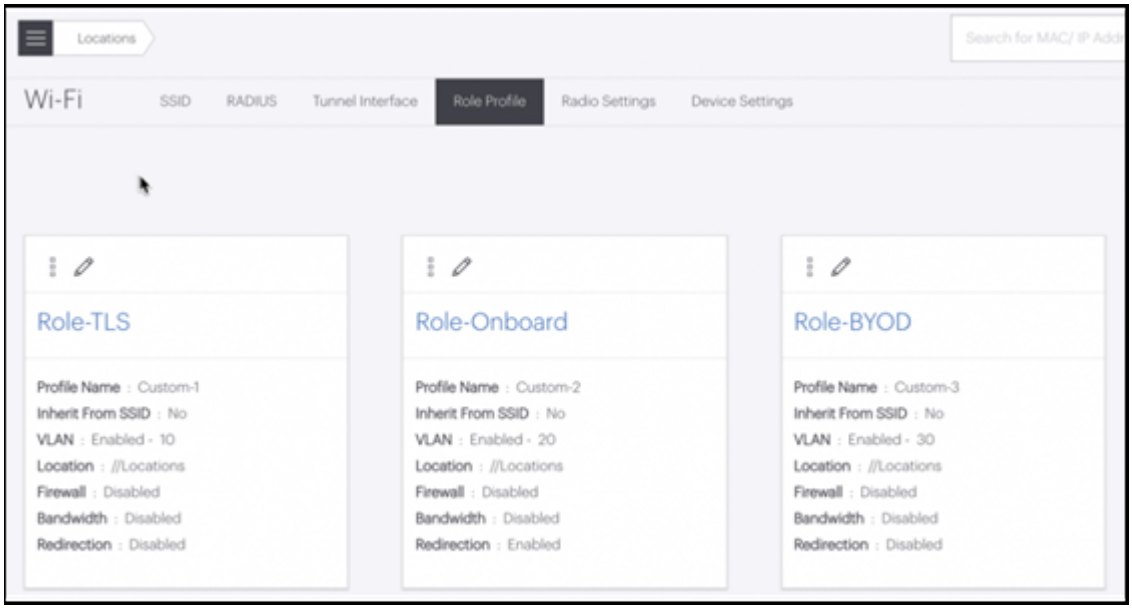
| Role Name | VLAN ID | Redirection |
|---|---|---|
| Role-TLS | VLAN 1 | Disabled |
| Role-Onboard | VLAN 2 | • Enabled<br>• In the **Redirect URL** field, enter the IP/URL of the ClearPass certificate-onboarding portal where you want to redirect users.<br>• Enable **HTTPS Redirection**<br>• Under **Websites 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:

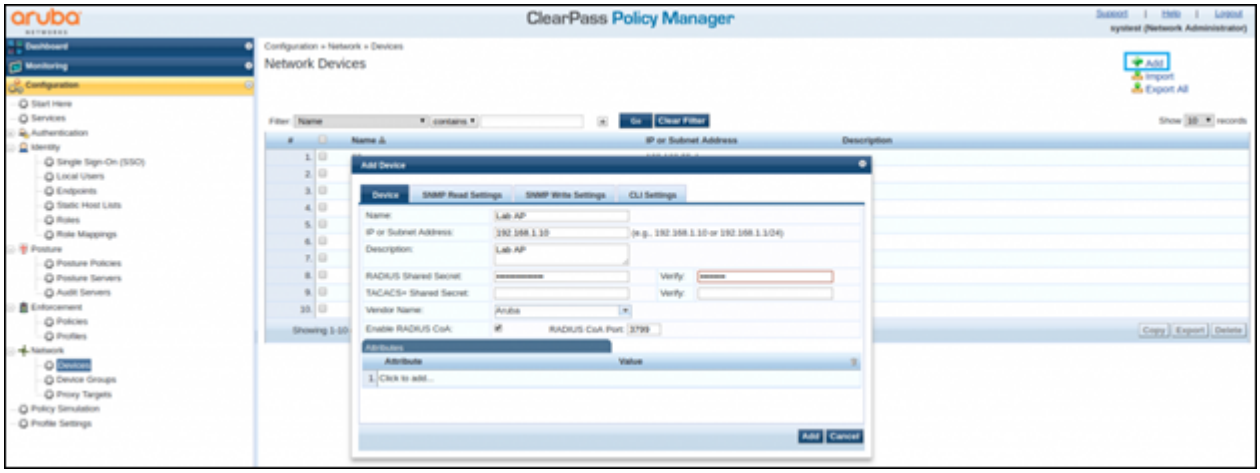
1. Add Arista APs as authorized ClearPass RADIUS clients.
2. Point ClearPass to the Active Directory.
3. Define a new Certificate Authority.
4. Create a Certificate-Onboarding Portal, from where the user installs the client-side certificate.
5. Define the Role-Based Access Control mechanism.
6. Create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

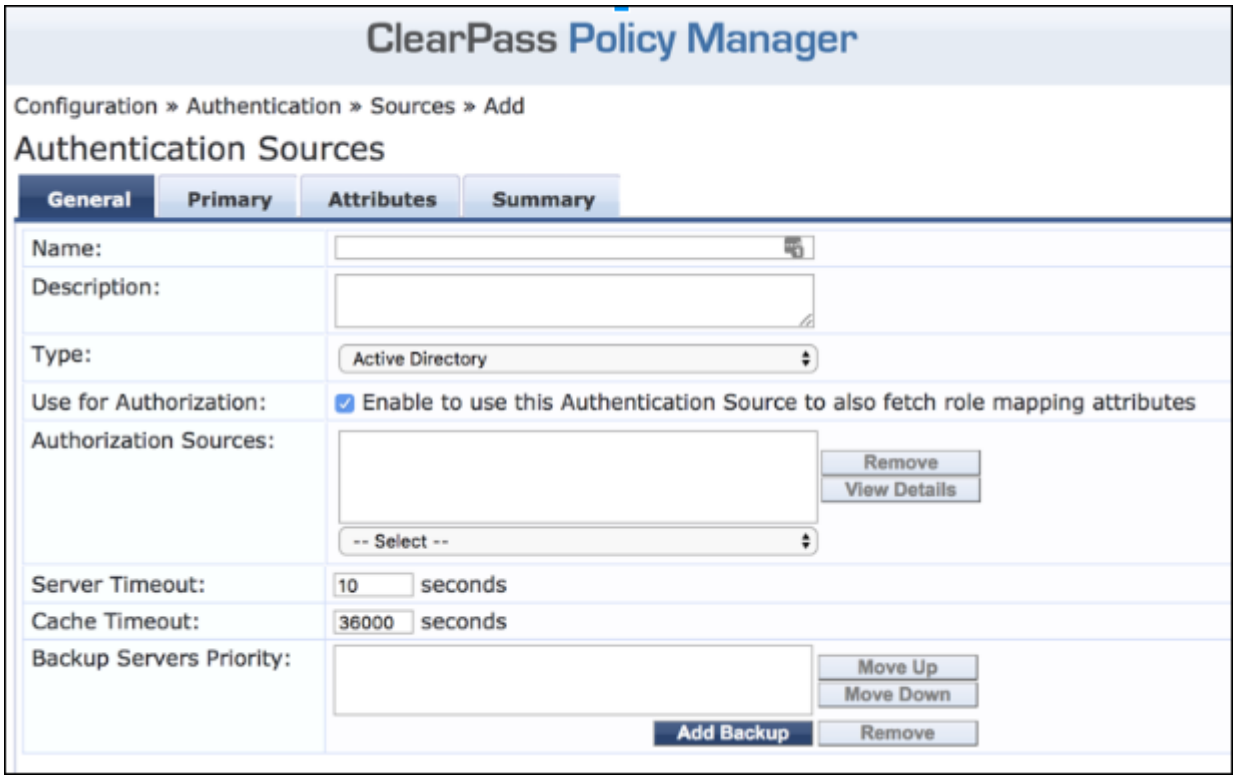
You can add Arista APs as authorized clients of ClearPass RADIUS under **Configuration > Network > Devices** in the ClearPass Policy Manager as shown below. Click **Add** and the Add Device window appears. Enter the Arista AP information in the Name, IP or Subnet Address, Description (optional), and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




### 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.

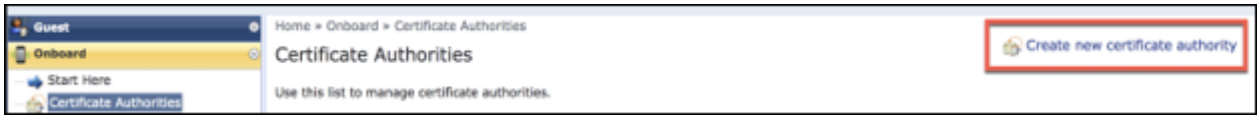
You can point ClearPass to the AD under **Configuration > Authentication > Sources > Add** as shown below.




## 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.




This video by ClearPass explains the process.

## Certificate-Onboarding Portal

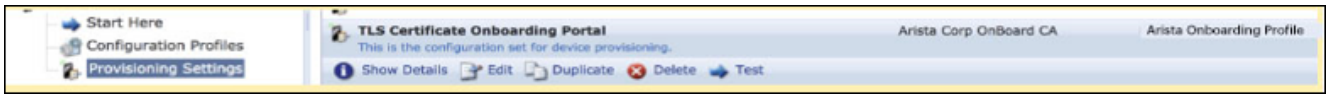
The next step is to create the certificate-onboarding portal. WiFi clients will be redirected to this portal to generate and install client certificates for EAP-TLS.

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.

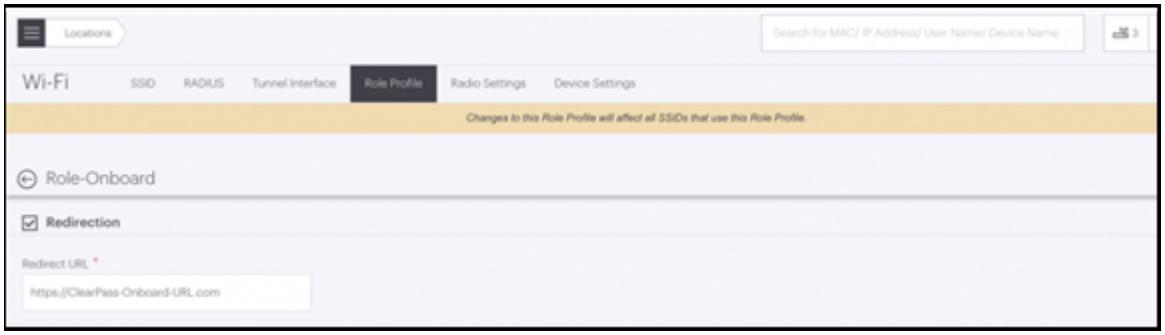

Next, create a Provisioning Profile using the Configuration Profile.


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.




## Role-Based Access Control

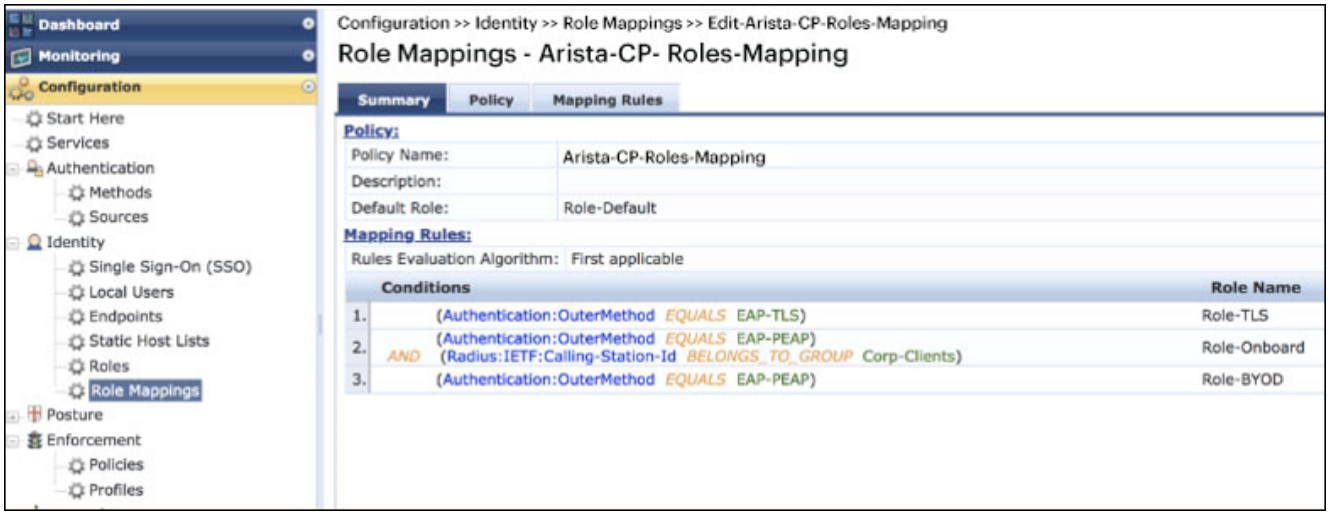
The ClearPass workflow to configure Role-Based Access Control consists of the following steps:

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.

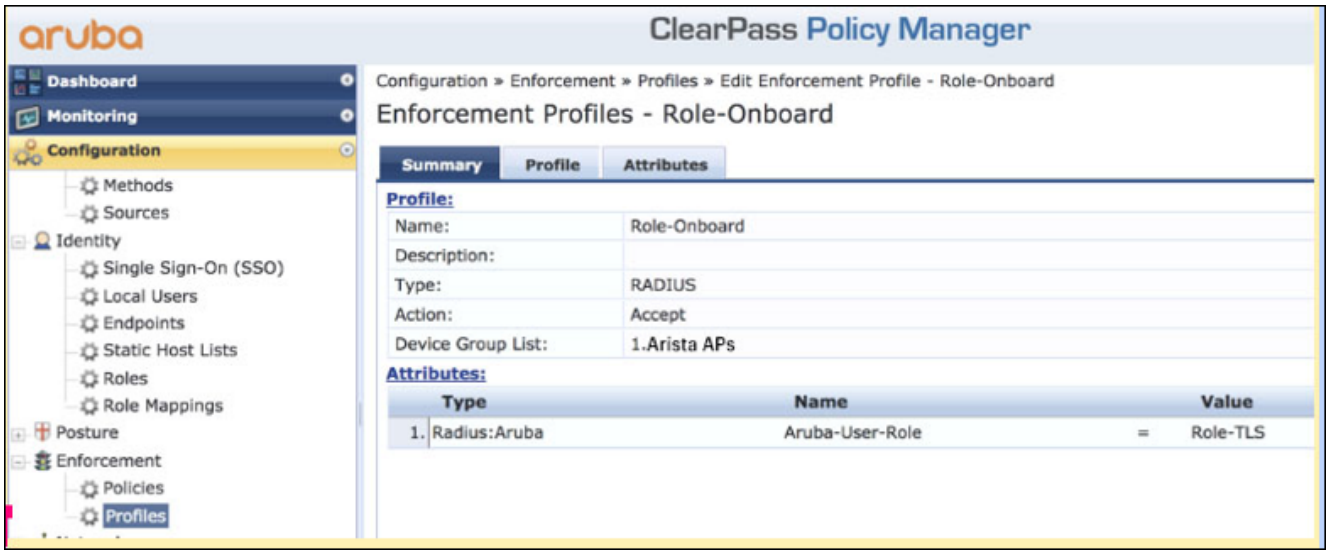
Each step is described in detail below.

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

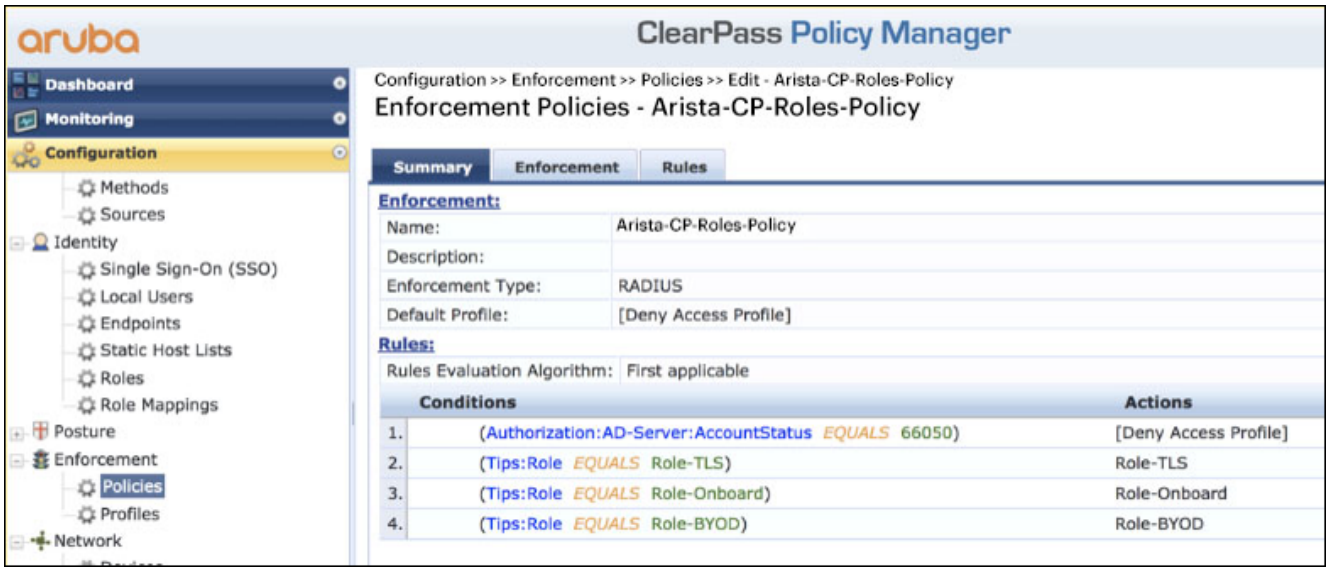

2. Under Identity > Role Mappings, define a Role Mapping—a set of conditions that decide which role is assigned to an authenticated client. "Role-Default" is assigned if none of the conditions is met, but this scenario will never arise in our case. Note: The group Corp-Clients (used in Condition #2 below, 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.



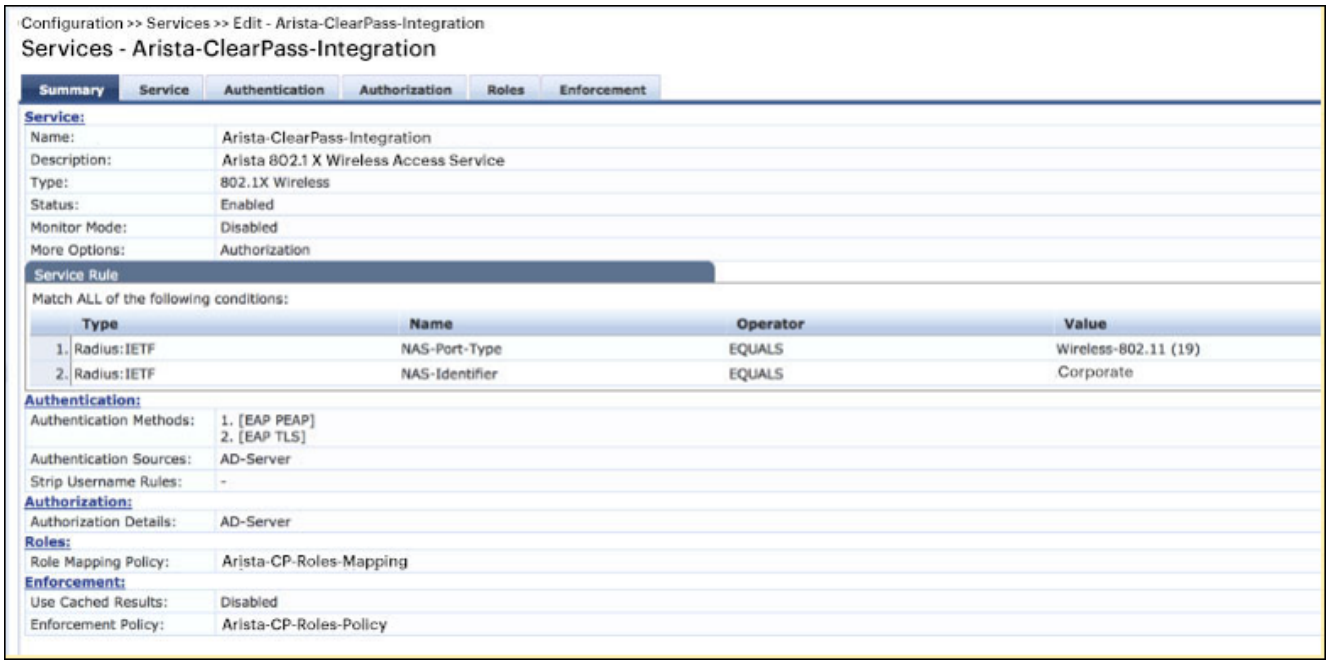

3. Define the three Enforcement Profiles, one for each role. Enforcement Profiles are basically actions—in our case, values that ClearPass RADIUS must return in the "Access Accept" message. You can define Enforcement Profiles under Configuration > Enforcement > Profiles. The "Role-Onboard" profile is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




4. 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.




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.




# Approaches to Guest User Onboarding

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

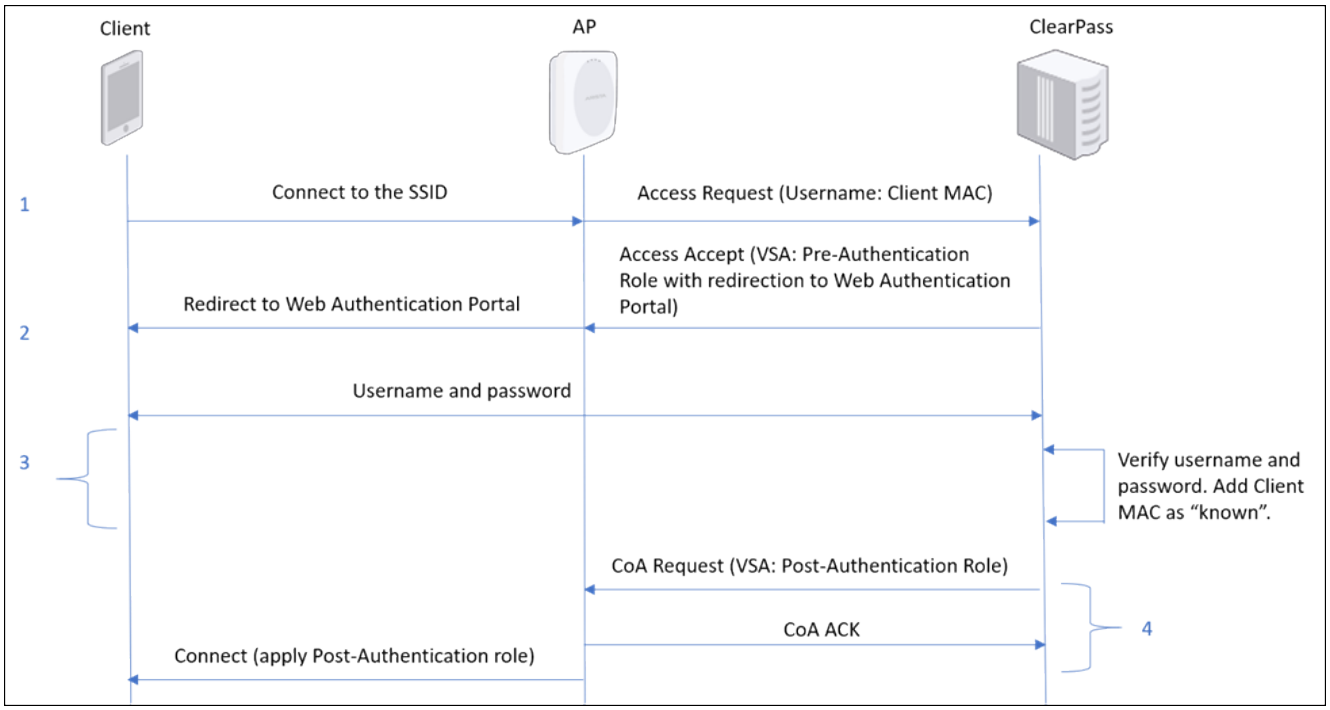
Using Role Profiles: In this approach, you configure CloudVision Cognitive Unified Edge to assign two roles: a pre-authentication role and a post-authentication role. The pre-authentication role redirects guest clients to a web-authentication portal and the post-authentication role grants access to guest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



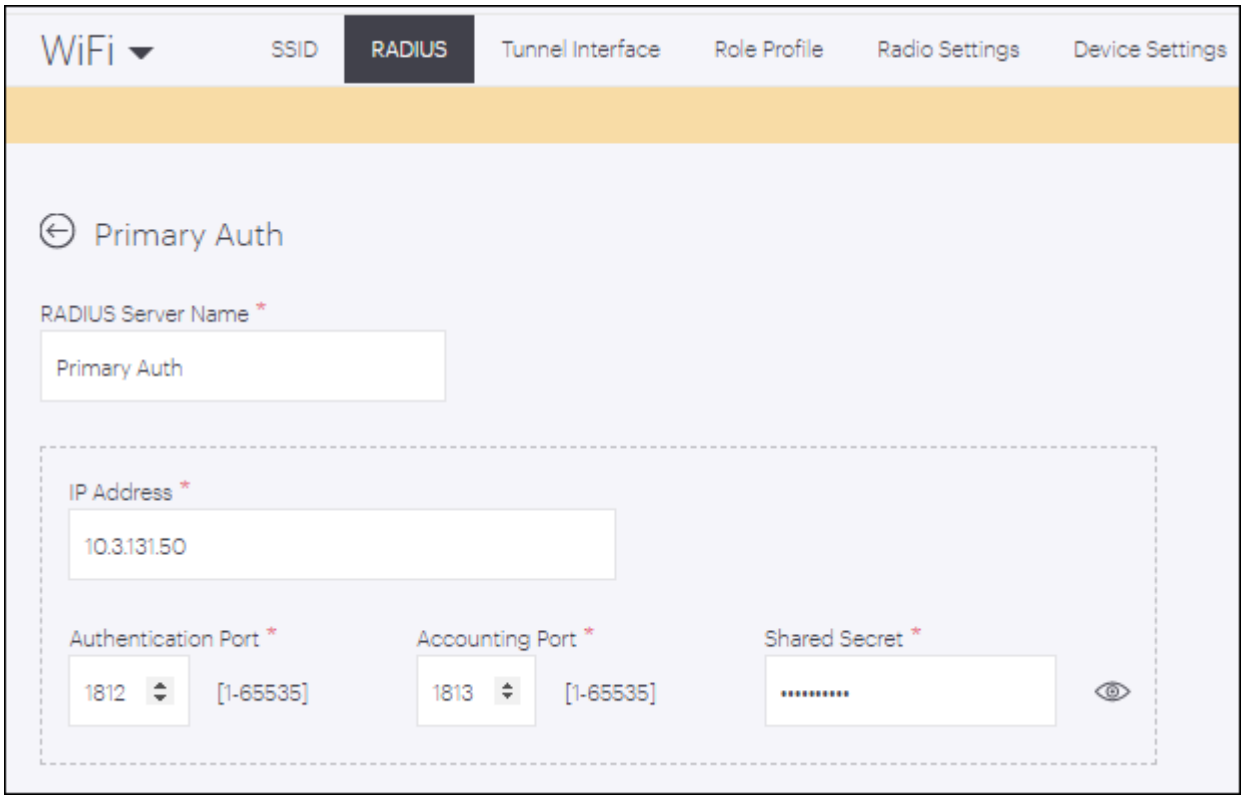

1. When the client first connects to the SSID, the Wi-Fi access point (AP) sends an Access Request containing the client's MAC address to ClearPass.
2. ClearPass responds with an Access-Accept message containing the Pre-Authentication role.The Pre-Authentication role redirects the client to the ClearPass 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

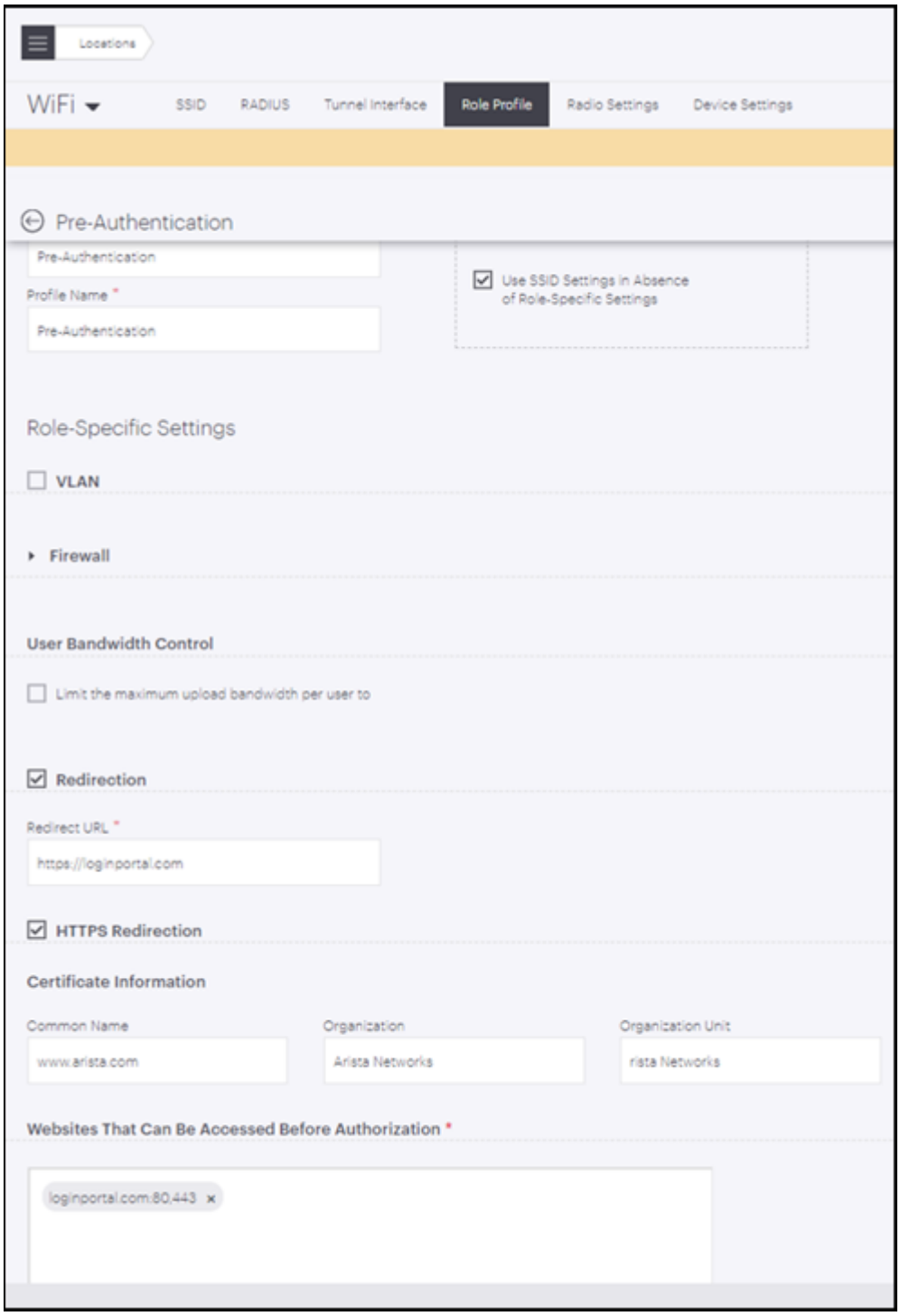
Under Configure > WiFi > RADIUS profile, select "Add RADIUS Server" and enter the ClearPass server details as shown below.




## Pre-Authentication Role

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

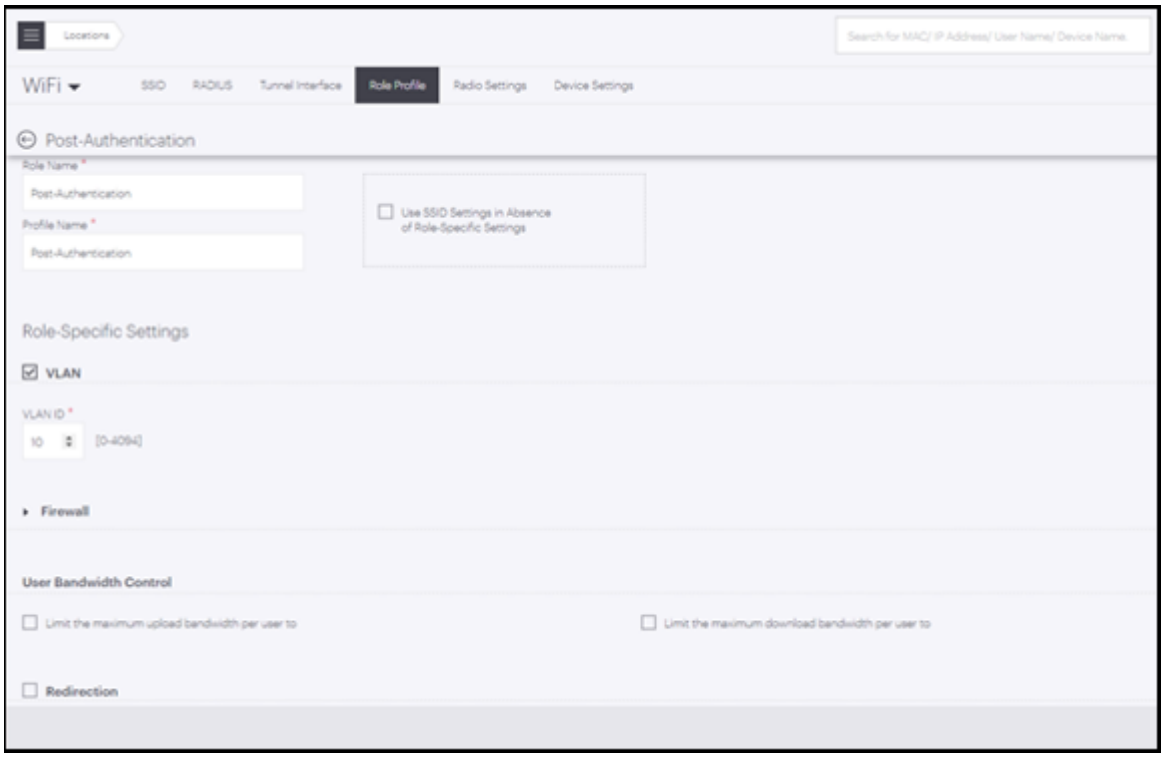
Note: You must add the web authentication portal URL, and ports 80 and 443 to the "Websites That Can Be Accessed Before Authorization" list.




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.

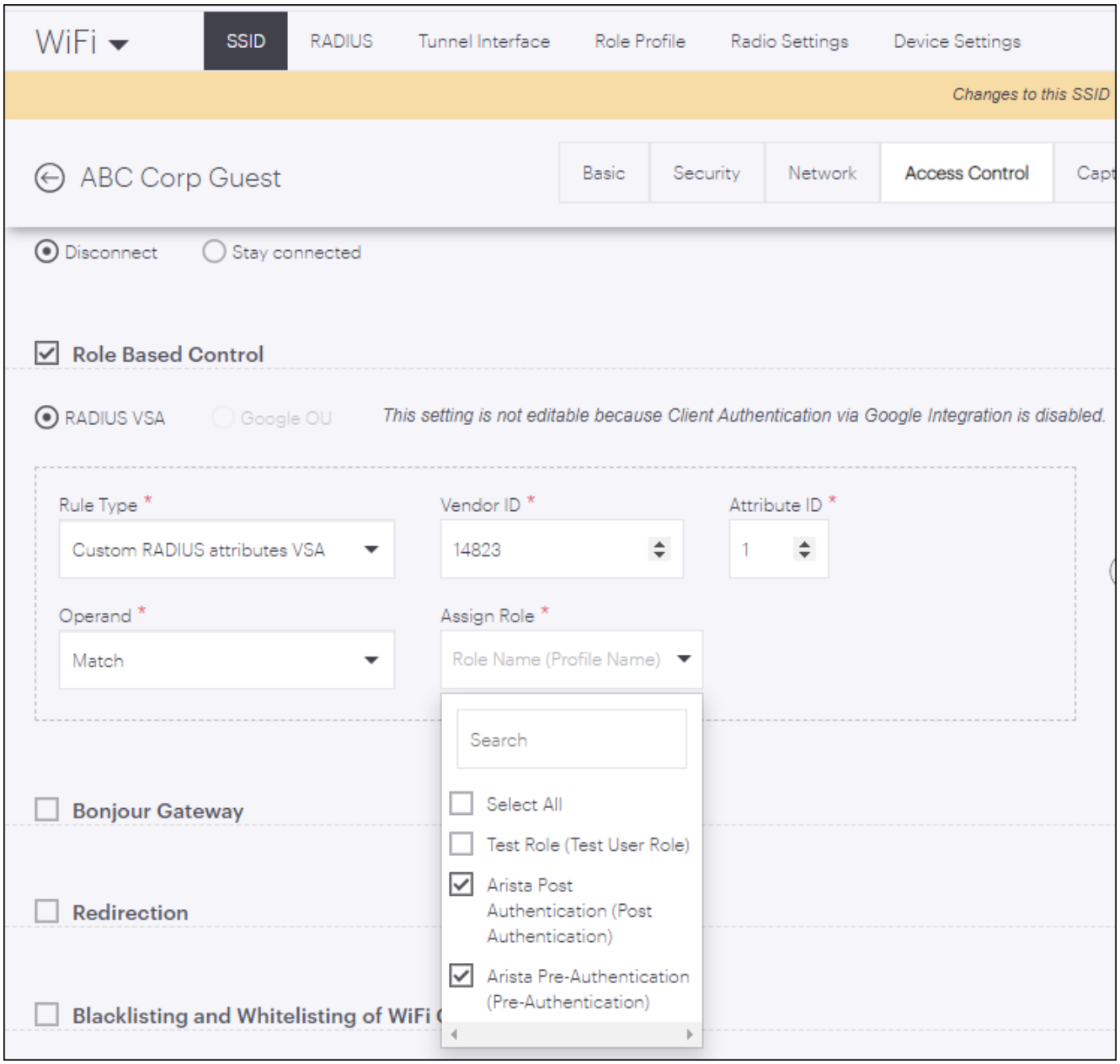



You need to configure ClearPass to return this role in the Change Of Authorization (CoA) message it sends to the AP.

### RADIUS MAC Authentication and Role-Based Control

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

1. 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.




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

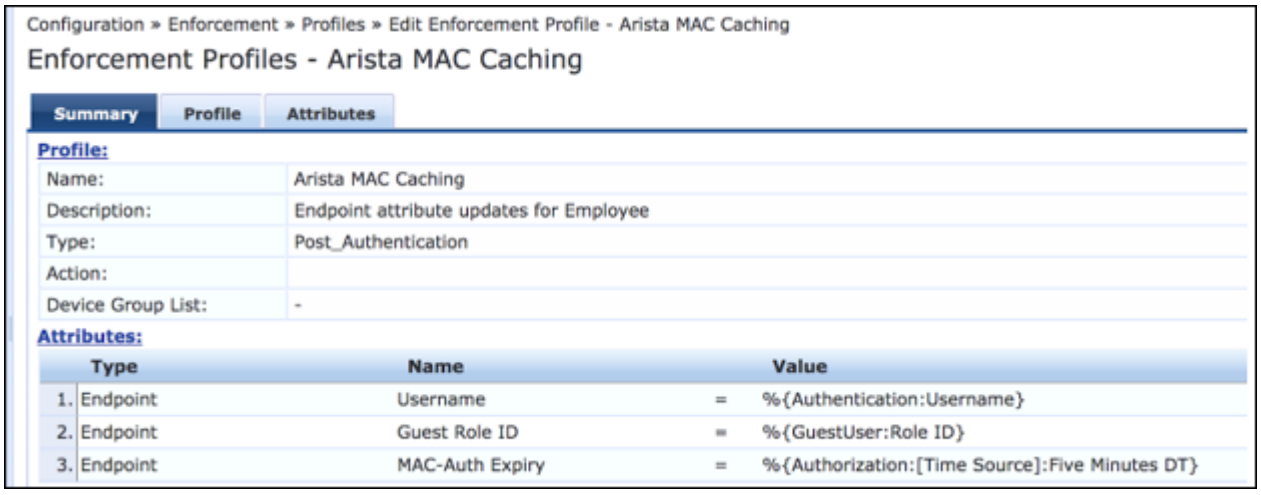
Each of these is described in detail below.

### 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

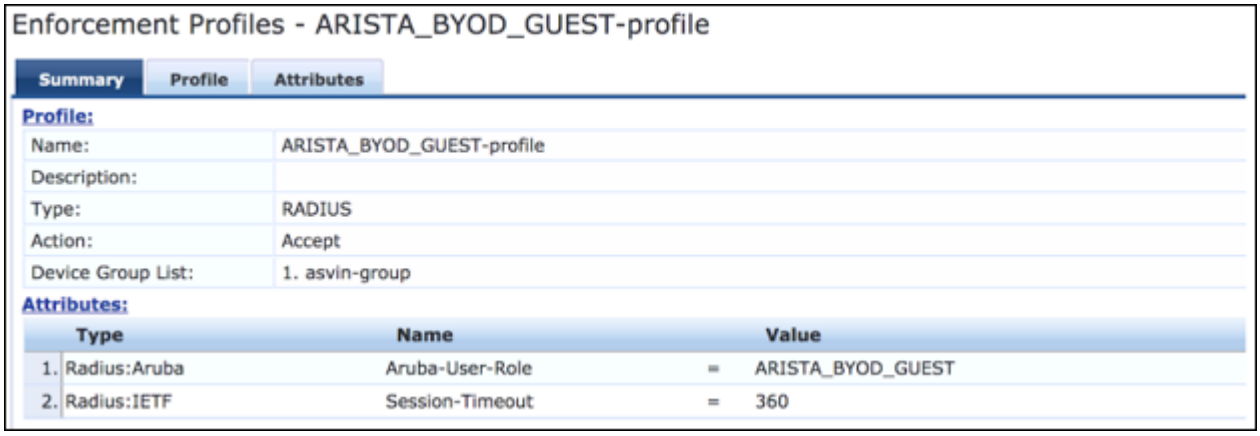
You can define Enforcement profiles under **Configuration > Enforcement > Profiles**. The MAC Caching Enforcement Profile is shown below.



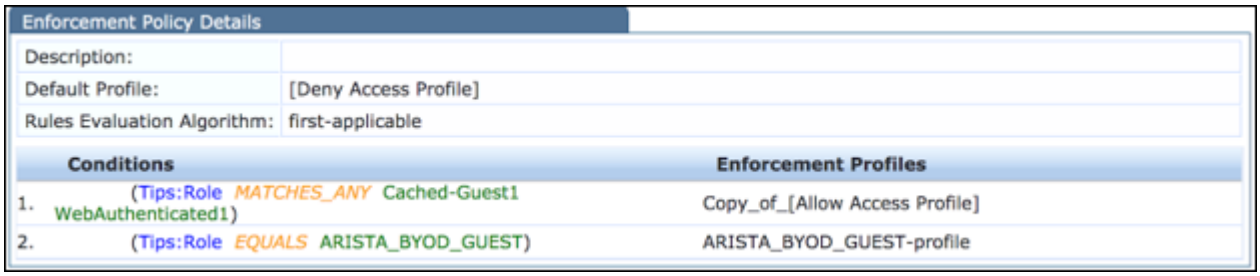

Note: The MAC-Authentication Expiry is set to five minutes in the figure above, which means that a guest user reconnecting within five minutes of a successful authentication will not need to re-authenticate.

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

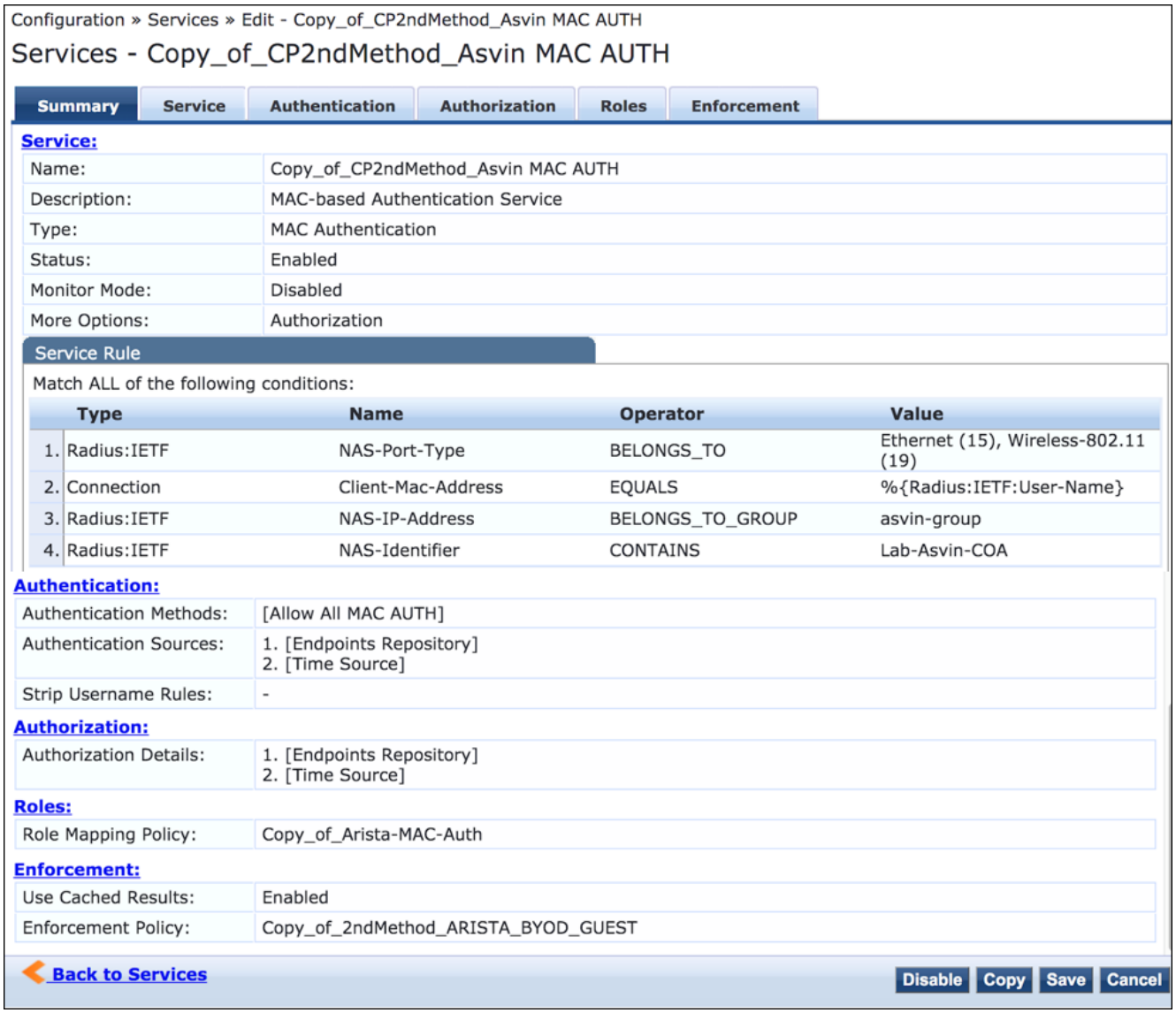
client matches a web-authenticated or cached guest, apply the “Post Auth” role. If any of the conditions are not met, then the default profile, i.e. “Deny”, kicks in.




Enforcement 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.




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




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


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.

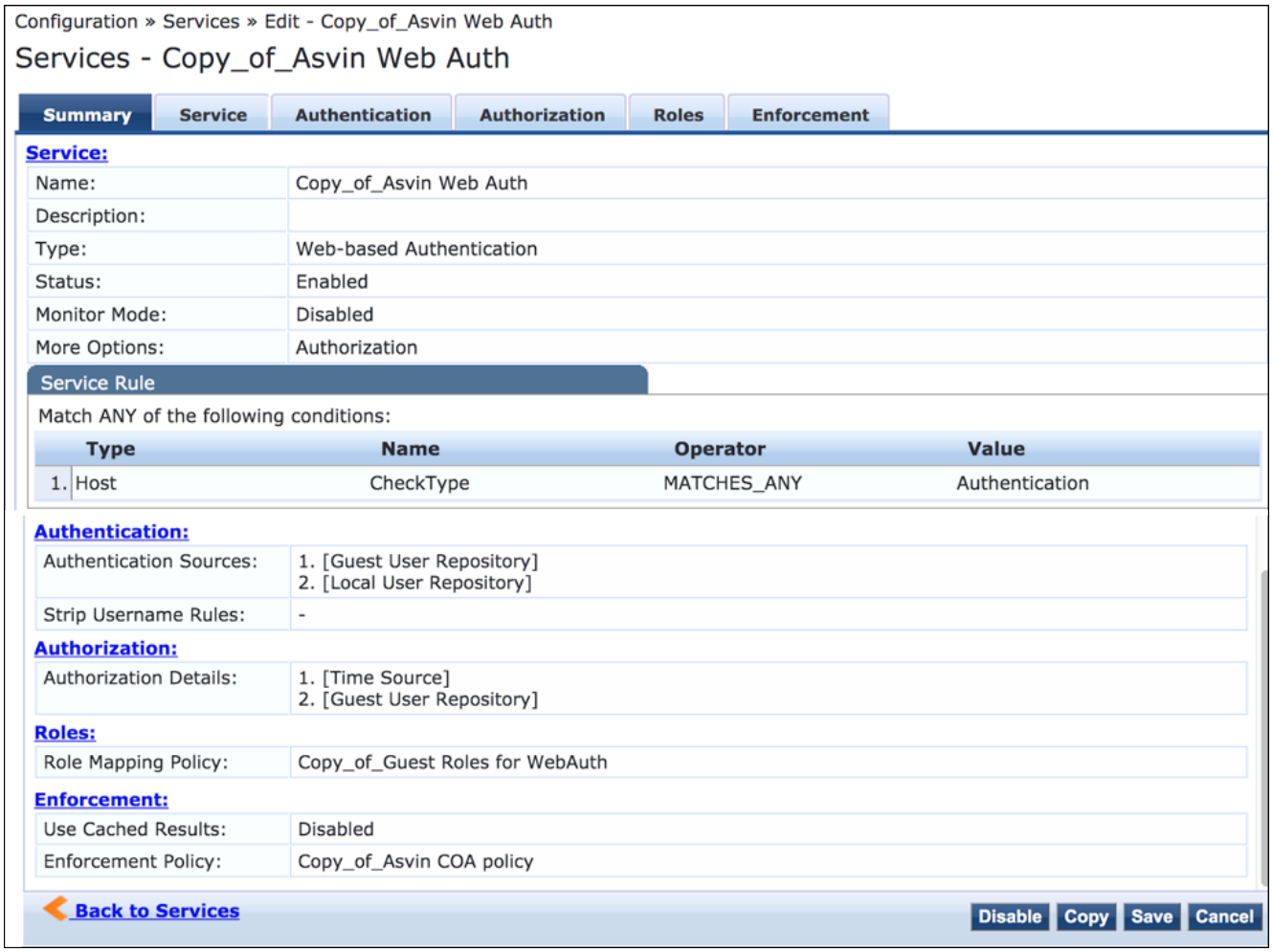
**Enforcement Policy Details**

| | |
|---|---|
| Description: | |
| Default Profile: | [Deny Access Profile] |
| Rules Evaluation Algorithm: | first-applicable |

| | Conditions | Enforcement Profiles |
|---|---|---|
| 1. | (Tips:Role *MATCHES_ANY* Cached-Guest1 WebAuthenticated1) | Copy_of_[Allow Access Profile] |
| 2. | (Tips:Role *EQUALS* 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.

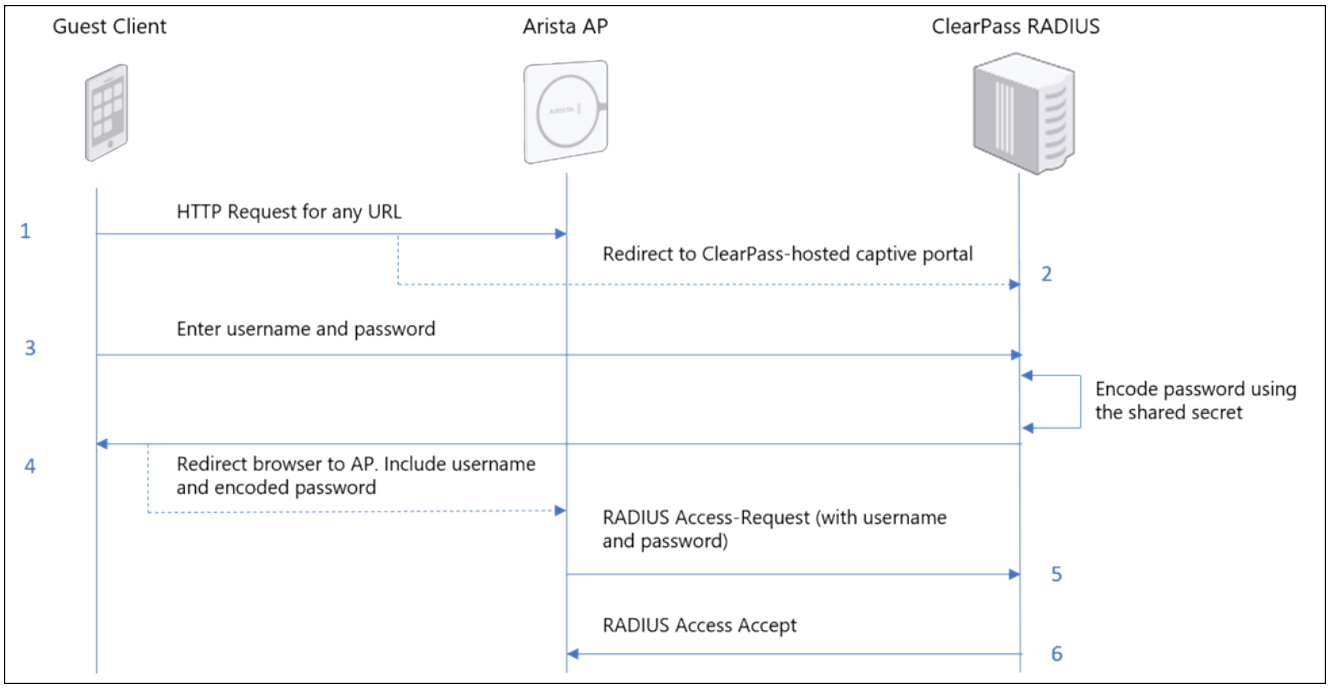



The process to configure the Web Authentication Service is the same as that of the MAC Authentication Service.

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.




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.

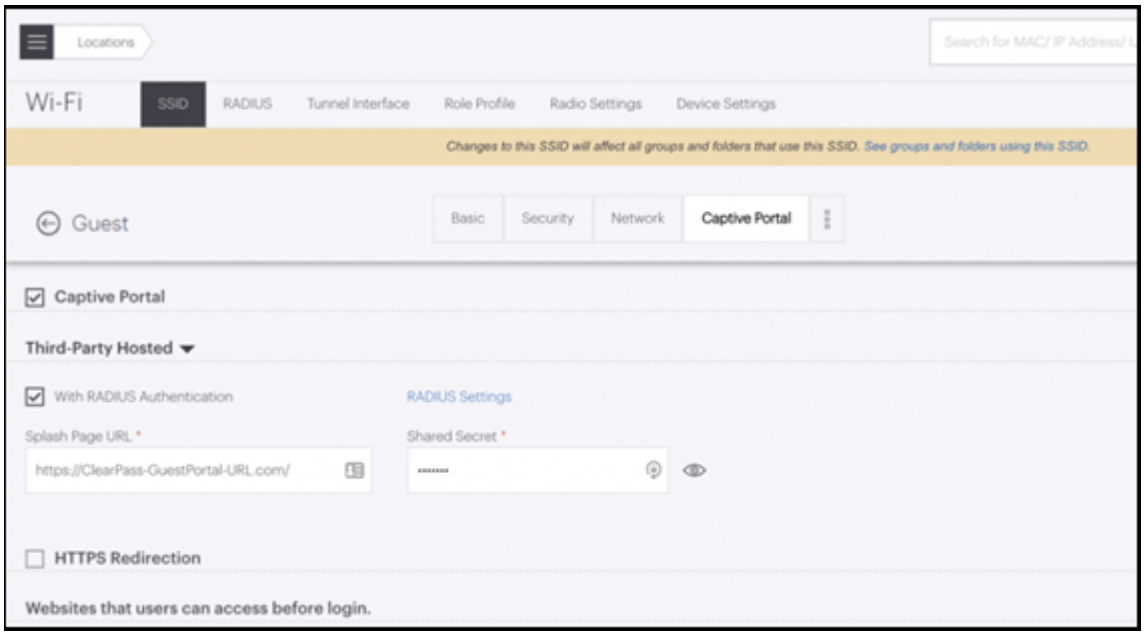
## CloudVision Cognitive Unified Edge Configuration

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.

1. 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.




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

## ClearPass Configuration

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.

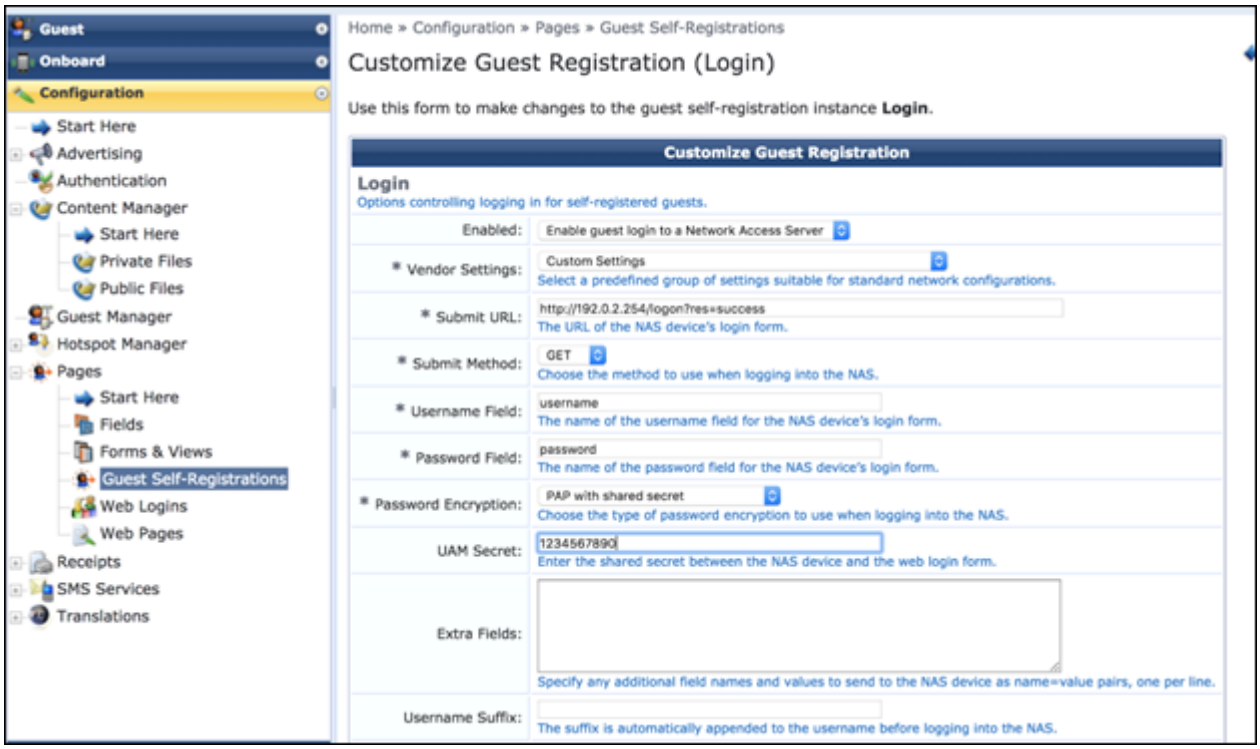
Broadly, the ClearPass configuration for Guest access consists of two steps:

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.




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.

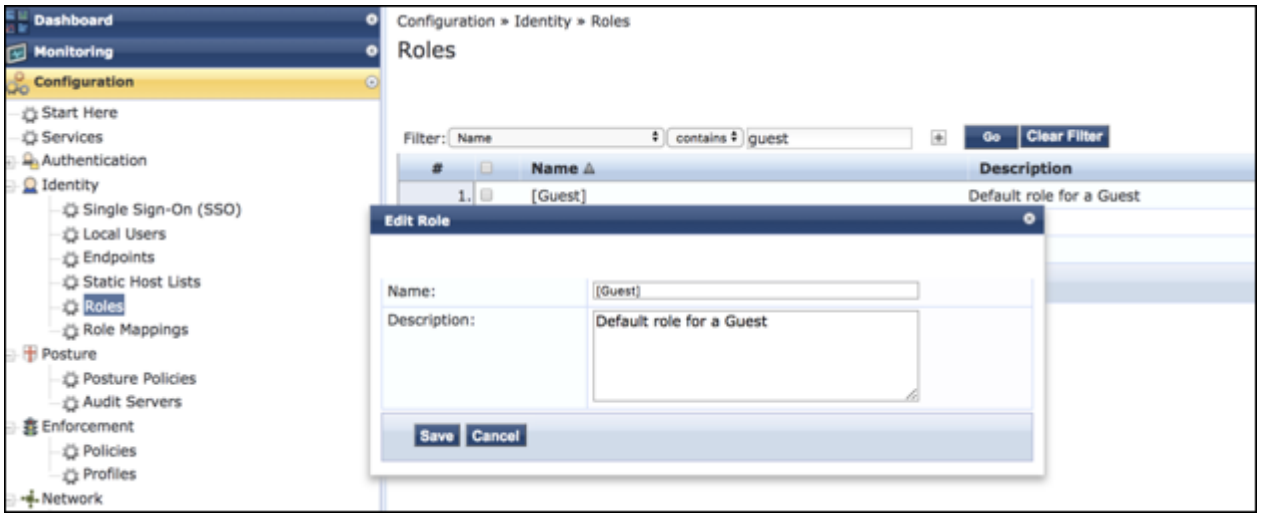
### Guest Access Control

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.

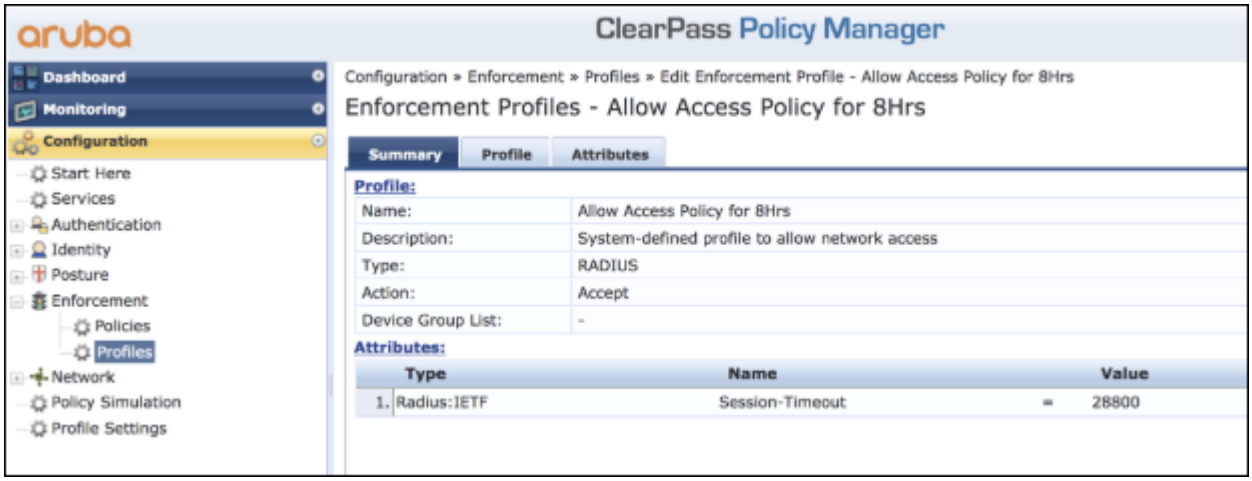
Each step is described in detail below.

1. Create the “Guest” role as shown below.

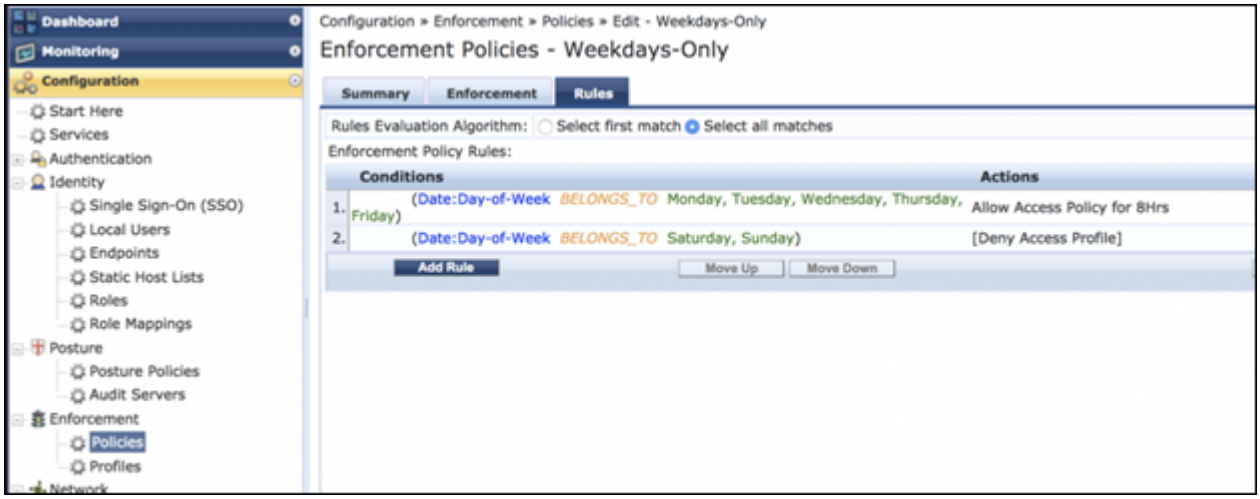



2. Because the Guest SSID has only one role, the workflow does not require any mapping as such. Select "Guest" as the Default Role and as the Role Name for whatever condition shows up in the Role Mapping below.


3. 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.



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.




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".