Creating a Network That Uses an Enterprise AAA Server

You can create a network that authenticates users against a remote authentication, authorization, and accounting (AAA) server. Before you create a network, write down the IP address, port number, and shared secret of the primary and secondary (if any) RADIUS server that you want to use to authenticate network users.

In non-proxy mode, an AP makes the RADIUS requests directly to the RADIUS server. The outbound connection is from the AP to the IP/FQDN of RADIUS on the RADIUS port in use by the RADIUS service. If this is an internet/ external RADIUS system, the APs must be able to reach the server from their locations, presumably via NAT or public routing.

For proxy mode, the controller makes the outbound RADIUS queries on behalf of the AP to the RADIUS system. Therefore, in this instance, the Cloud controller performs the outbound connection on the required port, and there is no firewall requirements for the customer (given that the Cloud is making the request). If you are hosting the RADIUS system, you must allow inbound connectivity to a routable or NAT'd IP address on the RADIUS port that is configured in the WLAN. In proxy mode, all the RADIUS requests from the AP to the controller passes over the existing control tunnel.

Complete the following steps to create a network that uses a remote AAA server.

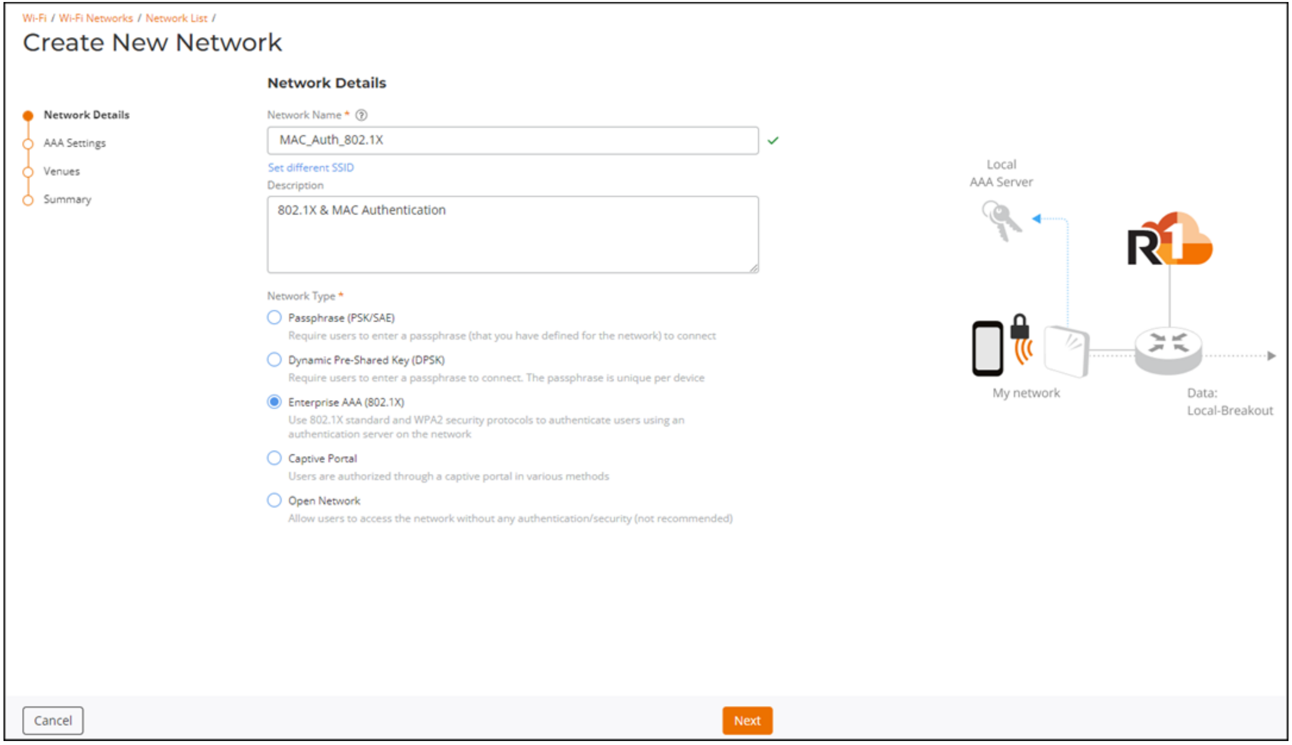
1. On the navigation bar, click Wi-Fi > (and then) Wi-Fi Networks > (and then) Wi-Fi Networks List.
   The Wi-Fi Networks page is displayed.

2. On the upper-right corner, click Add Wi-Fi Network. Alternatively, select an Enterprise AAA (802.1X) network setting that you want to copy and click Clone at the top of the table.
   The Create New Network page is displayed.

3. Complete the following settings in the Network Details page.
   - Network Name: Enter a name (up to 32 characters) that you want assign to the network.
   - Set different SSID: Use this option to configure the SSID different from the network name.
   - Description: Enter a description (up to 64 characters) to help you identify the network using.
   - Network Type: Select Enterprise AAA (802.1X).

   When the network type is selected, a structure diagram of an Enterprise AAA (802.1X) type of network is displayed.

Enterprise AAA (802.1X) Network



Wi-Fi / Wi-Fi Networks / Network List /

Create New Network

Network Details

Network Name * MAC_Auth_802.1X

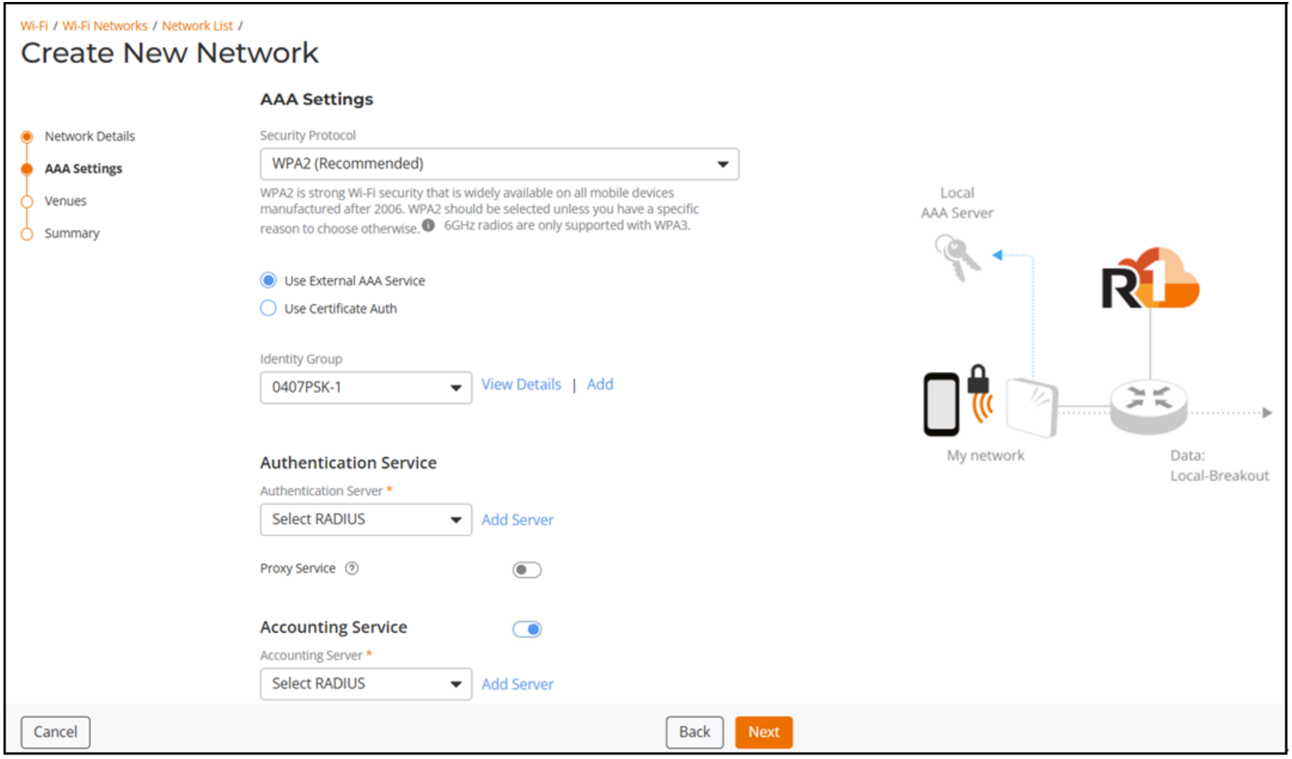
Description: 802.1X & MAC Authentication

Network Type *

- ○ Passphrase (PSK/SAE) — Require users to enter a passphrase (that you have defined for the network) to connect
- ○ Dynamic Pre-Shared Key (DPSK) — Require users to enter a passphrase to connect. The passphrase is unique per device
- ● Enterprise AAA (802.1X) — Use 802.1X standard and WPA2 security protocols to authenticate users using an authentication server on the network
- ○ Captive Portal — Users are authorized through a captive portal in various methods
- ○ Open Network — Allow users to access the network without any authentication/security (not recommended)

4. Click Next.
   The Enterprise AAA (802.1X) Settings page is displayed.

Enterprise AAA (802.1X) Settings Page



Wi-Fi / Wi-Fi Networks / Network List /

Create New Network

AAA Settings

Security Protocol: WPA2 (Recommended)

WPA2 is strong Wi-Fi security that is widely available on all mobile devices manufactured after 2006. WPA2 should be selected unless you have a specific reason to choose otherwise. 6GHz radios are only supported with WPA3.

- ● Use External AAA Service
- ○ Use Certificate Auth

Identity Group: 0407PSK-1

Authentication Service

Authentication Server * Select RADIUS

Proxy Service: off

Accounting Service: on

Accounting Server * Select RADIUS

5. Complete the settings on the Enterprise AAA (802.1X) Settings page.
   - Security Protocol : Select WPA or WPA2 (Recommend) from the drop down list. By default, WPA2

(Recommend) is selected.

> Note: For robust Wi-Fi security, WPA2 (Wi-Fi Protected Access 2) is an excellent choice. Widely supported on most mobile devices since 2006, it offers a strong foundation. However, if you're using cutting-edge technology with 6 GHz Wi-Fi radios, WPA3 might be necessary for optimal connection.

- By default, Use External AAA Service is selected. If you want to use a certificate authority, select Use Certificate Auth and select a certificate template from the Certificate Template drop-down or click Add to add a certificate template. Refer to *Adding a Certificate Template (GUID-20546881-B7BF-4ECB-BE83-F872CF04CC2B.html)* for instructions on how to add a certificate template.
- Identity Group: Select an identity group from the drop-down or click Add to add an identity group. Refer to *Adding an Identity Group (GUID-60E97713-D793-4659-86BF-94F8BF209EA6.html)* for instructions on how to add an identity group. To view details about the identity group, click View Details. The Identity Group sidebar is displayed.

  > Note:
  > - When an identity group is selected, all devices joining the network will automatically become an identity within that group, as displayed on the Identity Group page.
  > - Users have the option to either select an existing identity group from the list or create a new one.
  > - During network editing, the initially selected identity group cannot be removed; however, it can be changed to a different identity group.
  > - The identity configuration section is not applicable to the MAC Registration List when MAC Authentication is enabled.

- Authentication Service: Select the existing RADIUS Server from the drop down list or complete the following steps to add a new RADIUS Server.

  a. Click Add Server and configure a new RADIUS Server. Refer to *Creating a Radius Server Profile (GUID-F0DFD674-D2E0-42F8-AA09-CBCBE9E419BF.html)*.

- Proxy Service: Toggle switch to ON to enable the proxy service.

  > Note: Use the controller as proxy in 802.1X networks. A proxy AAA server is used when APs send authentication/accounting messages to the controller and the controller forwards these messages to an external AAA server.

- Accounting Service: Toggle the switch to ON to enable this option and select the existing RADIUS Server from the drop down list or complete the following steps to add a new RADIUS Server.

  a. Click Add Server and configure a new RADIUS Server. Refer to *Creating a Radius Server Profile (GUID-F0DFD674-D2E0-42F8-AA09-CBCBE9E419BF.html)*.

- Proxy Service: Toggle switch to ON to enable the proxy service.

  > Note: Use the controller as proxy in 802.1X networks. A proxy AAA server is used when APs send authentication/accounting messages to the controller and the controller forwards these messages to an external AAA server.

- MAC Authentication: Toggle the switch to ON to enable the MAC Authentication feature and select a MAC Address Format from the drop-down.

Supported MAC address format are:

- Upper case MAC address separated by colons: 70:EA:5A:78:A1:A0
- Upper case MAC address separated by hyphens: 70-EA-5A-78-A1-A0
- Upper case MAC in a continuous string: 70EA5A78A1A0
- Lower case MAC address separated by colons: 70:ea:5a:78:a1:a0
- Lower case MAC address separated by hyphens: 70-ea-5a-78-a1-a0
- Lower case MAC in a continuous string: 70ea5a78a1a0

Note:

- MAC Authentication provides an additional level of security for corporate networks. Client MAC addresses are passed to the configured RADIUS servers for authentication and accounting.
- By default, the MAC Authentication is disabled.
- Changing the MAC Authentication option requires you to re-create the Enterprise AAA (802.1X) network.Currently, there is no edit option for this feature.

In the 802.1X and MAC Authentication method, MAC authentication is the first layer of security—a list of authorized MAC addresses is configured on the network device first. Devices with MAC addresses that are not on the list are denied access to the network. The 802.1X authentication method uses a RADIUS server to verify the user’s identity (for example, username, password) before granting access to the network. A RUCKUS AP grants access to UE only after both the MAC authentication and 802.1X authentication are successful.

6. Click Show more settings.
   By default, the VLAN sub-tab is displayed. Each sub-tab includes additional Wi-Fi configuration options to configure the settings of your preference. Refer to *Configuring Additional Settings for a Wi-Fi Network (GUID-8AE1D265-5C9B-4B71-9A5C-A57C3CFA586A.html)* to configure each of the available settings.

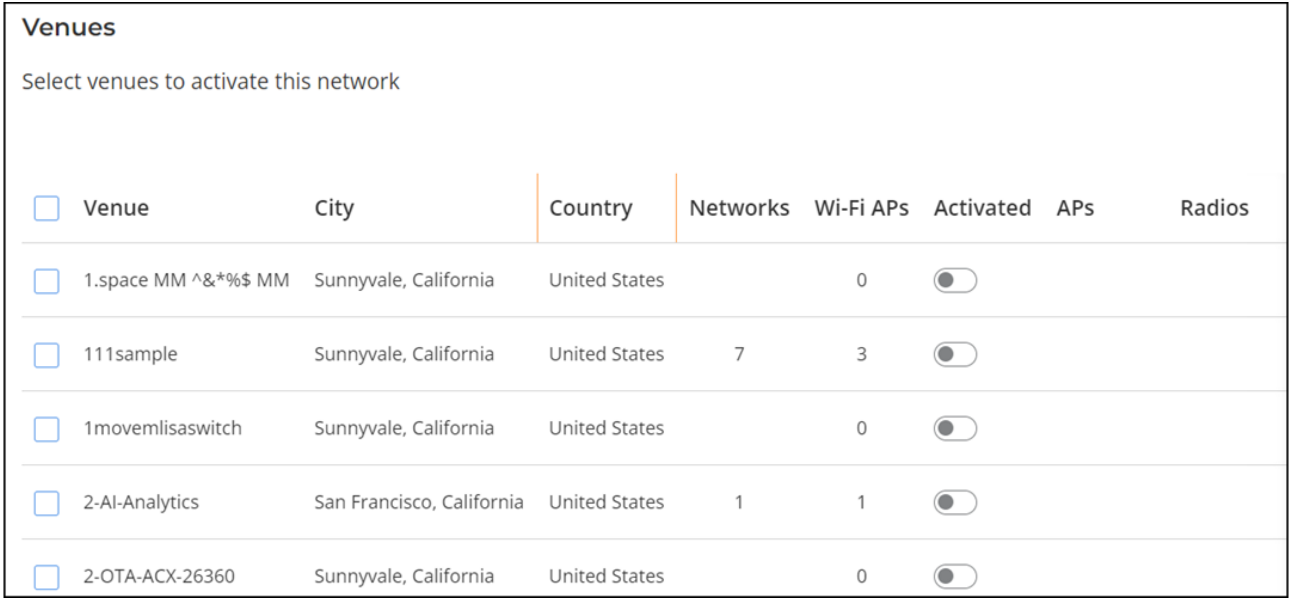
   Note:

   Demonstration of Advanced Settings for a Wi-Fi Network. This video explains advanced settings for a Wi-Fi network and walks you through the process of configuring them.

Click to play video in full screen mode. (https://play.vidyard.com/Jm3S4CCwJX2Z2N8E9qAZdJ)

7. Click Next to go to the Venues page and select venues to activate this network.
   The Venues page is displayed.

   Venues Page



Venues

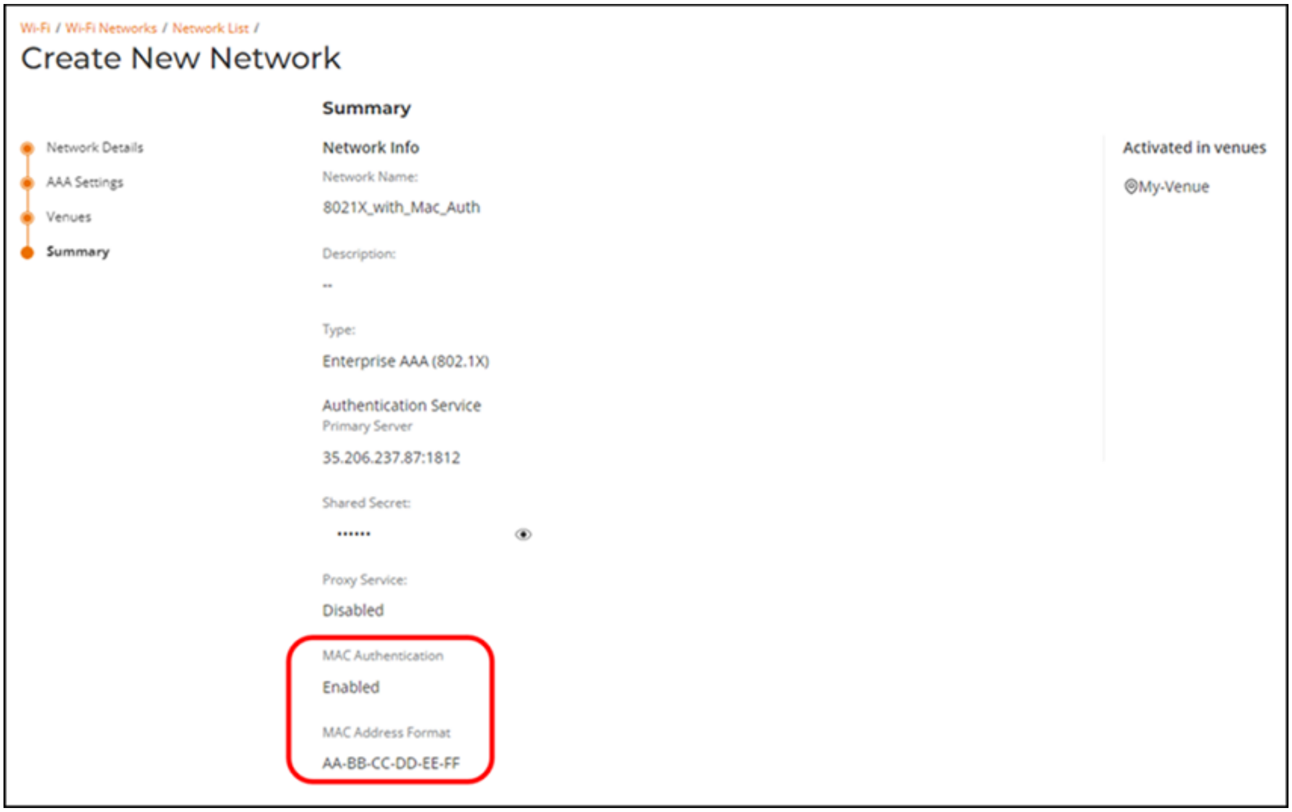
Select venues to activate this network

□	Venue	City	Country	Networks	Wi-Fi APs	Activated	APs	Radios
□	1.space MM ^&*%$ MM	Sunnyvale, California	United States		0	○		
□	111sample	Sunnyvale, California	United States	7	3	○		
□	1movemlisaswitch	Sunnyvale, California	United States		0	○		
□	2-AI-Analytics	San Francisco, California	United States	1	1	○		
□	2-OTA-ACX-26360	Sunnyvale, California	United States		0	○		

8. Click Next.

   Example: The Summary page is displayed.

   Network Summary



Summary

Network Info

Network Name:
8021X_with_Mac_Auth

Description:
--

Type:
Enterprise AAA (802.1X)

Authentication Service
Primary Server
35.206.237.87:1812

Shared Secret:
••••••

Proxy Service:
Disabled

MAC Authentication
Enabled

MAC Address Format
AA-BB-CC-DD-EE-FF

Activated in venues
My-Venue

9. Review the settings that you configured. To display the Shared Secret in plain text, click the eye icon.

10. Click Finish.