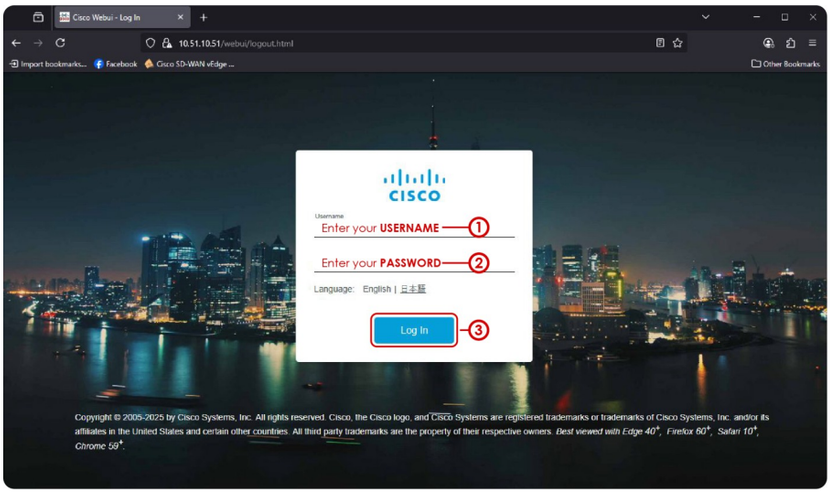
Wireless Enterprise: RADIUS Configuration (C9800AXI-AP-K9 IOS-XE)

This guide will walk you through configuring the C9800AXI-AP-K9 Embedded Wireless Controller using **802.1X with RADIUS Single Sign-On (SSO)**.

Access the Web GUI

Start by accessing the C9800AXI-AP-K9 by opening its IP address on a web browser.

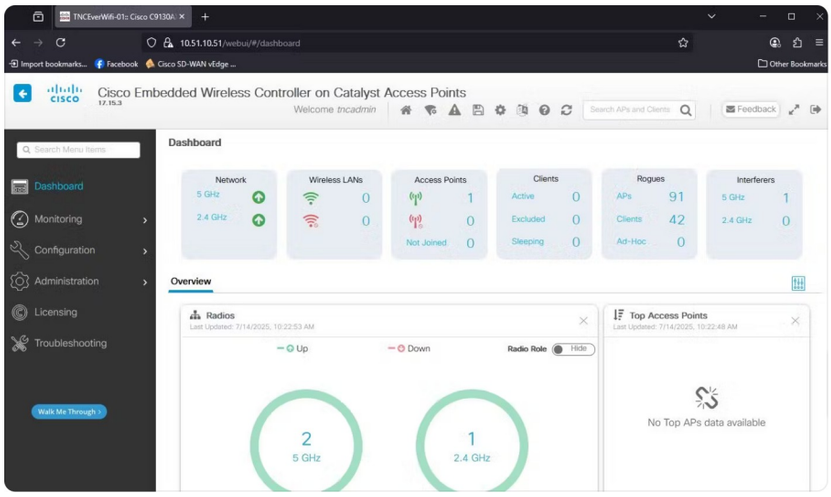


Enter the **Username (1)** and **Password (2)**, then **Login (3).**

> *In case of a forgotten username and password, simply access the CLI (Command Line Interface) of the Controller and enter the following commands on Privilege EXEC mode:*

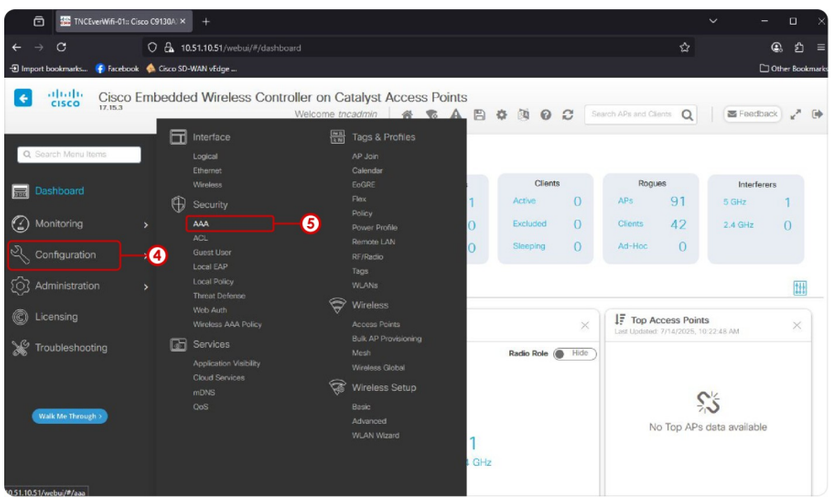
```
!@C9800AXI-AP-K9
conf t
 username admin privilege 15 secret pass
 ip http authentication local
 end
```

Once you've logged in, you should gain access to the dashboard.

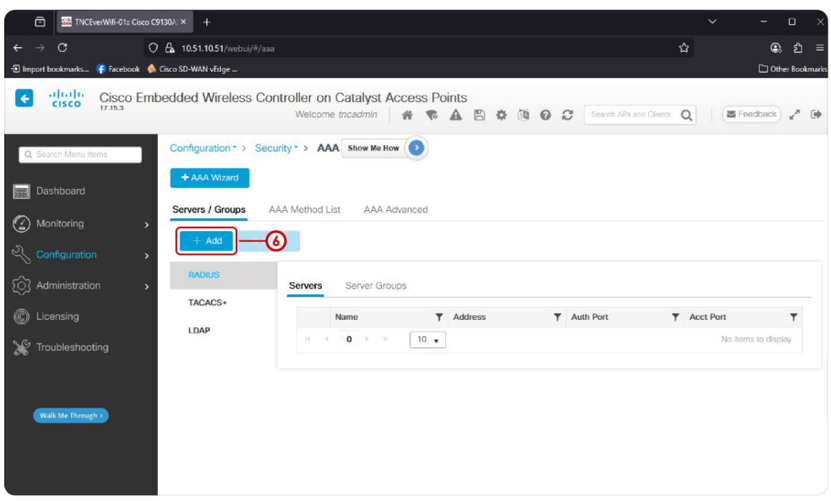


Add the RADIUS Server

On the side navigation menu, select **Configuration (4)** > then, under Security, select **AAA (5)**

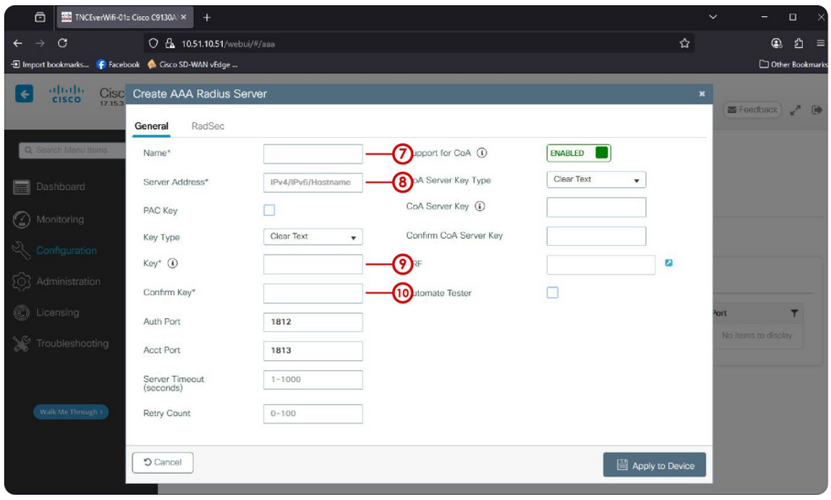


Under Servers/Groups, **Add (6)** a RADIUS Server

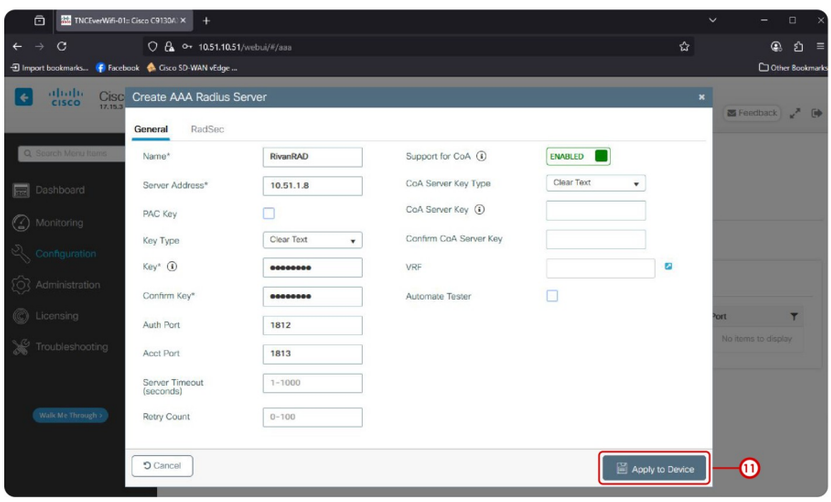


Fill in the following information:

- **Name (7)** of the Radius Server. This information is local to the controller.
- **Server Address (8)** the IP address of the Radius Server. Make sure the IP is pingable from the Controller's CLI, or attempt to ping the IP of the controller from where the Radius server is configured (Ex. Windows Server, Linux, etc.)
- **Key (9 & 10)** the shared secret configured on the Radius Server.

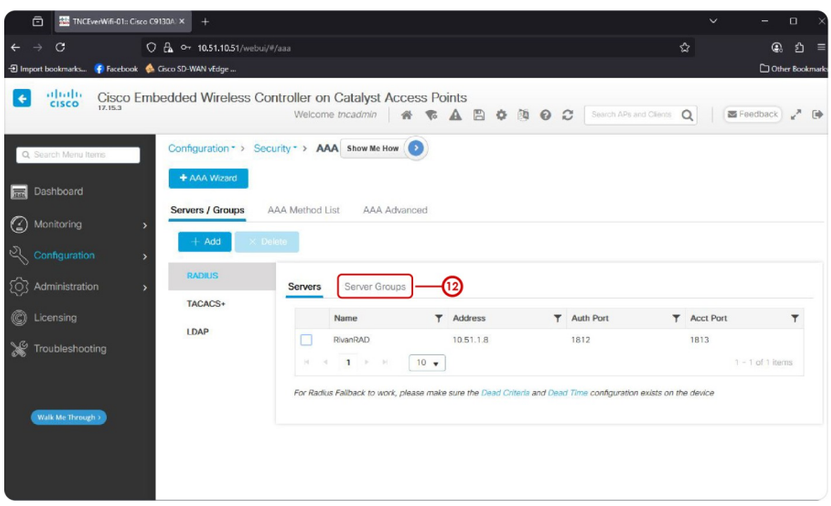


Example output:



Once filled in, **Apply to Device (11)**

Next, select **Server Groups (12)**



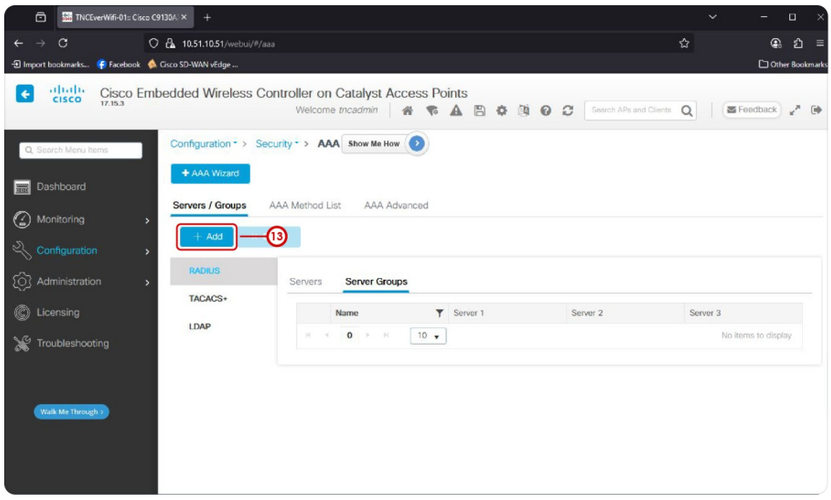
Why Server Groups?

Load Balance and Fail-over

If you only have one Radius Server you won't need to configure Server Groups.

HOWEVER, for best practice and future possibilities, assigning the current Radius Server to its own group, albeit by itself, would make it easier to add additional Radius Server's in the future.

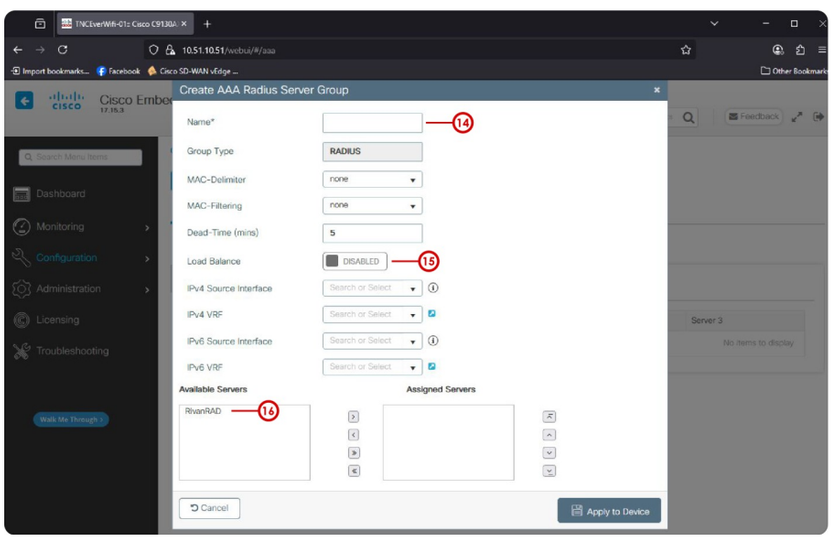
With that, **Add (13)** a Radius Server Group.



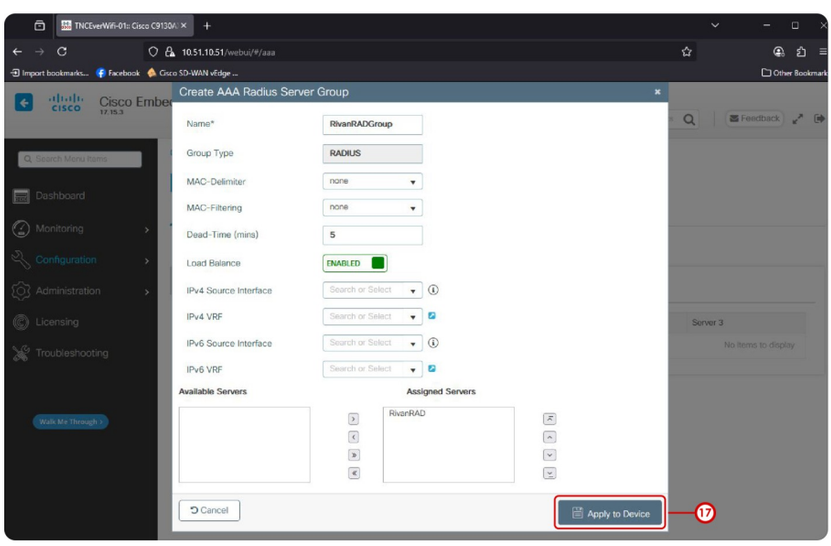
Provide a **Name (14)** for the Radius Server Group and turn on **Load Balance (15).**

Then under the Available Servers panel, select the name of your Radius Server, in this example, it's **RivanRAD (16).**

Then select the arrow button, **>**, to add the server to the Assigned Servers panel.



Example output:

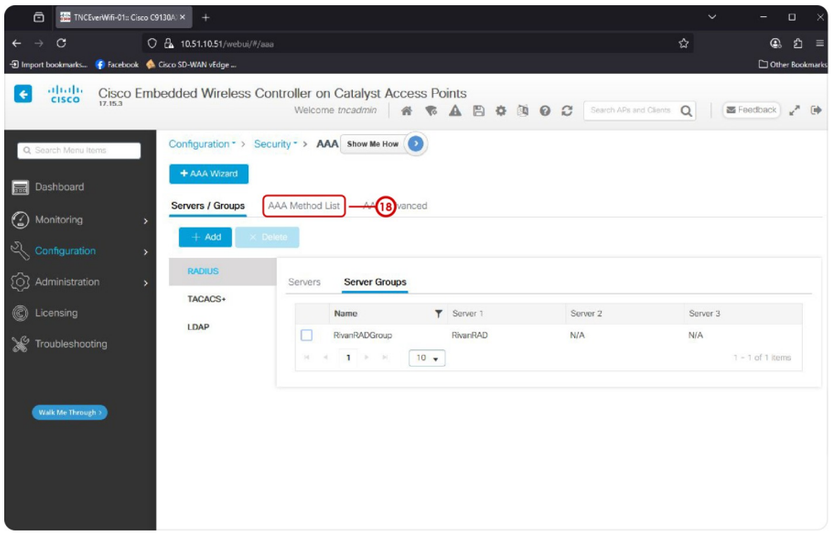


Then, **Apply to Device (17)**

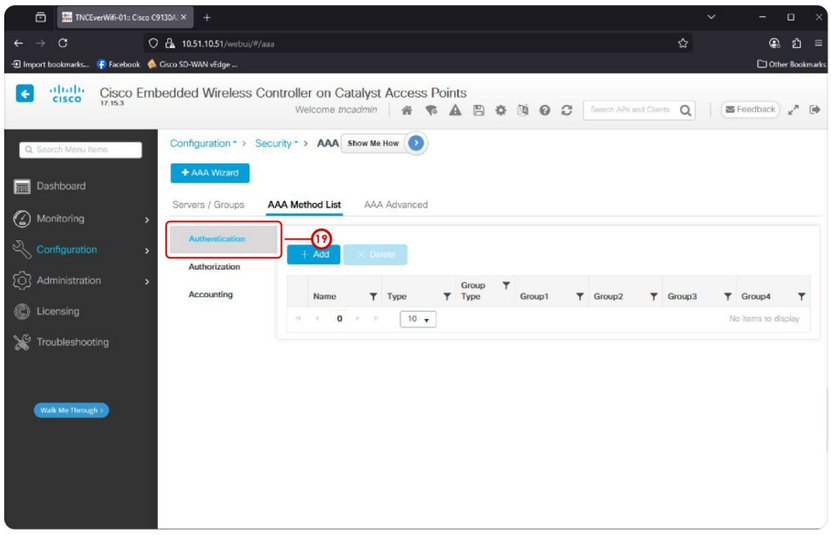
Once applied, the Server is know known by the controller.

However, it has yet to assign the Radius Server to **Authenticate**, **Authorize**, and **Account** for its potential users.

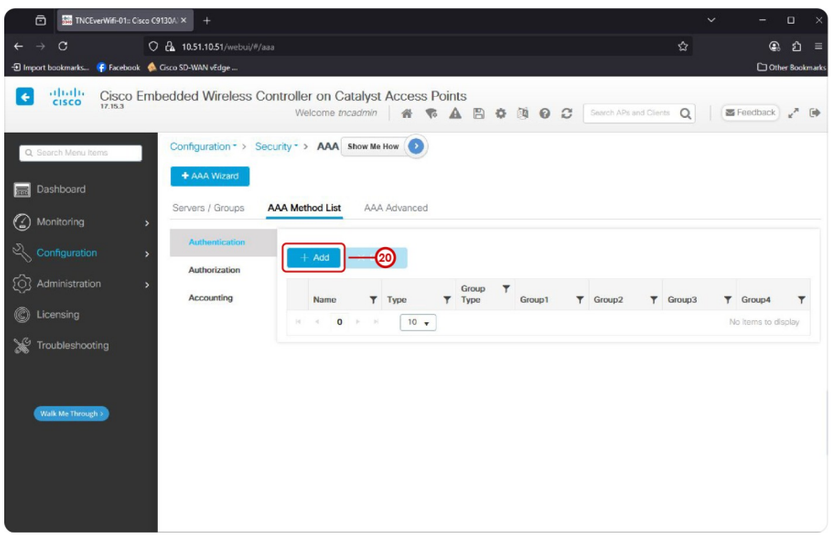
To configure the radius server for AAA, select **AAA Method List (18)**



Make sure the **Authentication (19)** tab is selected.

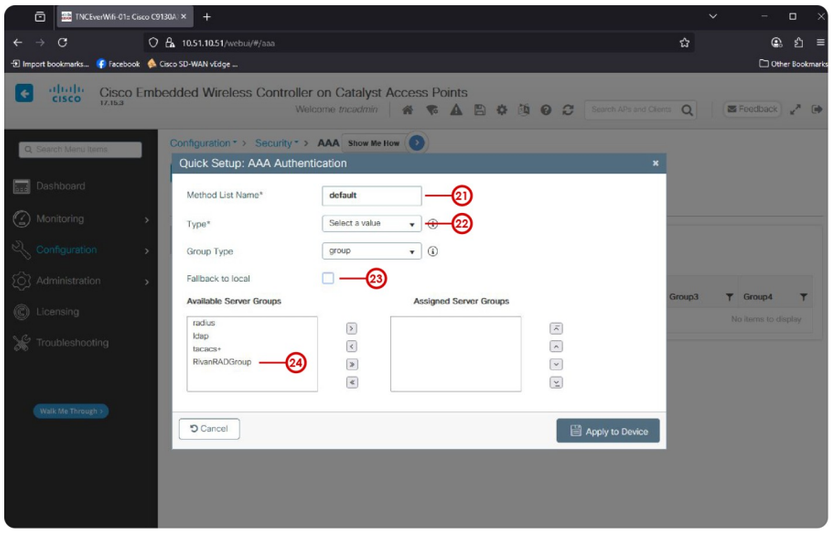


Then, **Add (20)** a Radius Server/Group to be assigned for Authentication.

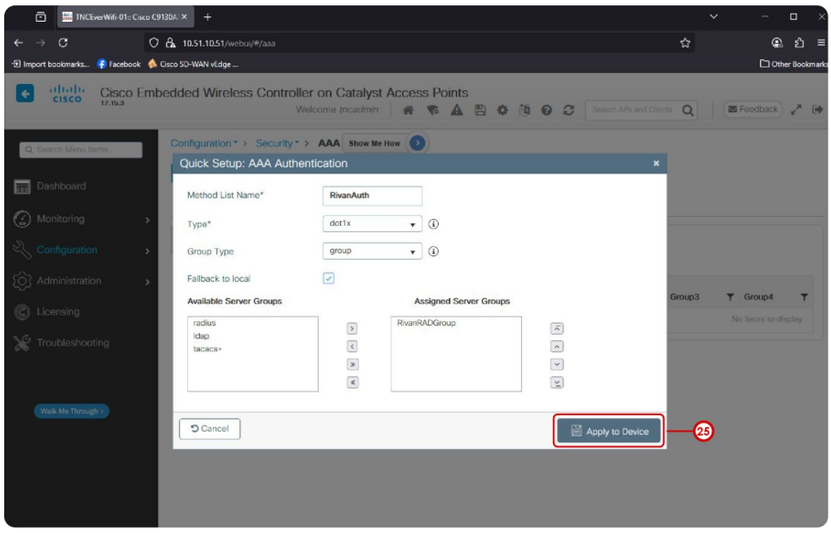


Fill in the following information:

- **Method List Name (21)**
- **Type (22)** this is used for MAC filtering, simply choose **Network.**
- **Fallback to local (23)** even though we don't have Radius configured on the controller, it wouldn't be a bad idea to select the box.
- Select your Radius Server Group, in this example it's **RivanRADGroup (24)**. Then just like before, select the arrow button, > , to add the Server Group to the Assigned Server Groups panel.

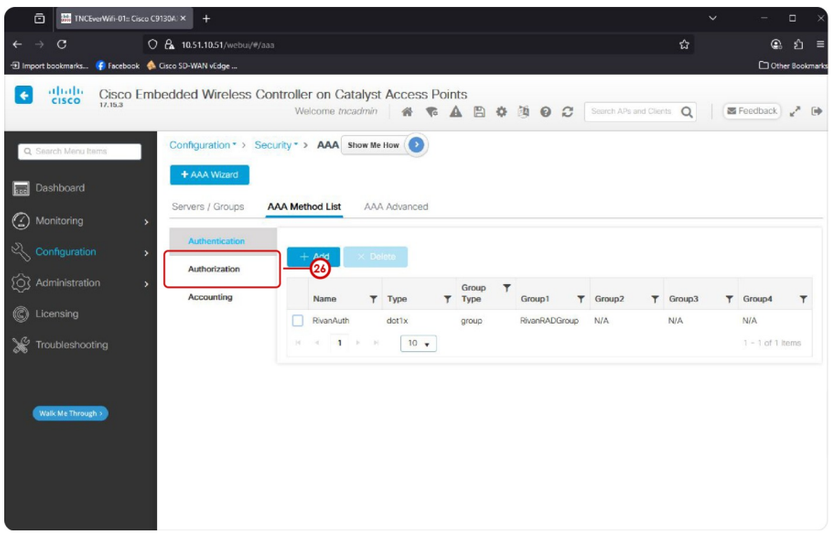


Example output:

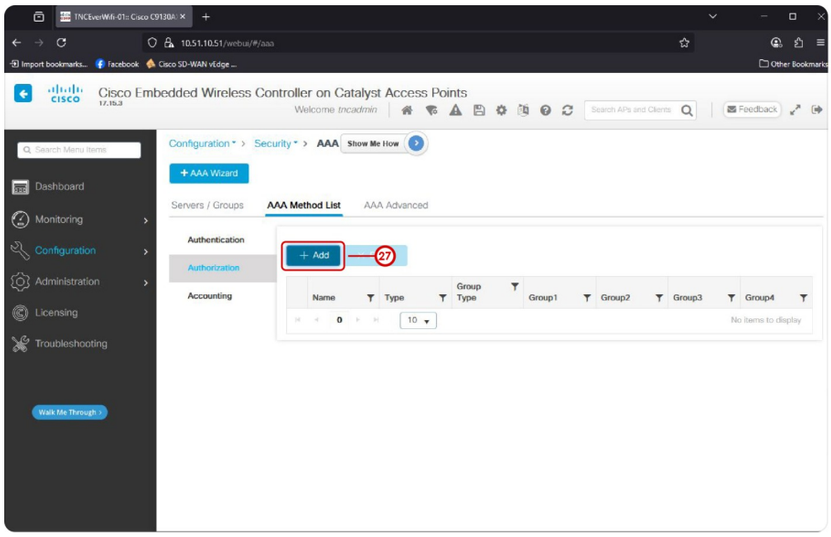


Then, **Apply to Device (25)**

Now do the same for **Authorization (26)**

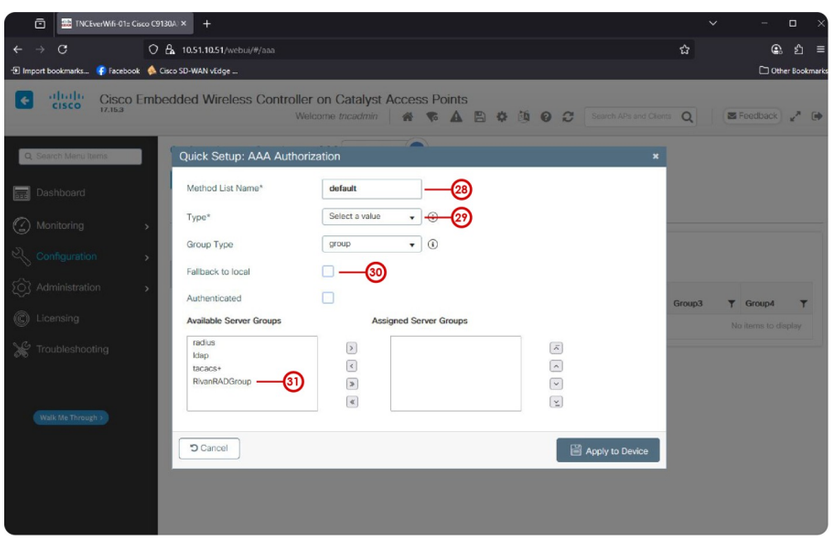


Add (27) a Radius Server/Group to be assigned for Authorization.

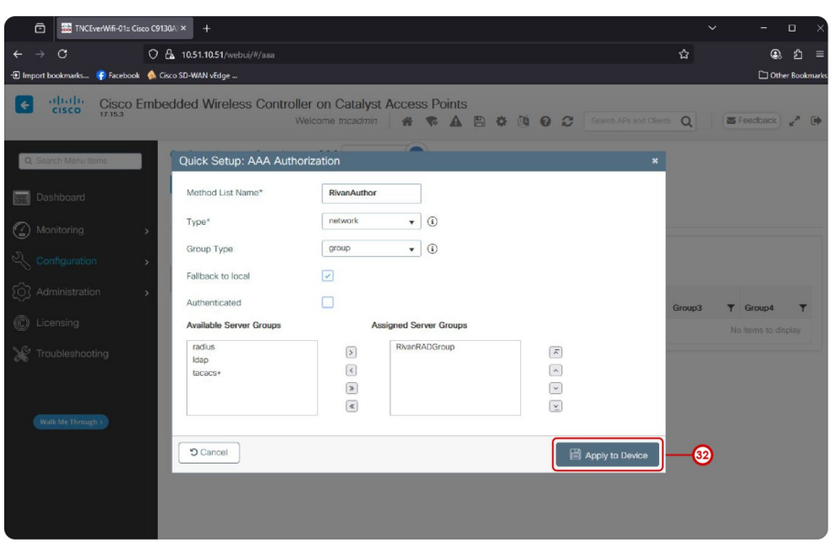


Fill in the following information:

- **Method List Name (28)**
- **Type (29)** this is used for MAC filtering, simply choose **Network.**
- **Fallback to local (30)** even though we don't have Radius configured on the controller, it wouldn't be a bad idea to select the box.
- Select your Radius Server Group, in this example it's **RivanRADGroup (31)**. Then just like before, select the arrow button, > , to add the Server Group to the Assigned Server Groups panel.

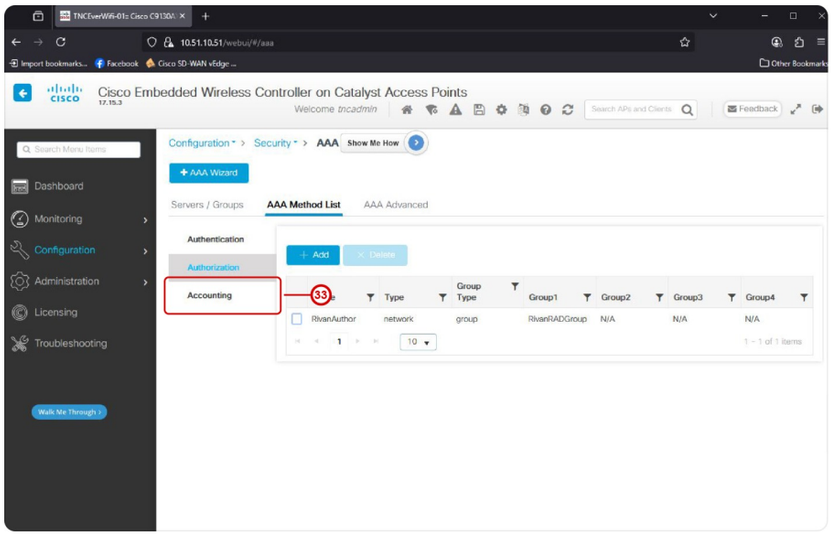


Exaple output:

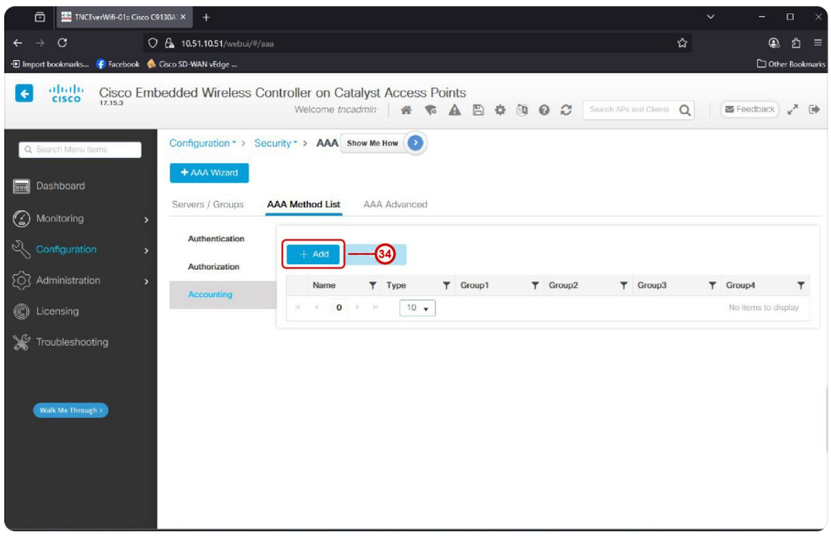


Then, **Apply to Device (32)**

Now, select **Accounting (33)**

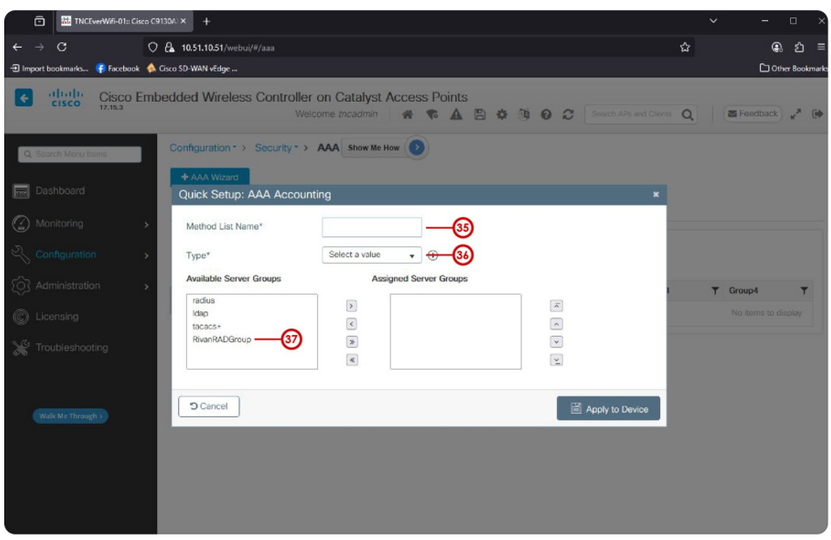


Add (34) a Radius Server/Group to be assigned for Accounting.

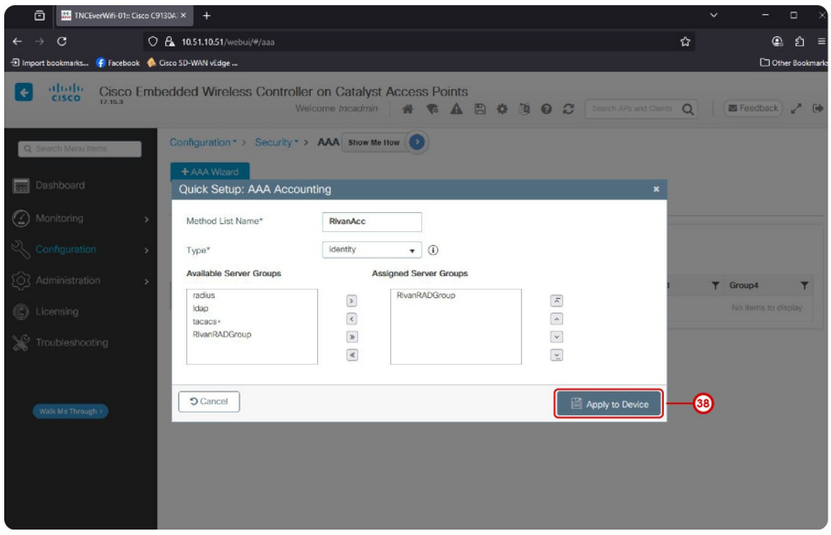


Fill in the following information:

- **Method List Name (35)**
- **Type (36)** this specifies what the Radius Server will keep track of in order to account for users, simply choose **Identity.**
- Select your Radius Server Group, in this example it's **RivanRADGroup (37)**. Then just like before, select the arrow button, > , to add the Server Group to the Assigned Server Groups panel.



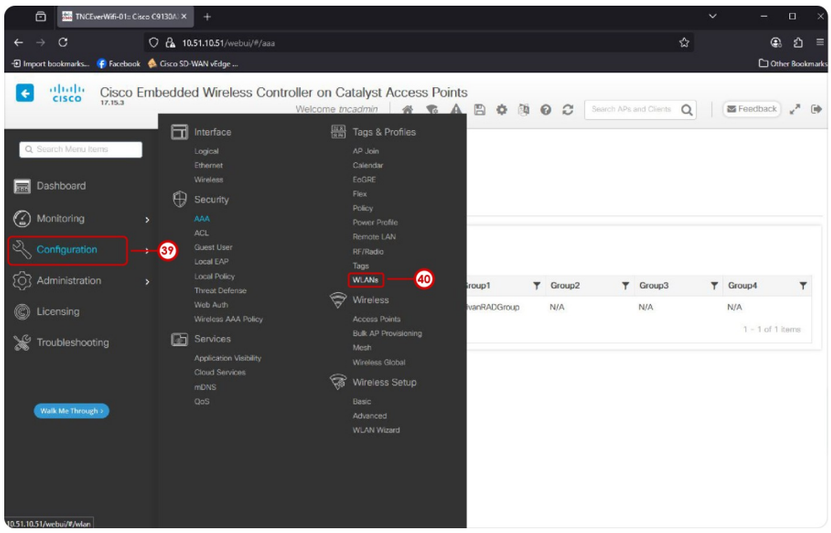
Example output:



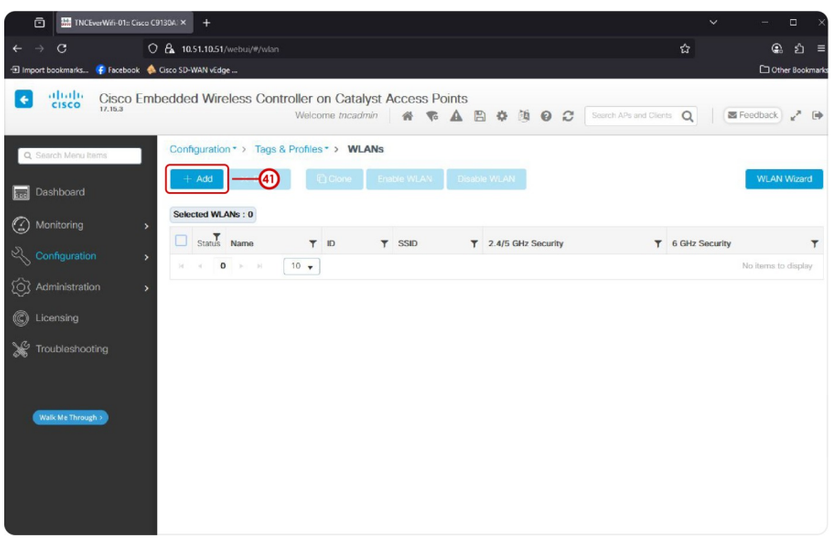
Finally, **Apply to device (38)**

Setup a WLAN for Enterprise Security

On the side navigation menu, select **Configuration (39)** > then, under Security, select **WLANs (40)**

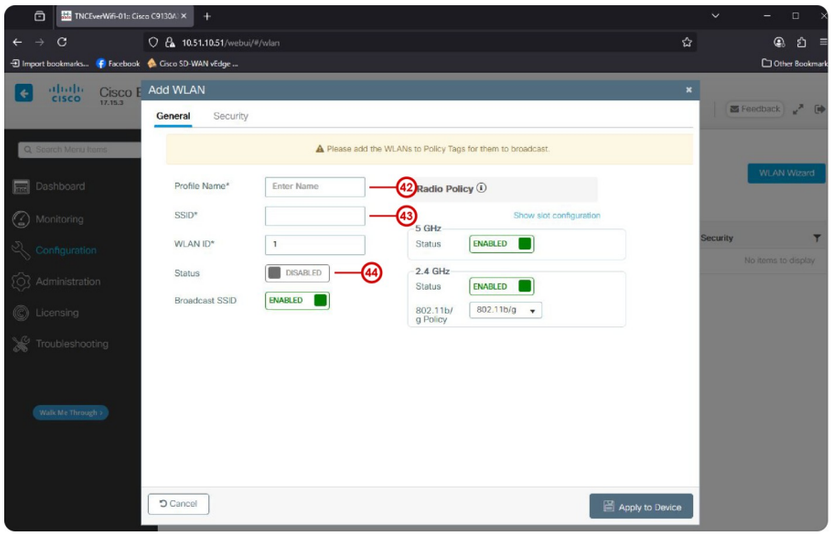


On the WLANs page, **Add (41)** a WLAN.

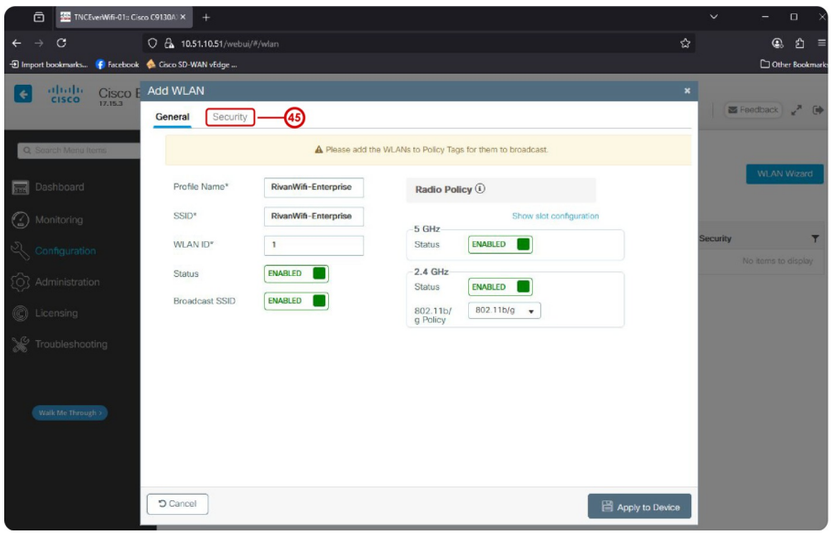


Fill in the following information:

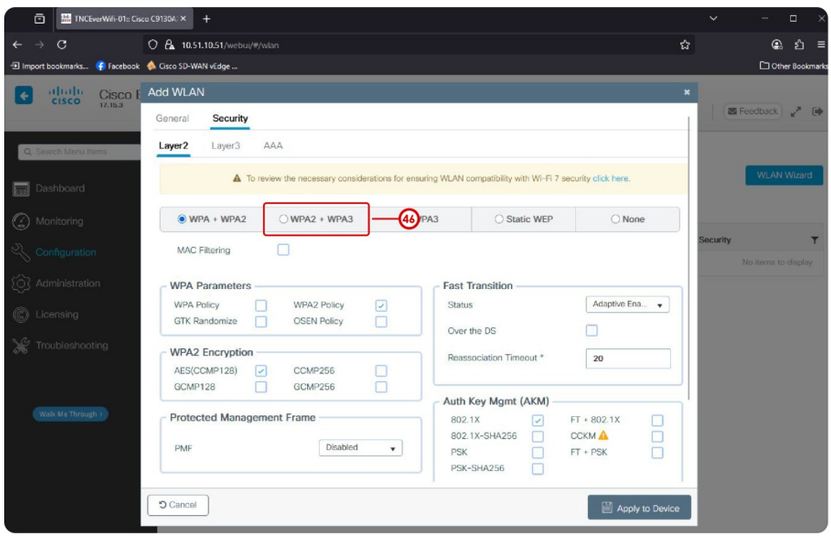
- **Profile Name (42)** will be automatically assigned as the **SSID (43)**
- **Status (44)** Enable the WLAN to be ready to broadcast wireless frames.



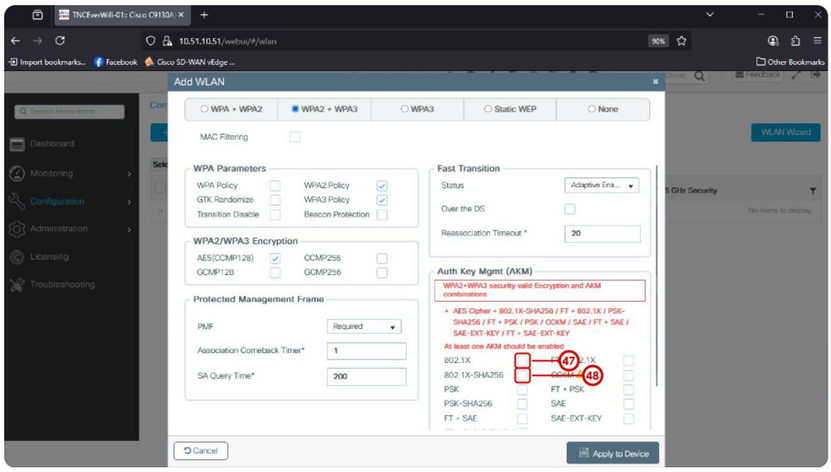
Then, select **Security (45)**



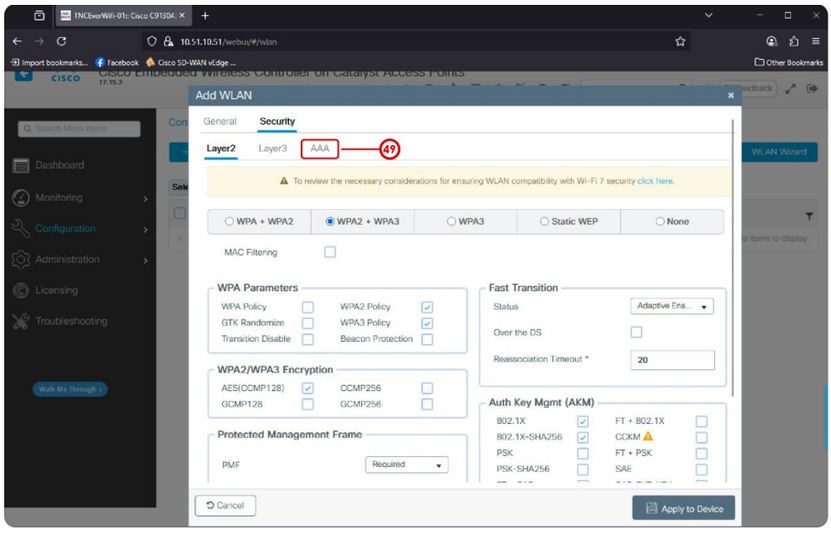
There are plenty of options, for this example we will choose **WPA2 + WPA3 (46)**



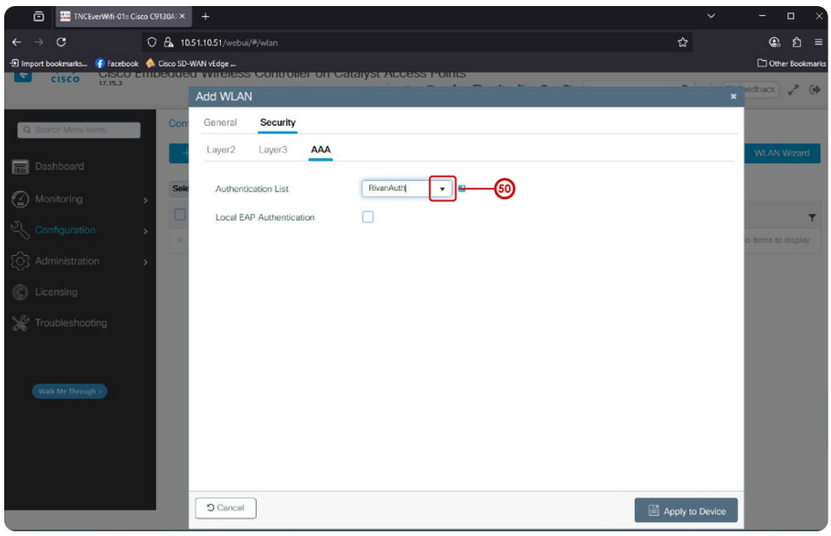
For **Auth**entication and **Key Management**, select **802.1X (47)** and **802.1X-SHA256 (48).**



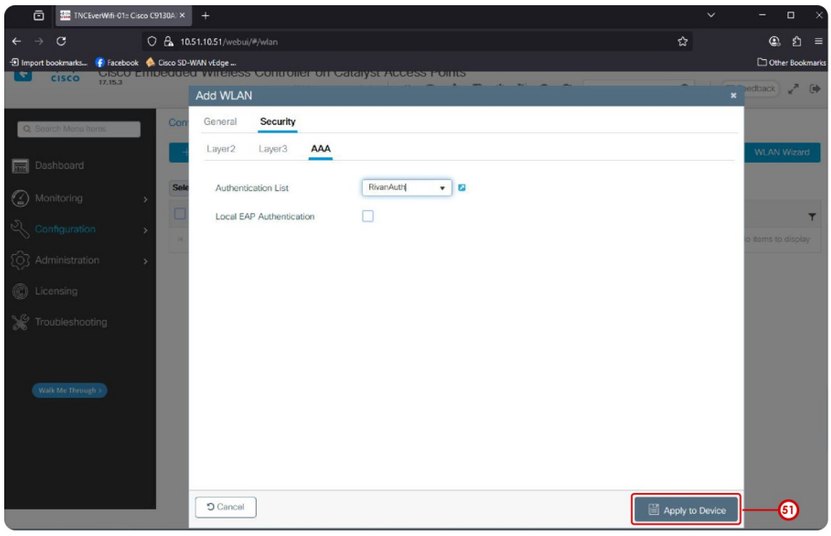
Then, select the **AAA (49)** tab.



Then, for **Authentication List (50)**, choose the Radius Server/Group that was chosen for Authentication.



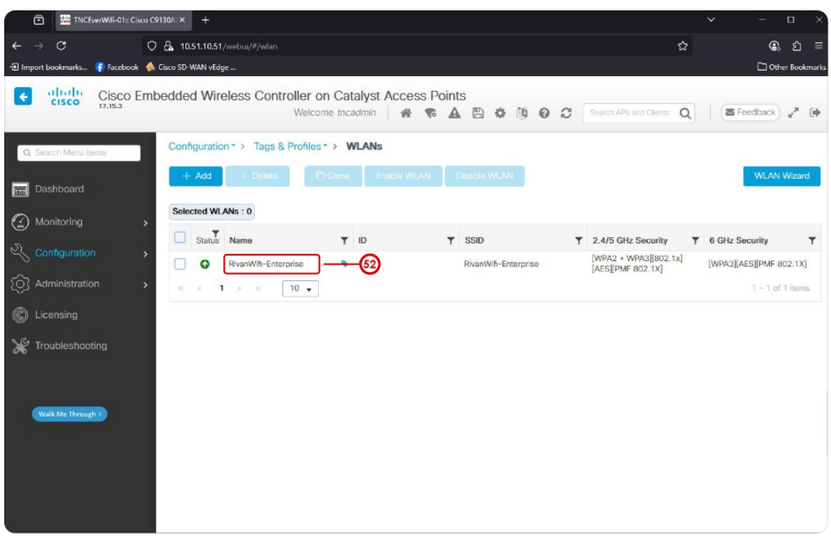
Expected output:



Then, **Apply to Device (51)**

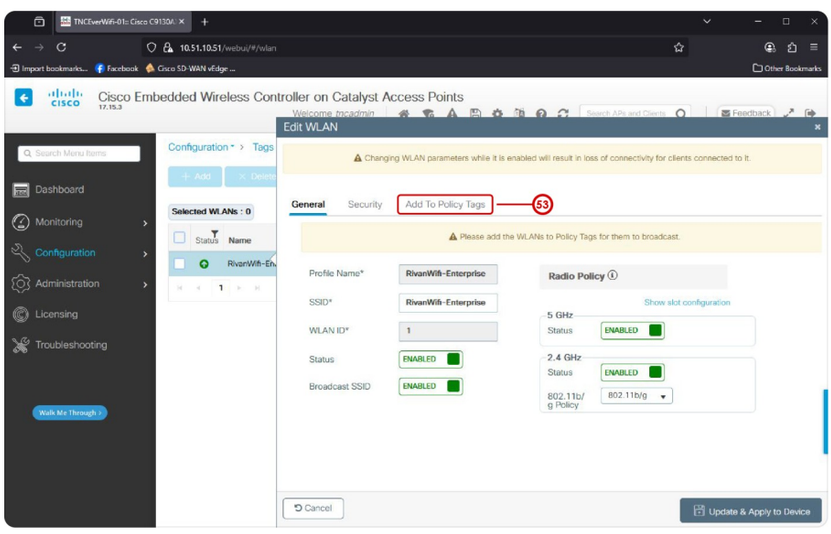
Now, even though the WLAN is configured to be Enabled, it still won't broadcast wireless frames because the WLAN needs to have a policy tag assigned to it.

Simply select the recently created WLAN, in this case it's **RivanWifi-Enterprise (52)**

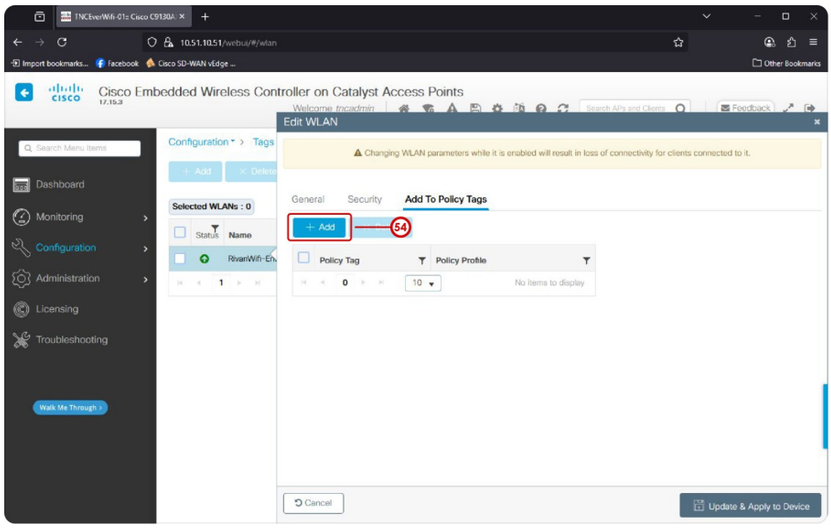


You will see an informational message telling use that WLANs need to be added to Policy Tags for them to broadcast.

Select the **Add to Policy Tags (53)** tab.

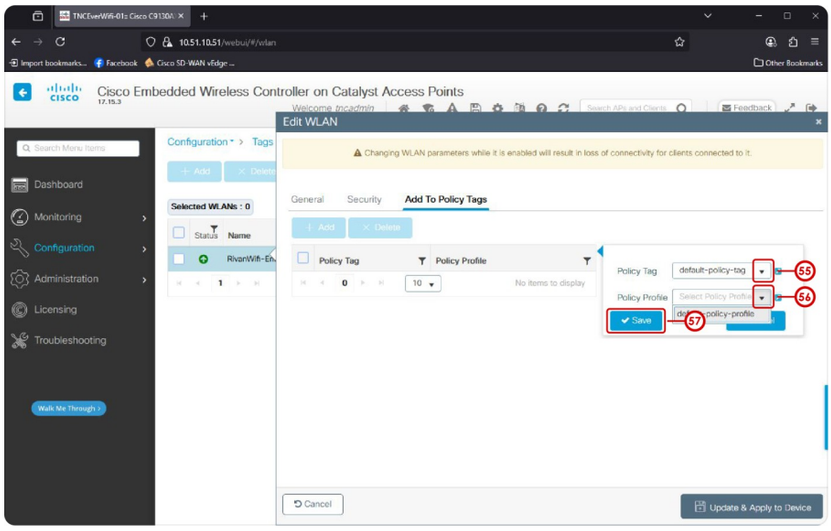


Add (54) a Policy Tags.

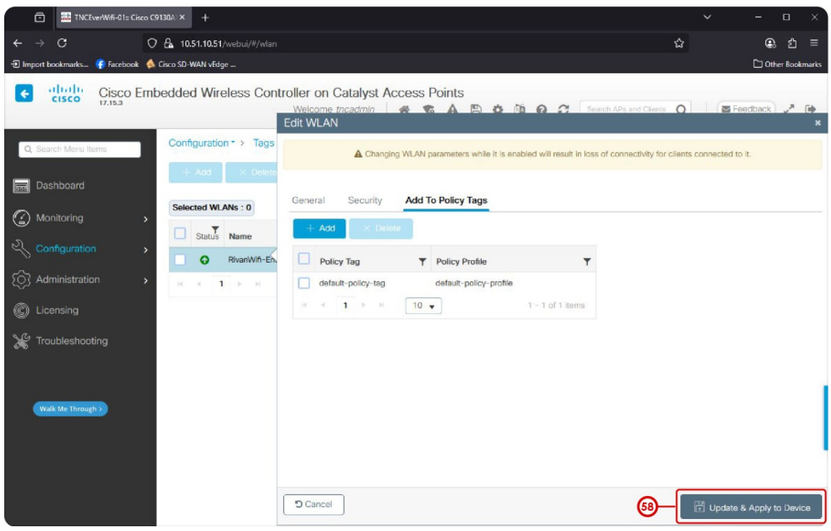


Then simply choose the default **Policy Tag (55)** and **Policy Profile (56)**, unless you have already configured your own.

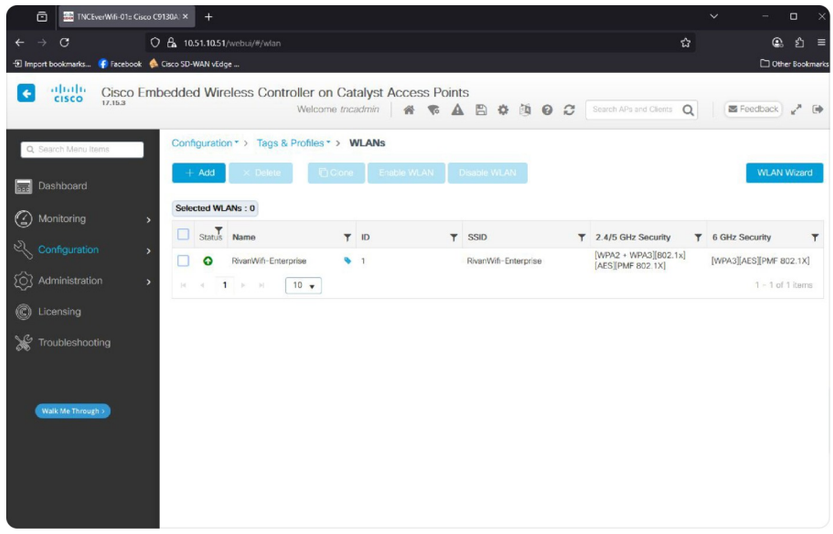
Once set, select **Save (57)**



Expected output:



Finally, confirm your configurations by selecting **Update & Apply to Device (58)**



Congratulations!!! You've configured a WLAN with **Enterprise Wireless Security :D**