Objective

Remote Authentication Dial In Service (RADIUS) is a network protocol which is used for centralized authentication, authorization and accounting purposes. When a user wants to access some resources on a network, the user identity has to be verified first. The access point requests user credentials which are then passed to a RADIUS server to grant access with the use of the RADIUS protocol. Credentials generally include a username and a password or security certificate from the user. These credentials are verified by the server based on an authentication scheme, upon which the RADIUS server can allow or block the user access to the network resources.

This article explains how to configure RADIUS server settings on an AP541N Access Point.

Applicable Device

• AP541N Access Point

Software Version

• AP541-K9-2.0(4)

RADIUS

Step 1. Log in to the Access Point Configuration Utility and choose Wireless > Wireless Network Setup (VAPs). The Wireless Network Setup (VAPs) page opens:

![Wireless Network Setup (VAPs) page](image)

Step 2. Expand the Global RADIUS server settings.

Step 3. Enter the primary RADIUS server IPv4 address in the RADIUS IP Address field.

Step 4. Enter the primary RADIUS key. If created, the key authenticates communication between the AP and RADIUS server.

Note: You can use multiple RADIUS servers to authenticate users. If the primary RADIUS server fails, then the others are tried in sequence.
Step 5. Enter up to 3 backup RADIUS IP addresses.

Step 6. Enter 3 backup RADIUS Keys for the Addresses. If backup servers are created, the key authenticates communication between the AP and RADIUS server.

Step 7. (Optional) To enable RADIUS server, check the **Enable Radius Accounting** check box. This creates a log of resource usage by the clients. It includes time and the amount of data transmitted and received by the client via access point.

Step 8. Click **Apply** to save the settings. This enables the RADIUS accounting.