ARISTA

Configure A Basic Corporate SSID

Table of Contents

Configure A Basic Corporate SSID

(Applicable to software release 8.9.0 and higher)

To configure an SSID in CloudVision WiFi (CVW), go to **Configure > WiFi > SSID**. CVW groups SSID settings into nine function-based tabs:

- Basic
- Security
- Network
- Access Control
- Analytics
- Captive Portal
- RF Optimization
- SSID Scheduling
- Traffic Shaping & QoS.

Note: The Basic, Security, and Network tabs are mandatory. You must save the settings under these tabs before you can turn an SSID on.

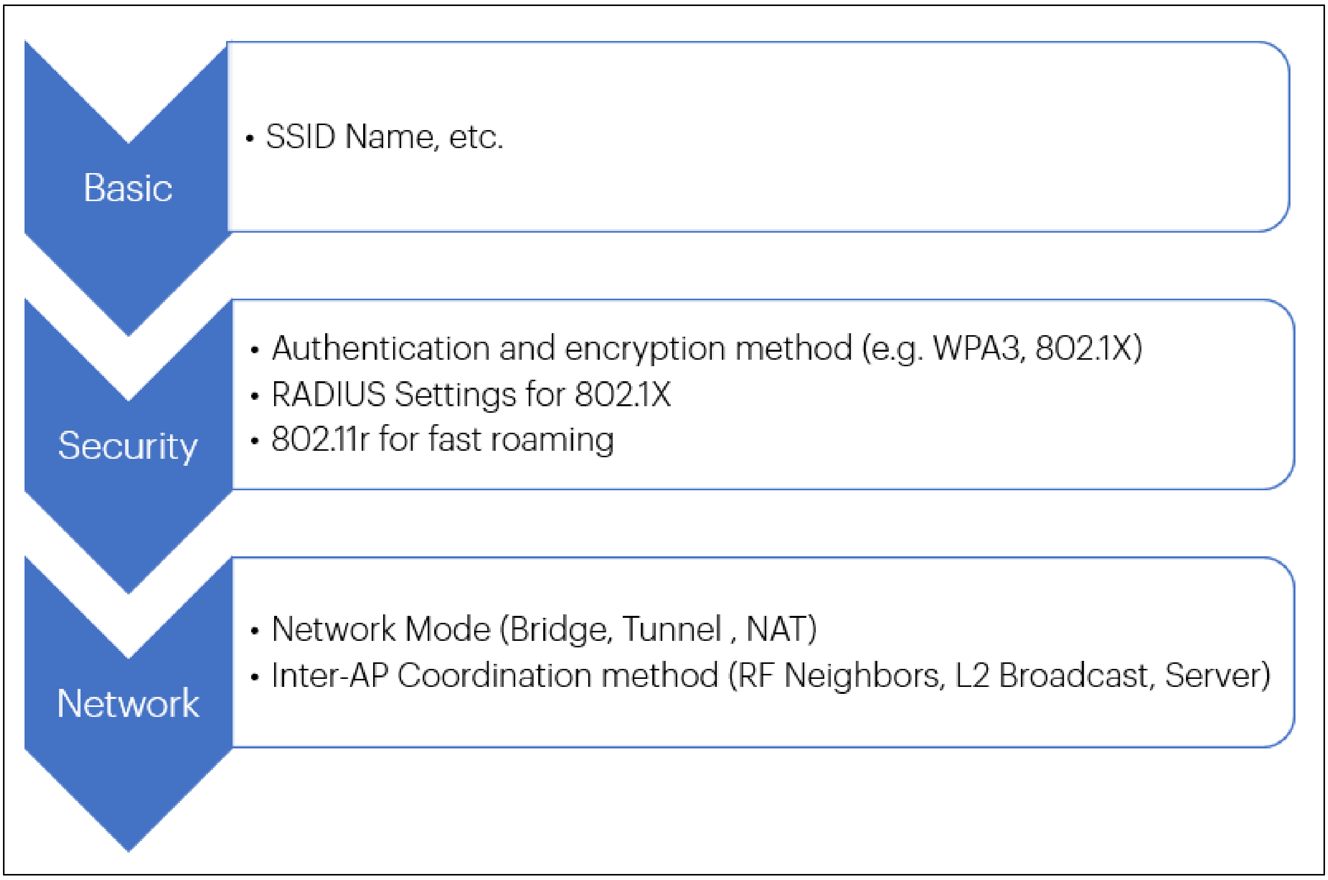
You can set up an open SSID (i.e., one without any authentication) with default network settings in just three clicks: simply click **Next** in the Basic and Security tabs, and click **Save & Turn SSID On** in the Network tab. An enterprise network, however, requires robust authentication mechanisms and encryption that can't be achieved with a basic three-click setup.

Enterprise networks typically have at least two different SSIDs: a corporate SSID for their employees and a guest SSID for visitors. The corporate SSID allows employees to access the internet as well as resources on the corporate intranet, whereas the guest SSID allows visitors to access the internet but not the enterprise intranet resources.

Let's configure a basic, secure corporate SSID using the three mandatory tabs.

Configure a Secure Corporate SSID

This section describes the mandatory Basic, Security, and Network tabs to set up a secure corporate SSID. The following figure shows the workflow and the key settings under each tab.



Basic

- SSID Name, etc.

Security

- Authentication and encryption method (e.g. WPA3, 802.1X)
- RADIUS Settings for 802.1X
- 802.11r for fast roaming

Network

- Network Mode (Bridge, Tunnel , NAT)
- Inter-AP Coordination method (RF Neighbors, L2 Broadcast, Server)

Typically, a corporate SSID:

- uses WPA3 enterprise (i.e., WPA3 with 802.1X RADIUS authentication) and
- operates on a bridged network.

Basic Settings

The steps to configure the basic SSID settings are as follows:

1. To create an SSID, go to **Configure > WiFi > SSID** and click **Add New SSID**. The Basic tab appears.
2. Enter the **SSID Name**. This is what the WiFi access point (AP) advertises to clients in the SSID beacon. The **SSID Profile Name** is internal; it's not advertised in the beacon.
3. Select **Private** as the SSID type. You would select Guest for the guest SSID.
4. Click **Next** to move to the Security tab.

Security Settings

Enterprise networks typically use a RADIUS server for 802.1X authentication of WiFi clients. Arista WiFi supports integration with commonly used identity management solutions including Forescout, ClearPass, and ISE.

The steps to configure the corporate SSID security settings are as follows:

1. Select the authentication method under the **Select Security Level** dropdown. For this corporate SSID, we select **WPA3** with the **WPA3 Enterprise** option. WPA3 offers more robust protection than WPA2.

Note:

- WPA3 is supported only on 802.11ax APs. Do not select WPA3 or WPA2/WPA3 Mixed Mode for SSIDs that run on any non-802.11ax APs.
- Select **WPA2/WPA3 Mixed Mode** if you're not sure that all the clients connecting to the SSID support WPA3. In the mixed mode, clients that support WPA3 can connect with WPA3 and ensure higher data security and privacy, while legacy clients that do not support WPA3 can connect to the same SSID using WPA2.

2. The WPA3 Enterprise option uses WPA3 and 802.1X authentication with a RADIUS server. Under the **Primary** tab, select the primary **Authentication Server** from the drop down menu containing the RADIUS profiles. If you haven't yet configured a RADIUS profile, you can do so by clicking the **Add/Edit** option below the primary Authentication Server drop down.

3. To configure a **RADIUS profile**, enter the following:

- **RADIUS Server Name**. This is simply a name you can assign to identify the RADIUS profile. This is the name that appears in the SSID Authentication Server and Accounting Server drop down lists.
- The **IP Address** of the RADIUS server.
- The **Authentication Port** number and the **Accounting Port** number to be used for the respective messages.
- The **Shared Secret** used by the AP to authenticate with the RADIUS server.

4. Select an **Accounting Server** if you want the SSID to support RADIUS accounting features. Similarly, select and configure the secondary RADIUS servers for redundancy and failover.

5. The **Retry Parameters** define the number of times the AP will try to reach the RADIUS server before considering it down and initiating the changeover from primary to secondary or vice versa.

6. The **Called Station** and **NAS ID** can be used to pass additional information to the RADIUS server for policy and decision making. You can define these as per your need using upto four different parameters—the MAC address of the AP, the location of the AP, the SSID, and the name of the AP—to differentiate requests from different APs.

7. The **Fast Handoff Support** options optimize the WiFi client roaming experience by reducing the number of steps that a client has to go through when re-associating with another AP. For details on how Fast Handoff works, see the Fast Handoff section on the WiFi Help portal.

8. Enable **Dynamic VLANs** if you want the RADIUS server to assign a VLAN to an authenticating WiFi client from the list of VLANs you specify.

9. A **Change Of Authorization** (CoA) message from the RADIUS server can be used to change some settings of an authenticated user session. For example, you can use CoA to assign VLANs to a user or to

assign roles to a user when implementing Role-Based Access Control.

Note: For CoA, open Port 3799 on your firewall from the RADIUS server to the AP.

10. Enable **Prefer Primary RADIUS Server** if you want the authentication to fall back to the primary RADIUS server once it comes back up after a failover. This helps if, for example, your secondary RADIUS servers have lower capacity than the primary servers. Another example where this helps is when enterprises use two data centers, each one configured as the "secondary" of the other. You would then want the authentication to fall back to the primary or "home" data center RADIUS server once it comes back up.

Once an AP detects a failover to the secondary RADIUS server, it waits for the **Dead Time** interval before falling back to the primary. This ensures that fallback doesn't happen too soon, allowing time for the primary server to stabilize if it had been flapping.

11. Select the type of **Framed IPv6 Address** that you want the RADIUS Accounting message to report to an authenticated WiFi client. The choice depends on whether your network uses solicited IPv6 addresses or unsolicited ones obtained via SLAAC (Stateless Address Autoconfiguration). For solicited IPv6 addresses, select **Report Full IPv6 Address**; for the unsolicited case, select **Report Only IPv6 Prefix**.

12. For any authentication that uses WPA, WPA2, WPA/WPA2 Mixed Mode,or WPA2/WPA3 Mixed Mode, enable the **Mitigate WPA/WPA2 Key Reinstallation Vulnerabilities in Clients**. This mitigates a known crack in the WPA and WPA2 mechanisms. WPA3 does not have this vulnerability, so the option is not needed for WPA3.

13. **802.11w** protects the Deauthentication, Disassociation, and Robust Action management frames, and prevents some spoofing attacks. The Integrity Group Temporal Key (IGTK) is used to provide integrity check for multicast management action frames, and the Pairwise Transient Key (PTK) is used to encrypt and protect unicast management action frames.

- With the **802.11w Management Frame Protection** drop down you can make 802.11w Required (i.e., mandatory), Optional or Disabled. **Note**: For WPA3, 802.11w is mandatory, so the drop down is set to Required and cannot be edited. For WPA2/WPA3 Mixed Mode, it is set to Optional and cannot be edited, since it is mandatory for WPA3 clients but not for WPA2 clients.
- The **Group Management Cipher Suite** is the combination of security and encryption algorithms used to protect management frames. Arista uses the AES-128-CMAC algorithm, so that's what is selected by default.
- Association frames are not protected as they need to be open for a client to establish an association with an AP. To make sure that a client Association Request isn't spoofed, the AP sends a Security Association (SA) query to a client requesting association. A genuine client responds to the protected frames. The **SA Query Max Timeout** is the time for which the AP waits for a client to respond to an SA query. If the AP receives no response within this period, it ignores the client. Since clients that spoof Association Requests don't respond, the AP rejects them. The **SA Query Retry Timeout** is the time for which a client can request to associate with the AP after the SA Query max timeout.

14. **802.11r** or Fast Transition (FT) speeds up roaming by allowing clients to re-establish security and QoS parameters before they associate with the new AP.

- Select **Over the DS** if you want to declare a preference for clients to roam by using the Over the Distribution System (DS) mode of roaming. With over-the-DS, the client exchanges messages with the target AP over the wired network via the current AP that it is connected to. This improves the roaming experience but increases AP-to-AP traffic in the wired network.
  Note: Selecting Over the DS is just declaring a preference; clients are free to decide how to roam from one AP to another. When you don't select Over the DS, clients roam over the air; but even when you select it, a client can ignore your preference and choose to roam over the air.
- Select **Mixed Mode** to allow both 802.11r compatible and 802.11r non-compatible clients to connect to the SSID.

For details on how 802.11r works, see the 802.11r section on the WiFi Help portal.

Note: WPA3 uses a different key derivation method and 802.11r is not supported with WPA3.

Network Settings

Most enterprise campuses use a bridged network for their traffic. The NAT mode is best suited for deployments where you need the APs to hand out IP addresses, a special case of which is Remote APs (RAPs) that form VPN tunnels with the enterprise gateway.

For our corporate SSID, we will consider the bridged mode since that's what most enterprise networks use. The steps to configure the corporate SSID network settings are as follows:

1. Enter the SSID **VLAN ID.** All packets of this SSID use this VLAN.
2. Select the **Bridged** mode. This is the most commonly used mode for enterprise networks; APs bridge all SSID traffic between the client and the switch.
3. With **Layer 2 Traffic Inspection and Filtering** (L2TIF) enabled on an SSID, APs running the SSID send all packets to a wired endpoint, i.e., a tunnel endpoint or a switch. You can then configure the wired endpoint to inspect and filter traffic. An effect of enabling L2TIF on an SSID is that two clients associated with the SSID cannot communicate directly with each other on the wireless link; their packets are sent to the gateway. What happens to these packets depends on the policies configured at the gateway. For details, see the L2TIF section on the WiFi Help portal.
4. With **Inter-AP Coordination**, APs exchange information with each other to improve WiFi network performance. You can select one of the following methods for APs to exchange information: RF Neighbors, L2 Broadcast, or This Server.