Authorized Wi-Fi Policy

Table of Contents

Authorized Wi-Fi Policy

This site will be decommissioned on July 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.

Arista wireless intrusion prevention system (WIPS) uses a variety of patented techniques to automatically and accurately classify Wi-Fi access points (APs) and clients as follows.

- Authorized: Owned and officially deployed by the enterprise,
- External: Legitimate Wi-Fi devices in the enterprise vicinity, and
- Rogue: Unauthorized Wi-Fi devices on the enterprise network.

An Authorized Wi-Fi Policy forms the basis of this automatic device classification; it can be defined in terms of:

1. The characteristics of the official enterprise Wi-Fi network, e.g., SSID name, whether or not the SSID is a guest SSID, the type of authentication and encryption used, a mapping of SSIDs to specific enterprise subnetworks they are allowed to run on, allowed vendors, etc.
2. A pre-classification of Wi-Fi APs as potentially authorized or rogue based on whether or not they are connected to one of the monitored enterprise subnetworks (enabled by default), or based on the signal strength (RSSI) with which those APs are visible to Arista WIPS.

You can implement an authorized Wi-Fi policy in two ways: either using the SSID Profile settings to validate the configuration running on your Arista Wi-Fi APs or by creating an Authorized Wi-Fi Profile for each SSID. Each method is described below.

Using SSID Profile Settings

You may choose to simply leverage the settings of the SSID Profiles in use to validate the configuration running on the enterprise Wi-Fi APs; this can be done by enabling the **Use SSID Profiles to verify managed access point configuration** option as shown below.

Note: This option is enabled by default. You will have to disable it if you choose to define your enterprise authorized Wi-Fi policy in terms of Authorized Wi-Fi Profiles.

Authorized Wi-Fi Profile per SSID

The figure below shows an Authorized Wi-Fi Profile for a corporate SSID. The SSID must conform to the restrictions set by the profile. For example, the SSID must run on an Arista AP because that’s the only allowed AP vendor; similarly, it must use PSK authentication.

When an SSID configuration does not match the authorized Wi-Fi policy, the SSID is marked as a Misconfigured SSID. As shown in the figure below, you can filter on the **Classification** column under **Monitor > WIPS > Access Points** to find APs running misconfigured SSIDs.

You can select an AP to see the SSIDs that are misconfigured and to view the reasons for the configuration mismatch. Active APs running misconfigured SSIDs are marked orange on the Monitor > WIPS and the Monitor > WiFi tabs.

Advanced Settings

Under **Configure > WIPS > Authorized Wi-Fi Policy**, you can define Advanced Settings that allow you to pre-classify access points (APs) and define No-Wi-Fi networks.

Access Point Pre-Classification

Pre-classification of access points helps WIPS identify potential authorized and rogue APs. As shown in the figure below, by default, access points connected to a monitored subnet are pre-classified as potentially authorized or rogue. These APs then show up with the appropriate classification on the **Monitor > WIPS** tab. This helps if, for instance, an unclassified AP is connected to the network. The AP appears on the Monitor > WIPS tab. You can then re-classify it appropriately as either rogue or authorized and—for rogue APs—take appropriate action.

You can also have WIPS pre-classify APs based on the signal strength with which they are visible. As shown in the figure below, if you enable signal strength based pre-classification, CloudVision Cognitive Unified Edge allows you to define a signal strength threshold. APs with signal strength greater than the threshold are automatically classified as potentially authorized or rogue.

Relying on signal strength based classification alone, however, is not advisable, especially if you plan to enable automatic intrusion prevention. First, if a legitimate AP from a neighboring facility is visible with a signal strength higher than the threshold, then classifying it as rogue could disrupt legitimate Wi-Fi connections to the AP. Therefore, use this classification only if you are sure that no unauthorized Wi-Fi operates in the vicinity of your location. Second, signal strength based classification will not detect rogue APs that operate with a signal strength weaker than the threshold (smartphones running Wi-Fi hotspots, for example).

Define No-Wi-Fi Networks

Security-sensitive environments might need to ensure that no Wi-Fi network operates at certain locations. As shown in the figure below, you can define "No-Wi-Fi" networks for a location, i.e., specify subnets where no Wi-Fi is allowed. If you define such networks, an AP detected on the network at that location is automatically classified as a rogue AP, even if it conforms to the authorized policy.