Configuring the Wi-Fi Direct Client Policy

Wi-Fi Direct Client Policy

Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy altogether for WLANs.

This section contains the following subsections:

Restrictions for the Wi-Fi Direct Client Policy

- Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only.

- Cisco APs in FlexConnect mode (even in central authentication and central switching) is not supported.

- We do not recommend enabling this feature in a mixed AP mode deployment (some APs in FlexConnect mode and some APs in local mode). Such types of deployment is not supported or tested in FlexConnect mode.

- If WLAN applied client policy is invalid, the client is excluded with the exclusion reason being 'Client QoS Policy failure'.

Configuring the Wi-Fi Direct Client Policy (GUI)

Step 1   Choose **WLANs** to open the WLANs page.

Step 2   Click the WLAN ID of the WLAN for which you want to configure the Wi-Fi Direct Client Policy. The **WLANs > Edit** page appears.

Step 3   Click the **Advanced** tab.

Step 4   From the **Wi-Fi Direct Clients Policy** drop-down list, choose one of the following options:

- **Disabled**—Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate
- **Allow**—Allows Wi-Fi Direct clients to associate with the WLAN
- **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with the WLAN
- **Xconnect-Not-Allow**—Enables AP to allow a client with the Wi-Fi Direct option enabled to associate, but the client (if it works according to the Wi-Fi standards) will refrain from setting up a peer-to-peer connection

Step 5   Save the configuration.

Configuring the Wi-Fi Direct Client Policy (CLI)

Step 1   Configure the Wi-Fi Direct Client Policy on WLANs by entering this command:

config wlan wifidirect {**allow** | **disable** | **not-allow**} *wlan-id*

The syntax of the command is as follows:

- **allow**—Allows Wi-Fi Direct clients to associate with the WLAN

- **disable**—Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate

- **not-allow**—Disallows the Wi-Fi Direct clients from associating with the WLAN

- **xconnect-not-allow**—Enables AP to allow a client with the Wi-Fi Direct option enabled to associate, but the client (if it works according to the Wi-Fi standards) will refrain from setting up a peer-to-peer connection

- *wlan-id*—WLAN identifier

Step 2   Save your configuration by entering this command:

save config

Monitoring and Troubleshooting the Wi-Fi Direct Client Policy (CLI)

Procedure

- Monitor and troubleshoot the Wi-Fi Direct Client Policy by entering theses commands:

    - **show wlan wifidirect** *wlan-id*—Displays status of the Wi-Fi Direct Client Policy on the WLAN.

- **show client wifiDirect-stats**—Displays the total number of clients associated and the number of clients rejected if the Wi-Fi Direct Client Policy is enabled.