



Fast Roaming

This chapter describes how to configure the Fast Roaming settings. It contains the following topics:

- [Fast Roaming](#), on page 1
- [Configuring Fast Roaming](#), on page 1
- [Configuring Remote Key Holder List Profiles](#), on page 2

Fast Roaming

Fast roaming, also known as IEEE 802.11r or Fast BSS Transition (FT), allows a client device to *roam* quickly in environments implementing the WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server every time it roams from one access point to another.

Fast transition roaming is an amendment to the IEEE 802.11 standard that permits continuous connectivity aboard wireless devices in motion, with fast and secure handoffs from an AP to another managed AP in a seamless manner. In order to ensure voice quality and network security, a portable station must be able to maintain a secure, low-latency voice call while roaming between APs that are handling other traffic.

This device supports the FBT (Fast BSS Transition) as defined in 802.11r for fast handoff with WPA2 Enterprise security. For Voice over WI-FI Enterprise, only a subset of the features defined in 802.11r are supported. The fast BSS transition decreases latency during roaming.

FBT is enabled per VAP per radio.



Note Before you configure FBT on a VAP, be sure to verify that the VAP is configured with WPA2 security, pre-authentication disabled and MFP disabled.

Configuring Fast Roaming

These steps give a general description of how to configure fast roaming:

-
- Step 1** Select **Fast Roaming > Roaming Table**.
 - Step 2** Click **+** to add a new row to the roaming table.
 - Step 3** Configure the following parameters:

- **Enable** — This option is checked by default.
- **BSSID** — Select the VAP (**2.4GVAP 0** or **5G VAP 0**) to enable.
- **Mobility Domain** — Specifies the Mobility Domain identifier (MDID) of the FBT VAP. The MDID is used to indicate a group of APs within an ESS, between which a STA can use fast BSS transition services. Fast BSS transitions are allowed only between APs that have the same MDID and are within the same ESS. They are not allowed between APs with different MDIDs or in different ESSs.
- **FT Mode** — Fast Transition protocol allows Mobile Station (MS) to fully authenticate only with the first AP in the domain (the group of APs that support FT Protocol and are connected over Distribution System (DS)), and use shorter association procedure with the next APs in the same domain. Choose one of the following methods of FT:
 - **Over Air** — In the Over Air method the Mobile Station communicates over a direct 802.11 link to the new AP.
 - **Over DS** — In the Over DS method the MS communicates with the new AP via the old AP.
- **R0 Key Holder** — Specifies the NAS identifier to be sent in the radius Access Request Message. The NAS Identifier is used as R0 Key holder ID.
- **R1 Key Holder** — Specifies the R1 Key Holder ID that names the holder of PMK-R1 in the authenticator.
- **Remote Key Holder List** — Select a Remote Key Holder List from the drop down menu that you have created.

Step 4 Click **Apply**.

Note To delete or modify a roaming setting, select it and then click **Delete** or **Edit**.

After configuring the FBT settings, click **Apply** to save the settings. Changing some settings might cause the AP to stop and restart the system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when the WLAN traffic is low.

Configuring Remote Key Holder List Profiles

To configure Remote R0 Key Holder List profiles:

- Step 1** Select **Fast Roaming > Remote Key Holder List Profile**.
- Step 2** Click **+** to add a new profile or **edit** to modify an existing profile. The **Remote Key Holder List Profiles** page is displayed.
- Step 3** Specify a name for the Remote Key Holder List Profile.
- Step 4** Configure the following parameters. A maximum of 10 entries of R0 Key holders are allowed to be configured per VAP.
 - **MAC Address** — Enter the destination's VAP MAC address which is the R0 key holder. The RRB PULL message is sent to this AP MAC address to fetch the PMKR1 key. This MAC address must be unique across all the VAPs.
 - **NAS ID** — NAS ID configured on the destination FBT enabled VAP.
 - **RRB Key** — Key used to encrypt RRM protocol messages.

Step 5

Repeat steps 1 through 4 and then configure the R1 key holder in the Remote R1 Key Holder Data List. A maximum of 10 entries of R1 key holders are allowed to be configured per VAP. The key holder data is configured per VAP.

- **MAC Address** — Destination's VAP MAC address which is the R1 Key holder. The PMKR1 is sent in RRB PUSH message to this AP MAC address. This MAC Address must be unique across all the VAPs.
- **R1 Key Holder** — The R1 key Holder ID that names the holder of PMK-R1 in the authenticator.
- **RRB Key** — Key used to encrypt RRM protocol messages.

Note After you configure the Remote Key Holder Data List settings, you can click **Restore** to restore the old settings, or click **Apply** to save the settings. Click **Cancel** to go back before **Fast Roaming** page.

Click **Apply** after copying or deleting a profile.

Caution Clicking **Export** for selected profile/s will export only those profiles. Clicking **Export** with no profiles selected will **Export** all the profiles.
