



Configuring Sticky PMKID Caching

- [802.11i Sticky Key Caching, on page 1](#)
- [Restrictions for Sticky Key Caching, on page 1](#)
- [Configuring Sticky Key Caching \(CLI\), on page 2](#)

802.11i Sticky Key Caching

The controller supports sticky key caching (SKC). With sticky key caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client.

In SKC, the client stores each Pairwise Master Key ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

SKC is useful only in cases where you have a small number of clients, which roam among a small number of APs.

This section contains the following subsections:

Restrictions for Sticky Key Caching

- The controller supports SKC for up to eight APs per client. If a client roams to more than 8 APs per session, the old APs are removed to store the newly cached entries when the client roams. We recommend that you do not use SKC for large scale deployments.
- SKC works only on WPA2-enabled WLANs.
- SKC does not work across controllers in a mobility group.
- SKC works only on local mode APs.

Configuring Sticky Key Caching (CLI)

Step 1 Disable the WLAN by entering this command:

```
config wlan disable wlan_id
```

Step 2 Enable sticky key caching by entering this command:

```
config wlan security wpa wpa2 cache sticky enable wlan_id
```

By default, SKC is disabled and opportunistic key caching (OKC) is enabled.

Note SKC works only on WPA2 enabled WLANs.

You can check if SKC is enabled by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier..... 2
Profile Name..... new
Network Name (SSID)..... new
Status..... Disabled
MAC Filtering..... Disabled
Security
  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Disabled
    WPA2 (RSN IE)..... Enabled
      TKIP Cipher..... Disabled
      AES Cipher..... Enabled
  Auth Key Management
    802.1x..... Disabled
    PSK..... Enabled
    CCKM..... Disabled
    FT(802.11r)..... Disabled
    FT-PSK(802.11r)..... Disabled
  SKC Cache Support..... Enabled
    FT Reassociation Timeout..... 20
    FT Over-The-Air mode..... Enabled
    FT Over-The-Ds mode..... Enabled
  CCKM tsf Tolerance..... 1000
  Wi-Fi Direct policy configured..... Disabled
  EAP-Passthrough..... Disabled
```

Step 3 Enable the WLAN by entering this command:

```
config wlan enable wlan_id
```

Step 4 Save your settings by entering this command:

save config
