802.11w Management Frame Protection MFP

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Management frames such as authentication, de-authentication, association, dissociation, beacons, and probes are used by wireless clients to initiate and tear down sessions for network services. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to attack a client associated with the AP.

The 802.11w amendment applies only to a set of robust management frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, Deauthentication, and Robust Action frames.

Configuration

802.11w is configured on a per-SSID basis via the Meraki Dashboard, and disabled by default. To enable, an administrator may set 802.11w to Enabled or Required on the Wireless > Configuration > Access control page. Enabled allows for mixed operation, by allowing legacy devices that do not support 802.11w to associate while also allowing devices that support 802.11w to use the 802.11w features. Required will prevent clients that do not support 802.11w from associating with the SSID.

Monitoring & Troubleshooting 802.11w

When 802.11w MFP is enabled within an SSID, RSN parameters will be included in the AP's beacon and probe response frames. If Enabled is selected on the Meraki Dashboard, only the Management Frame Protection Capable flag will be set. If Required is selected on the Meraki Dashboard, then the Management Frame Protection Required flag will also be set. These two flags advertise the 802.11w Management Frame Protection capabilities to the clients associating to a wireless network.
Additional encryption detail is also included in some management frames both to and from the client. Below is an example of a disassociation frame sent from a client to the Meraki AP:

```
IEE 0002.11 Disassociate, Flags: .p......C
Type/Subtype: Disassociate (0x000a)
Frame Control Field: 0xa000
Receiver address: 82:15:54:60:00:00 (82:15:54:60:00:00)
Destination address: 82:15:54:60:00:00 (82:15:54:60:00:00)
 transmitter address: apple_22:00:00:00:00:00 (38:ca:da:22:00:00)
 SSID: 82:15:54:60:00:00 (82:15:54:60:00:00)
....... .... = Fragment number: 0
1010 1110 0011 .... = Sequence number: 2787
Frame check sequence: 0x0bfe79f [correct]
CCMP parameters
  CCMP Ext. Initialization Vector: 0x000000000000
  Key Index: 0
Data (10 bytes)
  Data: 0663e6be438c36e8746
  [Length: 10]
```

Note the CCMP parameters and Data elements in the frame. The CCMP parameters indicate that the Data elements are encrypted. When the frame is received by the Meraki AP, it will be decrypted using the trusted keys established during association to validate that the frame came from the client.