Wireless Encryption and Authentication Overview

The MR supports a wide variety of encryption and authentication methods—from simple, open access to WPA2-Enterprise with 802.1X authentication. Encryption and authentication are configured in the MCC under the Configure tab on the Access Control page. Generally speaking, the encryption method is configured under “Association requirements”, while the authentication method is configured under “Network sign-on method”.

To associate to a wireless network, a client must have the correct encryption keys (association requirements). Once associated the wireless client may need to enter information (network sign-on method) before accessing resources on the wireless network.

The combinations of encryption and authentication methods that are supported are as follows:

<table>
<thead>
<tr>
<th>Association requirements</th>
<th>Network sign-on method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Direct access</td>
</tr>
<tr>
<td>Open (no encryption)</td>
<td>✓</td>
</tr>
<tr>
<td>MAC-based access control (no encryption)</td>
<td>✓</td>
</tr>
<tr>
<td>WEP (shared network key)</td>
<td>✓</td>
</tr>
<tr>
<td>WPA2-PSK (shared network key)</td>
<td>✓</td>
</tr>
<tr>
<td>WPA2-Enterprise with 802.1x authentication</td>
<td>✓</td>
</tr>
</tbody>
</table>

Open System Authentication

Open mode allows any device to connect to the wireless network. The major advantage of open mode is its simplicity: Any client can connect easily and without complex configuration. Open mode is recommended when there are guests who need to get onto the network, or more generally, when ease of connectivity is paramount and access control is not required.

In most environments, the administrator should ensure that wireless clients associated on an open network cannot access LAN resources, such as file shares.
Administrators can control access using VLAN tagging, or Firewall Rules.

MAC-based Access Control

MAC-based access control admits or denies wireless association based on the connecting device’s MAC address. When a wireless device attempts to associate, the Meraki AP queries a customer-premise RADIUS server with an Access-Request message. The RADIUS server can admit or deny the device based on the MAC address, responding to the Meraki AP with either an Access-Accept message or an Access-Reject message, respectively.

This authentication method requires no client-side configuration. However, it suffers from a poor user experience. Wireless clients that are denied wireless association simply cannot connect to the SSID, and they do not receive any explicit notification about why they cannot connect.

If this authentication method is selected, at least 1 RADIUS server must be configured on the Access Control page in the “RADIUS for MAC-based access control” section. This section includes a test tool that simulates the wireless device connecting to every Meraki AP in the network.

See the MAC-based Access Control Configuration guide on how to get started with MAC-based access control.

Pre-Shared Keys

A pre-shared key (PSK) allows anyone who has the key to use the wireless network.

Wired Equivalent Privacy (WEP) is the original 802.11 pre-shared key mechanism, utilizing RC4 encryption. WEP is vulnerable to being hacked; the encryption key can be derived by an eavesdropper who sees enough traffic. Only use WEP if it is not possible to utilize more advanced security—for instance, when there are legacy client devices in the network that do not support WPA/WPA2.

See the WEP Configuration guide on how to configure WEP encryption on a SSID.

WPA- and WPA2-Personal (Wi-Fi Protected Access) use stronger encryption than WEP. (WPA-Personal uses TKIP with RC4 encryption, while WPA2-Personal uses AES encryption.) WPA2-Personal is preferred.

Though it requires some client-side configuration, a PSK is relatively easy to configure. It can be a good choice when there is a small number of users or when clients do not support more sophisticated authentication mechanisms, such as WPA2-Enterprise. A deployment based on a PSK does not scale well, however. With a large number of users, it becomes more difficult to change the PSK, an operation that should be performed periodically to ensure that the PSK has not been shared with unwanted users.

See the WPA Configuration guide on how to configure WPA encryption on a SSID.

WPA2-Enterprise with 802.1X Authentication

802.1X is an IEEE standard framework for encrypting and authenticating a user who is trying to associate to a wired or wireless network. WPA-Enterprise uses TKIP with RC4 encryption, while WPA2-Enterprise adds AES encryption.

802.1X can be transparent to wireless users. For example, Windows machines can be configured for single sign-on, such that the same credentials that a user enters to log into his machine are passed automatically to the authentication server for wireless authentication. The user is never prompted to re-enter his credentials.

802.1X utilizes the Extensible Authentication Protocol (EAP) to establish a secure tunnel between participants involved in an authentication exchange. The MR supports multiple EAP types, depending on whether the network is using a Meraki-hosted authentication server or a customer-hosted authentication server. The
The following table shows the EAP types supported by the MR access points:

<table>
<thead>
<tr>
<th>EAP Mode</th>
<th>Customer RADIUS</th>
<th>Meraki RADIUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEAPv0/EAP-MSCHAPv2</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>EAP-TTLS/MSCHAPv2</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>PEAPv1/EAP-GTC</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

WPA2-Enterprise with 802.1X authentication is configured to use a customer-hosted on-premises Custom RADIUS server. The RADIUS server must be configured to allow authentication requests from the IP addresses of the Meraki access points.

802.1X is typically only performed once a user’s credentials have been entered into the machine.

Identity Sources

WPA2-Enterprise requires a identity source in order to authenticate users when they connect to the network. The Access points each interface with the identity source at time of the client association. Below are the identity sources that can be used with WPA2-Enterprise.

- **Meraki RADIUS - Cloud Hosted**
  - Network-wide Users can connect and login with PEAP and EAP-TTLS
  - Systems Manager Sentry WiFi Security configures endpoint devices to connect with EAP-TLS
- **Custom RADIUS - Customer Hosted**
  - Cisco Identity Services Engine (ISE)
  - FreeRADIUS
  - Juniper Steel-Belted RADIUS or UAC
  - ForeScout CounterACT
  - Aruba Clearpass