Configuring EAP-TLS Wireless Authentication with Systems Manager Sentry Wifi

Systems Manager Sentry Wi-Fi security provides automatic certificate-based EAP-TLS configuration in just a few clicks, eliminating the need for the use of a certificate authority (CA) and the additional management required for each device and user.

This article outlines how to integrate SM Sentry with Cisco Meraki MR access points for EAP-TLS wireless authentication.

Use Case

Commonly, network administrators want to configure different settings for corporate owned devices, employee owned devices, and guests. Each group of users will likely have their own separate SSID, with an additional SSID for onboarding:

<table>
<thead>
<tr>
<th>SSID</th>
<th>Use Case</th>
<th>Default SSID Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corp</td>
<td>Corporate-owned devices only</td>
<td>Full access on Corporate VLAN</td>
</tr>
<tr>
<td>BYOD</td>
<td>Employee-owned devices</td>
<td>Limited Corporate access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Some apps optionally limited</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Higher bandwidth than Guest</td>
</tr>
<tr>
<td>Guest</td>
<td>All others</td>
<td>Filtered Internet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rate limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No corporate devices</td>
</tr>
<tr>
<td>Corp-onboarding</td>
<td>Onboarding to Corp network only</td>
<td>Restricted to onboarding</td>
</tr>
</tbody>
</table>
Configuring EAP-TLS using Systems Manager Sentry WiFi Security

The following instructions explain how to apply EAP-TLS wireless access to corporate-owned devices tagged as "Corp" in our example Systems Manager network.

1. In Dashboard, navigate to Wireless > Configure > SSID and enable/name each SSID. The example image below shows four SSIDs: SL-corp, SL-byod, SL-guest and SL-corp-onboarding:

   Configuration overview
   
<table>
<thead>
<tr>
<th>SSIDs</th>
<th>SL-corp</th>
<th>SL-byod</th>
<th>SL-guest</th>
<th>SL-corp-onboarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>enabled $</td>
<td>enabled $</td>
<td>enabled $</td>
<td>enabled $</td>
</tr>
<tr>
<td>Name</td>
<td>rename</td>
<td>rename</td>
<td>rename</td>
<td>rename</td>
</tr>
<tr>
<td>Access control</td>
<td>edit settings</td>
<td>edit settings</td>
<td>edit settings</td>
<td>edit settings</td>
</tr>
<tr>
<td>Encryption</td>
<td>802.1X with Meraki RADIUS</td>
<td>802.1X with custom RADIUS</td>
<td>Open</td>
<td>Open</td>
</tr>
<tr>
<td>Sign-on method</td>
<td>None</td>
<td>None</td>
<td>Click-through splash page</td>
<td>Systems Manager Sentry</td>
</tr>
</tbody>
</table>

2. Navigate to Wireless > Configure > Access Control:

3. Select the device tags to be associated with EAP-TLS. This automatically creates a Systems Manager profile for the SL-corp SSID to use EAP-TLS and installs a client certificate from the Dashboard for each client (this profile will not appear under Systems Manager > Manage > Settings). Note that wireless authentication settings should be provisioned from either the SSID side, as described in this article, or the MDM profile side in Systems Manager > Manage > Settings and not both.
Sentry Wifi security is not to be confused with Sentry enrollment, as shown in the splash page configuration below. Sentry enrollment is typically deployed as a separate SSID (SL-corp-onboarding in this article) to initially enroll devices into Systems Manager, while Sentry security grants secure wifi access to devices *already* enrolled.

4. Click **Save Changes**. EAP-TLS is now configured for all devices tagged *corp* in Systems Manager.
# Sentry WiFi Device Operating System Compatibility

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Sentry WiFi Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS</td>
<td>Yes</td>
</tr>
<tr>
<td>macOS</td>
<td>Yes</td>
</tr>
<tr>
<td>tvOS</td>
<td>No</td>
</tr>
<tr>
<td>Windows 10</td>
<td>Yes(^1)</td>
</tr>
<tr>
<td>Android</td>
<td>Yes(^2)</td>
</tr>
<tr>
<td>Samsung Knox 3.0+</td>
<td>Yes(^3)</td>
</tr>
<tr>
<td>Chrome OS</td>
<td>No</td>
</tr>
</tbody>
</table>
1. Local user accounts only. In a multi-user environment on a single device the Sentry WiFi profile may need to be pushed for each user.

2. Android 6+ in BOYD mode or Device Owner mode. Android 5 does not work with Sentry WiFi.

3. A passcode is required on the device while in Knox mode.