Meraki Wireless Enterprise Standard

# 1. Wireless Profiles – Corporate vs Guest

This section defines the wireless profile settings Cisco uses in Meraki deployments for Corporate and Guest SSIDs.  
Corporate: WPA3-Enterprise (802.1X), full LAN access, fast roaming enabled.  
Guest: WPA2-PSK or Captive Portal, internet-only access, client isolation enabled.

# 2. RF Profile Settings (Enterprise Wireless with Meraki)

RF Profiles are used to manage radio settings across APs. Cisco’s best practices include using dual-band operation,  
AI-RRM, 12 Mbps minimum bitrates for corporate SSID, and Zero-Wait DFS on supported APs.

# 3. Roaming Enhancements & Radio Optimization

Meraki supports 802.11r/k/v for fast, secure roaming. AI-RRM optimizes channels and transmit power using telemetry data.  
Zero-Wait DFS allows radar detection without client disruption.

# 4. Best Practices from RF Profiles

Use per-band RF tuning. Enable multicast-to-unicast conversion. Suppress broadcast/multicast. Use AI-RRM for large deployments.

# 5. SSID Configuration Templates

Corporate SSID:

SSID Name: Corporate-WiFi  
Security: WPA3-Enterprise (802.1X)  
Roaming: 802.11r/k/v enabled  
VLAN: Dynamic via RADIUS  
RF: AI-RRM, Zero-Wait DFS, RX-SOP -80 dBm

Guest SSID:

SSID Name: Guest-WiFi  
Security: Captive portal (open or click-through)  
Roaming: Disabled  
VLAN: Dedicated guest VLAN  
RF: RX-SOP -85 dBm, client isolation enabled, multicast-to-unicast enabled

# 6. Meraki Tagging Strategy for Large Campus Wireless Design

Use *Network Tags* for site segmentation, access control, and reporting.

Use *Device Tags* for AP-specific roles,  
SSID availability, and RF tuning. Tags enable flexible management and visibility.

# 7. Design-Level Recommendations for Campus Environments

Use geographic and functional tags (e.g., CampusA-Floor1, Lobby).

Align tags with VLANs, SSIDs, and roaming domains.  
Enable tag-based configuration filtering and dashboard role segmentation.

# 8. Tagging Methods

Web UI (Manual): Use for small deployments and initial setup.

Dashboard API (Scalable): Use for large networks, automation, and role-based tagging.

# 9. Recommendation for Most Teams

Use the Dashboard UI for early-stage or small-scale tagging. For scale, adopt API-based tagging workflows using Meraki Python SDK or Postman.

# 10. Meraki Enterprise Wireless Standard (Baseline for Large Corporate Deployment)

Establish standard SSIDs (Corporate, Guest, IoT), RF profiles, VLANs, roaming, and monitoring policies.  
Design for Layer 2 roaming domains, centralized RADIUS, adaptive policies, and secure onboarding.

# 11. Meraki API-Driven Wireless Operations Model

Day 0: Use APIs for network creation, RF profile config, tagging.  
Day 1: Automate device onboarding, SSID setup, alerting.  
Day 2: Operationalize telemetry, events, and optimization with MQTT, Webhooks, and MV Sense.

# 12. Meraki Wireless API Use-Case Reference Architecture

API use cases span from design to optimization: create networks, push config templates, manage firmware, receive event alerts, analyze client movement, and remediate issues.  
Use Postman or Python SDK to get started.

## Appendix

### SSID Profile / Configuration settings

**Corporate SSID (Trusted Employee Network):**

* **SSID Name:** Corporate
* **Wi-Fi Standard:** **WPA3-Enterprise (802.1X)**
* **Authentication:** Identity-based (802.1X with RADIUS)
* **Traffic Control:** Full LAN access
* **VLAN Assignment:** Dynamic or Static based on group policy
* **Firewall Rules:** Internal resource access allowed
* **Bandwidth Limits:** Optional / none
* **Client Isolation:** Disabled
* **Roaming Enhancements:** Enabled (Fast roaming, 802.11r)
* **Air Marshal / WIPS:** Enabled for rogue detection

**Guest SSID (Untrusted Visitor Network):**

* **SSID Name:** Guest
* **Wi-Fi Standard:** **WPA2-PSK or Click-through Splash Page**
* **Authentication:** Open or captive portal (with splash page)
* **Traffic Control:** Internet only (blocked from LAN)
* **VLAN Assignment:** Dedicated guest VLAN
* **Firewall Rules:** Strict – deny LAN, allow web
* **Bandwidth Limits:** Enforced per-client (e.g., 1 Mbps)
* **Client Isolation:** Enabled (to prevent inter-guest communication)
* **Roaming Enhancements:** Disabled or limited
* **Air Marshal / WIPS:** Enabled to prevent bridging attacks

### RF Profile Settings (Enterprise Wireless with Meraki)

RF Profiles are used in Meraki to apply consistent radio settings across groups of APs.

Radio Settings

**Applied per SSID or per band in RF Profiles:**

|  |  |  |
| --- | --- | --- |
| **Setting** | **Corporate SSID** | **Guest SSID** |
| **Band Selection** | Dual band (2.4 GHz + 5 GHz + 6 GHz if supported) | Typically 2.4 GHz + 5 GHz |
| **Min Bitrate (Mbps)** | 12 Mbps or higher (for client experience and roaming efficiency) | 6–12 Mbps (to support wider range of devices) |
| **Transmit Power** | Adaptive / Controlled | Lower to minimize interference |
| **Client Balancing** | Enabled selectively (802.11v with MR29+) | Disabled by default |
| **Band Steering** | Enabled | Enabled (but may vary per location) |
| **Min RSSI Threshold (RX-SOP)** | Configured to mitigate co-channel interference (more aggressive) | Less aggressive, to allow legacy clients |
| **DFS Channels** | Enabled with Zero-Wait DFS where supported (e.g., MR56, MR57, CW9166) | May be disabled for compatibility |
| **Multicast to Unicast Conversion** | Enabled (especially for AAA VLAN override scenarios) | Enabled to maintain VLAN segmentation |
| **Client Load Balancing** | Disabled in high-density environments | Disabled by default |
| **Fast Roaming (802.11r/OKC)** | Enabled | Disabled or not required |

**Roaming Enhancements & Radio Optimization**

* **AI RRM (AI Radio Resource Management):** Actively used for channel and power optimization across Meraki cloud.
* **Flexible Radio Assignment (FRA):** Enabled to convert radios between 2.4GHz/5GHz/6GHz as needed.
* **Enhanced Busy Hour:** Defers optimizations to non-peak times.

**Best Practices from RF Profiles**

* Use **Per-band RF tuning** (vs blanket settings).
* Enable **Zero-Wait DFS** for better channel agility.
* Use **AI-RRM** for larger campuses (>200 APs per domain).
* Configure **minimum bitrate >12 Mbps** for corporate SSID to encourage clients to connect to stronger signals and reduce airtime waste.

### Corporate SSID Configuration Template

**SSID Name:** Corporate-WiFi  
**Purpose:** Trusted internal users (employees, contractors)  
**Security:** WPA3-Enterprise (802.1X)

**RF Profile**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| **Band Selection** | Dual-band with Band Steering |
| **Radio Mode** | Flexible Radio Assignment (FRA) |
| **Channel Width** | 20 MHz (2.4 GHz), 40 MHz or 80 MHz (5 GHz), 80 MHz (6 GHz if supported) |
| **Min Bitrate** | 12 Mbps |
| **Client Balancing** | Disabled (enable only if 802.11v clients are dominant) |
| **Min RSSI (RX-SOP)** | -80 dBm |
| **DFS Channels** | Enabled with Zero-Wait DFS (supported APs only) |
| **Multicast-to-Unicast** | Enabled |
| **Fast Roaming** | Enabled (802.11r and OKC) |
| **Load Balancing** | Off in high-density deployments |
| **Airtime Fairness** | Enabled |
| **Targeted Devices** | Windows/macOS laptops, iPhones, Androids, iPads |

**SSID Settings**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| **Authentication Method** | WPA3-Enterprise (802.1X) |
| **RADIUS Servers** | 2–3 with source-based sticky load balancing |
| **VLAN Assignment** | Dynamic VLAN via RADIUS return attribute |
| **Firewall Rules** | Allow all internal resources |
| **Traffic Shaping** | Optional, based on Group Policy |
| **Content Filtering** | Optional (none by default) |
| **Client Isolation** | Disabled |
| **Splash Page** | Disabled |
| **Group Policies** | Enforced via RADIUS attributes |
| **SSID Availability** | Enabled always or scheduled based on office hours |
| **IPv6 Support** | Dual-stack (enable IPv6 infrastructure on MR/APs) |

### Guest SSID Configuration Template

**SSID Name:** Guest-WiFi  
**Purpose:** Internet-only access for visitors  
**Security:** Captive portal with splash page

**RF Profile**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| **Band Selection** | Dual-band |
| **Channel Width** | 20 MHz (2.4 GHz), 40 MHz (5 GHz) |
| **Min Bitrate** | 6 Mbps (for compatibility) |
| **Client Balancing** | Off |
| **Min RSSI (RX-SOP)** | -85 dBm |
| **DFS Channels** | Optional (disable if legacy clients have issues) |
| **Multicast-to-Unicast** | Enabled |
| **Fast Roaming** | Disabled |
| **Airtime Fairness** | Enabled |
| **Targeted Devices** | Smartphones, tablets, laptops (including legacy) |

**SSID Settings**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| **Authentication Method** | Open SSID with Click-through Splash Page |
| **VLAN Assignment** | Static Guest VLAN (e.g., VLAN 200) |
| **Firewall Rules** | Deny LAN, Allow Internet only |
| **Traffic Shaping** | Bandwidth limit per client (e.g., 1 Mbps up/down) |
| **Content Filtering** | Optional (block adult/illegal content) |
| **Client Isolation** | Enabled |
| **Splash Page** | Meraki-hosted or custom branded splash |
| **Group Policies** | Default "Guest" policy |
| **SSID Availability** | Always enabled or restricted to business hours |
| **IPv6 Support** | Enable only if supported and tested |

### Meraki Tagging Strategy, Large Campus Wireless Design

**1. Network Tags**

**Scope:** Applied to a *Meraki Network* (a logical grouping of APs, switches, MXs at a site)

**Recommended Use Cases:**

|  |  |  |
| --- | --- | --- |
| **Function** | **Tag Example** | **Purpose** |
| **Summary Reports** | Campus-North, Building-IT | Roll up usage, health, or performance by area |
| **Organization Overview** | Retail, Warehouse, Education | Filter entire site types for centralized views |
| **Camera Roles** | Security-CCTV, Entrance-Cam | Not Wi-Fi-specific but helps segment security monitoring |
| **Dashboard RBAC** | Zone-East, Zone-West | Restrict admin access to specific network zones |
| **Location Analytics** | Student-Zone, Staff-Zone | Enable footfall analysis or heat mapping by zone |
| **Site-to-Site VPN** | Trusted-Hub, Branch-Spoke | Automatically define VPN topology policies via templates |

**Best Practices:**

* Use **geographic naming**: CampusA-Building1, CampusB-Library
* Define tags for **functional zones** (e.g., Lecture-Hall, Admin-Block)
* Integrate with **RBAC roles** to restrict dashboards for local IT/contractors
* Use tags to **group sites by policy**, especially in **template-based automation**

**2. Device Tags**

**Scope:** Applied to *individual APs*, switches, cameras, etc., within a network

**Recommended Use Cases:**

|  |  |  |
| --- | --- | --- |
| **Function** | **Tag Example** | **Purpose** |
| **Summary Reports** | AP-HighDensity, AP-Outdoor | Identify performance-impacting areas |
| **Organization Overview** | AP-Shared, AP-Dedicated | Understand shared vs specific AP functions |
| **Location Analytics** | Zone-Entrance, Zone-Cafeteria | Filter analytics data for fine-grained location analysis |
| **SSID Availability/VLAN Assignment** | AP-GuestOnly, AP-CorpOnly | Use for conditional SSID broadcast per AP |
| **Filtering Mechanism** | Exclude-Report, Maintenance | Exclude specific devices from dashboards or auto-reports |

**Best Practices:**

* Tag **APs by physical location**: Floor1, Floor2, Lobby, HallA
* Tag **special-purpose APs**: AP-RetailKiosk, AP-TrainingRoom
* Use for **selective SSID broadcasting** (e.g., only broadcast Guest-WiFi on Lobby APs)
* Combine with automation/API for **mass configuration** or **firmware rollouts**

### Design-Level Recommendations for Campus Environments

1. **Define a campus-wide tagging taxonomy**:
   * Example: CampusA-Floor1, CampusA-Lab, CampusA-Outdoor
   * Keep it **short but meaningful** and **consistent**
2. **Apply Network Tags for macro segmentation**:
   * Helps dashboard filtering, license tracking, and operational isolation
   * Automates policy/template assignments
3. **Use Device Tags for micro-level granularity**:
   * Helps fine-tune radio profiles or SSID settings per AP type or zone
   * Enables conditional SSID availability or VLAN assignment logic
4. **Leverage APIs + Tags for automation**:
   * Automate SSID broadcasting changes based on time of day or building occupancy
   * Dynamically adjust VLAN mappings or isolate areas during maintenance

The **most common and simplest method** to apply Meraki **Network and Device Tags**—especially in large campus deployments—is via the **Meraki Dashboard Web UI**, but for **scalability and automation**, the **Meraki Dashboard API** is strongly recommended.

Here’s a practical overview of both approaches:

**1. Meraki Dashboard Web UI (Simple & Manual)**

**Applying Network Tags:**

1. Go to **Organization > Overview**
2. Select the Network (e.g., CampusA-Floor1)
3. Click **Edit**
4. In the **Tags** field, add tags like: CampusA, Floor1, AdminZone
5. Click **Save**

**Applying Device Tags (e.g., to Access Points):**

1. Go to **Wireless > Access Points**
2. Select an AP (or multi-select using checkboxes)
3. Click **Edit**
4. Add tags like: Lobby, HighDensity, GuestOnly
5. Click **Save Changes**

**Pros**:

* Intuitive for small networks or occasional changes
* No scripting or tooling required

**Cons**:

* Manual process – error-prone and slow for >50 devices
* No version control or audit trail

**2. Meraki Dashboard API (Scalable & Repeatable)**

Best for **large-scale deployments**, **automation**, and **CI/CD integrations**.

**Quick Example – Device Tags (Python):**

python

import meraki

dashboard = meraki.DashboardAPI(api\_key='YOUR\_API\_KEY')

# Example: tagging an AP

response = dashboard.devices.updateDevice(

serial='Q2XX-XXXX-XXXX',

tags=['Lobby', 'HighDensity']

)

print(response)

**Tools That Support Tags Easily:**

* **Postman** collections (official Meraki workspace)
* **Meraki Python SDK** (great for loops/conditional tagging)
* **Terraform Meraki Provider** (infra-as-code tagging by site)
* **Automation tools** (Ansible, Cisco DNA Center integrations)

**Pros**:

* Scalable to thousands of devices
* Repeatable and can be templated
* Easily integrated into deployment pipelines
* Auditable and version-controlled

**Cons**:

* Requires basic scripting/API familiarity
* Requires API key and org permissions

**Recommendation for Most Teams**

* Use **Web UI** for:
  + Initial setup
  + Small sites or pilot environments
  + Visual QA or troubleshooting
* Use **API** for:
  + Multi-site deployments (campuses, branches)
  + Ongoing operations automation (e.g., dynamic SSID adjustments)
  + Integration with **CMDB**, **CI/CD**, or **zero-touch provisioning**

For a **large corporate deployment** that supports both **hybrid** (onsite + remote) and **federated** (multi-entity/shared services) workforce models, your standard must address:

* **Design consistency**
* **Operational flexibility**
* **Security posture**
* **Roaming experience**
* **Visibility and scalability**

### Meraki Enterprise Wireless Standard (Baseline for Large Corporate Deployment)

**1. SSID Strategy**

|  |  |  |
| --- | --- | --- |
| **SSID** | **Purpose** | **Key Settings** |
| Corporate-WiFi | Trusted user access | WPA3-Enterprise, 802.1X, RADIUS, VLAN override |
| Guest-WiFi | Visitors and untrusted BYOD | Captive portal, bandwidth shaping, client isolation |
| IoT-WiFi *(optional)* | Headless devices | WPA2-PSK, static VLAN, limited network access |

**Best Practices**:

* Limit to **3–4 SSIDs**
* Use **identity-based policies** for segmentation instead of separate SSIDs when possible

**2. RF Profile Standards**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Profile** | **Bands** | **Bitrate** | **Power** | **Roaming** | **Notes** |
| Corp-HighDensity | 5 GHz / 6 GHz preferred | ≥12 Mbps | Dynamic | 802.11r/k/v | For offices, auditoriums |
| Corp-Standard | Dual Band | ≥12 Mbps | Moderate | 802.11r | For general areas |
| Guest-RF | Dual Band | ≥6 Mbps | Low | Disabled | Wider compatibility |
| IoT-RF | 2.4 GHz only | ≥6 Mbps | Fixed Low | Disabled | For legacy headless devices |

**3. VLAN / IP Strategy**

* Use **dynamic VLAN assignment** for corporate SSID via RADIUS
* Allocate **/23 or /22** subnet per roaming domain
* Use **VLAN pooling** (R30+) where subnet summarization is required
* Enforce **Layer 2 roaming domains** with ≤200 APs per domain
* Keep **wireless VLANs distinct from wired** where segmentation is required

**4. Security & Access Control**

|  |  |
| --- | --- |
| **Component** | **Setting** |
| **802.1X (WPA3-Enterprise)** | Mandatory for internal users |
| **RADIUS** | Up to 3 per SSID; prefer sticky LB or failover |
| **AAA VLAN override** | Enabled, with switch validation |
| **Client Isolation** | Guest + IoT SSIDs only |
| **Firewall Rules** | Deny LAN on Guest, restrict IoT-to-Corp |
| **Group Policies** | Role-based bandwidth, content filtering, Layer 3/7 controls |
| **Fast Roaming** | 802.11r/OKC on Corp SSID |
| **SGTs (Adaptive Policy)** | Optional, for TrustSec integration |

**5. SSID Availability**

* Use **Device Tags** for selective SSID broadcasting (e.g., only broadcast Guest-WiFi at front desk/lobby)
* Disable SSIDs on APs where not relevant via dashboard scheduling

**6. Roaming & Performance Enhancements**

* Enable **802.11r/k/v** on Corporate
* Use **AI-RRM** (default in Meraki cloud) for RF tuning
* Enable **Zero-Wait DFS** on supported APs
* Suppress broadcast/multicast using built-in features (enabled by default)

**7. Management & Operations**

|  |  |
| --- | --- |
| **Feature** | **Usage** |
| **Network Tags** | For site segmentation: CampusA, Building1, RetailZone |
| **Device Tags** | For AP roles: Lobby, MeetingRoom, GuestOnly |
| **Firmware Strategy** | Use stable track (MR29.x or MR30.x); staggered upgrades |
| **Client Analytics** | Enabled by default; use for device and roaming insights |
| **Air Marshal (WIPS)** | Enabled on all APs for rogue detection |
| **Monitoring** | Use Meraki Health, Location Analytics, and Roaming Analytics dashboards |
| **Change Control** | Document SSID/RF/Firewall templates for consistency |
| **Alerting** | Configure org-wide alerts for outages, rogue APs, DHCP failures, etc. |

**8. End User Experience**

* Enable **splash page branding** for Guest WiFi
* Support **BYOD via captive portal or separate SSID**
* Ensure seamless **hybrid access** with posture checks if integrating with ISE or Umbrella
* Monitor **roaming failure types** (e.g., Ping-Pong, Bad, Disconnected) in dashboard

### Meraki API-Driven Wireless Operations Model

**Day 0 – Design & Preparation**

|  |  |  |
| --- | --- | --- |
| **API** | **Use Case** | **Benefit** |
| **Dashboard API** | - Automate network/org/site creation - Apply config templates (SSIDs, VLANs, firewall rules, tags) - Upload floor plans and place APs | Accelerates baseline deployment, reduces human error |
| **MV Sense API** | - Fetch existing camera placements to overlay with Wi-Fi zones | Helps align security + RF planning |
| **Scanning API** | - Pre-wireless asset placement planning using BLE/mac tracking simulations | Design for density-aware location services |
| **Wireless Telemetry (MQTT)** | - Connect to telemetry collector for site modeling | Pre-integration with IoT/OT use cases in smart campuses |

**Day 1 – Deployment & Go-Live**

|  |  |  |
| --- | --- | --- |
| **API** | **Use Case** | **Benefit** |
| **Dashboard API** | - Bulk provision devices - Auto-assign tags - Enforce consistent RF profiles across campuses | Streamlined deployment across sites |
| **Webhook API** | - Notify deployment milestones (e.g., AP online, config mismatch) to chat/email/ITSM | Real-time deployment observability |
| **Captive Portal API** | - Custom onboarding flows with splash page branding or SAML auth | Enforces branding, security, or policy in guest/BYOD networks |
| **Scanning API** | - Validate BLE beacon and client presence with real-time movement logs | Ensures wayfinding and asset tracking are operational |

**Day 2 – Operations, Monitoring, Optimization**

|  |  |  |
| --- | --- | --- |
| **API** | **Use Case** | **Benefit** |
| **Dashboard API** | - Real-time client monitoring - Firmware compliance audits - Location-based alerting - Scheduled report exports | Centralized and automated health checks |
| **Webhook API** | - Event-driven triggers (e.g., rogue AP detected, DHCP failure) pushed to ITSM, Slack, or PagerDuty | Faster MTTR and event correlation |
| **Scanning API** | - Monitor footfall, dwell time in zones (e.g., meeting rooms, stores) | Improve physical layout or zone coverage |
| **Wireless Telemetry (MQTT)** | - Feed live AP telemetry (RSSI, channel usage, client density) to external analytics platforms | Enables proactive RF tuning, occupancy analytics |
| **MV Sense API** | - Correlate crowd density from cameras with AP performance/load | Integrated physical + RF visibility (crowd impact on Wi-Fi) |
| **Captive Portal API** | - Audit guest logs, session durations, and block suspicious MACs | Improves guest compliance, enhances NAC |
| **MQTT (sensors)** | - Monitor temp/humidity sensors near APs (for overheating detection) | Hardware protection, env. awareness in edge/IoT deployments |

**Strategic Integration Examples**

* **ServiceNow/ITSM:** Integrate Webhook + Dashboard API for ticket automation.
* **Splunk/ELK:** Feed telemetry + event logs for historical Wi-Fi analytics.
* **Power BI/Tableau:** Build dashboards using MV Sense, MQTT, and Dashboard API data.
* **Digital Twin & RTLS**: Use Scanning + Telemetry APIs with Cisco DNA Spaces or a third-party RTLS system.

**Recommendations for Getting Started**

|  |  |
| --- | --- |
| **Step** | **Action** |
| 1 | Get an **API key** from the Meraki dashboard (org-level admin) |
| 2 | Use **Postman or Python SDK** to test basic GET requests |
| 3 | Identify 3–5 Day 2 tasks (e.g., rogue alerting, client health, firmware checks) to automate |
| 4 | Build a simple integration (e.g., Webhook → Slack or ServiceNow) |
| 5 | Align API use with **CCoE/NetOps goals** (e.g., zero-touch, AIOps, or Wi-Fi SLOs) |

### Meraki Wireless API Use-Case Reference Architecture

*For Large Campus or Enterprise Networks (Hybrid + Federated Models)*

**Day 0 – Design & Preparation**

|  |  |  |
| --- | --- | --- |
| **Task** | **API** | **Outcome** |
| Auto-create networks for each site | Dashboard API → createNetwork | Site networks aligned with your tagging and naming conventions |
| Upload floorplans with AP positions | Dashboard API → uploadFloorPlan & updateDevice | Visual heat maps, location context for clients |
| Apply SSID templates & RF profiles | Dashboard API → updateNetworkWirelessSsid & createNetworkRfProfile | Ensures standardized settings from Day 1 |
| Assign network & device tags | Dashboard API → updateNetwork, updateDevice | Logical grouping for operations and filtering |

**Day 1 – Deployment & Go-Live**

|  |  |  |
| --- | --- | --- |
| **Task** | **API** | **Outcome** |
| Bulk claim and configure APs | Dashboard API → claimNetworkDevices, updateDevice | Streamlined device onboarding with tags, names, locations |
| Configure SSIDs with access control | updateNetworkWirelessSsid | Ensure Guest vs Corp SSID best practices are applied |
| Setup Webhooks for events | Webhook API | Get real-time alerts on AP status, DHCP failures, rogue detection |
| Custom guest onboarding | Captive Portal API | Integrate splash pages, branding, authentication |
| Client test & validation | Dashboard API → getNetworkClients, getDeviceClients | Validate that devices connect, roam, and receive policies correctly |

**Day 2 – Operations & Optimization**

|  |  |  |
| --- | --- | --- |
| **Task** | **API** | **Outcome** |
| Trigger alerts to Slack/ITSM | Webhook API + Webhook listener | Event-driven ops (e.g., rogue AP → create SNOW ticket) |
| Monitor client health & SNR | Dashboard API → getDeviceClients, getNetworkClientLatencyStats | Track bad roamers, latency, disconnects |
| Analyze client movement | Scanning API + Telemetry API (MQTT) | Real-time and historic analytics for roaming, density |
| Auto-remediate rogue APs | Dashboard API → updateNetworkWirelessAirMarshal | Quarantine or shut down interference |
| Visualize usage trends | MV Sense API, Dashboard API | Build custom Power BI/Splunk dashboards for SSID usage, AP load |
| Firmware compliance reports | Dashboard API → getOrganizationFirmwareUpgrades | Detect APs running unsupported versions |

**Python Starter Script Example**

*Bulk tag APs and apply RF profile*

python

import meraki

API\_KEY = 'YOUR\_API\_KEY'

ORG\_ID = 'YOUR\_ORG\_ID'

NETWORK\_ID = 'YOUR\_NETWORK\_ID'

RF\_PROFILE\_ID = 'YOUR\_RF\_PROFILE\_ID'

dashboard = meraki.DashboardAPI(API\_KEY)

# Get all APs in the network

devices = dashboard.networks.getNetworkDevices(NETWORK\_ID)

for device in devices:

if 'MR' in device['model']:

# Add tags and apply RF profile

dashboard.devices.updateDevice(

serial=device['serial'],

tags=['Lobby', 'HighDensity'],

floorPlanId=None, # Optional: attach to a floor plan

)

dashboard.networks.assignNetworkWirelessRfProfile(

networkId=NETWORK\_ID,

serials=[device['serial']],

rfProfileId=RF\_PROFILE\_ID

)

**Postman Collection Starter (Key APIs)**

Here are a few suggested requests you can load into a Postman Collection:

**GET All Networks**

* **GET** https://api.meraki.com/api/v1/organizations/{{orgId}}/networks

**Update SSID Settings**

* **PUT** https://api.meraki.com/api/v1/networks/{{networkId}}/wireless/ssids/{{ssidNumber}}

json

{

"name": "Corporate-WiFi",

"enabled": true,

"authMode": "8021x-radius",

"radiusServers": [

{

"host": "192.168.1.1",

"port": 1812,

"secret": "radiusSecret"

}

],

"wpaEncryptionMode": "WPA3"

}

**Register a Webhook Receiver**

* **POST** https://api.meraki.com/api/v1/organizations/{{orgId}}/webhooks/receivers

json

{

"name": "Slack Alerts",

"url": "https://hooks.slack.com/services/T0000/B0000/XXXX",

"sharedSecret": "yourSecret"

}

**Suggested Tools & Resources**

|  |  |
| --- | --- |
| **Tool** | **Purpose** |
| **Postman Meraki Workspace** | Ready-made REST API calls |
| **Meraki Python SDK** (pip install meraki) | Automate & integrate easily |
| **Webhook.site** | Test real-time events |
| **Node-RED or Flask** | Build simple webhook receivers or telemetry processors |
| **Cisco DNA Spaces** | For advanced telemetry and location intelligence |

### AI-Enhanced RRM (Radio Resource Management) in Meraki

designed to dynamically optimize RF parameters (channel, transmit power, etc.) using telemetry and historical analytics — **without disrupting production environments**, especially during business hours.

**Enterprise customers** can trial, evaluate, and operationalize **AI-RRM** safely:

**1. How to Use AI-RRM in Production with Business Hour Awareness**

Meraki AI-RRM is designed to:

* Collect RF telemetry data over **2 weeks**
* Make optimized changes **outside of busy hours**
* Minimize channel changes during work hours

**To use AI-RRM with minimal user impact:**

|  |  |
| --- | --- |
| **Setting** | **Recommendation** |
| **Enable AI-RRM** | Default in Meraki Cloud (available with R13 and supported APs like MR36, MR46, MR57) |
| **Enable “Busy Hour Optimization”** | This defers RRM changes to non-business hours using learned traffic patterns |
| **Do NOT set static channels/power manually** | Let Meraki Cloud control these during trial |
| **Run for at least 2 weeks** | AI-RRM needs ~14 days of telemetry to train optimization models |
| **Use dedicated RF Profile** | Apply to a subset of APs initially (e.g., one floor or zone) for evaluation |
| **Enable Flexible Radio Assignment (FRA)** | If supported, helps AI-RRM optimize band allocation automatically |

**2. Telemetry AI-RRM Collects (Inputs)**

During the learning phase, AI-RRM collects:

|  |  |
| --- | --- |
| **Data Type** | **Description** |
| **Neighbor Discovery Protocol** | Identifies co-channel and adjacent-channel APs |
| **Interference Duty Cycle** | How much time is spent on interference (from Wi-Fi and non-Wi-Fi sources) |
| **Noise Floor** | Measures background RF noise to estimate RF health |
| **Channel Utilization** | Percentage of airtime used on each channel |
| **AP Neighbor** | Signal strength and load of adjacent APs |
| **AP Radio Channel Power** | Output power level per radio |
| **AP Radio / AP Channel** | Which radios are operating on which channels and bands |
| **RRM Measurement Interference** | AP-to-AP and AP-to-client interference data |
| **RRM Measure Noise** | Raw environmental noise measurement per band |
| **RRM Coverage Client Info** | Client signal strength and SNR per AP |
| **RRM Measurement Load** | Number of clients and traffic per AP/channel |

**3. What AI-RRM Does with This Data (Outputs)**

|  |  |
| --- | --- |
| **Function** | **How AI-RRM Uses Telemetry** |
| **Auto Channel Assignment** | Minimizes co-channel/adjacent interference based on actual usage patterns |
| **Transmit Power Optimization** | Ensures coverage without excessive overlap or holes |
| **Band Steering / FRA** | Places radios optimally in 2.4, 5, or 6 GHz |
| **Roaming Optimization** | Uses busy hour data to minimize client disruption (roaming SNR thresholds) |
| **Suppression of Channel Flaps** | Avoids frequent changes by using trend-based adjustments (especially post-busy hours) |

**4. Suggested Evaluation Plan (14+ Day Trial)**

|  |  |
| --- | --- |
| **Day** | **Action** |
| 0–1 | Enable AI-RRM on test RF profile; apply to ~10–20 APs |
| 2–14 | Let system learn — do not manually adjust power/channel |
| 7 | Review intermediate analytics in dashboard: RF Health, Channel Distribution, Client SNR |
| 14 | Review changes made by AI-RRM in event logs and AP settings |
| 15+ | Expand profile to additional areas or campuses if performance is improved |

**Additional Considerations**

* **Business Hours Awareness** is built-in: changes are staged for non-peak periods by default.
* **AP Downtime** is minimized: no reboot is required for RRM updates.
* **Historical Data** remains visible in dashboard: track before/after changes for proof.

### Preferred options for "Corp-Guest" authentication

**1. Open Network with WPA3 Enhanced Open (OWE)**

**Enhanced Open = Opportunistic Wireless Encryption**

|  |  |
| --- | --- |
| **Feature** | **Description** |
| **Security Level** | Encryption without authentication (no password). |
| **Standards** | WPA3 OWE (RFC 8110). |
| **Encryption** | Yes (unauthenticated encryption via DPP). |
| **User Experience** | Seamless connection — no password prompt. |

**Pros:**

* **Improved security** over legacy open Wi-Fi (encrypts traffic).
* **Great for casual guests** where ease of access is a priority.
* **No captive portal** or PSK management needed.

**Cons:**

* **No identity verification** — anyone within range can connect.
* **Not compatible with older client devices** (pre-2018).
* **Minimal control or policy enforcement** without external tools (e.g., NAC overlay).

**2. Password-Protected Network with WPA3-Personal**

**WPA3-SAE = Simultaneous Authentication of Equals**

|  |  |
| --- | --- |
| **Feature** | **Description** |
| **Security Level** | High — resists offline dictionary attacks. |
| **Standards** | WPA3-Personal (SAE handshake). |
| **Encryption** | Yes — AES-GCMP encryption. |
| **User Experience** | Simple password entry at first connection. |

**Pros:**

* **Strong protection** vs WPA2-PSK (resistant to key cracking).
* **Simple guest experience** — one password shared securely.
* **Compatible with NAC overlays** (e.g., Meraki Group Policies, VLAN tagging).

**Cons:**

* **Still shared credentials** — hard to audit or revoke selectively.
* **Password sprawl** if shared widely or long-term.
* **Needs regular rotation** unless using dynamic PSK (DPSK).

**3. Web Authentication (Captive Portal) or WPA2-PSK**

**Legacy Guest Access Method**

|  |  |
| --- | --- |
| **Feature** | **Description** |
| **Security Level** | Moderate (depends on back-end integration). |
| **Standards** | WPA2 + HTTP(S) captive portal. |
| **Encryption** | WPA2-PSK (Pre-Shared Key). |
| **User Experience** | Connect to Wi-Fi, then authenticate via web browser. |

**Pros:**

* **Familiar model** used widely in enterprises, hotels, universities.
* **Granular policy enforcement** via Cisco ISE / ClearPass (e.g., time limits, sponsor approval).
* **Supports identity mapping**, even for unauthenticated guests.

**Cons:**

* **Web redirect dependent on browser behavior** (Apple CNA, Android issues).
* **WPA2 less secure** than WPA3 options.
* **Multiple user experience failure points** (redirect fails, certificate warnings).

**Recommended Strategy for Enterprise Guest Access (Corp-Guest):**

|  |  |
| --- | --- |
| **Use Case** | **Recommended Option** |
| **Ease of use, public events** | WPA3 Enhanced Open |
| **Secure enterprise guesting** | WPA3-Personal + Dynamic PSK (DPSK) |
| **Auditable/sponsored access** | Captive Portal (ISE/CP) + Web Auth or Voucher |

**Bonus**: Combining **WPA3-Personal with DPSK** (unique keys per guest or device) via Meraki or Aruba improves **security, auditability, and UX** dramatically without complex onboarding.

### Wi-Fi SSID Comparison Matrix

Three common enterprise SSIDs **Corp-IT**, **Corp-BYOD**, and **Corp-Guest**

[designed to support **Zero Trust principles**, **secure onboarding**, and **segmentation**]

**SSID Comparison Matrix: Corp-IT vs BYOD vs Guest (DPSK & Captive Portal)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Feature / Attribute** | **Corp-IT** | **Corp-BYOD** | **Corp-Guest (DPSK)** | **Corp-Guest (Captive Portal)** |
| **SSID Name (Example)** | Corp-IT | Corp-BYOD | Corp-Guest | Corp-Guest |
| **Authentication Type** | WPA3-Enterprise (EAP-TLS) | WPA2/WPA3-Enterprise (PEAP/MSCHAPv2 or EAP-TLS) | WPA3-Personal with Dynamic PSK | Open or WPA2-PSK + Captive Portal |
| **Credential Source** | User/Device Cert via MDM/AD | AAD/LDAP or user enrollment | Unique PSK per user/device | Self-registration or sponsor approval |
| **Device Type** | Managed endpoints (laptops, mobiles) | Unmanaged or semi-managed BYOD | Unmanaged guest/BYOD | Visitors/guests (any device) |
| **User Identity Visibility** | Full (username, device ID) | Partial (username only) | Low (PSK mapped to MAC or session) | High (portal input + tracking via RADIUS) |
| **Network Access Control (NAC)** | ISE / ClearPass (802.1X enforcement) | ISE / ClearPass (optional posture) | Role/VLAN assignment via DPSK profile | Role/VLAN assigned post-auth via RADIUS |
| **Security Level** | Very High | Medium to High | Medium | Low to Medium |
| **Encryption Strength** | Strong (WPA3 + certs) | Moderate to Strong | Strong (SAE handshake) | Moderate (WPA2 or open with HTTPS) |
| **Ease of Onboarding** | Seamless (via MDM auto-enroll) | Moderate (user config needed) | Easy (DPSK via email/portal) | Easy (web browser redirect) |
| **Internet Only / Internal Access** | Internal + Internet | Internal + Internet (limited) | Internet-only or DMZ | Internet-only |
| **Session Auditability** | Strong (logs tied to identity) | Moderate | Session bound to PSK/MAC | Session bound to IP/cookie |
| **Revocation / Session Control** | Cert revocation + RADIUS | ISE/CP CoA | Key expiration or revocation (DPSK) | RADIUS CoA, time-based expiry |
| **Recommended Use Case** | Staff & corporate-managed devices | Employee-owned personal devices | Known guests, recurring contractors | Walk-in visitors, casual users |

**Notes:**

* **Corp-IT** requires full MDM and certificate lifecycle.
* **Corp-BYOD** supports employee-owned devices but with tighter posture checks.
* **Corp-Guest (DPSK)** offers **better security than captive portals**, suitable for **contractors or repeat guests**.
* **Corp-Guest (Captive Portal)** supports **walk-in or casual guests** needing quick access.

**SSID Comparison Matrix: Corp-IT vs BYOD vs Guest**

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | **Corp-IT** | **Corp-BYOD** | **Corp-Guest** |
| **SSID Name (Example)** | Corp-IT | Corp-BYOD | Corp-Guest |
| **Device Type** | MDM-managed devices (laptops, tablets, phones) | Unmanaged employee devices | Visitors, contractors |
| **Authentication Type** | **802.1X with EAP-TLS (certificate-based)** | **Self-service onboarding + EAP-TLS** | **WPA3-Personal (DPSK)** or **Captive Portal** |
| **Credential Source** | X.509 certificate issued via MDM | AD login via portal + certificate provision | Guest pass, DPSK, or portal credentials |
| **NAC Integration** | Yes – ISE / ClearPass | Yes – ISE / ClearPass | Optional – for sponsored or timed access |
| **VLAN Assignment** | Dynamic (Corp VLAN) | Dynamic (BYOD VLAN) | Guest VLAN (Internet-only) |
| **Access Scope** | Full access to internal resources | Limited internal access, mail, collaboration | Internet access only, firewall-restricted |
| **Device Compliance Check** | Enforced via MDM (patch, AV, OS version) | Optional via posture check or onboarding agent | None (or basic OS/Browser check) |
| **Encryption** | WPA3-Enterprise (GCMP) | WPA3-Enterprise (GCMP) | WPA3-Personal (SAE) or WPA2 + Captive Portal |
| **Segmentation Method** | VLAN, SGT/TrustSec, ACLs | VLAN, Group Policy | VLAN, L3 ACL, Client Isolation |
| **User Identity Linked?** | Yes | Yes | Optional (if portal or DPSK mapping used) |
| **Guest Self-registration?** | No | No | Yes – sponsor or automated |
| **Ideal For** | Corporate staff with managed endpoints | Employees using personal devices | External visitors with no corporate identity |

**How Users Get Credentials (WPA3-Personal with DPSK)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Method** | **How It Works** | **User Experience** | **Use Case Fit** |
| **Guest Pass** | Admin or sponsor pre-generates a **guest pass** that includes the unique key. | User receives pass via email/SMS and connects with WPA3 using the key. | Visitor access (planned guests) |
| **DPSK (Auto)** | A **unique pre-shared key is generated** per user/device. Provisioned by ClearPass, ISE, or Meraki dashboard. | Admin/sponsor or self-service portal provides key. Easy copy/paste into device Wi-Fi settings. | BYOD, guest, contractors |
| **Portal Credentials** | User registers through a **self-service captive portal** (sponsored or open). A DPSK is generated and displayed or sent via SMS/email. | After registration, user receives a personal key and uses it to connect to WPA3 network. | Walk-in guests, unmanaged users |

**What Makes DPSK Ideal**

* Each **device or user has a unique PSK**, so there's no shared risk across users.
* In platforms like **Meraki** or **Aruba ClearPass**, the key can be **bound to MAC address**, user identity, or expire automatically.
* Keys can be **revoked** or **rotated** without impacting others.

**Corp-Guest Workflow (with DPSK + Portal)**

1. User connects to an open onboarding SSID (Corp-Onboard).
2. User completes registration on captive portal (name, sponsor email).
3. Back-end system (ISE / ClearPass / Meraki) generates a unique DPSK.
4. DPSK is displayed or emailed/SMS to the user.
5. User connects to the WPA3-Personal SSID (Corp-Guest) using that unique key.

Corp-Guest Workflow (with Captive Portal)

* When you introduce a **Captive Portal**, the authentication **no longer occurs at the Wi-Fi association phase**. Instead, it is deferred until **after the device joins the network**. This **changes both the security model and workflow**.

**Workflow (WPA2 + Captive Portal)**

1. **Guest connects to open or WPA2-PSK SSID** (e.g., Corp-Guest).
2. **DHCP and DNS allowed** — enough to reach the Captive Portal.
3. Redirect to **Guest Portal** via HTTP interception.
4. User enters **credentials**, self-registers, or enters a sponsor-provided access code.
5. **NAC (ISE/ClearPass)** validates credentials and:
   * Tags the session (CoA or RADIUS Accept)
   * Assigns VLAN or ACL (Internet-only)
6. Session is now active, and user has Internet access.

**WPA3-Personal vs WPA2 + Captive Portal**

|  |  |  |
| --- | --- | --- |
| **Feature** | **WPA3-Personal (DPSK)** | **WPA2 + Captive Portal** |
| **Authentication timing** | At association | Post-association (after IP/DNS) |
| **Encryption level** | Strong (SAE handshake, per-user key) | WPA2 (shared key or open, weaker) |
| **User Identity Tracking** | Per DPSK or device | Through portal login/sponsor form |
| **Guest Identity Validation** | Not inherently – requires MDM/NAC | Yes – via portal form |
| **Device Compatibility** | Best for modern OS | Works with older devices too |
| **Session control / audit** | Bound to key/MAC | Bound to session cookies or RADIUS acct |
| **Ease of use** | Seamless once configured | May involve multiple redirects |

**So When Would You Use Captive Portal?**

* You need **walk-up guest registration** without IT involvement.
* You want **identity tracking** via name/email/SMS code.
* You require **sponsor approval** workflows.
* You support a **broad range of devices**, including those with limited WPA3 support.

**Important Notes**

* **Captive Portal ≠ WPA3-Personal**. Most vendors don’t support *both* simultaneously because WPA3-Personal pre-authenticates users.
* **WPA3-Enhanced Open** can provide **opportunistic encryption (OWE)** with no auth, but lacks user ID.
* If security is paramount, prefer **WPA3-Personal with DPSK**, and layer NAC for session control.
* If **frictionless guest onboarding** is more critical, **WPA2 + Captive Portal** is still very common.

Guest use-cases

* "Guest: Sponsor User Creation"
* "CWA Chaining"
* they serve different purposes and apply to different user journeys.

**Comparison Summary**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Sponsor User Creation** | **CWA Chaining** |
| Purpose | Create/manage guest accounts | Multi-phase WebAuth + Auth chaining |
| Identity Assurance | Yes (via sponsored credentials) | Yes (via certs, usernames, posture) |
| Captive Portal | Yes | Yes (with redirect ACL) |
| MAB Support | Optional | Required to initiate chaining |
| Guest Device Trust Level | Low (Internet-only) | Moderate to High (BYOD, posture possible) |
| Enterprise Use Case | Lobby, Visitors, Contractors | BYOD onboarding, Partner access |

**Guest: Sponsor User Creation**

**What it is:**

A **sponsor** (usually an employee or receptionist) creates temporary **guest credentials** via a captive portal or ISE sponsor portal.

**How it works:**

1. Sponsor logs into the **ISE Sponsor Portal**.
2. Creates a new guest account (name, email, phone number, duration, etc.).
3. Credentials are sent to the guest (via SMS/email).
4. Guest connects to the Guest SSID and logs in using the credentials.

**Use Case:**

* Controlled guest access with **accountability**.
* Used in **lobby check-ins**, **conferences**, **contractor access**, etc.

**Pros:**

* More secure and auditable.
* Enables **policy-based access** (e.g., Internet-only).
* Sponsors can **expire or revoke** access.

**CWA Chaining (Central Web Authentication Chaining)**

**What it is:**

A more advanced **guest or BYOD onboarding** method where **authentication continues beyond just web login**.

It typically **links multiple phases**: MAC authentication → WebAuth → Identity validation (via cert or username).

**How it works (e.g., for BYOD or advanced guest):**

1. Device connects to Guest SSID.
2. ISE performs **MAB (MAC Authentication Bypass)** to identify the device.
3. ISE applies a redirect ACL and forwards to a **web portal**.
4. User completes WebAuth (e.g., username/pass or certificate).
5. ISE **"chains"** this result back to the original session using **session correlation**, allowing full access or BYOD provisioning.

**Use Case:**

* Used for **advanced guest**, **BYOD onboarding**, or **employee fallback** flows.
* Ensures **identity assurance** even after initial WebAuth.

**Pros:**

* Allows **multi-phase onboarding**.
* Can integrate with **certificate issuance**, **endpoint posture**, or **provisioning flows**.

### Distributed Layer 3 Roaming (DL3R)

|  |  |
| --- | --- |
| **Without DL3R – No Coordination Between APs** | * Without DL3R, wireless clients assume they remain in the same Layer 2 domain when roaming between access points (APs). * As a result, clients continue using their original IP address even if they’ve moved to a new VLAN or subnet. * Since the receiving AP considers this an invalid IP, it drops the traffic. * The client must then detect the subnet change and issue a new DHCP request—a process that can take seconds to minutes depending on the device and OS. * This delay severely impacts latency-sensitive applications like voice and video, resulting in poor user experience. |
| **Without DL3R – New DHCP Request Logic** | * In a non-DL3R environment, when a client roams into a new subnet, the traffic is effectively blackholed until the client identifies the need for a new IP via DHCP. * The delay stems from the client's OS behavior, not the network. * Some clients take a long time to issue a new DHCP request, which introduces performance and connectivity issues—especially in high-mobility environments like healthcare, warehousing, or enterprise voice deployments. |
| **DL3R Connect Logic** | * DL3R avoids centralized tunneling by implementing a distributed control and data plane across all APs. * When a client first associates with an AP, it receives an IP from the AP’s local VLAN. * That AP becomes the anchor, and it pushes the client’s MAC/IP/VLAN mapping to all APs in the network. * These APs store the client entry, including DHCP lease information, and pre-select candidate APs in the same subnet for tunnel redundancy. * This distributed model eliminates the bottlenecks of centralized controllers and scales better across large environments. |
| **DL3R – Roam to New AP Not in Same VLAN** | * When a client roams to an AP in a different VLAN/subnet, the new AP checks its synchronized client database. * If a match is found, the AP forms an automatic tunnel back to the anchor (or a candidate AP) in the original subnet. * This tunnel allows the client to retain its original IP address, maintaining session continuity. * Tunnels are formed dynamically and torn down when no longer needed (e.g., client disconnects for >30 seconds). * This method ensures seamless roaming and application persistence across Layer 3 boundaries. |
| **Summary** | DL3R enables seamless mobility for wireless clients across subnets by leveraging:   * A distributed client database synchronized across all APs. * Automatic tunneling to maintain original IP sessions. * Elimination of Layer 3 handoff delays and DHCP reinitiation. It is particularly beneficial in environments with high mobility and real-time applications, offering a scalable and performance-optimized solution compared to traditional centralized Layer 3 roaming approaches. |