

# Specifications

|  |   |
|--|---|
| <b>Management</b>  | Unauthorized software and app installation monitoring and notification  |
| Managed via the web with Meraki's secure browser based dashboard   | Install enterprise apps   |
| Centralized administration of managed devices  |   |
| Organization level two-factor authentication   | <b>Content Management</b>   |
| Role-based administration  | Custom deployment of files, documents, apps (Android and iOS)   |
| Inventory data export to CSV   | Update and deploy the latest file version to devices (Android and iOS)  |
| Remote command line  | Manage and distribute app licenses (iOS and macOS with VPP)   |
| Administrative event log and activity log  | Device license assignment (iOS with VPP)  |
| Automatic alerts for installed software, geofencing, enrollment, and security reporting  | Deploy iBook licenses   |
| Copy profiles across different networks  | Home screen layout (iPad only)  |
| Install available OS updates (iOS and macOS - requires DEP)  |   |
| <b>Security</b>  | <b>Device Restrictions</b>  |
| Device location using device WiFi, IP address, and GPS data  | Restrict use of camera (iOS and Android)  |
| Containerization, separation of managed and unmanaged data (via managed open-in with iOS and Android for Work with Android)                              | FaceTime, Siri, iTunes Store, multiplayer gaming, and Apple Music (iOS)   |
| Unenrollment monitoring and notification   | Restrict content consumption (YouTube, explicit music & podcasts, content rated movies, TV shows, and apps) (iOS) |
| Antivirus, antispware, firewall, disk encryption, passcode and password, screenlock timeout , and jailbreak and root detection                           | Force encrypted backup (iOS) and encrypted storage (Android)  |
| Restrict access to iCloud (iOS)  | Enforce passcode policies and failed entry device wipe policy (Android, iOS, Mac, PC)                             |
| Restrict users to accept untrusted TLS certificates (iOS)  | Single App or Kiosk mode (Android and iOS)  |
| Force encrypted backup (iOS) and encrypted storage (Android)   | Autonomous Single App mode (iOS)  |
| Global HTTP Proxy (iOS)  | Automatic and whitelisted content filter (iOS)  |
| Enforce passcode policies and failed entry device wipe policy (Android, iOS, Mac, PC)  | Restrict use of AirDrop (iOS)   |
| Scan client device for Systems Manager before allowing network access (Android, iOS, Mac, PC)  | Restrict changes to cellular data usage for apps ( iOS)   |
| Simple Certificate Enrollment Protocol (SCEP)  | Toggle Voice and Data Roaming Settings (iOS)  |
| Customer Certificate Signing for certificate provisioning  | Restrict which Airplay devices are listed (iOS)   |
| Access rights to limit Dashboard control (e.g. cannot erase BYOD devices iOS and Mac)  | Keep device name up-to-date (iOS)   |
| Dynamic profile management - security compliance, geofence management, time schedule, minimum running OS, App black/whitelist, and data limit thresholds | Manage unmanaged apps (iOS)   |
| Lost Mode (iOS)  | Lock wallpaper and device name (iOS)  |
| Always-on, On-demand, and Per-app VPN, AnyConnect VPN  | Managed domains, Safari autofill domains (iOS)  |
|  | Notification settings and disallowing changes to notification settings (iOS)                                      |
|  | Show/hide apps (iOS)  |
| <b>Software and App Management</b>   | <b>Troubleshooting and Live Tools</b>   |
| Inventory installed software and apps  | Remote device lock, unlock, and wipe (Android, iOS, Mac, and Windows)   |
| Custom deployment of software and public App Store and Google Play apps  | Remote reboot and shutdown (Mac and Windows)  |
| Integration with Apple App Store and Apple's Volume Purchase Program   | Remote desktop and screenshot (Mac and Windows)   |
| Integration with Google Play Store and Android for Work  | Access device process list (Mac and Windows)  |
| Host files up to 3GBs on the Meraki cloud  | Send instant notification to device (Android, iOS, Mac, and Windows)  |
| Software installation via .msi or .exe on PC and .dmg on Mac   | Monitor active TCP connections, TCP stats, and routing table (Mac and Windows)                                    |
| Software uninstallation (Mac and Windows)  | Selective Wipe (Android, iOS, and Mac)  |
| Uninstallation of apps (Android and iOS)   | Toggle voice, data roaming, and hotspot (iOS)   |
| Restrict app installation  | Command Kiosk-mode or Single App mode on demand (Android and iOS)   |
| Restrict in-app purchase   | Initiate Airplay remotely (iOS)   |

---

## Network Configuration Deployment

Deploy WiFi settings including WPA2-PSK & WPA2-Enterprise (Android, iOS, Mac, and Windows)

Deploy VPN configuration and authentication settings (Android, iOS, Mac, and Windows)

Deploy server side digital certificates (Android, iOS, Mac, and Windows)

Scan client device for Systems Manager before allowing network access (Android, iOS, Mac, and Windows)

Deploy Airplay destinations and passwords

Cisco ISE MDM API Integration

---

## Sentry Security

Sentry Policies - Network policy enforcement based on posture (Android, Chrome, iOS, Mac, and Windows)

Sentry Enrollment - Integrated self service onboarding (Android, iOS, Mac, and Windows)

Sentry WiFi Security - Single click EAP-TLS deployment (Android, iOS, Mac, & Windows)

Sentry VPN Security - Auto provision mobile client VPN (Android, iOS, Mac)

Sentry WiFi Settings - Auto configure WLAN settings (Android, iOS, Mac, and Windows)

Sentry VPN Settings - Auto configure VPN settings (Android, iOS, Mac, and Windows)

---

## Device Enrollment

App enrollment (iOS and Android)

Auto enrollment through DEP (iOS 7+ and macOS 10.10+)

On-device enrollment (iOS, Android, Mac, Windows)

Integration with Apple Configurator & Profile Manager (iOS and Mac)

SMS or email enrollment invitation (iOS, Android, Mac, Windows)

Local installer deployment (Mac and Windows)

Integration with Active Directory's GPO (Windows)

Quarantine devices upon enrollment (Android, Chrome, iOS, Mac, Windows)

Chrome OS Device Management through G Suite and G Suite for Education

Multi-user authentication - dynamically change device software, settings, and access

---

## Monitoring

Hardware vitals and specs reporting

Network access, connectivity, signal strength monitoring

Restriction compliance monitoring

Device location with device WiFi connection, IP address, and GPS data

Battery, storage, RAM and CPU usage, outage monitoring

Override location based on network/IP information (e.g. when GPS isn't an option)

---

## Automatic Provisioning

Group Policy integration into the Cisco Meraki hardware stack

Dynamic tags based on mobile identity including geolocation, security posture, and time

Active Directory and LDAP group integration to automatically apply tags, owners, & users

Automatically distribute and revoke App licenses with VPP

---

## Email Settings

Exchange ActiveSync email account provisioning (Android and iOS)

Restrict outgoing mail to only the managed account in mail app (iOS)

Use custom domains and domain formats

Force the use of SSL when using ActiveSync

Enable S/MIME when using ActiveSync

Managed app settings for email in Gmail app (Android and iOS)

Use device owners to automatically insert e-mail addresses specific to users on a device

---

## Chrome OS Management

Lock, disable, and control devices

Set and manage user and device level settings

Whitelist users to sign in to devices

Enable Auto updates

Enable Kiosk mode

Wifi and VPN configuration

Enable Safe browsing

Manage Power settings

Configure browser bookmarks, security, and content filters

---

## Cellular Data Management

Generate global and individual reports for cellular data usage (Android and iOS)

Monthly counter and plan start date for tracking usage by plan (Android and iOS)

Policies to specify single or multiple data limit thresholds (Android and iOS)

Use policies to take action on devices going over their data limit (Android and iOS)

Restrict changes to cellular data usage for apps (iOS)

Toggle data roaming and personal hotspot (iOS)