Systems Manager

Multi-platform
Enterprise Mobility Management

Overview

Meraki Systems Manager provides cloud-based, over-the-air centralized Enterprise Mobility Management (EMM). Simply administer distributed deployments of all of your devices through a powerful web-based dashboard.

Managed devices connect securely to Meraki's cloud, enabling device tracking, software and app deployment, content delivery, enforcement of security policies, identity management, and Cisco network integration. End user permissions can change automatically from policy information such as time of day, geolocation, security posture, and user group.

As Cisco's EMM solution, Systems Manager supports a variety of platforms allowing for the diverse ecosystem often found in today's mobile centric world. This places Systems Manager in prime position to alleviate the concerns of security teams in regulated industries, empower teachers to run their digital classroom, and ease the burden of enterprise IT teams with distributed sites. Meraki solves the mobility management needs of today and whatever comes next.

MOBILE DEVICE MANAGEMENT (MDM)

Total device management for mobile and desktop

- Provision settings and restrictions
- Inventory management and device tracking
- Full device wipe and selective wipe
- Remote viewing and troubleshooting
- Native remote desktop support
- Android, Chrome, iOS, macOS, Windows, & Windows Phone

MOBILE CONTENT MANAGEMENT (MCM)

Control and provision content and file-sharing

- Deliver content through proprietary file sharing & backpack
- Enable shared use of mobile devices
- Enterprise file sync and sharing (EFSS) Dropbox integration
- Access policies for file distriubtion, replacement, and deletion
- Conditional access to files including copy/paste and e-mail attachments

MOBILE APPLICATION MANAGEMENT (MAM)

Industry-leading ease of use brought to software management

- Deploy in-house developed and public apps
- Enterprise app store and cloud hosting
- Native app containerization with Android for Work, iOS managed open-in
- Managed-app configuration
- Volume app licensing

MOBILE IDENTITY (MI)

Simple and comprehensive policy management

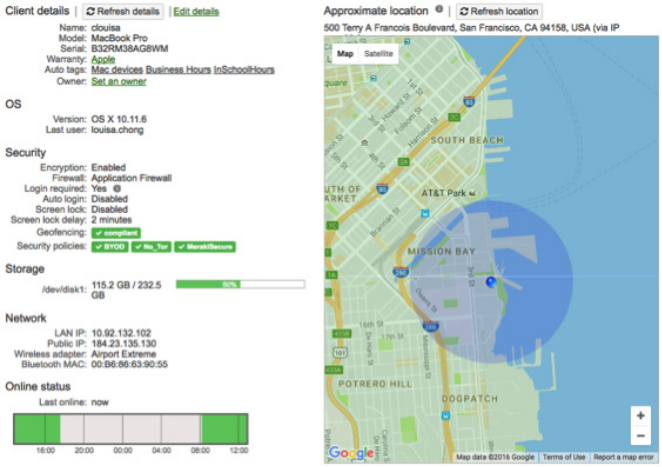
- Control access by OS type, security compliance, time of day, geolocation, and user groups
- Indentity access management (IAM) including files, apps, settings & certs
- Limited access roles for granular administrive access to Dashboard
- Automated network policy management on Cisco networks
- Active Directory, LDAP, and OAuth integration

Cloud Architecture and Scalability

Meraki's cloud architecture provides a highly flexible system for mobility management. Whether an organization starts with one device or one hundred thousand, there is no difference in the components required or the complexity to deploy. Simple and quick to get started, powerful and scalable for the long term.

Mobility management is a symbiotic partnership between device manufacturer (e.g. Apple, Google, Microsoft) and EMM vendor. Meraki's cloud infrastructure and agile development model delivers features and support for new EMM functions at lightning speed, with no patches or software installs required.

With Systems Manager, Meraki offers the industry's only end-to-end solution which unifies EMM with network elements such as WLAN, WAN and LAN. This is achieved through native network integration and uses a single pane of glass management dashboard. Gain complete visibility and control from the top of the network to the edge while also enabling typically complex security features in a couple clicks. The intuitive Meraki dashboard enables IT professionals to configure and deploy in just minutes without specialized training or dedicated staff.



Onboarding and Enrollment

Systems Manager has a flexible onboarding process with a number of currated enrollment options. These options can vary based on the type of device and the style of onboarding. Bring Your Own Device (BYOD) can be easily managed alongside the stricter requirements of an organization owned device.

Enroll devices seemlessly through built-in integration with platforms such as Apple's Device Enrollment Program (DEP), Systems Manager Sentry, via a web-based self-service portal directly on the mobile device, or by installing an app from an app store. Supervise iOS devices over-the-air with DEP or integrate with existing Apple Configurator deployments.

With Android for Work, create personal and work profiles and optionally implement device ownership. For macOS and Windows devices, utilize programs like DEP and Work Access. Alternately, Systems Manager can be deployed over the air or on individual machines via a lightweight installer.

Once enrolled, each device downloads its configuration from the Meraki cloud applying device restrictions, network, and security policies automatically — eliminating manual device provisioning.

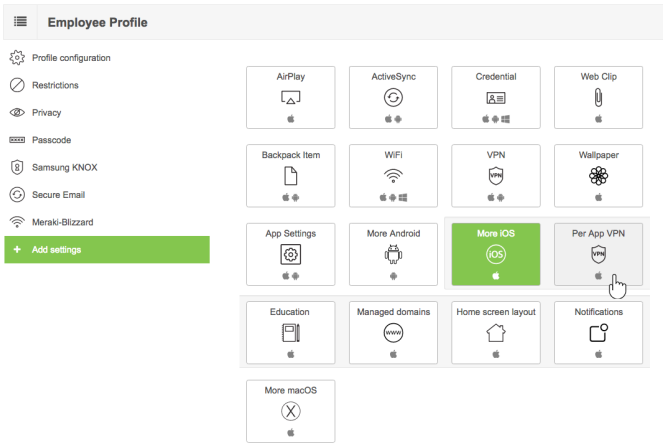
Profiles & Settings

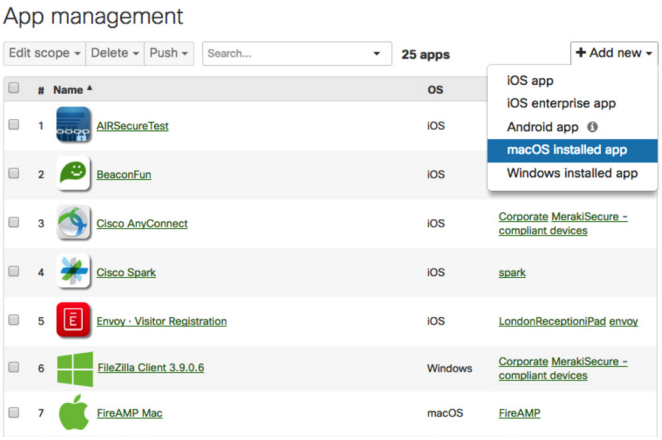
Profiles & settings provide a comprehensive suite for the wide range of device provisioning needs. This can contain everything from device restrictions and permissions to FileVault encryption as well as e-mail, device privacy, WiFi, VPN, wallpaper, notifications, contacts, Web Clips, managed app settings, education and Apple Classroom, and much more.

Combining profiles & settings with Mobile Identity establishes a powerful way to dynamically and intelligently distribute the required settings to the correct device given time of day, OS type, security compliance, geolocation, and user groups considerations.

Meraki provides the answer to complex mobility requirements while maintaining industry-leading ease of use aimed to create a delightful experience for administrators and end users.

Mobile provisioning becomes simple click or drag-and-drop.





Apps, Software, and Containerization

Total application management requires control, distribution, and visibility over not just apps but also app licenses, software inventory, and containerization requirements. Systems Manager installs public apps by integrating with the Apple App Store and Google Play Store. Private apps are also managed seamlessly through cloud-hosting or locally hosting apps and installers for enterprise app and software deployments. The needs of today's application security are met through a mixture of app blacklists and whitelists, permission management and restrictions, and native containerization through Android for Work (Android) and a comprehensive implementation of managed open-in (iOS).

Mobile Identity also integrates with software management to provide a way to create granular policies and automation for all application needs.

Solve complex requirements with managed app settings, software encryption, separation, and permissions. Simplify mobile application and software deployments to a couple clicks.

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

Rapid Deployment and Scalability

Meraki's cloud management platform enables mobile device initiatives to quickly scale to deployments of massive scale. This is accomplished in part by the reliability and flexibility of the Cisco Meraki cloud and the complete support of different enrollment methods. Devices can be enrolled and onboarded both automatically for zero-touch administration or manually for more flexibility in other use cases. Enrollment is done through profiles and/or lightweight installers (agents).

Automated Enrollment Methods

iOS and macOS devices can be enrolled in Systems Manager out of the box by utilizing Apple's Device Enrollment Program. This provides a seemless deployment of Apple devices without the need for administrators to physically touch devices.

Windows devices can be enrolled over the air using Work Access. Deployments using the lightweight installer can be done dynamically using an Active Directory Group Policy Object (GPO) for all the devices in a Windows domain.

Android for Work enabled devices can be automatically enrolled when adding a company account for a work domain managed by Google and bound to their Systems Manager network.

Systems Manager Sentry Enrollment

Sentry enrollment also provides zero-touch deployment for administrators. Without Systems Manager, unmanaged devices trying to join the network are first sent to a splash page to install Systems Manager. Only after enrollment can devices gain access to the network and corporate resources.

Manual Enrollment

For all deployment models, Systems Manager offers a web-based self-enrollment process directly on the mobile device or by installing a downloadable app from an app store. Systems Manager also integrates with Apple Configurator, provides QR codes for enrollment, and supports the distribution of enrollment URLs via e-mail and SMS.

Administration and Management

Systems Manager is designed to help you keep your managed devices up-to-date with the latest user demands and organization requirements, while lowering the IT burden. Deploy policies and changes seamlessly from the cloud, across thousands of devices at once.

Automated Device Provisioning

Devices are provisioned based on user group, OS type, security compliance, time of day, and geolocation. Automatically deliver apps, network, and security settings specific to each device & user.

Email Configuration

Enable provisioning of email accounts and mail settings including encryption, stored mail history duration, and access permissions on enrolled Apple iOS and Android devices.

Deploy Software

Systems Manager installs software on any number of PCs and Macs. Upload to the cloud or locally host MSI or EXE files for PCs or DMGs for Macs, select the machines, and let the Meraki cloud do the rest. If a device is unavailable, the software will be enqueued and installed the next time it comes online.

Deploy Apps

For iOS devices, Systems Manager is integrated with the Apple App Store and Apple's Volume Purchase Program. Google Play and the Amazon Appstore are supported on Android devices. Additionally, enterprise apps are supported on both iOS and Android. Systems Manager makes it easy to distribute apps to ten users or thousands and on any number of devices.

Enforce Restrictions

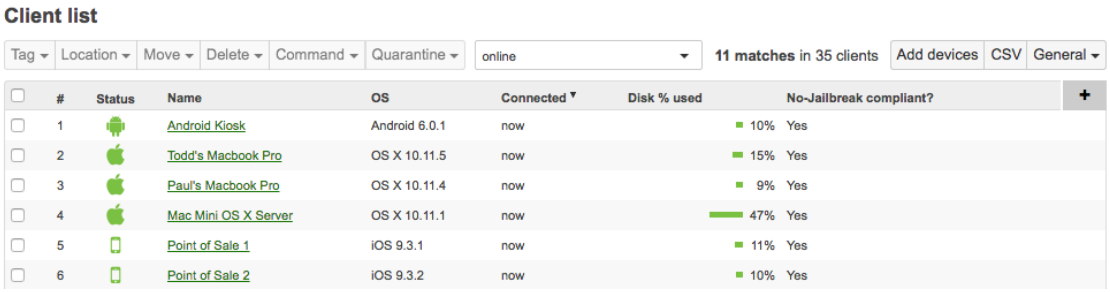
Restrictions allow organizations to control how devices are used. Disable FaceTime, the App Store, and control gaming and media content consumption by content rating. Restrict access to iCloud services to disallow backup of sensitive information to Apple's infrastructure. Disallow applications and application permissions.

Security Compliance

Systems Manager helps organizations protect mobile devices and data with customizable security policies. Deploy fine-grained policies to check whether devices are encrypted, locked, jailbroken, and running the latest OS version before dynamically assigning device settings, apps, and content in order to secure resources and data. Require a passcode on devices before pushing Exchange settings, limit jailbroken devices to the guest network, or revoke privileges if devices violate security policies.

Full Device Wipe and Selective Wipe

Systems Manager provides a mechanism to prevent enterprise data from getting into the wrong hands. The selective wipe feature removes all configuration profiles and apps that have been previously pushed to a device via EMM, while keeping the device enrolled for the purposes of tracking. Full device wipe, or factory reset, removes everything, including the management profile, to completely erase all data and remove the device from Systems Manager.



Visibility, Diagnostics, and Control

Systems Manager starts to monitor managed devices as soon as they enroll. Policies continue to be applied to devices anywhere in the world, even if they lose internet connectivity. Live diagnostics tools help with troubleshooting and daily administration tasks. Use Systems Manager's visibility of devices, users, software and applications on your network to provide end to end security and management right from the dashboard.

Asset Management

Systems Manager gathers available information from the device's GPS, WiFi connection, and IP address to provide a device's physical location, down to street-level accuracy. Privacy controls are available to turn off location reporting for sensitive devices and users.

Systems Manager provides built-in software inventory management, simplifying software license management, even in multiplatform environments. See all installed software on managed computers and apps on mobile devices. Alternatively, type the name of a particular application in a Google-like search bar to search through a comprehensive list of installed software across managed devices. Easily identify devices running outdated software, track down compliance or licensing issues, or uninstall unauthorized software right from the dashboard.

Manage hardware inventory using Systems Manager's built-in catalog of machines by CPU type and speed, system model, or operating system build. Systems Manager also tracks wireless adapter details, including make, model and driver version, helping track down connectivity issues.

Live Troubleshooting and Diagnostics

Systems Manager provides a suite of real-time diagnostic tools. Initiate remote desktop, take a screenshot, see the current process list, and remotely reboot or shutdown Macs and PCs. For remote desktop access, Systems Manager automatically configures a VNC server and establishes a secure end-to-end tunnel back to the dashboard. These tools enable complete remote systems management, even in complex network environments with multiple firewalls or NAT gateways.

Manage daily requests for iOS and Android devices, like remotely clearing the passcode, locking a device, or even erasing data in the event that the device is compromised. Monitor device statistics like battery charge and device memory usage centrally from the dashboard.

Email Notification Alerts

Configure fine-grained alert policies to send email notifications to monitor devices, software, compliance, and connectivity. Be notified when unauthorized software is installed on a managed device, when specified devices (like critical servers) go offline, and when the Systems Manager agent or profile is removed from a managed device.

Privacy Settings

When applicable, ensure user privacy by limiting access to device location and BSSID tracking. Access rights can be used to limit administrative capabilities over managed devices including disabling remote desktop, software inventory, reading device profiles, installing applications, and the ability to remote wipe devices.

Cellular Data Management

Set limits for cellular data usage across all managed devices. Create multiple policies for different plan thresholds, and attach policies to apps and settings in order to restrict access, data, and functionality if a device goes over a plan's limit. Track data usage over time as well as on demand while recieving e-mail alerts and taking action dynamically given data limit violations.

Network Integration – Systems Manager Sentry

Systems Manager is unique in the EMM market as it is part of a complete and integrated IT stack which includes wireless, switching, security, security cameras, and phones and is entirely managed by one single pane of glass. As part of Cisco Meraki's end-to-end IT solution, Systems Manager provides visibility and functionality not available with standalone EMM products. This gives an IT team more time to focus on their organization's mission instead of spending time on integration or complex configuration. Device on-boarding, settings assignment, application management, and network access, are just some IT responsibilities that can be simplified, automated, and dynamically updated with Systems Manager Sentry.

Systems Manager continuously keeps track of mobile identity and device posture and will dynamically adjusts policies to match. Security threats are constantly evolving which makes deploying a safe and secure connectivity infrastructure paramount to any organization. When Systems Manager is deployed on a Meraki network infrastructure, it enables context-aware security and connectivity. Below is a list of features found in the Systems Manager Sentry suite.

Sentry Enrollment

Integration with Meraki access points (MR series) enables network administrators to only allow devices managed with Systems Manager to access the network. Sentry enrollment also provides zero-touch deployment for administrators through a user self-service portal. Without Systems Manager, unmanaged devices trying to join the network are sent to a splash page to install Systems Manager. Only after enrollment can devices gain access to the network and coporate resources.

Sentry Policies

Meraki network settings such as firewall rules, traffic shaping policies, and content filtering can be dynamically changed based on mobile identity information from Systems Manager. Network access is controlled, updated, and remediated automatically based on granular policies ranging from OS type and time schedule to security posture and current user.

Sentry WiFi Security

Automatically provision EAP-TLS WLAN authentication with unique certificates without a need to manage a certificate authority or radius server. When a device fails security compliance, e.g. due to the user disabling the antivirus or jailbreaking a device, have Systems Manager remove the certificate from the device and the device from the network.

Requires: Systems Manager (SM) and Meraki Wireless (MR)

Sentry VPN Security

Provision VPN automatically including unique usernames and passwords while controlling access based on security compliance, time of day, user group, and geolocation.

Requires: Systems Manager (SM) and Meraki Security (MX)

Sentry WiFi Settings

Provision WiFi settings automatically to connect managed devices to a Meraki MR wireless network. Sentry WiFi settings eliminate the need for an administrator to enter manual WiFi settings and configuration or update when there are changes to an MR network in the same organization.

Sentry VPN Settings

Provision VPN settings automatically to connect managed devices to a Meraki MX security appliance. No need to insert manual VPN settings or update given changes to an MX network in the same organization.

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

Multi - OS Management

Android 4.0+ (Android for Work 5.0+)
including phones, tablets & more;

Chrome OS (G Suite or G Suite for Education acct.)
including Chromebook, Chromebox & more

iOS 5+ (Systems Manager App requires iOS 7+)
including Apple iPad, iPod Touch, and iPhone

macOS 10.7+
including Macbook, iMac, Mac mini, Mac Pro & more

Windows 10, 8.1, 8, 7, and Windows Phone
including Surface, tablets, desktops, laptops & more

Windows Server 2016, 2012, 2008 R2

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

Specifications

Supported Platforms
Android 4 or higher including phones, tablets & more (Android for Work requires 5.0+)
Chrome OS including Chromebook & more (G Suite or G Suite for Education account)
iOS 5 or higher including iPad, iPod Touch, & iPhone (SM app requires iOS 7 or higher)
macOS 10.7 or higher including Macbook, iMac, Mac mini, Mac Pro, & more
Microsoft Server 2016, 2012, 2008 R2
Windows 10, 8.1, 8, 7 including Surface, tablets, desktops, laptops, & more
Windows Phone 10, 8.1 including Surface, Lumia, HTC, Nokia, & more

Management
Managed via the web with Meraki's secure browser based dashboard
Centralized administration of managed devices
Organization level two-factor authentication
Role-based administration
Inventory data export to CSV
Remote command line
Administrative event log and activity log
Automatic alerts for installed software, geofencing, enrollment, and security reporting
Copy profiles across different networks
Install available OS updates (iOS and macOS - requires DEP)

Security
Device location using device WiFi, IP address, and GPS data
Containerization, separation of managed and unmanaged data (via managed open-in with iOS and Android for Work with Android)
Unenrollment monitoring and notification
Antivirus, antispyware, firewall, disk encryption, passcode and password, screenlock timeout , and jailbreak and root detection
Restrict access to iCloud (iOS)
Restrict users to accept untrusted TLS certificates (iOS)
Force encrypted backup (iOS) and encrypted storage (Android)
Global HTTP Proxy (iOS)
Enforce passcode policies and failed entry device wipe policy (Android, iOS, Mac, PC)
Scan client device for Systems Manager before allowing network access (Android, iOS, Mac, PC)
Simple Certificate Enrollment Protocol (SCEP)
Customer Certificate Signing for certificate provisioning
Access rights to limit Dashboard control (e.g. cannot erase BYOD devices iOS and Mac)
Dynamic profile management - security compliance, geofence management, time schedule, minimum running OS, App black/whitelist, and data limit thresholds
Lost Mode (iOS)
Always-on, On-demand, and Per-app VPN, AnyConnect VPN

Software and App Management
Inventory installed software and apps
Custom deployment of software and public App Store and Google Play apps
Integration with Apple App Store and Apple's Volume Purchase Program
Integration with Google Play Store and Android for Work
Host files up to 3GBs on the Meraki cloud
Software installation via .msi or .exe on PC and .dmg on Mac
Software uninstallation (Mac and Windows)
Uninstallation of apps (Android and iOS)
Restrict app installation
Restrict in-app purchase
Unauthorized software and app installation monitoring and notification
Install enterprise apps

Content Management
Custom deployment of files, documents, apps (Android and iOS)
Update and deploy the latest file version to devices (Android and iOS)
Manage and distribute app licenses (iOS and macOS with VPP)
Device license assignment (iOS with VPP)
Deploy iBook licenses
Home screen layout (iPad only)

Device Restrictions
Restrict use of camera (iOS and Android)
FaceTime, Siri, iTunes Store, multiplayer gaming, and Apple Music (iOS)
Restrict content consumption (YouTube, explicit music & podcasts, content rated movies, TV shows, and apps) (iOS)
Force encrypted backup (iOS) and encrypted storage (Android)
Enforce passcode policies and failed entry device wipe policy (Android, iOS, Mac, PC)
Single App or Kiosk mode (Android and iOS)
Autonomous Single App mode (iOS)
Automatic and whitelisted content filter (iOS)
Restrict use of AirDrop (iOS)
Restrict changes to cellular data usage for apps (iOS)
Toggle Voice and Data Roaming Settings (iOS)
Restrict which Airplay devices are listed (iOS)
Keep device name up-to-date (iOS)
Manage unmanaged apps (iOS)
Lock wallpaper and device name (iOS)
Managed domains, Safari autofill domains (iOS)
Notification settings and disallowing changes to notification settings (iOS)
Show/hide apps (iOS)

Troubleshooting and Live Tools
Remote device lock, unlock, and wipe (Android, iOS, Mac, and Windows)
Remote reboot and shutdown (Mac and Windows)
Remote desktop and screenshot (Mac and Windows)
Access device process list (Mac and Windows)
Send instant notification to device (Android, iOS, Mac, and Windows)
Monitor active TCP connections, TCP stats, and routing table (Mac and Windows)
Selective Wipe (Android, iOS, and Mac)
Toggle voice, data roaming, and hotspot (iOS)
Command Kiosk-mode or Single App mode on demand (Android and iOS)
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 Managment 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

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)

Teacher's Assistant
Teacher portal with limited access roles (e.g. limit device visibility to those only in the classroom or only during specific times)
Lock devices into single app mode
Configurable time schedules
Initiate AirPlay on an iOS device to an Apple TV
Push files to students using backpack
Full support for Apple Classroom
Multi-user and shared tablet support for both Apple and Android devices

Native Systems Manager API