Systems Manager

Endpoint Management

Overview

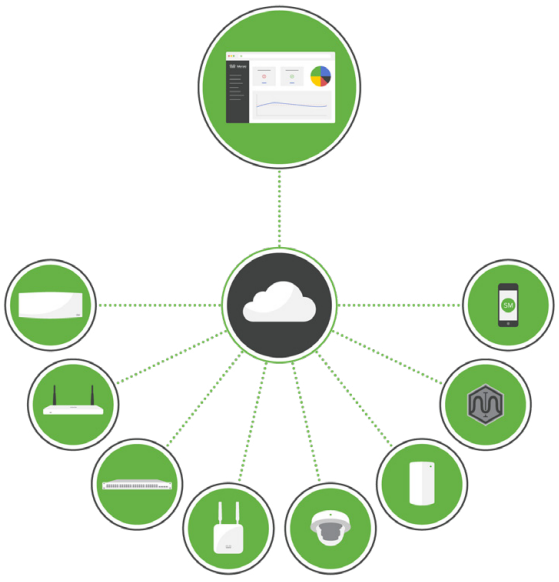
As Cisco's endpoint management solution, Cisco Meraki™ Systems Manager supports a variety of platforms, allowing for the diverse ecosystem often found in today's mobile-centric world. This places Systems Manager in prime position to alleviate the concerns of security teams in various industries, empower teachers to run their digital classrooms, and ease the burden of enterprise IT teams with distributed sites.

Systems Manager offers centralized, cloud-based tools for endpoint management with far-reaching scalability for growing organizations. With the easy-to-use web-based dashboard, organizations can manage distributed deployments quickly from any location.

Meraki Systems Manager offers an array of capabilities for endpoint management detailed in this document for the provisioning, monitoring and securing of end devices.

Native network integration

Meraki Systems Manager's integration with Cisco Meraki networking products allows organizations to unify IT administration from one cloud dashboard. The Meraki dashboard helps enable administration of WAN, LAN, security appliances, security cameras, and endpoint management from one interface. The intuitive nature of the dashboard allows IT professionals to configure and deploy in just minutes, without requiring specialized training or dedicated staff.



Native network integration – systems manager sentry

Meraki Systems Manager is unique in the endpoint management market due to its native network integration. As part of the Cisco Meraki networking portfolio, Meraki Systems Manager has been designed from the ground up to share intelligence with Cisco Meraki network and security products—allowing IT teams to automate decisions about network and data access depending on the state of a given device, including installed software, security profiles, location, and more.

As part of Cisco Meraki's end-to-end IT solution, Systems Manager provides visibility and functionality not available with stand-alone endpoint management products. Device onboarding, settings assignment, application management, and network access are just some IT responsibilities that can be simplified, automated, and dynamically updated with Systems Manager.

Systems Manager continuously tracks mobile identity and device posture and will dynamically adjust 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.

The Systems Manager Sentry suite of features refer to the cross-product integrations that Systems Manager supports with Meraki's wireless, switching, and security appliance portfolio. 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 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 wi-fi

Administrators can provision Wi-Fi settings automatically to connect managed devices to a Meraki MR wireless network. EAP-TLS WLAN authentication can be automatically provisioned with unique certificates without a need to manage a certificate authority, RADIUS server, or PKI. Sentry Wi-Fi settings eliminate the need for an administrator to enter manual Wi-Fi settings or make configuration updates when there are changes to an MR network in the same organization.

When a device fails security compliance, e.g. due to the user disabling the antivirus or jailbreaking a device, Systems Manager can automatically remove the certificate from the device and revoke access to the network (requires Systems Manager (SM) and Meraki Wireless (MR)).

Sentry VPN

VPN settings can be automatically provisioned to connect managed devices to a Meraki MX security appliance hosting client VPN. Changes to VPN configurations on the MX side are automatically reflected in Systems Manager without any manual action needed.

Client VPN can be conditionally granted and revoked automatically based on security compliance, time of day, user group, and geolocation (requires Systems Manager (SM) and Meraki Security (MX)).

Meraki Systems Manager has integrations with Cisco® security and networking products including Cisco Umbrella™, Cisco Advanced Malware Protection (AMP) for Endpoints (Cisco Clarity), Cisco Identity Services Engine (ISE), Cisco Aironet™ Wireless, Cisco AnyConnect® VPN software, Meraki MR access points, and Meraki MX security appliances.

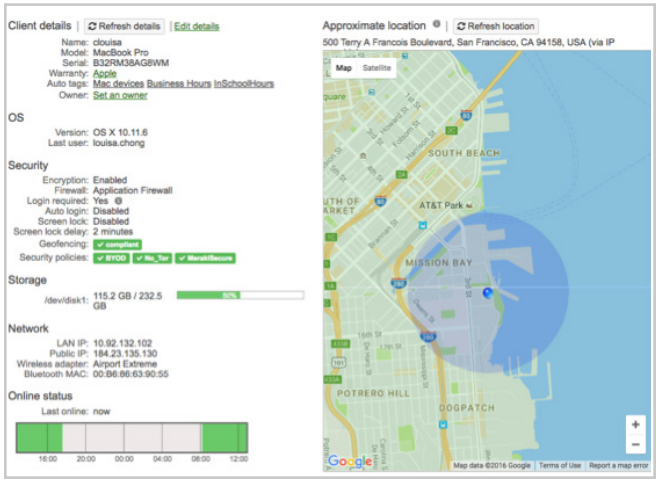
Onboarding and enrollment

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

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

With Android Enterprise (Android for Work), personal and work profiles can be created while optionally implementing device ownership for superior device control and visibility. For macOS and Windows devices, administrators can utilize programs like DEP. Alternately, Systems Manager can be deployed over the air or on individual machines via a lightweight installer.

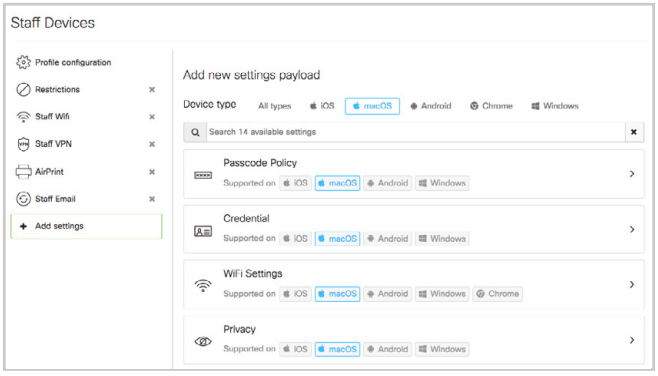
Once enrolled, each device downloads its configuration from the Meraki cloud, applying restrictions plus network and security policies automatically—eliminating manual device provisioning.



Profiles and settings

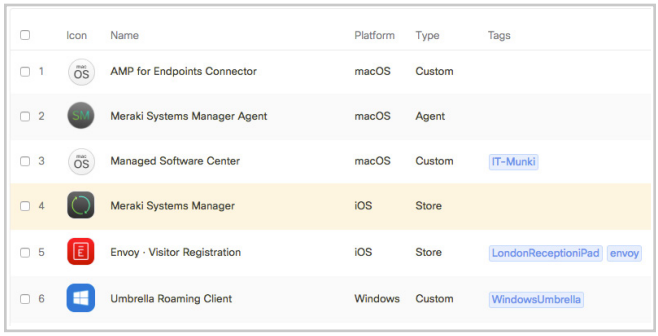
Configuration profiles and settings provide a comprehensive suite for a wide range of device provisioning needs. This can contain everything from device restrictions and permissions to FileVault encryption as well as e-mail, device privacy, Wi-Fi, VPN, wallpaper, notifications, contacts, web clips, managed app settings, education and Apple Classroom, and much more.

Profiles and settings can dynamically and intelligently distribute the required settings to the correct device given time of day, OS type, security compliance, geolocation, and user group 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.



	Icon	Name	Platform	Type	Tags
1		AMP for Endpoints Connector	macOS	Custom	
2		Meraki Systems Manager Agent	macOS	Agent	
3		Managed Software Center	macOS	Custom	IT-Munki
4		Meraki Systems Manager	iOS	Store	
5		Envoy · Visitor Registration	iOS	Store	LondonReceptioniPad envoy
6		Umbrella Roaming Client	Windows	Custom	WindowsUmbrella

Application security is met through a mixture of app blacklists and whitelists, permission management, native containerization through Android Enterprise, and a comprehensive implementation of managed open-in (iOS). Systems Manager enables IT administrators to solve complex requirements with managed app settings, software encryption, separation, and permissions. Mobile application and software deployments are simplified to a few clicks.

Administration and management

Systems Manager is designed to keep managed devices up-to-date with the latest user demands and organization requirements while lowering the IT burden, enabling policies and changes to be deployed 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. Apps, network, and specific security settings can be automatically delivered to each device and user.

Deploy apps

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

Deploy software

Systems Manager installs software on any number of PCs and Macs. Administrators can upload to the cloud or locally host MSI or EXE ffiles (PCs) or PKG files (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. Systems Manager also supports Mac apps through the Apple App Store.

Email configuration

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

Enforce restrictions

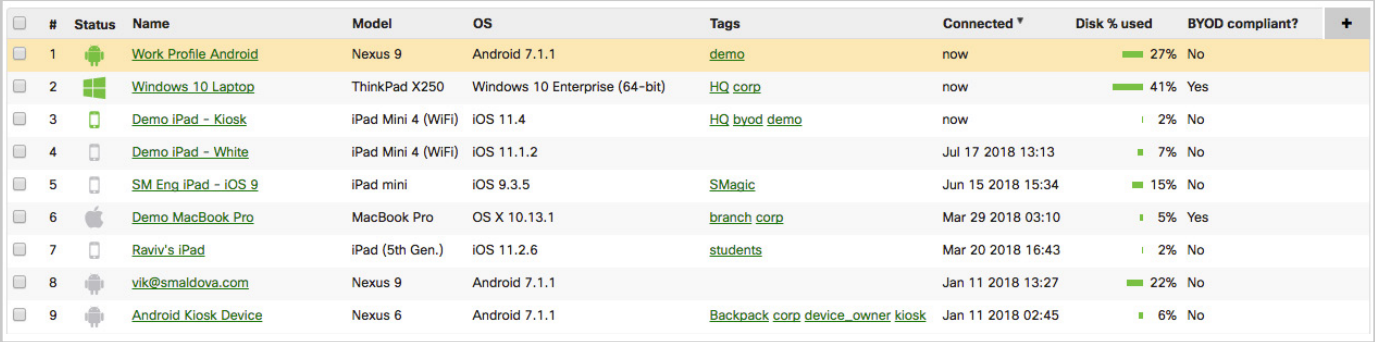
Restrictions allow organizations to control how devices are used. FaceTime, the App Store, and control gaming and media content consumption can be disabled by content rating. Restrict access to iCloud services to disallow backup of sensitive information to Apple's infrastructure. Applications and application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

Security compliance

Systems Manager helps organizations protect mobile devices and data with customizable security policies. Fine-grained policies can be deployed 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. A passcode can be required on devices before pushing exchange settings, while limiting jailbroken devices to the guest network or revoking 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 Systems Manager, 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.



#	Status	Name	Model	OS	Tags	Connected	Disk % used	BYOD compliant?
1		Work Profile Android	Nexus 9	Android 7.1.1	demo	now	27%	No
2		Windows 10 Laptop	ThinkPad X250	Windows 10 Enterprise (64-bit)	HQ corp	now	41%	Yes
3		Demo iPad - Kiosk	iPad Mini 4 (WiFi)	iOS 11.4	HQ byod demo	now	2%	No
4		Demo iPad - White	iPad Mini 4 (WiFi)	iOS 11.1.2		Jul 17 2018 13:13	7%	No
5		SM Eng iPad - iOS 9	iPad mini	iOS 9.3.5	SMagic	Jun 15 2018 15:34	15%	No
6		Demo MacBook Pro	MacBook Pro	OS X 10.13.1	branch corp	Mar 29 2018 03:10	5%	Yes
7		Raviv's iPad	iPad (5th Gen.)	iOS 11.2.6	students	Mar 20 2018 16:43	2%	No
8		vik@smaldova.com	Nexus 9	Android 7.1.1		Jan 11 2018 13:27	22%	No
9		Android Kiosk Device	Nexus 6	Android 7.1.1	Backpack corp device_owner kiosk	Jan 11 2018 02:45	6%	No

Visibility, diagnostics, and control

Systems Manager monitors devices as soon as they enroll. Policies apply to devices anywhere in the world, even if they lose internet connectivity. Live diagnostics tools help with troubleshooting and daily administration tasks. By using Systems Manager, visibility of devices, users, software, and applications on the network provide end-to-end security and management right from the dashboard.

Asset management

Systems Manager gathers available information from the device's GPS, Wi-Fi connection, and IP address to provide a device's physical location down to street-level accuracy. It also provides built-in software inventory management, simplifying even in multiplatform environments. Systems Manager easily identifies devices running outdated software and will track down compliance or licensing issues or uninstall unauthorized software right from the dashboard. Hardware inventories can be managed using Systems Manager's built-in catalog of machines by CPU, system model, or operating system build. Systems Manager also tracks wireless adapter details, including make, mode, and driver version, helping isolate connectivity issues.

Live troubleshooting and diagnostics

Systems Manager provides a suite of real-time diagnostic tools. IT administrators can initiate remote desktop, take a screenshot, see the current process list, and remotely reboot or shut down devices. For remote desktop access, Systems Manager automatically configures a VNC server and establishes a secure end-to-end tunnel. Daily IT support requests are easily managed, like remotely clearing the passcode, locking a device, or erasing data. Device statistics, like battery charge and device memory usage, can be monitored centrally from the dashboard.

Automatic alerts

Systems Manager enables IT administrators to configure fine-grained alert policies to send email notifications to monitor devices, software, compliance, and connectivity. Notifications can be alerted when unauthorized software is installed on a managed device, when specific devices (like critical servers) go offline, and when the Systems Manager agent or profile is removed from a managed device.

Privacy settings

When applicable, administrators can 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, command line requests, software inventory, reading device profiles, installing applications, and the ability to wipe devices.

Cellular data management

Systems Manager allows administrators to set limits for cellular data usage across all managed mobile devices. Multiple policies can be created for different plan thresholds and attached to apps and settings in order to restrict access if a device goes over a plan's limit. Administrators can track data usage over time as well as on demand while receiving e-mail alerts and taking action dynamically, given data limit violations. Additionally, per-app data usage rules can be set on iOS devices to customize which managed apps can use roaming and cellular data.

Multi - OS management

Android enterprise 7.0+
including phones, tablets, and more

Chrome OS (G Suite for enterprise)

iOS 10+
including Apple iPad, iPhone

macOS 10.10+
including Macbook, iMac, Mac mini, Mac Pro, and more

tvOS 10+

Windows 10 (build 1703+)
including Surface, tablets, desktops, laptops, and more

Windows server 2016+

SM specifications

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 Wi-Fi, 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 time-out, 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)
- 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)

SM specifications

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 auto-fill 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 Wi-Fi 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 Wi-Fi security–single click EAP-TLS deployment (Android, iOS, Mac, & Windows)
- Sentry VPN security–auto provision mobile client VPN (Android, iOS, Mac)
- Sentry Wi-Fi settings–auto configure WLAN settings (Android, iOS, Mac, and Windows)
- Sentry VPN settings–auto configure VPN settings (Android, iOS, Mac, and Windows)

SM specifications

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
- Multiuser 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 Wi-Fi 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 email 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 automatic updates
- Enable kiosk mode
- Wi-Fi 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)