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 access can change automatically from policy information such as time of day, geolocation, security posture, and current user.

As Cisco's EMM solution, Systems Manager supports a variety of platforms allowing for the diverse ecosystem often found in today's mobile and cloud 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 estates.

MOBILE DEVICE MANAGEMENT (MDM)

Total device management for mobile and desktop

- Provision settings and restrictions
- Inventory management and device tracking
- Remote wipe; full device and enterprise only
- Remote viewing and troubleshooting
- Native remote desktop support

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 Open-in
- Managed-app configuration
- Volume app purchasing

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 files distriubtion, replacement, and deletion
- Conditional access to files including copy/paste and e-mail attachments

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)–files, apps, settings & certs
- Limited access roles for granular administrive access to Dashboard
- Automated network policy management on Cisco networks
- Active Directory/LDAP integration