cisco Meraki

Systems Manager

Plattformübergreifendes Enterprise-Mobility-Management

Überblick

Meraki Systems Manager ermöglicht Cloud-basiertes, kabelloses und zentralisiertes Enterprise-Mobility-Management (EMM). Verwalten Sie sämtliche Endgeräte in Ihrem Unternehmen über ein einziges, leistungsstarkes, webbasiertes Dashboard.

Die verwalteten Geräte stellen eine sichere Verbindung zur Meraki Cloud her, welche die Geräteverfolgung, die Software-, App- und Inhaltsbereitstellung, die Durchsetzung von Sicherheitsrichtlinien, das Identitätsmanagement und die Integration in das Cisco Netzwerk erlauben. Endnutzer-Berechtigungen können gemäß Richtlinieninformationen wie der Tageszeit, den Standortinformationen, dem Sicherheitsstatus und der Benutzergruppe automatisch und dynamisch geändert werden.

Systems Manager unterstützt als EMM-Lösung von Cisco verschiedene Plattformen, um den vielfältigen Ecosystemen in unserer zunehmend auf Mobilgeräte ausgerichteten Welt Rechnung zu tragen. Damit ist Systems Manager ideal positioniert, um die Herausforderungen von Sicherheitsteams in regulierten Branchen zu bewältigen, Kursleitern digitale Schulungsräume bereitzustellen und IT-Teams, die verteilte Standorte verwalten müssen, zu entlasten. Die Meraki Lösung ist so für sämtliche der aktuellen und künftigen Anforderungen an ein Mobility-Management gewappnet.

MOBILE DEVICE MANAGEMENT (MDM)

Umfassendes Gerätemanagement für Mobilgeräte und Desktops

- Bereitstellung von Einstellungen und Beschränkungen
- Bestandsmanagement und Geräteverfolgung
- Vollständige und selektive Zurücksetzung von Geräten
- Remote-Überwachung und Fehlerbehebung
- Native Remote-Desktop-Unterstützung
- Android, Chrome, iOS, Mac OS, Windows und Windows Phone

MOBILE APPLICATION MANAGEMENT (MAM)

Benutzerfreundlichstes Software-Management der Branche

- Bereitstellung intern entwickelter und öffentlich verfügbarer Apps
- Enterprise App Store und Cloud-Hosting
- Native App-Containerisierung mit Android for Work und verwalteter „Open-in“ Funktion in iOS
- Konfiguration verwalteter Apps
- Volumenlizenzen für Apps

MOBILE CONTENT MANAGEMENT (MCM)

Kontrolle und Bereitstellung von Inhalten und Dateifreigabe

- Bereitstellung von Inhalten über die proprietäre Dateifreigabe- und Backpack-Funktion
- Ermöglichung von gemeinsamer Nutzung von Mobilgeräten
- EFSS-Dropbox-Integration (Enterprise File Sync and Sharing)
- Zugriffsrichtlinien für das Verteilen, Ersetzen und Löschen von Dateien
- Kontrollierter Zugriff auf Dateien, einschließlich Kopieren/Einfügen und E-Mail-Anlagen

MOBILE IDENTITY (MI)

Einfache und umfassende Richtlinienverwaltung

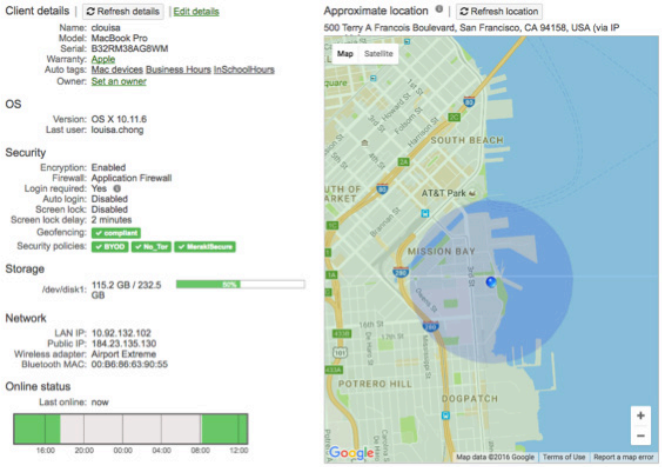
- Zugriffskontrolle nach Betriebssystemtyp, Einhaltung von Sicherheitsrichtlinien, Tageszeit, Standortinformationen und Benutzergruppen
- Identitätszugriffsmanagement (IAM), einschließlich Dateien, Apps, Einstellungen und Zertifizierungen
- Rollen mit begrenztem Zugriff für genau bestimmten Administratorzugriff auf das Dashboard
- Automatisierte Netzwerkrichtlinienverwaltung in Cisco Netzwerken
- Integration von Active Directory, LDAP und OAuth

Cloud-Architektur und Skalierbarkeit

Die Meraki Cloud-Architektur bietet ein hochgradig flexibles System für das Mobility-Management. Ganz gleich, ob eine Organisation mit einem Gerät oder hunderttausend Geräten beginnt – es werden genau dieselben Komponenten benötigt, und die Bereitstellung ist unkompliziert. Die leistungsstarke und skalierbare Lösung kann schnell und einfach eingeführt werden und ist zukunftssicher.

Das Mobility-Management ist eine symbiotische Partnerschaft zwischen dem Gerätehersteller (z.B. Apple, Google oder Microsoft) und dem EMM-Anbieter. Dank unserer Cloud-Infrastruktur und unserem flexiblen Entwicklungsmodell sind wir bei Meraki in der Lage, regelmäßig neue Funktionen und entsprechenden Support anzubieten – ganz ohne Patches oder Softwareinstallationen.

Mit Systems Manager bietet Meraki die branchenweit einzige End-to-End-Lösung, in der das EMM mit Netzwerkkomponenten wie WLAN, WAN und LAN vereint wird. Dies wird durch die native Netzwerkintegration und ein zentrales Management-Dashboard erzielt. Sie erhalten umfassende Transparenz und Kontrolle über das gesamte Netzwerk. Zudem können Sicherheitsfunktionen, die häufig sehr komplex sind, bereits mit einigen wenigen Klicks aktiviert werden. Aufgrund der intuitiven Bedienung können IT-Teams das Meraki-Dashboard in Minutenschnelle konfigurieren und bereitstellen. Spezielle Schulungen oder spezialisierte Mitarbeiter werden nicht benötigt.



Onboarding und Anmeldung

Systems Manager hat einen flexiblen Onboarding-Prozess mit einigen ausgewählten Anmeldungsoptionen. Diese Optionen können je nach Gerätetyp und der Art des Onboarding-Prozesses variieren. Endnutzer-eigene Geräte (Bring Your Own Device, BYOD) können ganz einfach gemeinsam mit unternehmenseigenen Geräten, welche zumeist strengeren Anforderungen unterliegen, verwaltet werden.

Die Anmeldung der Geräte erfolgt nahtlos dank der Integration in Plattformen wie das Programm zur Geräteregistrierung (DEP) von Apple, Systems Manager Sentry, einem webbasierten Self-Service-Portal direkt auf dem mobilen Gerät, oder über die Installation einer App aus einem App Store. Überwachen Sie iOS-Geräte drahtlos mit DEP oder nutzen Sie vorhandene Apple Configurator-Bereitstellungen.

Bei Android for Work können Sie private Profile und Arbeitsprofile erstellen und optional die Geräteinhaberschaft zuweisen. Für macOS- oder Windows-Geräte können Sie Programme wie DEP und den Arbeitsplatzzugriff verwenden. Alternativ kann Systems Manager drahtlos bereitgestellt oder auf einzelnen Geräten über ein kompaktes Installationsprogramm eingesetzt werden.

Nach der Anmeldung lädt jedes Gerät seine Konfigurationsdaten aus der Meraki Cloud herunter, anhand derer die Gerätebeschränkungen und Netzwerk-/Sicherheitsrichtlinien automatisch angewendet werden. Für die Bereitstellung sind somit keinerlei manuelle Schritte notwendig.

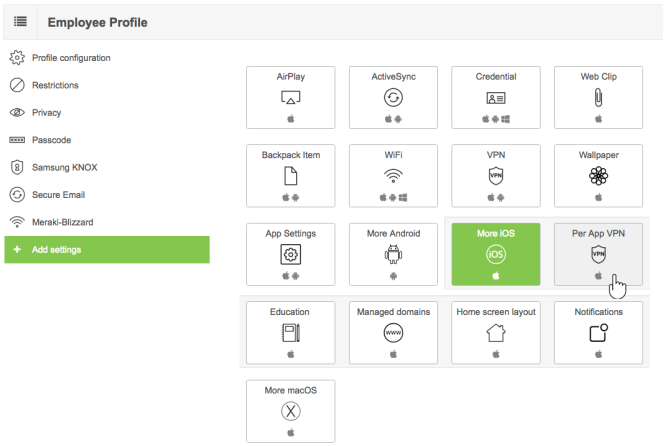
Cisco Systems, Inc. | 10 Finsbury Square, London EC2A 1AF, Großbritannien | +44 (0)20 7871 2776 | sales@meraki.com

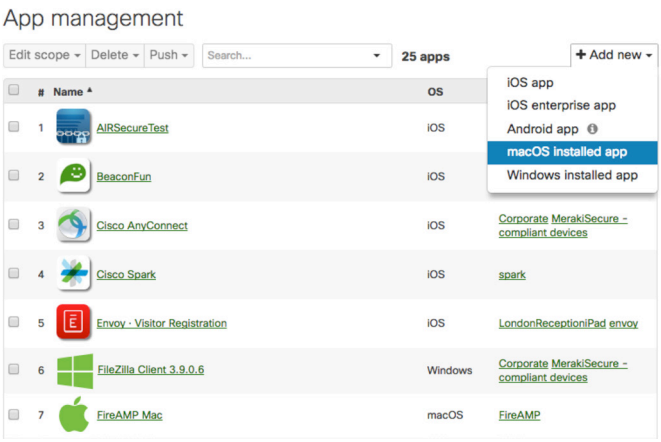
Profile und Einstellungen

Profile und Einstellungen stellen ein umfassendes Portfolio für die zahlreichen Anforderungen der Gerätbereitstellung zur Verfügung. Dazu gehören etwa Gerätebeschränkungen und -berechtigungen, FileVault-Verschlüsselungen, Einstellungen für E-Mails, Datenschutz auf Geräten, WiFi, VPN, Hintergrundbilder, Benachrichtigungen, Kontakte, Web Clips, verwaltete Apps, Schulungen oder Apple Classroom – und noch viel mehr.

Werden die Profile und Einstellungen mit der mobilen Identität verknüpft, können die erforderlichen Einstellungen dynamisch und intelligent für die richtigen Geräte festgelegt werden, entsprechend den Anforderungen von Tageszeit, Betriebssystemtyp, Einhaltung von Sicherheitsrichtlinien, Standortinformationen und Benutzergruppen.

Meraki ist damit als Lösung optimal für auch komplexeste Mobility-Anforderungen geeignet und bietet dabei als benutzerfreundlichstes Managementsystem eine intuitive und angenehme Umgebung für Administratoren und Endbenutzer.





Apps, Software und Containerisierung

Zu einem umfassenden Anwendungsmanagement gehören Kontrolle, Verteilung und Transparenz – nicht nur für Anwendungen, sondern auch für App-Lizenzen, den Softwarebestand und die Containerisierung. Systems Manager installiert öffentlich verfügbare Anwendungen durch die Integration in den Apple App Store und den Google Play Store.

Private Anwendungen werden ebenfalls nahtlos über Cloud-Hosting oder lokal über Anwendungen und Installationsprogramme für die Bereitstellung von Unternehmensanwendungen und Software verwaltet.

Systems Manager wird auch modernsten Anforderungen an Anwendungssicherheit durch eine Kombination aus Blacklists und Whitelists für Apps, Berechtigungsmanagement und -beschränkungen sowie native Containerisierung von Android for Work (Android) und eine umfassende Implementierung von Managed Open-in (iOS) gerecht.

Die mobile Identität kann auch in das Software-Management integriert werden, um die Erstellung granularer Richtlinien und die Automatisierung für alle Anwendungsanforderungen zu ermöglichen.

Komplexe Anforderungen können mithilfe von Einstellungen für verwaltete Apps, Software-Verschlüsselung, Trennung und Berechtigungen erfüllt werden. Die Bereitstellung mobiler Anwendungen und Software ist dadurch mit wenigen Klicks möglich.

Cisco Systems, Inc. | 10 Finsbury Square, London EC2A 1AF, Großbritannien | +44 (0)20 7871 2776 | sales@meraki.com

Schnelle Bereitstellung und Skalierung

Mit der Meraki Cloud-Management-Plattform können in kürzester Zeit groß angelegte Bereitstellungen von Mobilgeräten durchgeführt werden. Dies wird unter Anderem auch durch die Zuverlässigkeit und Flexibilität der Cisco Meraki Cloud und die vollständige Unterstützung verschiedener Anmeldungsmethoden ermöglicht. Geräte können sowohl automatisch und ohne Administratoreingriff angemeldet und integriert werden, als auch manuell, um ein flexibleres Vorgehen in bestimmten Anwendungsfällen zu ermöglichen. Die Anmeldung erfolgt über Profile und/oder kompakte Installationsprogramme (Agents).

Automatisierte Anmeldungsmethoden

iOS- und Mac OS-Geräte können sofort über das Device Enrollment Program von Apple in Systems Manager angemeldet werden. Dadurch wird eine nahtlose Bereitstellung von Apple-Geräten ermöglicht, ohne dass Administratoren diese physisch einrichten müssen.

Windows-Geräte können über die Funktion „Arbeitszugriff“ drahtlos angemeldet werden. Bereitstellungen mit dem kompakten Installationsprogramm können dynamisch über ein Active Directory-Gruppenrichtlinienobjekt für alle Geräte in einer Windows-Domäne erfolgen.

Mit Android for Work kompatible Geräte können automatisch angemeldet werden, indem ein Unternehmenskonto in einer Unternehmensdomäne hinzugefügt wird, die von Google verwaltet wird und mit dem Systems Manager-Netzwerk verknüpft ist.

Anmeldung mit Systems Manager Sentry

Mit der Sentry-Anmeldung ist ebenfalls die Bereitstellung ohne Administratoreingriff möglich. Nicht verwaltete Geräte ohne Systems Manager, die auf das Netzwerk zugreifen möchten, werden zuerst auf eine Splash-Seite weitergeleitet, um Systems Manager zu installieren. Erst nach der Anmeldung können Geräte Zugriff auf das Netzwerk und die Unternehmensressourcen erhalten.

Manuelle Anmeldung

Systems Manager bietet für alle Bereitstellungsmodelle ein webbasiertes Self-Service-Anmeldungsportal direkt auf dem Mobilgerät oder über eine App, die aus einem App Store heruntergeladen werden kann. Systems Manager kann auch in Apple Configurator integriert werden, stellt QR-Codes zur Anmeldung bereit und unterstützt die Verteilung der Anmeldungs-URLs per E-Mail und SMS.

Administration und Management

Mit Systems Manager können Sie sicherstellen, dass alle verwalteten Geräte die aktuellen Benutzer- und Unternehmensanforderungen erfüllen. Und das bei geringerer Belastung für Ihre IT-Teams, denn Richtlinien und Änderungen können jetzt einfach aus der Cloud auf Tausende Geräte gleichzeitig verteilt werden.

Automatisierte Gerätebereitstellung

Geräte werden auf Basis von Benutzergruppen, Betriebssystemtypen, Einhaltung von Sicherheitsrichtlinien, Tageszeit und Standortinformationen bereitgestellt. Sie können alle Apps sowie die entsprechenden Netzwerk- und Sicherheitseinstellungen automatisch an jedes Gerät und jeden Benutzer verteilen.

E-Mail-Konfiguration

Diese Einstellung ermöglicht die Bereitstellung von E-Mail-Konten und -Einstellungen (einschließlich Verschlüsselung, dem gespeicherten E-Mail-Verlauf und Zugriffsberechtigungen) auf angemeldeten Apple iOS- und Android-Geräten.

Software bereitstellen

Systems Manager installiert Software auf einer beliebigen Anzahl von PCs und Macs. Laden Sie MSI- oder EXE-Dateien für PCs oder DMG-Dateien für Macs in die Cloud hoch, oder hosten Sie sie lokal, wählen Sie die Computer aus, und überlassen Sie den Rest der Meraki Cloud. Auf Geräten, die zu diesem Zeitpunkt nicht mit dem Netzwerk verbunden sind, wird die Software installiert, sobald sie das nächste Mal online gehen.

Apps bereitstellen

Bei iOS-Geräten ist Systems Manager mit dem Apple App Store und dem Apple Volume Purchase Program integriert, bei Android-Geräten mit Google Play und dem Amazon App Store. Ebenfalls unterstützt werden Unternehmensanwendungen – sowohl für iOS- als auch für Android-Geräte. Mit Systems Manager können Sie Anwendungen für zehn oder für tausende Benutzer und auf beliebig vielen Geräten bereitstellen.

Cisco Systems, Inc. | 10 Finsbury Square, London EC2A 1AF, Großbritannien | +44 (0)20 7871 2776 | sales@meraki.com

Implementieren von Einschränkungen

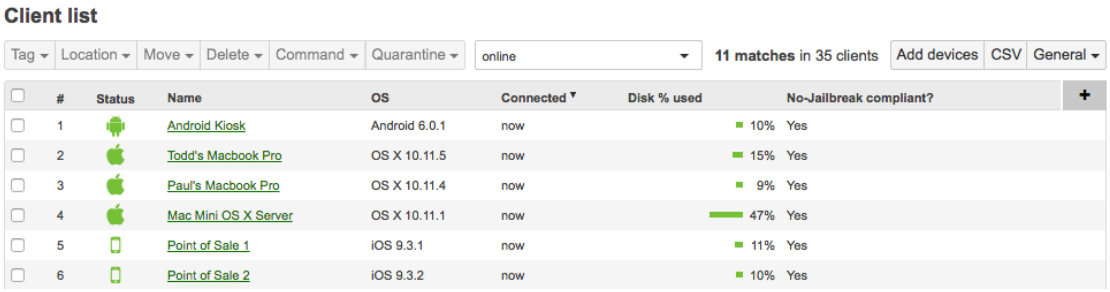
Mithilfe von Einschränkungen können Organisationen festlegen, wie Geräte verwendet werden sollen. So können etwa FaceTime oder der App Store deaktiviert oder anhand von Inhaltskategorien die Nutzung von Spielen und Medieninhalten eingestellt werden. Durch Sperren des Zugriffs auf iCloud-Dienste kann zudem verhindert werden, dass Sicherungskopien von vertraulichen Daten in der Infrastruktur von Apple gespeichert werden. Zudem kann das Speichern von Anwendungen und Anwendungsberechtigungen verhindert werden.

Sicherheit und Compliance

In Systems Manager können Organisationen Mobilgeräte und Daten mithilfe von anpassbaren Sicherheitsrichtlinien schützen. Legen Sie präzise Richtlinien fest, um zu überprüfen, ob Geräte verschlüsselt, gesperrt oder per Jailbreak entsperrt wurden und ob die aktuellste Betriebssystemversion ausgeführt wird, bevor Sie Geräteeinstellungen, Apps und Inhalte dynamisch zuweisen. So schützen Sie Ressourcen und Daten. Ebenfalls möglich: Die Einrichtung einer Passcode-Abfrage als Bedingung für die Übertragung von Exchange-Einstellungen, die Beschränkung des Zugriffs per Jailbreak entsperrter Geräte auf das Gastnetzwerk oder die Aufhebung von Berechtigungen von Geräten, die Sicherheitsrichtlinien verletzen.

Vollständige und selektive Zurücksetzung von Geräten

Diese Funktion von Systems Manager hilft zu verhindern, dass Unternehmensdaten in die falschen Hände gelangen. Die selektive Zurücksetzung durch Systems Manager entfernt alle mittels EMM auf das Gerät übertragenen Konfigurationsprofile und Apps, lässt das Gerät aber zu Nachverfolgungszwecken weiter angemeldet. Bei der vollständigen Zurücksetzung oder dem Zurücksetzen auf die Werkseinstellungen wird alles, einschließlich des Managementprofils, entfernt, um alle Daten vollständig zu löschen und das Gerät aus Systems Manager zu entfernen.



Transparenz, Diagnose und Kontrolle

Bei jedem verwalteten Gerät, das angemeldet wird, beginnt Systems Manager umgehend mit der Überwachung der gemanagten Services und stellt gleichzeitig sicher, dass alle Richtlinien jederzeit und standortunabhängig angewendet werden – auch dann, wenn die Internetverbindung des Geräts unterbrochen wird. Dank Live-Diagnosetools gehen zudem die Behebung von Problemen sowie alltägliche Administrationsaufgaben leichter von der Hand. Systems Manager vereint alles in einem zentralen Dashboard: einen transparenten Überblick über alle Geräte, Benutzer, Software und Anwendungen in Ihrem Netzwerk, End-to-End-Sicherheit und umfassendes Management.

Ressourcenmanagement

Systems Manager ermittelt anhand der GPS-Daten, Wi-Fi-Verbindung und IP-Adresse den straßenabschnittsgenauen Standort eines Geräts. Bei Geräten und Benutzern mit sensiblen Daten kann die Standortweitergabe in den Datenschutzeinstellungen deaktiviert werden.

Systems Manager bietet integrierte Funktionen zur Verwaltung des Softwarebestands, die das Software-Lizenzmanagement erheblich vereinfachen – auch in Multiplattform-Umgebungen. Sie können eine Liste mit allen Softwareprodukten und Apps anzeigen lassen, die auf den verwalteten Mobilgeräten installiert sind. Alternativ dazu können Sie den Namen einer bestimmten Software oder App in eine Google-ähnliche Suchleiste eingeben

Cisco Systems, Inc. | 10 Finsbury Square, London EC2A 1AF, Großbritannien | +44 (0)20 7871 2776 | sales@meraki.com

und so in einer umfassenden Liste aller installierten Software und Apps nach dem gewünschten Eintrag suchen. Außerdem können Sie Geräte mit veralteter Software erkennen, Compliance- oder Lizenzierungsproblemen auf den Grund gehen und direkt über das Dashboard unzulässige Software deinstallieren.

Organisieren Sie den Hardwarebestand mithilfe der integrierten Gerätekatalogisierung von Systems Manager nach CPU-Typ oder -Leistung, Systemmodell oder Betriebssystemversion. Systems Manager erfasst zudem die Details des Funkadapters wie z.B. Hersteller, Modell und Treiberversion, und unterstützt Sie dadurch bei der Behebung von Verbindungsproblemen.

Live-Fehlerbehebung und -Diagnose

Systems Manager bietet zahlreiche Tools für die Echtzeit-Diagnose, mit deren Hilfe Sie Remote-Desktop-Sitzungen durchführen, Screenshots erstellen, die aktuelle Prozessliste anzeigen und die verschiedenen Mac- und PC-Systeme per Fernzugriff neu starten oder herunterfahren können. Für den Remote-Desktop-Zugriff konfiguriert Systems Manager automatisch einen VNC-Server und richtet einen sicheren End-to-End-Tunnel zurück zum Dashboard ein. Selbst in komplexen Netzwerkumgebungen mit zahlreichen Firewalls oder NAT-Gateways ist mit diesen Tools eine vollständige Systemverwaltung mittels Remote-Zugriff möglich.

Vom Löschen des Passcodes über das Sperren eines Geräts bis hin zum Löschen von Daten auf einem kompromittierten Gerät – alle alltäglichen Bedienungsroutinen für iOS- und Android-Geräte lassen sich per Remote-Zugriff durchführen. Darüber hinaus können auch Geräte-Statistiken wie der Akkuladestand oder die interne Speichernutzung zentral über das Dashboard eingesehen werden.

E-Mail-Warnmeldungen

Konfigurieren Sie präzise Warnrichtlinien, um E-Mail-Benachrichtigungen für die Überwachung von Geräten, Software und Netzwerkverbindungen zu senden. Lassen Sie sich benachrichtigen, wenn nicht autorisierte Software auf einem verwalteten Gerät installiert wurde, wenn bestimmte Geräte (z.B. kritische Server) offline gehen oder wenn der Systems Manager-Agent oder das Systems Manager-Profil von einem verwalteten Gerät entfernt wird.

Datenschutzeinstellungen

Sie können gegebenenfalls die Privatsphäre der Benutzer schützen, indem Sie den Zugriff auf den Gerätestandort und die BSSID-Verfolgung begrenzen. Mithilfe von Zugriffsrechten können Administrationsfunktionen für verwaltete Geräte beschränkt werden. Dazu gehören die Deaktivierung der Remote-Desktop-Unterstützung, des Software-Bestands, das Abrufen des Geräteprofils, das Installieren von Anwendungen und die Remote-Zurücksetzung von Geräten.

Mobilfunk-Datenmanagement

Legen Sie Grenzwerte für die Mobilfunkdatennutzung für alle verwalteten Geräte fest. Sie können mehrere Richtlinien für verschiedene Grenzwerte festlegen und Richtlinien für Anwendungen und Einstellungen zuweisen, um den Zugriff, die Datennutzung und die Funktionen einzuschränken, falls ein Gerät die Grenzwerte eines Tarifs überschreitet. Verfolgen Sie die Datennutzung im Zeitverlauf oder rufen Sie sie nach Bedarf ab. Sie können zudem E-Mail-Warnungen bei Überschreitungen der Datengrenzwerte erhalten und dann dynamisch Maßnahmen ergreifen.

Netzwerkintegration – Systems Manager Sentry

Systems Manager ist auf dem EMM-Markt einzigartig, da er Teil eines umfassenden und integrierten IT-Portfolios ist, zu dem Wireless-, Switching- und Sicherheitslösungen, Überwachungskameras und Telefone zählen, und welches vollständig über eine zentrale Oberfläche verwaltet wird.

Als Teil der End-to-End-IT-Lösung von Cisco Meraki bietet Systems Manager die Transparenz und die Funktionen, die in eigenständigen EMM-Produkten nicht verfügbar sind. Dadurch kann sich ein IT-Team auf die Mission der Organisation konzentrieren und muss weniger Zeit mit Integrationen oder komplexen Konfigurationen verbringen. Systems Manager Sentry kann IT-Aufgaben wie das Geräte-Onboarding, die Zuordnung von Einstellungen, das Anwendungsmanagement und den Netzwerkzugriff vereinfachen, automatisieren und dynamisch aktualisieren, indem die mobile Identität und der Gerätezustand laufend überwacht und Richtlinien dynamisch daran angepasst werden.

Sicherheitsbedrohungen entwickeln sich ständig weiter, daher ist die Bereitstellung einer geschützten Infrastruktur für sichere Verbindungen für eine Organisation von allergrößter Bedeutung. In einer Meraki-Netzwerkinfrastruktur bietet Systems Manager kontextsensitive Sicherheit und Netzwerkverbindungen. Im Folgenden finden Sie eine Liste der Funktionen des Systems Manager Sentry Programmpakets.

Sentry-Anmeldung

Durch die Integration in Meraki Access-Points (MR-Serie) können Netzwerkadministratoren den Netzwerkzugriff auf Geräte beschränken, die mit Systems Manager verwaltet werden. Die Sentry-Anmeldung ermöglicht zudem die Bereitstellung ohne Administratoreingriff über ein Self-Service-Portal für Benutzer. Nicht verwaltete Geräte ohne Systems Manager, die auf das Netzwerk zugreifen möchten, werden auf eine Splash-Site weitergeleitet, um Systems Manager zu installieren. Erst nach der Anmeldung können Geräte Zugriff auf das Netzwerk und die Unternehmensressourcen erhalten.

Sentry-Richtlinien

Meraki-Netzwerkeinstellungen wie Firewall-Regeln, Traffic-Shaping-Richtlinien und Content-Filterung können gemäß den Informationen zur mobilen Identität von Systems Manager dynamisch geändert werden. Der Netzwerkzugriff wird mithilfe von granularen Richtlinien zum Betriebssystemtyp, Zeitplan, Sicherheitsstatus und aktuellen Benutzer kontrolliert, aktualisiert und gegebenenfalls aufgehoben.

Sentry-Wi-Fi-Sicherheit

Sie können automatisch EAP-TLS-WLAN-Authentifizierungen mit eindeutigen Zertifikaten bereitstellen, ohne eine Zertifizierungsstelle oder einen RADIUS-Server verwalten zu müssen. Wenn ein Gerät die Sicherheitsrichtlinien nicht einhalten kann, weil der Benutzer beispielsweise die Antivirussoftware deaktiviert oder einen Jailbreak auf dem Gerät durchgeführt hat, kann Systems Manager das Zertifikat von diesem Gerät löschen und das Gerät aus dem Netzwerk entfernen.

Erforderlich: Systems Manager (SM) und Meraki Wireless (MR)

Sentry-VPN-Sicherheit

Sie können VPN automatisch bereitstellen, einschließlich eindeutiger Benutzernamen und Kennwörter. Gleichzeitig haben Sie die Kontrolle über den Zugriff basierend auf der Einhaltung der Sicherheitsrichtlinien, Tageszeit, Benutzergruppe und Standortinformationen.

Erforderlich: Systems Manager (SM) und Meraki Security (MX)

Sentry-WiFi-Einstellungen

Sie können Wi-Fi-Einstellungen automatisch bereitstellen, damit verwaltete Geräte eine Verbindung zu einem Meraki MR-Wireless-Netzwerk herstellen können. Dank der Sentry-WiFi-Einstellungen müssen Administratoren keine manuellen WiFi-Einstellungen und -Konfigurationen oder -Updates vornehmen, wenn ein MR-Netzwerk in derselben Organisation geändert wird.

Sentry-VPN-Einstellungen

Sie können VPN-Einstellungen automatisch bereitstellen, damit verwaltete Geräte eine Verbindung zu einer Meraki MX Security-Appliance herstellen können. Sie müssen keine manuellen VPN-Einstellungen oder -Updates vornehmen, wenn ein MX-Netzwerk in derselben Organisation geändert wird.

Cisco Systems, Inc. | 10 Finsbury Square, London EC2A 1AF, Großbritannien | +44 (0)20 7871 2776 | sales@meraki.com

Management mehrerer Betriebssysteme

Android 4.0 oder höher (Android for Work 5.0 oder höher)
einschließlich Telefonen, Tablets und mehr

Chrome OS (Konto von G Suite oder G Suite for Education)
einschließlich Chromebook, Chromebox und mehr

iOS 5 oder höher (Systems Manager App erfordert iOS 7 oder höher)
einschließlich Apple iPad, iPod touch und iPhone

Mac OS 10.7 oder höher
einschließlich MacBook, iMac, Mac mini, Mac Pro und mehr

Windows 10, 8.1, 8, 7 und Windows Phone

Cisco Systems, Inc. | 10 Finsbury Square, London EC2A 1AF, Großbritannien | +44 (0)20 7871 2776 | sales@meraki.com

Spezifikationen

Unterstützte Plattformen
Android 4 oder höher, einschließlich Telefonen, Tablets und mehr (Android for Work erfordert 5.0 oder höher)
Chrome OS, einschließlich Chromebook und mehr (Konto von G Suite oder G Suite for Education)
iOS 5 oder höher, einschließlich iPad, iPod touch und iPhone (SM App erfordert iOS 7 oder höher.)
Mac OS 10.7 oder höher, einschließlich MacBook, iMac, Mac mini, Mac Pro und mehr
Microsoft Server 2016, 2012 und 2008 R2
Windows 10, 8.1, 8 und 7, einschließlich Surface, Tablets, Desktops, Laptops und mehr
Windows Phone 10 und 8.1, einschließlich Surface, Lumia, HTC, Nokia und mehr

Management
Webbasiertes Management mit dem sicheren browserbasierten Dashboard von Meraki
Zentrale Administration der verwalteten Geräte
Zwei-Faktor-Authentifizierung auf Organisationsebene
Rollenbasierte Administration
Export von Bestandsdaten in CSV-Datei
Fernzugriff über Befehlszeile
Ereignis- und Aktivitätsprotokoll für Administratoren
Automatische Warnungen bezüglich installierter Software, Geofencing und Anmeldung sowie der Erstellung von Sicherheitsberichten
Netzwerkübergreifendes Kopieren von Profilen
Installation verfügbarer Betriebssystemupdates (für iOS und Mac OS ist DEP erforderlich)

Sicherheit
Gerätelokalisierung anhand von Wi-Fi-Verbindung, IP-Adresse und GPS-Daten
Containerisierung, Trennung von verwalteten und nicht verwalteten Daten (über Managed Open-in unter iOS und Android for Work unter Android)
Abmeldungsüberwachung und -benachrichtigung
Antivirus, Antispyware, Firewall, Festplattenverschlüsselung, Passcode und Passwort, Zeitlimit für Bildschirmsperre, Jailbreak- und Root-Erkennung
Sperren des Zugriffs auf iCloud (iOS)
Sperren der Annahme vertrauenswürdiger TLS-Zertifikate seitens der Nutzer (iOS)
Erzwingung von verschlüsselter Sicherung (iOS) und verschlüsselter Speicherung (Android)
Globaler HTTP-Proxy (iOS)
Anwendung von Passcode-Richtlinien und der Richtlinie für die Zurücksetzung von Geräten bei Falscheingabe (Android, iOS, Mac und PC)
Überprüfung der Client-Geräte auf das Vorhandensein von Systems Manager vor der Genehmigung des Netzwerkzugriffs (Android, iOS, Mac und PC)
Simple Certificate Enrollment Protocol (SCEP)
Kundenseitige Zertifikatsignatur zur Zertifikatbereitstellung
Einschränkung der Zugriffsrechte auf Dashboard-Kontrollen (z. B. Bereinigung von BYOD-iOS- und -Mac-Geräten)
Dynamische Profilverwaltung – Einhaltung der Sicherheitsrichtlinien, Geofencing-Management, Zeitplan, Mindestbetriebssystem, Blacklist/Whitelist für Apps und Grenzwerte für die Datennutzung
Modus „Verloren“ (iOS)
Stets verfügbares, On-Demand- und anwendungsbasiertes VPN, AnyConnect VPN

Software- und App-Management
Inventarisierung der installierten Software und Apps
Benutzerdefinierte Bereitstellung von Software und öffentlich verfügbaren Apps aus dem App Store und von Google Play
Integration in den Apple App Store und in das Apple Volume Purchase Program
Integration in den Google Play Store und Android for Work
Hosten von Dateien mit bis zu 3 GB in der Meraki Cloud
Softwareinstallation über MSI- oder EXE-Dateien auf PCs und DMG-Dateien auf Macs
Softwaredeinstallation (Mac und Windows)
Deinstallation von Apps (Android und iOS)
Beschränkung der App-Installation
Beschränkung von Käufen in einer App
Überwachung auf Installation unzulässiger Software und Apps und Ausgabe entsprechender Benachrichtigungen
Installation von Unternehmensanwendungen

Content-Management
Benutzerdefinierte Bereitstellung von Dateien, Dokumenten und Apps (Android und iOS)
Aktualisierung und Bereitstellung der neuesten Dateiversion für Geräte (Android und iOS)
Verwaltung und Verteilung von App-Lizenzen (iOS und Mac OS mit VPP)
Gerätelizenzzuordnung (iOS mit VPP)
Bereitstellung von iBook-Lizenzen
Layout des Hauptbildschirms (nur iPad)

Gerätebeschränkungen
Einschränkung der Kameranutzung (iOS und Android)
FaceTime, Siri, iTunes Store, Multiplayer-Spiele und Apple Music (iOS)
Einschränkung des Medienkonsums (YouTube, anstößige Musik und Podcasts, Filme, Fernsehshows und Apps mit Altersbeschränkung) (iOS)
Erzwingung von verschlüsselter Sicherung (iOS) und verschlüsselter Speicherung (Android)
Anwendung von Passcode-Richtlinien und der Richtlinie für die Zurücksetzung von Geräten bei Falscheingabe (Android, iOS, Mac und PC)
Einzel-App- oder Kioskmodus (Android und iOS)
Autonomer Einzel-App-Modus (iOS)
Automatische Inhaltsfilterung mit Whitelist (iOS)
Einschränkung der Nutzung von AirDrop (iOS)
Einschränkung von Änderungen an der Mobilfunkdatennutzung für Apps (iOS)

Umschalten von Einstellungen für Sprach- und Daten-Roaming (iOS)

Einschränkung der Liste der angezeigten Airplay-Geräte (iOS)

Gerätenamen stets auf dem neuesten Stand (iOS)

Management nicht verwalteter Apps (iOS)

Sperren des Hintergrundbildes und Gerätenamens (iOS)

Verwaltete Domänen, Safari AutoFill-Domänen (iOS)

Benachrichtigungseinstellungen und Verhindern von Änderungen an den Benachrichtigungseinstellungen (iOS)

Einblenden/Ausblenden von Apps (iOS)

Fehlerbehebung und Live-Tools

Sperren, Entsperren und Zurücksetzen von Geräten per Remote-Zugriff (Android, iOS, Mac und Windows)

Neustart und Herunterfahren per Remote-Zugriff (Mac und Windows)

Remote-Desktop und -Screenshot (Mac und Windows)

Zugriff auf Geräteprozessliste (Mac und Windows)

Senden von Sofortbenachrichtigungen an das Gerät (Android, iOS, Mac und Windows)

Überwachung aktiver TCP-Verbindungen, TCP-Statistiken und Routing-Tabellen (Mac und Windows)

Selektive Zurücksetzung (Android, iOS und Mac)

Umschalten von Einstellungen für Sprachdaten, Daten-Roaming und Hotspots (iOS)

Aufrufen des Kiosk- oder Einzel-App-Modus nach Bedarf (Android und iOS)

Starten von AirPlay per Fernzugriff (iOS)

Bereitstellung der Netzwerkkonfiguration

Bereitstellung der Wi-Fi-Einstellungen, einschließlich WPA2-PSK und WPA2-Enterprise (Android, iOS, Mac und Windows)

Bereitstellung der VPN-Konfiguration und Authentifizierungseinstellungen (Android, iOS, Mac und Windows)

Bereitstellung der serverseitigen digitalen Zertifikate (Android, iOS, Mac und Windows)

Überprüfung der Client-Geräte auf das Vorhandensein von Systems Manager vor der Genehmigung des Netzwerkzugriffs (Android, iOS, Mac und Windows)

Bereitstellung von AirPlay-Zielen und -Passwörtern

Cisco ISE MDM-API-Integration

Sentry-Sicherheit

Sentry-Richtlinien – Durchsetzung von Netzwerkrichtlinien auf Basis des Sicherheitsstatus (Android, iOS, Windows und Mac)

Sentry-Anmeldung – integriertes Self-Service-Onboarding (Android, iOS, Mac und Windows)

Sentry-Wi-Fi-Sicherheit – EAP-TLS-Bereitstellung mit nur einem Klick (Android, iOS, Mac und Windows)

Sentry-VPN-Sicherheit – automatische Bereitstellung eines Mobile Client VPN (Android, iOS und Mac)

Sentry-Wi-Fi-Einstellungen – automatische Konfiguration der WLAN-Einstellungen (Android, iOS, Mac und Windows)

Sentry-VPN-Einstellungen – automatische Konfiguration der VPN-Einstellungen (Android, iOS, Mac und Windows)

Geräteanmeldung

App-Anmeldung (iOS und Android)

Automatische Anmeldung über DEP (iOS 7 oder höher und Mac OS 10.10 oder höher)

Anmeldung auf dem Gerät (iOS, Android, Mac und Windows)

Integration in Apple Configurator und Profil-Manager (iOS und Mac)

Anmeldungseinladung per E-Mail oder SMS (iOS, Android, Mac und Windows)

Lokale Bereitstellung eines Installationsprogramms (Mac und Windows)

Integration in Active Directory-Gruppenrichtlinienobjekt (Windows)

In-Quarantäne-Stellen von Geräten bei der Anmeldung (Android, Chrome, iOS, Mac und Windows)

Chrome OS-Gerätemanagement über G Suite und G Suite for Education

Authentifizierung für mehrere Benutzer – dynamische Änderung der Gerätesoftware, Einstellungen und Zugriffsberechtigungen

Überwachung

Reporting zu wichtigen Hardwaredaten und Spezifikationen

Überwachung von Netzwerkzugriff, Anbindung und Signalstärke

Überwachung der Einhaltung von Beschränkungen

Gerätelokalisierung anhand von Wi-Fi-Verbindung, IP-Adresse und GPS-Daten

Überwachung von Akku, Speicher, RAM-/CPU-Nutzung, Ausfällen

Überschreiben der Standortangaben auf Basis der Netzwerk-/IP-Informationen (z. B. wenn GPS nicht verfügbar ist)

Automatische Bereitstellung

Integration von Gruppenrichtlinien in den Cisco Meraki Hardware-Stack

Dynamische Tags auf Basis der mobilen Identität, einschließlich Standortinformationen, Sicherheitsstatus und Zeit

Integration von Active Directory- und LDAP-Gruppen zur automatischen Anwendung von Tags, Eigentümern und Benutzern

Automatische Verteilung und Widerruf von App-Lizenzen mit VPP

E-Mail-Einstellungen

Bereitstellung eines Exchange ActiveSync-E-Mail-Kontos (Android und iOS)

Beschränkung ausgehender E-Mails auf das verwaltete Konto in Mail-App (iOS)

Verwendung von benutzerdefinierten Domänen und Domänenformaten

Durchsetzung der Verwendung von SSL bei der Nutzung von ActiveSync

Aktivierung von S/MIME bei der Nutzung von ActiveSync

Verwaltung der App-Einstellungen für E-Mails in der Gmail App (Android und iOS)

Verwendung der Geräteeigentümer für die automatische Eingabe der E-Mail-Adressen für Benutzer auf einem Gerät