Systems Manager

端點管理

概觀

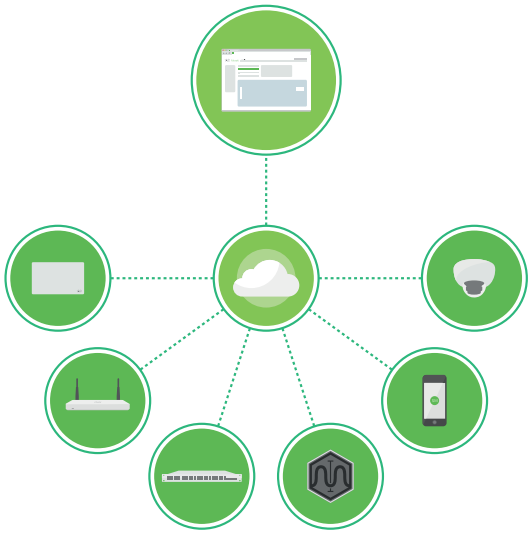
做為 Cisco 的端點管理解決方案，Cisco Meraki™ Systems Manager 可支援各種平台，讓您在現今以行動為主的世界中適應更多樣化的生態系統。Systems Manager 占有舉足輕重的地位，可減緩各行各業安全團隊的擔憂、協助教師設置數位教室，並透過分散式網站減輕企業 IT 團隊的負擔。

Systems Manager 提供集中式、以雲端為基礎的端點管理工具，以及為不斷拓展的組織提供廣泛的擴展能力。透過易於使用的 Web 儀表板，組織可以從任何位置快速管理分散式部署。

Meraki Systems Manager 提供各式各樣的端點管理功能，本文針對佈建、監控和保護終端裝置提供詳細的說明。

原生網路整合

Meraki Systems Manager 整合了多項 Cisco Meraki 網路產品，可讓組織透過單一雲端儀表板整合 IT 系統管理作業。Meraki 儀表板可透過單一介面，協助支援 WAN、LAN、安全性設備、保全攝影機和端點管理等管理作業。儀表板採用直覺的設計本質，IT 專業人員只要幾分鐘的時間即可完成設定和部署，無須專業訓練或專屬員工。



原生網路整合 – Systems Manager Sentry

Meraki Systems Manager 具備原生網路整合，是端點管理市場中與眾不同的解決方案。做為 Cisco Meraki 網路產品組合的一部分，Meraki Systems Manager 已重新設計，能夠與 Cisco Meraki 網路和安全性產品分享智慧功能，這可讓 IT 團隊自動化決策流程，根據指定裝置的狀態自動判斷是否可存取網路和資料，包括已安裝的軟體、安全性設定檔、位置等。

做為 Cisco Meraki 端對端 IT 解決方案的一部分，Systems Manager 提供無法在獨立端點管理產品中取得的可見度和功能。裝置上線、設定指派、應用程式管理和網路存取，這些都是可透過 Systems Manager 進行簡化、自動化和動態更新的一些 IT 責任。

Systems Manager 會持續追蹤行動身分識別和裝置狀態，並視情況動態調整原則。安全性威脅持續演進，因此組織都將部署安全且安心的連線基礎結構視為首要之務。在 Meraki 網路基礎結構上部署 Systems Manager 後，即可支援情境感知的安全性和連線。

Systems Manager Sentry 功能套件是指 Systems Manager 在 Meraki 無線、交換器服務和安全性設備產品組合中所支援的跨產品整合。以下是 Systems Manager Sentry 套件的功能清單。

Sentry 註冊

透過與 Meraki 存取點 (MR 系列) 整合，網路系統管理員能夠僅允許 Systems Manager 管理的裝置存取網路。Sentry 註冊也透過使用者自助式入口網站，為系統管理員提供零觸控部署。在沒有 Systems Manager 的狀態下，會將嘗試加入網路的未受管理裝置傳送到安裝 Systems Manager 的啟動頁面。只有在完成註冊後，裝置才能存取網路和企業資源。

Sentry 原則

您可根據 Systems Manager 的行動身分識別資訊動態變更 Meraki 網路設定，例如防火牆規則、流量整形原則和內容篩選。網路存取會根據 OS 類型和時間排程以及安全性狀態和目前使用者等精細原則，自動進行控制、更新和補救。

Sentry Wi-Fi

系統管理員可自動佈建 Wi-Fi 設定，將代管裝置連接到 Meraki MR 無線網路。EAP-TLS WLAN 驗證可透過唯一的憑證自動進行佈建，無須管理憑證授權單位、RADIUS 伺服器或 PKI。當相同組織的 MR 網路有所變更時，Sentry Wi-Fi 設定可讓系統管理員無須進入手動 Wi-Fi 設定或進行組態更新。

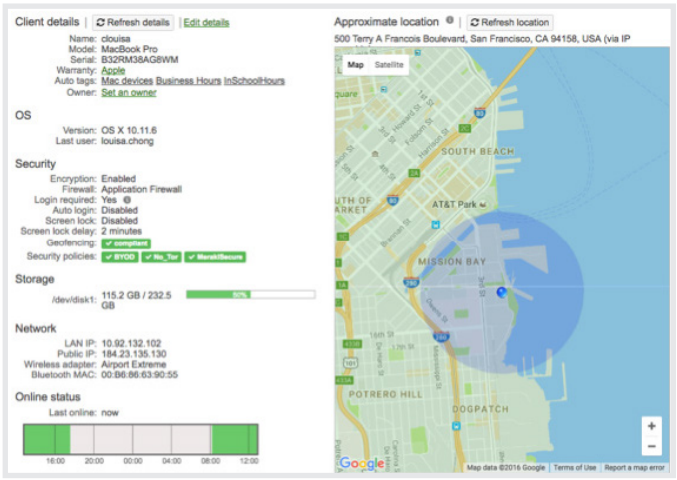
當裝置違反安全性時 (例如使用者停用防毒或讓裝置越獄)，Systems Manager 可自動移除該裝置的憑證，並撤銷裝置對網路的存取權。需要：Systems Manager (SM) 和 Meraki 無線 (MR)

Sentry VPN

系統可自動佈建 VPN 設定，將代管裝置連接到託管用戶端 VPN 的 Meraki MX 安全性設備。MX 端的 VPN 組態變更會自動反映在 Systems Manager 中，無須執行任何手動操作。

系統能根據安全性合規性、時段、使用者群組和地理位置，自動有條件地授予和撤銷用戶端 VPN。需要：Systems Manager (SM) 和 Meraki 安全性 (MX)

Meraki Systems Manager 整合了 Cisco® 安全性和網路產品，包括 Cisco Umbrella™、適用於端點的 Cisco 進階惡意程式碼防護 (AMP) (Cisco Clarity)、Cisco 身分識別服務引擎 (ISE)、Cisco Aironet™ 無線、Cisco AnyConnect® VPN 軟體、Meraki MR 存取點和 Meraki MX 安全性設備。



上線和註冊

Systems Manager 提供彈性靈活的上線程序，以及多種專業註冊選項。這些選項可根據裝置類型和上線方式而有所不同。您可以使用較嚴格的組織自有裝置規定輕鬆管理自攜裝置 (BYOD)。

若要順暢地註冊裝置，可以採用 Apple 裝置註冊計劃 (DEP) 等內建整合平台、Systems Manager Sentry 註冊、直接使用行動裝置上的 Web 自助式入口網站，或是從 App Store 安裝應用程式。透過 DEP 無線監督 iOS 裝置，或整合現有 Apple Configurator 部署。

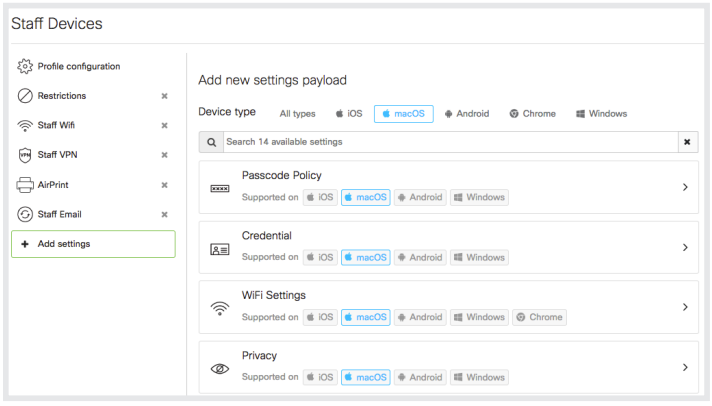
透過 Android Enterprise (Android for Work)，您可建立個人和公司設定檔，同時選擇是否要實作裝置擁有權，以獲得優異的裝置控制和可見度。針對 macOS 和 Windows 裝置，系統管理員可利用 DEP 等計劃。或者，您可透過無線方式或透過輕量型安裝程式在個別機器上部署 Systems Manager。

完成註冊後，每部裝置都會從 Meraki 雲端下載各自的組態，自動套用裝置限制、網路和安全性原則，無須手動佈建裝置。

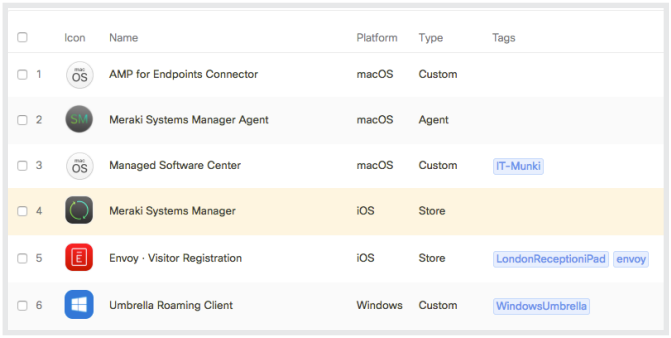
設定檔和設定

組態設定檔和設定可提供適用於各種裝置佈建需求的全方位套件。這包括像是裝置限制和 FileVault 加密權限，以及電子郵件、裝置隱私權、Wi-Fi、VPN、桌布、通知、聯絡人、網頁剪輯、代管應用程式設定、教育和 Apple Classroom 等內容。

設定檔和設定可動態設定，根據指定時段、OS 類型、安全性合規性、地理位置和使用者群組考量事項，將所需的設定智慧發佈到正確的裝置。Meraki 為複雜的行動需求提供解決之道，同時保有領先業界的易用性，旨在為系統管理員和使用者打造愉快體驗。行動佈建變得更簡單了，只要按一下滑鼠或拖曳即可。



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



	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

應用程式、軟體和容器化

完整的應用程式管理不只是針對應用程式，還需要控制、發佈應用程式授權、軟體清查和容器化需求，並深入了解其相關資訊。Systems Manager 透過與 Apple App Store 和 Google Play 商店整合來安裝公開應用程式。私人應用程式也可透過雲端託管或本機託管應用程式，以及企業應用程式安裝程式和軟體部署進行順暢的管理。

結合應用程式黑名單和白名單、權限管理、Android Enterprise 原生容器化，以及全方位實作 Managed Open-In (iOS)，確保符合應用程式安全性。Systems Manager 可讓 IT 系統管理員透過代管應用程式設定、軟體加密、隔離和權限解決複雜的需求。行動應用程式和軟體部署已化繁為簡，只要按幾下滑鼠即可。

系統管理和管理作業

Systems Manager 採用的設計可協助讓代管裝置保持最新狀態，掌握最新的使用者需要和組織需求，同時減輕 IT 負擔。從雲端在數千部裝置之間順暢地部署原則和變更。

自動化裝置佈建

裝置會根據使用者群組、OS 類型、安全性合規性、時段和地理位置進行佈建。應用程式、網路和特定安全性設定可自動傳送到每個裝置和使用者。

電子郵件組態

IT 系統管理員可在已註冊的 Apple iOS 和 Android 裝置上佈建電子郵件帳戶和郵件設定，包括加密、已儲存的郵件歷程記錄持續時間，以及存取權限。

部署軟體

Systems Manager 可將軟體安裝在任何數量的 PC 和 Mac 上。針對 PC 的 MSI 或 EXE 檔案或 Mac 的 PKG，系統管理員可將這些內容上傳到雲端或在本機進行託管、選取機器，然後讓 Meraki 雲端完成其餘的作業。如果裝置無法使用，軟體會加入佇列並在下次處於線上狀態時進行安裝。Systems Manager 也支援 Apple App Store 中的 Mac 應用程式。

部署應用程式

針對 iOS 和 macOS 裝置，Systems Manager 已與 Apple App Store 和 Apple 的大量採購方案整合。Android 裝置可支援 Google Play。此外，iOS 和 Android 皆可支援企業應用程式。Systems Manager 可讓您輕鬆地將應用程式發佈給十個或數千個使用者，或發佈到任何數量的裝置。

強制執行限制

限制可讓組織控制裝置的使用方式。您可透過內容分級，停用 FaceTime、App Store 和控制遊戲與媒體內容使用量。限制對 iCloud 服務的存取，禁止將敏感資訊備份到 Apple 基礎結構。您可選擇禁止應用程式和應用程式權限。

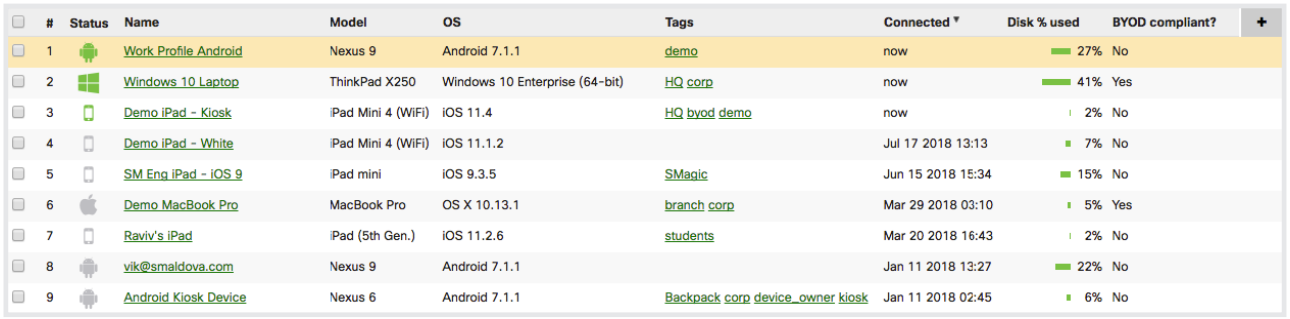
安全性合規性

Systems Manager 可協助組織透過可自訂的安全性原則保護行動裝置和資料。您可部署精細的原則，先檢查裝置是否已加密、鎖定、越獄和執行最新 OS 版本，然後動態指派裝置設定、應用程式和內容，以保護資源和資料。推送 Exchange 設定之前，可以規定要在裝置上輸入密碼，同時將越獄裝置限制在來賓網路，或在裝置違反安全性原則時撤銷權限。

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

完整裝置資料抹除和選擇性資料抹除

Systems Manager 提供的機制可防止企業資料落入錯誤的對象手中。選擇性資料抹除功能可移除之前透過 Systems Manager 推送到裝置的所有組態設定檔和應用程式，同時讓裝置保留註冊狀態以便進行追蹤。完整裝置資料抹除 (也稱為原廠重設) 則會移除包括管理設定檔在內的所有內容，完全清除所有資料並從 Systems Manager 移除裝置。



#	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

可見度、診斷和控制

Systems Manager 會在代管裝置註冊時立即進行監控。原則會套用到世界各地的裝置，即使網際網路連線中斷也不受影響。即時診斷工具可協助您進行疑難排解和每日管理工作。使用 Systems Manager，儀表板可透過對網路上裝置、使用者、軟體和應用程式的可見性直接提供端對端安全性和管理。

資產管理

Systems Manager 可從裝置的 GPS、Wi-Fi 連線和 IP 位址收集可用資訊，提供裝置的實體位置並達到街道等級的準確度。它還提供內建軟體清查管理，即使在多平台環境也能簡化軟體管理作業。Systems Manager 可直接從儀表板輕鬆識別執行過時軟體的裝置、追蹤合規性或授權問題，或解除安裝未經授權的軟體。透過 Systems Manager 內建的機器目錄，可根據 CPU、系統型號或作業系統組建管理硬體清查。Systems Manager 也會追蹤無線配接卡詳細資料，包括製造商、型號和驅動程式版本，協助隔離連線問題。

即時疑難排解和診斷

Systems Manager 提供即時診斷工具套件。IT 系統管理員能初始化遠端桌面、建立螢幕擷取畫面、查看目前的處理清單，以及從遠端將裝置重新開機或關機。針對遠端桌面存取，Systems Manager 會自動設定 VNC 伺服器並建立安全的端對端通道。您可輕鬆管理每日 IT 支援請求，例如從遠端清除密碼、鎖定裝置或清除資料。您可以從儀表板集中監控裝置統計資料，例如電池電量和裝置記憶體使用量。

自動警示

Systems Manager 可讓 IT 系統管理員設定精細的警示原則，傳送電子郵件通知以監控裝置、軟體、合規性和連線。您可以在以下情況收到通知：在代管裝置上安裝未經授權的軟體時、特定裝置 (例如關鍵伺服器) 離線時，以及從代管裝置移除 Systems Manager 代理程式或設定檔時。

隱私權設定

在適當情況下，系統管理員可限制對裝置位置和 BSSID 追蹤的存取權，藉此確保使用者隱私權。存取權可用來限制代管裝置的系統管理功能，包括停用遠端桌面、命令列請求、軟體清查、讀取裝置設定檔、安裝應用程式和抹除裝置資料的功能。

行動數據資料管理

Systems Manager 可讓系統管理員設定所有代管行動裝置上的行動數據使用量上限。可針對不同的方案閾值建立多個原則，並附加到應用程式和設定，以便在裝置超過方案上限的情況下限制存取權。系統管理員可視需要追蹤一段時間的數據使用量，同時收到電子郵件警示並根據指定數據上限的違反情況動態採取行動。此外，可在 iOS 裝置上設定每個應用程式的數據使用量規則，自訂哪些代管應用程式能使用漫遊和行動數據。

多重 OS 管理

Android Enterprise 5.0+
包括手機、平板電腦等

Chrome OS (G Suite for Enterprise)

iOS 9+
包括 Apple iPad、iPhone

macOS 10.7+
包括 Macbook、iMac、Mac mini、Mac Pro 等

tvOS

Windows 10
包括 Surface、平板電腦、桌上型電腦、筆記型電腦等

Windows Server 2016、2012、2008 R2

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

規格

管理
使用 Meraki 以瀏覽器為基礎的安全儀表板透過網路進行管理
代管裝置的集中式系統管理
組織層級雙重要素驗證
以角色為基礎的系統管理
可將清查資料匯出成 CSV
遠端命令列
系統管理事件記錄檔和活動記錄檔
針對已安裝的軟體、地理柵欄、註冊和安全性報告自動傳送警示
在不同的網路之間複製設定檔
安裝可用的 OS 更新 (iOS 和 macOS - 需要 DEP)

安全性
使用裝置 Wi-Fi、IP 位址和 GPS 資料找出裝置位置
容器化、隔離代管和非代管資料 (透過 iOS 的 Managed Open-In 和 Android 的 Android for Work)
未註冊監控和通知
防毒、反間諜功能、防火牆、磁碟加密、密碼、螢幕鎖定逾時，以及越獄和根偵測
限制對 iCloud 的存取權 (iOS)
限制使用者接受未受信任的 TLS 憑證 (iOS)
強制加密備份 (iOS) 和加密儲存裝置 (Android)
全域 HTTP Proxy (iOS)
強制執行密碼原則和失敗輸入裝置資料抹除原則 (Android、iOS、Mac、PC)
在允許網路存取前，先掃描用戶端裝置是否已安裝 Systems Manager (Android、iOS、Mac、PC)
簡單憑證註冊通訊協定 (SCEP)
可進行憑證佈建的客戶憑證簽署
限制儀表板控制的存取權限 (例如無法清除 BYOD 裝置 iOS 和 Mac)
動態設定檔管理 - 安全性合規性、地理柵欄管理、時間排程、最低執行 OS 版本、應用程式黑名單/白名單，以及數據上限閾值
遺失模式 (iOS)
全天候、隨需，以及依應用程式 VPN、AnyConnect VPN

軟體和應用程式管理
清查已安裝的軟體和應用程式
自訂部署軟體和 App Store 和 Google Play 公開應用程式
與 Apple App Store 和 Apple 大量採購方案整合
與 Google Play 商店和 Android for Work 整合
在 Meraki 雲端上託管最高 3 GB 的檔案
透過 .msi 或 .exe (PC) 和 .dmg (Mac) 執行軟體安裝
解除安裝軟體 (Mac 和 Windows)
解除安裝應用程式 (Android 和 iOS)
限制應用程式安裝
限制應用程式內購買
監控未經授權的軟體和應用程式安裝並傳送通知
安裝企業應用程式

內容管理
自訂部署檔案、文件、應用程式 (Android 和 iOS)
更新到最新版檔案並部署到裝置 (Android 和 iOS)
管理和分配應用程式授權 (具有 VPP 的 iOS 和 macOS)
裝置授權指派 (具有 VPP 的 iOS)
部署 iBook 授權
主畫面版面配置 (僅限 iPad)

裝置限制
限制使用相機 (iOS 和 Android)
FaceTime、Siri、iTunes Store、多重玩家遊戲，以及 Apple Music (iOS)
限制內容使用量 (YouTube、明確的音樂和播客、內容分級電影、電視節目和應用程式) (iOS)
強制加密備份 (iOS) 和加密儲存裝置 (Android)
強制執行密碼原則和失敗輸入裝置資料抹除原則 (Android、iOS、Mac、PC)
單一應用程式或資訊站模式 (Android 和 iOS)
自發單一應用程式模式 (iOS)
自動和已加入白名單的內容篩選 (iOS)
限制使用 AirDrop (iOS)
限制變更應用程式的行動數據使用量 (iOS)
切換語音與數據漫遊設定 (iOS)
限制列出哪些 Airplay 裝置 (iOS)
讓裝置名稱保持為最新狀態 (iOS)
管理非代管應用程式 (iOS)
鎖定桌布和裝置名稱 (iOS)
代管網域、Safari 自動填入網域 (iOS)
通知設定和不允許變更通知設定 (iOS)
顯示/隱藏應用程式 (iOS)

疑難排解和即時工具
遠端裝置鎖定、解除鎖定和資料抹除 (Android、iOS、Mac 和 Windows)
遠端重新開機和關機 (Mac 和 Windows)
遠端桌面和螢幕擷取畫面 (Mac 和 Windows)
存取裝置處理清單 (Mac 和 Windows)
將即時通知傳送給裝置 (Android、iOS、Mac 和 Windows)
監控主動 TCP 連線、TCP 統計資料和路由表 (Mac 和 Windows)
選擇性資料抹除 (Android、iOS 和 Mac)
切換語音、數據漫遊和熱點 (iOS)
隨需命令資訊站模式或單一應用程式模式 (Android 和 iOS)
從遠端啟動 Airplay (iOS)

網路組態部署
部署 Wi-Fi 設定，包括 WPA2-PSK 和 WPA2 企業版 (Android、iOS、Mac 和 Windows)
部署 VPN 組態和驗證設定 (Android、iOS、Mac 和 Windows)
部署伺服器端數位憑證 (Android、iOS、Mac 和 Windows)
在允許網路存取前，先掃描用戶端裝置是否已安裝 Systems Manager (Android、iOS、Mac 和 Windows)

部署 Airplay 目的地和密碼

Cisco ISE MDM API 整合

Sentry 安全性

Sentry 原則 – 根據狀態強制執行網路原則 (Android、Chrome、iOS、Mac 和 Windows)

Sentry 註冊 – 整合自助式上線 (Android、iOS、Mac 和 Windows)

Sentry Wi-Fi 安全性 – 只要按一下滑鼠即可部署 EAP-TLS (Android、iOS、Mac 和 Windows)

Sentry VPN 安全性 – 自動佈建行動用戶端 VPN (Android、iOS 和 Mac)

Sentry Wi-Fi 設定 – 自動設定 WLAN 設定 (Android、iOS、Mac 和 Windows)

Sentry VPN 設定 – 自動設定 VPN 設定 (Android、iOS、Mac 和 Windows)

裝置註冊

應用程式註冊 (iOS 和 Android)

透過 DEP 進行自動註冊 (iOS 7+ 和 macOS 10.10+)

裝置上註冊 (iOS、Android、Mac 和 Windows)

與 Apple Configurator 和 Profile Manager 整合 (iOS 和 Mac)

SMS 或電子郵件註冊邀請 (iOS、Android、Mac 和 Windows)

本機安裝程式部署 (Mac 和 Windows)

與 Active Directory GPO 整合 (Windows)

在註冊時隔離裝置 (Android、Chrome、iOS、Mac 和 Windows)

透過 G Suite 和 G Suite 教育版進行 Chrome OS 裝置管理

多使用者驗證 – 動態變更裝置軟體、設定和存取

監控

硬體重要指標和規格報告

網路存取、連線、訊號強度監控

限制合規性監控

包含裝置 Wi-Fi 連線、IP 位址和 GPS 資料的裝置位置資訊

電池、儲存空間、RAM 和 CPU 使用量、服務中斷監控

根據網路/IP 資訊覆寫位置 (例如在沒有 GPS 選項時)

自動佈建

將群組原則整合到 Cisco Meraki 硬體堆疊

根據行動身分識別進行動態標籤，包括地理位置、安全性狀態和時間

整合 Active Directory 和 LDAP 群組以自動套用標籤、擁有者和使用者

使用 VPP 自動發佈和撤銷應用程式授權

電子郵件設定

Exchange ActiveSync 電子郵件帳戶佈建 (Android 和 iOS)

將外寄郵件限制為僅限郵件應用程式中的代管帳戶 (iOS)

使用自訂網域和網域格式

在使用 ActiveSync 時強制使用 SSL

在使用 ActiveSync 時啟用 S/MIME

Gmail 應用程式中電子郵件的代管應用程式設定 (Android 和 iOS)

使用裝置擁有者，在裝置上自動插入使用者專屬的電子郵件地址

Chrome OS 管理

鎖定、停用和控制裝置

設定及管理使用者和裝置層級設定

將使用者加入白名單以登入裝置

啟用自動更新

啟用資訊站模式

Wi-Fi 和 VPN 組態

啟用安全瀏覽

管理電源設定

設定瀏覽器書籤、安全性和內容篩選

行動數據資料管理

產生行動數據使用量的全域和個別報告 (Android 和 iOS)

追蹤個別方案使用量時的每月計數器和方案開始日期 (Android 和 iOS)

指定單一或多重數據上限閾值的原則 (Android 和 iOS)

使用原則在裝置超過其數據上限時採取行動 (Android 和 iOS)

限制變更應用程式的行動數據使用量 (iOS)

切換數據漫遊與個人熱點 (iOS)