

管理裝置

VMware Workspace ONE UEM

您可以在 VMware 網站上找到最新的技術文件，網址如下：

<https://docs.vmware.com/tw/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2021 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

- 1 使用 Workspace ONE UEM 來管理裝置 5**
- 2 裝置清單檢視 7**
 - 在清單檢視中篩選裝置 13
 - 從清單檢視新增裝置 14
- 3 憑證管理 17**
- 4 合規原則 18**
 - 合規原則清單檢視 19
 - 檢視裝置頁面 20
 - 依平台而定的合規原則規則 21
 - 合規原則規則描述 22
 - 依平台而定的合規原則動作 23
 - 新增合規原則 25
 - 檢視裝置指派、合規原則 27
 - 使用健全狀況證明偵測遭破解裝置 28
 - 設定 Windows 桌上型電腦合規原則的健全狀況證明 28
 - 設定 Windows Phone 合規原則的健全狀況證明 29
- 5 自訂屬性 31**
- 6 裝置動作 35**
- 7 裝置指派 40**
- 8 裝置明細 44**
- 9 裝置註冊 47**
 - 透過 Workspace ONE Intelligent Hub 註冊裝置 48
 - 其他註冊工作流程 49
 - 其他註冊限制 49
 - 自動探索註冊 53
 - 基本註冊與目錄服務註冊 54
 - 自攜裝置 (BYOD) 註冊 57
 - 配置註冊選項 58
 - 封鎖清單和允許清單裝置登錄 64

- 裝置登記 65
- 註冊狀態 71
- 自我註冊與裝置註冊預備 73
- 使用者註冊企業群組優先順序 79
- Workspace ONE 直接註冊 80

10 裝置設定檔 84

- 設定檔處理 84
- 新增一般設定檔設定 87
- 裝置設定檔清單檢視 88
- 技術預覽：工作流程中使用的設定檔和設定檔資源 92
- 裝置設定檔編輯 93
- 合規設定檔 94
- 設定檔資源 95
 - 新增 Exchange 資源 97
 - 新增 Wi-Fi 資源 100
 - 新增 VPN 資源 102
- 地理柵欄區域 104
- 時間排程 106
- 檢視裝置指派、裝置設定檔 107

11 裝置標記 109

12 查閱值 113

13 BYOD 部署的隱私權 115

14 資源 125

- 技術預覽：建立時間範圍並指派給裝置 126

15 共享裝置 129

16 抹除保護 135

使用 Workspace ONE UEM 來管理裝置

1

管理團隊裝置中的裝置，並使用 Workspace ONE UEM 執行特定一組裝置上的功能。

您可以利用**監視器**來檢查資料流程，並利用**裝置儀表板**仔細查看您的裝置群。您可以使用**裝置清單檢視**來為裝置分組，並建立自訂清單。

您也可以產生**報告**，並使用**標記**來輕鬆識別裝置。您甚至可設立**自助入口網站 (SSP)**，讓終端使用者管理自己的裝置，以減輕服務台人員的負擔。如需詳細資訊，請參閱 [Workspace ONE UEM 的自助入口網站](#)。

裝置儀表板

裝置註冊後，您便可從 Workspace ONE UEM 的**裝置儀表板**管理這些裝置。

裝置儀表板不但可以提供重要的監控視角來掌握整個行動裝置團隊的狀況，同時還可讓您針對個別裝置快速採取行動。檢視您團隊中相關裝置資訊的圖形，比如裝置擁有權類型、合規性統計數據，以及平台和作業系統明細等。若要在顯示的類別中存取各個裝置組，可從**裝置儀表板**選取任何可用的資料檢視。

從**清單檢視**中，您可執行各種管理行動：傳送訊息、鎖定裝置、刪除裝置和變更與裝置相關的群組。

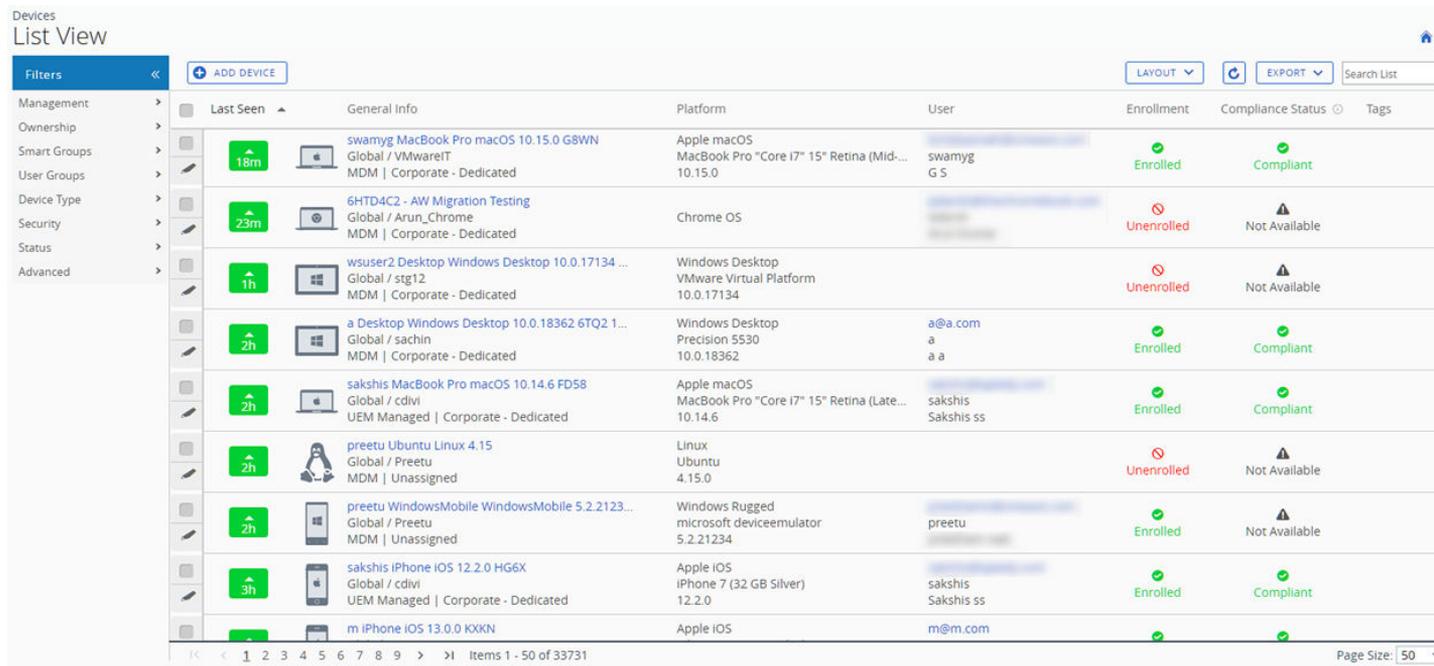
- **安全性** – 檢視您裝置團隊中造成安全性問題的主要原因。選擇任何一個圓環圖，即會顯示篩選後的**裝置清單**檢視，此清單包含所有受到所選安全性問題影響的裝置。若平台支援的話，您便能配置合規性原則在裝置上採取動作。
 - **已破解** – 部署中已遭破解 (越獄/根破解) 之裝置的數量與百分比。
 - **無密碼** – 尚未為安全性而配置密碼之裝置的百分比與數量。
 - **無加密** – 尚未為安全性而加密之裝置的百分比與數量。此數字無法說明 Android SD 卡上的加密情形。只有那些缺乏磁碟加密的 Android 裝置才會在圓環圖中回報。
- **擁有權** – 檢視在各個擁有權類別中的裝置總數。選擇條狀圖的任一區段，即會顯示一個篩選後的**裝置清單**視圖，該視圖含有已受到選定之擁有權類型所影響的裝置。
- **最後上線裝置總覽/明細** – 檢視最近與 Workspace ONE UEM MDM 伺服器通訊之裝置數量與百分比。例如，如果超過 30 天沒有看到多個裝置，請選擇相應的條狀圖，僅顯示那些裝置。然後，您可以選取所有經篩選的裝置並傳送查詢命令，讓裝置得以簽入。
- **平台** – 檢視在各個裝置平台類別中的裝置總數。選擇任一圖形，即會顯示一個篩選後的裝置清單檢視，內含所選平台的裝置。

- **註冊** – 檢視在各個註冊類別中的裝置總數。選取任一圖形，即會顯示一個篩選後的**裝置清單**檢視，內含所選註冊狀態的裝置。
- **作業系統明細** – 按照作業系統來檢視您團隊中的裝置。每個支援的作業系統都有個別圖表。選取任一圖形，即會顯示一個篩選後的**裝置清單**檢視，內含執行所選作業系統版本的裝置。

裝置清單檢視

2

使用 Workspace ONE UEM 中的 [裝置清單檢視]，在目前所選定的企業群組中查看裝置的完整清單。您也可以篩選視圖，僅檢視您想要查看的裝置類型。



最後上線時間欄位會顯示一個指示器，顯示自裝置簽入後所經過的分鐘數。該指示器會根據裝置處於非使用中狀態的時間長度，而顯示紅色或綠色。預設值為 480 分鐘 (8 小時)，但您可以自訂此值，方法為導覽至 **群組和設定 > 所有設定 > 裝置和使用者 > 一般 > 進階**，然後變更 **裝置非使用狀態逾時 (分鐘)** 值。

您可以隨時在 **一般資訊** 欄位中點選裝置的暱稱，開啟該裝置的詳細資料頁面。**暱稱**是您指派給裝置的標籤，藉此協助您區分相同品牌和型號的裝置。

依照特定的資訊，以欄位為排序依據並設定資訊篩選器來檢視活動。例如，按照 **合規狀態** 欄位排序，僅檢視目前已違規的裝置，並只針對這些裝置採取行動。搜尋所有裝置的暱稱或使用者名稱，來隔離某台裝置或某位使用者。

裝置清單檢視中的暫留快顯視窗

一般資訊 欄中的每個裝置在裝置暱稱旁邊右上方的資料夾形狀中都會有工具提示圖示。若輕觸此圖示 (行動觸控裝置) 或滑鼠游標暫留在圖示上 (PC 或 Mac)，將會顯示暫留快顯視窗。此快顯視窗包含的資訊包括 **暱稱**、**企業群組**、**群組 ID**、**管理**和**擁有權**。

在裝置清單檢視中的**註冊**和**合規狀態**欄位中可找到類似的工具提示圖示。這些工具提示圖示分別顯示**註冊日期**和**合規性違規**的暫留快顯視窗。

為裝置的清單檢視自訂配置

選取**版面配置**按鈕然後選擇**自訂**選項，即可在**裝置清單**檢視中顯示可看到的欄位完整清單。此檢視可讓您根據偏好顯示或隱藏裝置清單欄位。

您也可以選擇將您自訂的欄位視圖，套用在現有企業群組 (OG) 或其下層群組中的所有管理員。舉例來說，您可以從目前 OG 與其下層所有 OG 的**裝置清單**檢視中隱藏「資產編號」。

完成所有自訂項目後，選擇**接受**按鈕來儲存您各項欄位的偏好並套用此新欄位檢視。您可以隨時回到**版面配置**按鈕設定，調整您的欄位顯示喜好。

某些明顯的裝置清單檢視自訂配置欄包括下列內容。

- Android Management
- SSID (服務組識別碼或 Wi-Fi 網路名稱)
- Wi-Fi MAC 位址
- Wi-Fi IP 位址
- 公用 IP 位址

匯出清單檢視

您可以儲存完整**裝置清單**檢視的 XLSX 或 CSV (逗點分隔值) 檔案，這些檔案可在 MS Excel 中檢視及分析。如果您已在**裝置清單**檢視套用篩選條件，匯出的清單也反映篩選結果。

選取**匯出**按鈕，然後選取格式 (**XLSX** 或 **CSV**)，接著導覽至**監控 > 報告與分析 > 匯出**，以檢視並下載產生的報告。

在裝置清單檢視中搜尋

您可以搜尋某項裝置，以便快速存取裝置上的資訊，並在裝置上進行遠端操作。

若要執行搜尋，請導覽至**裝置 > 清單檢視**，然後選取**搜尋清單**列並且輸入使用者名稱、裝置暱稱或其他可用於識別裝置的元素。此動作會在目前的企業群組及所有子群組內，透過搜尋參數，開始搜尋所有的裝置。

裝置清單檢視動作按鈕叢集



在 [裝置清單檢視] 中選取一或多個裝置時，您可以使用動作按鈕叢集來執行一般動作，包括查詢、傳送 [訊息]、鎖定以及可透過**更多動作**按鈕存取的其他動作。

隨著不同的平台、裝置製造商、型號、註冊狀態，以及特定的 Workspace ONE UEM Console 組態，會有不同的裝置動作可供使用。

如需管理員可以使用主控台叫用的遠端動作完整清單，請參閱第 6 章 裝置動作。

遠端協助

您可以在單一的合格裝置上啟動**遠端協助**工作階段，讓您能夠遠端檢視畫面及控制裝置。此功能相當適合用於在您的團隊中的裝置上，進行疑難排解和執行進階組態。

若要使用此功能，您必須符合下列要求。

- 您必須具有有效的 Workspace ONE Assist 授權。
- 您必須是已獲指派角色的管理員，其中包含適當的 Assist 權限。
- 裝置必須安裝 Assist 應用程式。
- 支援的裝置平台：
 - Android
 - iOS
 - macOS
 - Windows 10
 - Windows Mobile

在**裝置清單檢視**中，選取合格裝置左側的核取方塊，**遠端協助**按鈕隨即顯示。選取此按鈕以啟動 [遠端協助] 工作階段。

如需詳細資訊，請參閱 [Workspace ONE Assist 指南](#)。

取消註冊的裝置

取消註冊裝置不一定能在 Workspace ONE UEM Console 中檢視，需視裝置過去是否登錄或保持註冊狀態而定。您也可存取在裝置從 UEM 主控台取消註冊之前，所執行的疑難排解記錄。

取消註冊的狀態

取消註冊的裝置是指具有以下三種情況之一的裝置。

- 1 裝置剛新增至 Workspace ONE UEM 但尚未登錄、註冊，因此未受到管理。此情況的裝置不會顯示在 UEM 主控台中。
- 2 新裝置已開始 Workspace ONE 註冊程序，並已透過 UEM 主控台登錄，但尚未註冊完成。此情況通常會發生在需要大量註冊裝置，且僅限已登錄裝置註冊的時候。允許已登錄裝置進行註冊的是裝置允許清單機制。處於此狀態的裝置會顯示在 UEM 主控台中，並標示為「取消註冊」。由於已登錄的裝置通常屬於註冊程序的一部分，因此裝置不會維持在這個情況太久。
- 3 如果裝置終端使用者從裝置上手動移除 MDM 設定檔，則裝置也會變為取消註冊。

如需詳細資訊，請參閱此頁面中標題為**刪除裝置**的區段。

存取在取消註冊前所作的疑難排解記錄

您可存取裝置取消註冊前所作的疑難排解/指令記錄。這些記錄能協助您全盤瞭解裝置歷史記錄。

- 1 導覽至**裝置 > 清單檢視**。
- 2 選擇您已知先前已取消註冊的裝置。您可選擇**篩選**清單視圖，讓清單僅顯示**狀態為取消註冊**的裝置。
結果：選取裝置時，系統會顯示**詳細資訊檢視**。
- 3 選取**更多**索引標籤下拉式清單，然後再依序選取**疑難排解**和**指令**索引標籤。

下一步：如果您不想將先前取消註冊的裝置再重新註冊到同一個客戶企業群組，可考慮永久刪除裝置記錄，如此一來，重新註冊時，裝置的歷史記錄便會是已清空狀態。請聯絡 Workspace ONE 支援人員進行安排。

裝置清單檢視中的大量動作

篩選裝置子集後，若要執行大量動作，可先選取裝置，再從動作按鈕叢集選取動作。



大量動作只能在裝置清單檢視中使用，而且您必須先從系統設定中啟用 (**群組與設定 > 所有設定 > 系統 > 安全性 > 受限動作**)。密碼保護動作需要 PIN 碼才能執行。

在**清單檢視**中選好裝置後，所選裝置的數目會顯示在動作按鈕旁邊。此數目也包括選定之已篩選裝置。

備註 在 [裝置清單檢視] 中，當您使用「Shift」鍵選取裝置區塊時可用的大量動作，可能會不同於使用 [全域] 核取方塊時的大量動作。

如需受影響動作的相關資訊，請參閱**第 6 章 裝置動作**；如需選擇方法的相關資訊，請參閱此頁面中標題為**在裝置清單檢視中選取裝置**的區段。

裝置清單檢視中的大量管理限制

您可以限制能夠接受大量動作指令的裝置總數，從而確保在管理大型的裝置團隊時能順利作業。

若要變更這些限制，請導覽至**群組與設定 > 所有設定 > 裝置和使用者 > 進階 > 大量管理**。上頭已列出多個裝置動作，您可以變更該動作所允許的裝置數量上限。

當您已備妥大量管理限制，而且已選好多台裝置時，「所選項目的數量」的旁邊便會出現一個連接：**由於大量的限制，某些動作已被停用**。這表示您選取的裝置數量超過某些裝置動作所允許的裝置數量上限。

您可以選取此連結，以瞭解已停用哪些動作。

將裝置清單檢視中的大量動作警告排入佇列

大量動作需要一些時間來處理。如果您啟動一個新的大量動作，而 Workspace ONE™ UEM 主控台又正在處理現有的大量動作，系統便會出現警告訊息。

Your previous bulk actions requested are still being processed. This request is run once the previous actions are complete. Do you want to continue with the current request?

選擇**是**來將新的大量動作加入佇列。選擇**否**來取消新的大量動作。

在裝置清單檢視中選取裝置

若要在頁面中選取個別裝置，只須勾選各裝置左側的勾選方格即可。您也可以跨頁面選取多個裝置。甚至還可以選取裝置團隊中的所有裝置，不過有可能會觸發受限動作警告。

選取裝置區塊

若要選取連續的裝置區塊，甚至橫跨多個頁面，請勾選區塊起始處的裝置勾選方格。接著，按住 **shift** 鍵，然後在區塊末尾處勾選裝置勾選方格。此動作類似於 Windows 和 Mac 環境中的區塊選擇功能，能夠將大量的動作套用到所選的裝置上。

選取所有裝置

使用全域勾選方格 (在**最後上線時間**欄位標題的左側) 來全選或取消全選清單中的所有裝置。如果您的**清單檢視**包含已篩選的裝置清單，您便可使用全域勾選方格來全選或取消全選所有已篩選的裝置。

當全域核取方塊出現綠色減號時 (☐)，表示已至少選取一部裝置，但並未全部選取。再次選取此圖示，便會變更為核取記號 (☑)，表示已選取清單中的所有裝置 (無論已篩選或未篩選)。第三次選取此圖示，則會再變更為空的核取方塊 (☐)，表示目前未選取清單中的任何裝置。

備註 在 [裝置清單檢視] 中，當您使用「Shift」鍵選取裝置區塊時可用的大量動作，可能會不同於使用 [全域] 核取方塊時的大量動作。

如需更多有關受影響動作的資訊，請參閱 [第 6 章 裝置動作](#)。

在所選的裝置上所設置之受限動作警告

在您所選的裝置團隊中，以所有裝置啟動某項動作時，便會出現一個警告訊息。

您正嘗試針對 [所選數量] 個裝置執行動作。此動作可能不適用於所有裝置。一些此動作的限制包括註冊狀態、管理類型、裝置平台、型號或作業系統。

此警告可用來確認一群具有眾多不同特色之製造商、作業系統和功能等大型裝置團隊。這和**大量管理限制**及其所產生的任何警告訊息皆無關。如您設有**大量管理限制**，系統便不會顯示這則**受限動作警告**訊息。

刪除裝置

您可以從 Workspace ONE UEM Console 刪除已註冊的裝置。

刪除裝置會造成下列三種影響。

- 1 該裝置會自裝置清單檢視中移除。
- 2 系統會執行 *企業抹除，從裝置中移除所有敏感性公司內容。
- 3 該裝置將被排除於所有裝置管理功能之外。

但是，已刪除的裝置仍維持在 UEM console 的登錄狀態，且會新增至允許清單中。此新增功能代表可輕鬆重新註冊已刪除的裝置。裝置可無限期維持此情況。您最多可在此允許清單中保留約 150,000 部裝置。若您需要保留更多裝置，請聯絡支援部門。

您可以隨時移除任何屬於允許清單裝置的登錄記錄，此舉會讓裝置在 UEM console 內呈現不顯示及未知的狀態。在此情況下的裝置可於未來進行註冊。

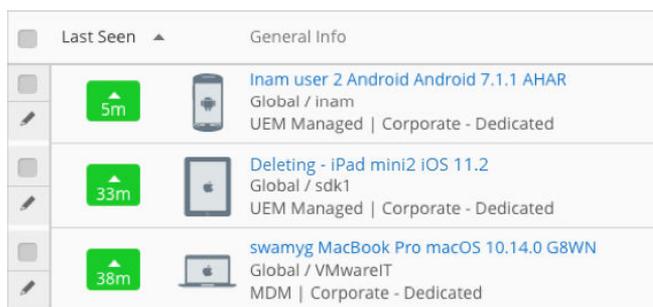
或者，您可以將裝置從允許清單中移除，然後新增至封鎖清單。如此可避免此裝置於日後進行註冊，有效地在您的機群中禁用該裝置。

如需深入瞭解封鎖清單與允許清單裝置，請參閱 [封鎖清單和允許清單裝置登錄](#)。

您可以從 [裝置清單檢視] 或 [裝置詳細資料檢視] 刪除裝置。

- 1 導覽至 **裝置 > 清單檢視**，然後按一下裝置清單左側的核取方塊，以選取您要刪除的裝置。
 - a 某些裝置無法從清單檢視中刪除。如果您想要刪除此類裝置，請導覽至 **裝置 > 清單檢視**，然後改在 **一般資訊** 欄位中點選裝置 **暱稱**。此動作會顯示 **詳細資料檢視**。**暱稱** 是您指派給裝置的標籤，藉此協助您區分相同品牌和型號的裝置。
- 2 找到 **更多動作** 按鈕，然後選取。
- 3 選取 **刪除裝置**，然後在確認提示中選取 **確定**。

結果：已刪除裝置的裝置清單檢視項目包含「刪除」指示器。



* 選取多個要刪除的裝置時，可能會觸發抹除防護功能。在抹除防護功能解除鎖定後抹除的任何裝置，都必須手動刪除。

舉例來說，如果您選擇了 25 個要刪除的裝置，而抹除防護功能在系統刪除 10 個裝置後啟動，則剩餘的 15 個裝置會在解除鎖定抹除防護後進行企業抹除，但和前 10 個裝置不同的是，這些裝置尚未從 UEM 中刪除。您必須手動刪除這些剩下的 15 個裝置。

如需詳細資訊，請參閱第 16 章 [抹除保護](#)。

本章節討論下列主題：

- [在清單檢視中篩選裝置](#)
- [從清單檢視新增裝置](#)

在清單檢視中篩選裝置

您可以套用篩選器，僅檢視您想要查看的裝置。選取**篩選**按鈕，以顯示下列所有篩選器，僅檢視符合您所選類別的裝置。

您可以任意指定所需數量的篩選器。在您選取**套用**按鈕 * 之前，裝置清單不會更新。

設定	描述
管理	顯示受到 APP 層級 管理的裝置，或由 Catalog 、 Container 或 MDM 管理的裝置。顯示以 未知 方式管理、處於 離線 狀態，或接受 所有 管理方式管理的裝置。
擁有權	顯示具有以下擁有權層級的裝置： 公司專用 、 公司共用 、 員工自用 或 未指派 。您可以一次篩選一或多個擁有權層級。
智慧群組	顯示屬於所選智慧群組的裝置。按一下 搜尋 文字方塊，然後從出現的智慧群組清單中選取。向下捲動以檢視以字母順序排列的智慧群組清單。
使用者群組	顯示屬於所選使用者群組的裝置。按一下 搜尋 文字方塊，然後從出現的使用者群組清單中選取。向下捲動以檢視以字母順序排列的使用者群組清單。
裝置類型	
平台	從完整的裝置平台清單中選取。您可以一次篩選多個平台。
Android 管理	僅在選取 Android 平台時可用。 您必須選取至少一個平台，然後按一下 套用 按鈕，然後才能選取管理類型。 篩選 Android 平台的特定裝置管理類型。您也可以 為裝置的清單檢視自訂配置 ，以顯示 [Android 管理] 欄位。此欄位也會顯示在 匯出清單檢視 中。
裝置型號 *	您必須選取至少一個平台，然後按一下 套用 按鈕，然後才能選取裝置型號。
作業系統版本 *	您必須選取至少一個平台，然後按一下 套用 按鈕，然後才能選取作業系統版本。選取多個平台時，會顯示依每個選取的平台分組的作業系統版本清單。
安全性	
破解	選取 已破解 、 未破解 、 未知 ，或以上 全部 。 已破解的裝置是指經過「越獄」(iOS 裝置) 或「根破解」(Android 裝置) 的裝置。
加密	選取 已加密 、 未加密 、 未知 ，或以上 全部 。
密碼	選取 密碼 、 無密碼 、 未知 或 全部 的密碼選項。
狀態	
註冊狀態	選取 已註冊 、 企業抹除擱置中 、 裝置抹除擱置中 、 取消註冊 或以上 全部 。

設定	描述
最後上線時間	根據裝置多久之前簽入來加以顯示。使用 最後上線時間 (天) 選項中的最小和最大文字方塊，以顯示在一段時間範圍內最後上線的裝置。包含輸入的數字：如果輸入 1，會顯示距離上次上線已超過 1 天，但未滿 2 天的所有裝置。如果輸入 2，會顯示距離上次上線已超過 2 天，但未滿 3 天的所有裝置。依此類推。如果輸入零，會顯示距離上次上線已超過 0 天，但未滿 1 天 (24 小時) 的所有裝置。 若要顯示最後上線時間早於 (或等於) 所輸入最大天數的裝置，請將最小值文字方塊保留空白。 若要顯示最後上線時間晚於 (或等於) 所輸入最小天數的裝置，請將最大值文字方塊保留空白。
合規性	選取 合規、不合規、等候合規性檢查、不適用、未知 ，或以上 全部 。
註冊記錄	從 過去一天、過去一週、過去一個月 或 所有 註冊日期中選取。
進階	
MAC 位址	依裝置的媒體存取控制位址來篩選。
IP 範圍	依目前指派的網際網路通訊協定位址來篩選裝置。在 IP 範圍起始值 和 IP 範圍結束值 的文字方塊內輸入 IP 位址，以顯示落在該範圍內的裝置。 目前的 IP 位址可能為眾多與裝置相關的 IP 位址之一。您可以在「裝置明細」的「網路」標籤中找到大多數 IP 位址。
標籤	依指派的標記來檢視裝置，且您可以從下拉式功能表搜尋和選取這些標記。
Tunnel	選取要顯示所有裝置、連線至通道的裝置，還是未連線至通道的裝置。
內容合規性	選取要顯示所有裝置、只有缺少必要文件的裝置，或是只有缺少最新版必要內容的裝置。
遺失模式	檢視所有裝置，或只有已啟用遺失模式的裝置。僅適用於 iOS 裝置。

套用多項篩選條件後，您可以查看**篩選條件**按鈕右側的圓形號碼徽章，以瞭解產生的清單中套用了多少篩選條件。

您可以選取**篩選條件**按鈕旁的「X」，藉此清除所有選取的篩選條件，並返回完整裝置清單。

從清單檢視新增裝置

可以新增或登記裝置，並包括其使用者指派、自訂屬性和標記等資訊。

程序

- 1 導覽至**裝置 > 清單檢視**，或**裝置 > 生命週期 > 註冊狀態**。
- 2 選取**新增裝置**按鈕。**新增裝置**頁面即會出現。請完成下列設定。

表 2-1. 使用者

設定	描述
搜尋文字	各裝置都需指派使用者。在此文字方塊中輸入搜尋參數並選取 搜尋使用者 按鈕來搜尋某使用者。您可以從搜尋結果中選取使用者，也可以選取 建立新的使用者 連結。

表 2-2. 建立新的使用者

設定	描述
安全性類型	請選取 基本 使用者或 目錄 使用者。如需詳細資訊，請參閱主題〈基本驗證〉和〈Active Directory 驗證〉。
使用者名稱	輸入要用來在環境中識別使用者的使用者名稱。
密碼、確認密碼	輸入並確認與使用者帳戶對應的密碼。
Email 地址	為使用者帳戶輸入 Email 地址。
註冊企業群組	作為裝置註冊之註冊企業群組 (OG) 的 OG。
顯示進階使用者詳細資料	顯示所有進階使用者詳細資料，包括有使用者名稱、使用者電話號碼和管理員名稱的完整資訊。另外也包括選擇性識別設定，例如：部門、員工 ID 和成本中心。 為您新增的使用者選取預設 使用者角色 ，以決定在使用已連結的裝置時，該名使用者應具有何種權限。如需詳細資訊，請參閱主題「使用者角色」。

表 2-3. 裝置

設定	描述
預期的暱稱	裝置的 預期的暱稱 是您指派給裝置的標籤，藉此協助您區分相同品牌和型號的裝置。您可以選擇手動輸入暱稱或結合查閱值。如需詳細資訊，請參閱第 12 章 查閱值 。
企業群組	從與裝置有關聯的下拉式功能表中選取企業群組。
擁有權	從下拉式功能表中選擇裝置所有權。請選取 無 、 公司專用 、 公司共用 或 員工自用 。
平台	從下拉式功能表為裝置選取平台。
顯示進階裝置資訊選項	顯示所有進階裝置資訊設定。

表 2-4. 進階裝置資訊設定

設定	描述
型號	從下拉式清單中選擇裝置型號。下拉式功能表的內容取決於您在 平台 下拉式功能表中所作出的選擇。
作業系統	從下拉式清單中選擇裝置的作業系統。下拉式功能表的內容取決於您在 平台 下拉式功能表中所作出的選擇。
UDID	輸入裝置的唯一識別碼。
序號	輸入裝置序號。
IMEI	輸入裝置的 15 位數的國際行動裝置識別碼 (International Mobile Station Equipment Identity)。
SIM	輸入裝置的 SIM 卡規格。
資產編號	輸入裝置的資產編號。該編號由企業內部建立，而此設定則是專為保留此資料點而提供的。

表 2-5. 傳訊

設定	描述
訊息類型	選取您要在環境註冊成功時，傳送至裝置的訊息類型 (無 、 SMS 或 Email)。
Email 地址	輸入您要傳送註冊訊息的 Email 地址。 僅當已將 訊息類型 選為 Email 時，才能使用此文字方塊。

表 2-5. 傳訊 (續)

設定	描述
Email 訊息範本	從下拉式功能表中選擇 Email 範本。您可以透過連結來開啟訊息範本頁面，並在其中建立 Email 訊息範本。
電話號碼	輸入您要傳送 SMS 文字訊息的電話號碼。 僅當已將 訊息類型 選為 SMS 時，才能使用此文字方塊。
SMS 訊息範本	從下拉式功能表中選擇 SMS 範本。您可以透過連結來開啟訊息範本頁面，並在其中建立 SMS 訊息範本。

- 3 (可選) 將**自訂屬性**指派至裝置。點選**新增**按鈕並提供**屬性**與其**數值**。
- 4 (可選) 將**標籤**指派至裝置。點選**新增**按鍵並從下拉式功能表中選取您要指派的標記。
- 5 選取**儲存**。

請考慮以數位憑證來保全您的企業資產。憑證能夠提供的驗證、穩定性和安全性層次，是密碼所無法比擬的。Workspace ONE UEM powered by AirWatch 使用數位憑證，進而解決整個裝置生命週期的安全性保證問題。

當行動化公司機密的內容逐漸成為一種常態，未經授權的存取和惡意的威脅不免也會隨之增加。即使您已經使用了強固的密碼來保護貴公司的電子郵件、Wi-Fi 和虛擬私人網路 (VPN)，您的基礎結構仍有可能會遭受暴力攻擊法、字典式攻擊，以及員工人為的錯誤。

撤銷和更新數位憑證

憑證核發後，Workspace ONE UEM 可讓您透過**憑證清單檢視**，管理已部署的數位憑證。管理員可以檢視憑證，並按照裝置、授權單位、使用者、設定檔、核發日期等項目來加以排序。您可以個別或大量撤銷和更新憑證。

憑證清單檢視提供部署憑證的摘要，也可讓您以個別方式或大量更新或撤銷憑證。在停用的使用者/裝置中找到並撤銷所有數位憑證，甚至早在合規到期日之前，就更新/輪換所有 Wi-Fi 的驗證憑證。

- 1 若要開始該程序，請導覽至**裝置 > 憑證 > 清單檢視**。
- 2 勾選一或多個空白的方格，即可識別並選取要更新或撤銷的數位憑證。
- 3 選取您要將動作套用至所選憑證的動作按鈕。從以下項目中選擇。
 - 更新
 - 撤銷

憑證整合資源

Workspace ONE UEM 所接受的每個憑證文件，均可透過造訪[憑證授權機構整合](#)取得詳細說明。

合規性引擎是一種由 Workspace ONE UEM powered by AirWatch 提供的自動化工具，確保所有裝置都遵守您定義的原則。這些原則可包含基本的安全性設定，例如需要密碼及強制執行某些預防措施，包括密碼強度、將特定應用程式加入封鎖清單，以及要求裝置簽入間隔時間。

一旦發現裝置不合規，合規引擎就會警告使用者解決合規問題，以避免裝置受到懲戒動作。舉例來說，合規引擎可以觸發一個訊息來傳送訊息，以告知使用者其裝置已不合規定。

此外，不合規的裝置無法指派裝置設定檔，並且也無法在裝置上安裝 APP。如果在指定時間內沒有更正錯誤，該裝置便會喪失您所指定之特定內容和功能的存取權。可用的合規原則和動作依平台而異。

倘若問題未被修正，您可以自動啟用升級，例如鎖定裝置並通知使用者與您聯繫以解除裝置的鎖定。這些升級步驟、懲戒動作、寬限期和訊息都可透過統一端點管理主控台來自訂。

合規性可以兩種方法來衡量。

- 即時合規 (RTC)

從裝置取得之未排程的樣本，用來判斷裝置是否合規。管理員可以透過隨選方式來請求這些樣本。

- 引擎合規

合規引擎是一種軟體演算法，這種演算法可接收並測量排定時間的範例，主要是決定裝置的合規。管理員可以在主控台中定義運行排程器的時間間隔。

這個一般總覽說明如何強制執行行動安全性原則。

- 1 選擇您的平台。

決定要在其上強制執行合規的平台。選取平台之後，您絕對不會看到不適用於該平台的選項。

- 2 建立您的原則。

自訂您的原則以涵蓋所有應用程式清單、破解狀態、加密、製造廠商、型號和作業系統版本、密碼以及漫遊等事項。

- 3 定義升級。

配置以時間 (小時或天數) 為主的行動，以採取分層漸進的方法來執行這些行動。

- 4 指定動作。

將 SMS、Email 或推播通知傳送給使用者的裝置，或者只向管理員傳送 Email。要求裝置簽入、移除或封鎖特殊設定的設定檔、安裝合規性設定檔、移除或封鎖 APP，以及執行企業抹除。

- 5 配置指派項目。

依照企業群組或智慧群組來指派您的合規原則，並透過裝置來確認指派內容。

確認 Windows 裝置的健全狀況

Windows 裝置可讓您在啟動時配置並掃描裝置的健全狀況，以確保您的企業資源安全無虞。如需詳細資訊，請參閱主題[使用健全狀況證明偵測遭破解裝置](#)，本文位於 docs.vmware.com 的 **Windows 桌面裝置管理**說明文件中。

本章節討論下列主題：

- [合規原則清單檢視](#)
- [依平台而定的合規原則規則](#)
- [新增合規原則](#)
- [使用健全狀況證明偵測遭破解裝置](#)

合規原則清單檢視

Workspace ONE UEM powered by AirWatch 內的 [合規性原則清單檢視] 讓您能夠查看所有使用中及非使用中的合規原則及其組態。

初始註冊時，裝置的合規狀態會被列於**擱置中**。建立、儲存和將某原則指派給一個已註冊裝置時，會使裝置的合規狀態變為**合規**或**不合規**。

同樣的，在**智慧群組**指派中所做的變更，僅會在智慧群組中出現新裝置時，讓裝置合規原則呈現**擱置**狀態。已指派給智慧群組的裝置，不會因為其智慧群組擴大 (或縮小) 其指派項目而變更其合規狀態。

若要檢視合規性原則清單視圖，請導覽至**裝置 > 合規性原則 > 清單視圖**。

Devices > Compliance Policies

List View

ADD Status Active Search List

Active	Name	Description	Managed By	Platform	Compliant/Non-Compliant/Pending/Assigned	
	!!!!!!!MDM Terms of Use Acceptance	MDM Terms of Use Acceptance	gandhi2	Apple iOS	0 / 0 / 0 / 0	
	!!!Application List	Application List	gandhi1	Android	0 / 0 / 0 / 0	
	!!Application List	Application List	gandhi2	Apple iOS	0 / 0 / 0 / 0	
	!!ios_Compromised Status	Compromised Status	gandhi2	Apple iOS	0 / 0 / 0 / 0	
	!Last Compromised Scan	Last Compromised Scan	gandhi2	Apple iOS	0 / 0 / 0 / 0	
	and_Application List	Application List	gandhi2	Android	0 / 0 / 0 / 0	
	and_Application List	Application List	gandhi2	Android	0 / 0 / 0 / 0	
	and_Compromised Status	Compromised Status	gandhi2	Android	0 / 0 / 0 / 0	
	and_Device Last Seen	Device Last Seen	gandhi2	Android	0 / 0 / 0 / 0	
	and_Last Compromised Scan	and_Last Compromised Scan	gandhi2	Android	0 / 0 / 0 / 0	
	and_Passcode	Passcode	gandhi2	Android	0 / 0 / 0 / 0	
	Application List	Application List	aman_comp	Apple iOS	0 / 0 / 0 / 0	
	Application List	Application List	fresh1	Apple iOS	0 / 0 / 0 / 0	
	Application List	Application List	i18n	Apple iOS	4 / 0 / 4 / 8	
	Application List	Application List	#MF	Apple iOS	0 / 0 / 0 / 0	
	Application List	Application List	#MMF	Apple iOS	0 / 0 / 0 / 0	
	Application List	Application List	hsam9940	Apple iOS	0 / 0 / 0 / 0	

設定	描述
狀態	篩選全部、使用中和非使用中狀態之間的清單。
動作功能表	檢視並編輯個別的原則、檢視已被指派原則的裝置，並且刪除您不需要再保留的原則。
合規/不合規/擱置中/已指派	在此欄列中所標示的數字具有超連結的功能；一旦點選後，便會顯示 檢視裝置 畫面，提供您有關所選的合規原則之特定狀態。 已指派狀態是合規、不合規和擱置中的裝置之摘要。 如需詳細資訊，請參閱 檢視裝置頁面 。
匯出按鈕	您可以使用 合規性原則 清單視圖的預設 Excel 格式 (XLSX) 或逗號分隔值格式 (CSV) 下載報告。

檢視裝置頁面

檢視裝置頁面可用來針對指派至所選原則的各個裝置，檢視其合規細節。當您在合規原則清單檢視中，選取了合規/不合規/擱置中/已指派任一欄列中所標示的超連結文字數字時，就會顯示此頁面。

若要在這四個狀態中篩選清單，請從狀態下拉式功能表中選取。已指派狀態是合規、不合規和擱置中狀態的摘要。

View Devices - Security Patch Version X

Status: Assigned

Status	Friendly Name	C/E/S	Platform/OS/Model	Organization Group	Last Compliance Check	Next Compliance Check	Actions Taken
Pending	g Android Android 8.0.0 AY5X	C	Android / Android 8.0.0 / Android	laforge		3/7/2018 8:15 AM	
Pending	g Android Android 9.0.0 0237	C	Android / Android 9.0.0 / Android	laforge		3/2/2018 5:40 AM	
Compliant	gaurav Android Android 8.1.0 ...	C	Android / Android 8.1.0 / Android	laforge	2/14/2018 3:24 AM	Next Sample	

Items 1-3 of 3 Page Size: 50

狀態欄位中列出三種裝置狀態。

- **合規** – 指派的合規原則已確定該裝置處於合規狀態。
- **不合規** – 指派的合規原則已確定該裝置處於不合規狀態。
- **擱置中** – 已排定時間要將合規原則指派給新註冊的裝置。

您也可以確認裝置的 **C/E/S** (擁有權)、**平台/作業系統/型號**、**組織群組**、**上次合規檢查**、**下次合規檢查**和**採取的動作**。「採取的動作」欄位會列出為處理不合規裝置而採取的動作。

您也可以選擇重新評估某特定裝置的合規性。選取**重新評估合規性** ()，即可預約合規性引擎並重新回報裝置上的合規性狀態。

依平台而定的合規原則規則

單一合規性原則並不能適用於由 Workspace ONE UEM powered by AirWatch 管理的所有平台。**新增合規原則**頁面以平台為基礎，因此只能看到適用於裝置的合規原則規則和動作。

使用下列表格來判斷哪些規則可以部署至您的裝置。

合規原則	Android 和 Android 舊版	Apple iOS	Apple macOS	Chrome OS	GNX	Windows Rugged	Windows 10 Desktop
應用程式清單	✓	✓	✓				
防毒狀態							✓
行動數據使用量	✓	✓					
行動訊息使用量	✓						
行動語音使用量	✓						
合規屬性							✓
破解狀態	✓	✓					✓
裝置最後上線時間	✓	✓	✓	✓	✓	✓	✓
裝置製造商	✓						
加密	✓	✓	✓				✓
防火牆狀態			✓				✓
可用磁碟空間		✓					
iBeacon 區域		✓					
互動式憑證設定檔到期日	✓	✓					
上次違規掃描	✓	✓					

合規原則	Android 和 Android 舊版	Apple iOS	Apple macOS	Chrome OS	GNX	Windows Rugged	Windows 10 Desktop
接受 MDM 使用條款	✓	✓	✓			✓	✓
型號	✓	✓	✓				
作業系統版本	✓	✓	✓	✓			✓
密碼	✓	✓					✓
漫遊*	✓	✓					✓
漫遊行動數據使用量*	✓	✓					
安全性修補版本	✓						
SIM 卡變更*	✓	✓					
系統完整性保護			✓				
Windows 自動更新狀態							✓
Windows 正版驗證							

備註 * 僅限電信進階使用者使用。

合規原則規則描述

合規原則規則允許您建立為原則構建堅實的基礎，並作為原則的組成部分。隨後的動作、升級與指派都會以這些規則為基礎。

設定	描述
應用程式清單	偵測已安裝在裝置中的特定封鎖清單應用程式，或偵測所有未列入允許清單的應用程式。您可禁止某些特定的應用程式 (例如社群媒體應用程式) 以及被廠商列入封鎖清單的應用程式，或僅准許使用您所指定的應用程式。 由於應用程式狀態在 iOS 裝置報告上的方式，應用程式僅在安裝程序全部完成後，才會達到「已安裝」狀態。因此，如果您正在建立用來測量 iOS 裝置應用程式清單的合規性規則，請考慮使用強制執行的動作以避免資料損毀。例如，企業抹除或裝置抹除。
防毒狀態	偵測防毒 APP 是否正在運作。合規性原則引擎會監控裝置的行動作業中心是否具有防毒解決方案。Windows 支援所有第三方防毒解決方案。
行動數據/訊息/語音使用量	偵測出終端使用者的裝置，在什麼時候超過了指派的電信計劃之特定的閾值。 當使用量超過預先決定的臨界值時，UEM 將無法限制實際使用量，此時 Workspace ONE UEM 只能提供通知。 為了讓此原則規則正常運作，您必須啟用進階電信，並將該電信方案指派給裝置。
合規屬性	將裝置中的屬性鍵與第三方端點安全性進行比對，傳回一個代表裝置合規性的布林值。僅適用於 Windows 桌面版裝置。
破解狀態	偵測裝置是否已遭破解。禁止使用已向 Workspace ONE UEM 註冊的越獄或根破解裝置。 越獄/根破解裝置會除去整體安全性設定，可能會將惡意軟體引入您的網路中，並提供存取企業資源的途徑。在 BYOD 環境下，員工擁有各種版本的裝置及作業系統，所以監控破解裝置狀態對此環境而言尤其重要。
裝置最後上線時間	偵測裝置是否未在配置的時間範圍內進行簽入。
裝置製造商	偵測裝置製造商，讓您能夠辨別特定的 Android 裝置。您可以特別禁止特定製造商或僅准許您指定的特定製造商。

設定	描述
加密	偵測裝置是否已啟用加密功能。Windows 支援所有第三方加密解決方案。
防火牆狀態	偵測防火牆 APP 是否正在運作。合規引擎會檢查裝置的行動作業中心是否具有防火牆解決方案。Windows 支援所有第三方防火牆解決方案。
可用磁碟空間	偵測裝置上可用的磁碟空間。
iBeacon 區域	偵測您的 iOS 裝置是否在 iBeacon 群組的區域內。
互動式憑證設定檔到期日	在指定的時間範圍內，偵測安裝在裝置上的設定檔何時會到期。
上次破解掃描	偵測裝置是否尚未在指定的時間排程內，呈報其破解狀態。
接受 MDM 使用條款	偵測終端使用者是否尚未在指定的時間內，接受目前的 MDM 使用條款。
型號	偵測裝置型號。您可以特別禁止特定型號或僅准許您指定的特定型號。
作業系統版本	偵測裝置的作業系統版本。您可以禁止特定的作業系統，或者僅准許您所指定的作業系統和版本。
密碼	偵測裝置上是否設有密碼。
漫遊*	偵測裝置是否處於漫遊狀態。
漫遊行動數據使用量*	針對靜態數據量 (以 MB 或 GB 為測量單位) 來偵測漫遊行動數據的使用量。
安全性修補版本	偵測 Google 上最新的 Android 裝置安全性修補日期。僅適用於 Android 6.0 版及更新版本。
SIM 卡變更*	偵測 SIM 卡是否已被取代。
系統完整性保護	即便由根使用者或具根權限的使用者執行的情況下，也可偵測 macOS 系統所擁有的檔案和目錄的專屬保護狀態，以防止無特定「權利」的程序修改。
Windows 自動更新狀態	偵測 Windows 自動更新是否已被啟動。合規性原則引擎會監控裝置的行動作業中心是否具有更新解決方案。如果行動作業中心並未顯示您的第三方解決方案，系統就會回報為未監控。
Windows 副本的正版驗證	偵測目前在裝置上所執行的 Windows 版本是否為正版軟體。

* 僅限電信進階使用者使用。

依平台而定的合規原則動作

由各平台所支援，且由合規原則所強制執行的動作列示如下。

表 4-1. 應用程式

合規原則動作	Android 和 Android 舊版	Apple iOS	Apple macOS	Chrome OS	GNX	Windows Rugged	Windows 桌面
封鎖/移除受管理 APP	✓	✓	✓				✓
封鎖/移除所有受管的應用程式	✓	✓	✓				✓

表 4-2. 指令

合規原則動作	Android 和 Android 舊版	Apple iOS	Apple macOS	Chrome OS	GNX	Windows Rugged	Windows 桌 面
變更漫遊設定。		✓ (iOS 5 以 上)					
企業抹除***	✓	✓	✓		✓		✓
企業重設	✓					✓	
作業系統更新 ****		✓					
請求裝置簽入		✓					✓
撤銷 Azure Tokens*。	✓	✓					

表 4-3. Email

合規原則動作	Android 和 Android 舊版	Apple iOS	Apple macOS	Chrome OS	GNX	Windows Rugged	Windows 桌面
封鎖 Email	✓	✓					

表 4-4. 通知

合規原則動作	Android 和 Android 舊版	Apple iOS	Apple macOS	Chrome OS	GNX	Windows Rugged	Windows 桌面
傳送 Email 給使用者**。	✓	✓	✓	✓		✓	✓
傳送 SMS 簡訊給裝置。	✓	✓					✓
傳送推播通知給裝置。	✓	✓	✓	✓			✓
傳送電子郵件給管理 員。	✓	✓	✓		✓	✓	✓

表 4-5. 設定檔

合規原則動作	Android 和 Android 舊版	Apple iOS	Apple macOS	Chrome OS	GNX	Windows Rugged	Windows 桌面
安裝合規設定檔。	✓	✓	✓				✓
封鎖/移除設定檔	✓	✓	✓				✓
封鎖/移除設定檔類型	✓	✓	✓				
封鎖/移除所有設定檔 ***	✓	✓	✓				✓

* 需要在設定 > 系統 > 企業整合 > 目錄服務 > 進階中啟用「針對識別服務使用 Azure AD」。會影響特定使用者的所有裝置，停用所有依賴 Azure Token 的 APP。

** 包含寄送副本給使用者管理員的選項。

*** 這些動作會造成在裝置回報合規狀態前，無法傳送設定檔。

**** iOS 9 到 10.2.1 的受監管 DEP 註冊裝置可執行作業系統更新動作。iOS 10.3 及更新版本的裝置只需受監管。

新增合規原則

新增合規原則的程序是由四個區段組成：規則、動作、指派和摘要。Workspace ONE UEM powered by AirWatch 以初始平台的所有平台特定選項作為基礎，因此主控台永遠不會出現您裝置無法使用的選項。

備註 只有 Motorola 裝置支援 Windows 堅固型合規 (企業必須執行重設動作才能強制執行合規)。

若要透過設定檔和自動化升級配置合規引擎，請完成合規原則標籤。

程序

- 1 導覽至**裝置 > 合規原則 > 清單檢視**，然後選取**新增**。
- 2 從**新增合規原則**頁面上選擇平台，以此作為您合規原則的基礎。
- 3 依第一個相符規則的**任何或全部**配置**規則**標籤，以偵測條件。
 - **新增規則** – 選取此項，以新增其他的規則和參數。如需詳細資訊，請參閱[依平台而定的合規原則規則及合規原則規則描述](#)。
 - **上一步和下一步** – 分別選擇回到上一步驟或進展到下一步驟或相關動作。

- 4 若要在原則中定義不合規的後果，請完成**動作**標籤。

可用的動作依平台而不同。在回報合規狀態之前，有些動作會禁止接收設定檔。如需進一步資訊，請參閱[依平台而定的合規原則動作](#)。

- 5 指明所要執行的**動作**和**升級**行為。

如果先前的**動作**不需使用者採取修正步驟來讓裝置合規，則**升級**僅是一個自動化的動作。

選擇選項和要執行的動作類型。

表 4-6. 動作和升級

設定	描述
標示為不合規勾選方格	<p>讓您能夠在裝置上執行動作而無需將其標示為不合規裝置。合規引擎透過遵守下列規則來達成任務。</p> <ul style="list-style-type: none"> ■ 在每項新加入的動作中，將「標示為不合規」的勾選方格預設為啟用 (勾選) 狀態。 ■ 如果某項動作已啟用「標示為不合規」的選項，那麼所有後續的動作和升級也會被標記為不合規 (勾選)，而且您也無法編輯這些後續的勾選方格。 ■ 如果某項動作已停用 (不勾選) 標示為不合規的選項，那麼下一步動作/升級即會預設為啟用 (勾選) 該選項，但您可以編輯該勾選方格。 ■ 如果動作/升級的「標示為不合規」選項已經停用，且裝置沒有通過合規規則，則裝置正式為「合規」。然後系統就會執行指定的動作。 ■ 除非有動作/升級的「標示為不合規」勾選方格已經啟用，否則裝置的狀態就會保持「合規」。只有這樣裝置才會被視為不合規。
應用程式	<p>封鎖或移除受管的應用程式。</p> <p>您也可藉由建立允許清單、封鎖清單或必要的應用程式清單來強制應用程式的合規性。</p>
指令	<p>啟動裝置簽入或執行企業抹除。</p>

表 4-6. 動作和升級 (續)

設定	描述
Email	<p>根據 Email 來封鎖使用者。</p> <p>如果您結合 Email 合規引擎使用行動 Email 管理，那麼「封鎖 Email」動作就會套用。若要存取此選項，請導覽至 Email > 合規原則 > Email 原則。此動作可讓您使用「裝置合規」原則 (例如：封鎖清單應用程式) 以及任何您所配置的電子郵件合規引擎原則。選擇此動作後，如果裝置違規時，單一裝置原則更新會觸發 Email 的合規性。</p>
通知	<p>通知某人違反合規。</p> <p>您可選擇以下選項來寄送通知。</p> <ul style="list-style-type: none"> ■ 傳送電子郵件給使用者。 ■ 將 SMS 簡訊* 傳送至裝置。 ■ 傳送推播通知給裝置。 ■ 傳送電子郵件給管理員。 <p>多封電子郵件可插入所提供之副本文字方塊並以逗點分隔。您也可以插入查閱值以寄送副本給使用者管理員；按一下「副本」文字方塊旁的加號，然後從下拉式功能表中選擇「{UsersManager}」。如需詳細資訊，請參閱第 12 章 查閱值。</p> <p>如為所有「通知」動作，您可以選擇使用訊息範本。如要使用此選項，請取消選取預設範本勾選方格，然後畫面就會顯示下拉式功能表，讓您可以選擇訊息範本。</p> <p>還有一個連結，若選取，將在新視窗中顯示訊息範本頁面。此頁面可讓您建立自己的訊息範本。</p> <p>* 為了讓您的裝置機群能夠使用 SMS 通知，您必須具備第三方閘道提供者的帳戶並配置閘道設定。導覽至群組與設定 > 所有設定 > 系統 > 企業整合 > SMS，然後完成 SMS 設定中說明的選項。</p>
設定檔	<p>安裝、移除或封鎖特定的裝置設定檔、裝置設定檔類型，或合規設定檔。</p> <p>合規性設定檔是以與「自動」和「可選的」裝置設定檔相同的方式來建立和儲存。導覽至資源 > 設定檔與基準 > 設定檔，然後依序選取新增與新增設定檔。選取平台，然後在一般設定檔標籤的指派類型下拉式設定中，選取「合規性」。但是，合規性設定檔只適用於新增合規原則頁面的動作標籤，當終端使用者違反合規原則時便可使用。從下拉式清單中選擇安裝合規性設定檔，然後選擇先前已儲存的合規性設定檔。</p>

表 4-7. 僅限升級

設定	描述
新增升級按鈕	建立升級作業。在新增升級作業時，最佳作法是每新增一項升級便提高額外的安全性動作。
在特定的時間間隔之後...	您可將升級的時間延遲幾分鐘、幾小時或幾天。
...執行下列動作	重複 – 您也可以勾選此方格來選擇要重複此升級動作的次數，之後再開始進行下一個排程動作。

對於 macOS 來說，您僅可執行以下的動作：

- 裝置抹除
- 將 Email 傳送給管理員
- 企業抹除
- 封鎖/移除設定檔
- 將 Email 傳送給使用者
- 封鎖/移除設定檔類型

- 將推播通知傳送給裝置
 - 封鎖/移除所有設定檔
- 6 若要決定哪些裝置受到合規原則約束 (或排除)，請完成「新增合規原則」頁面上的**指派**和**摘要**索引標籤。使用 [摘要] 索引標籤命名、完成及啟動原則。

設定	描述
管理者	選擇要管理此合規原則的企業群組。
已指派的群組	將此原則指派到一或多個群組。如需更多資訊，請參閱主題指派群組。
排除項目	如果要排除群組，請選擇 是 。然後，從 排除的群組 文字方塊中的可用群組清單選取。如需詳細資訊，請參閱主題 在設定檔及原則中排除群組 。
檢視裝置指派按鈕	查看受到此合規原則的指派所影響的裝置清單。

雖然「平台」是智慧群組的一項準則，但是在裝置設定檔或合規原則中所配置的平台，其重要性始終都比智慧群組的平台優先。舉例來說，如果某裝置設定檔是為 iOS 平台所建立的，即使智慧群組中含有 Android 裝置，設定檔還是只會指派到 iOS 裝置上。

- 7 在您決定此原則的指派後，請選擇**下一步**。
- 即會顯示**摘要**標籤。
- 8 提供此合規原則的**名稱**和有用的**描述**。
- 9 選擇下列其中一個選項。
- **完成** – 儲存您的合規原則，但不在指派的裝置上啟動它。
 - **完成並啟動** – 儲存並將該原則套用至所有受影響的裝置上。

檢視裝置指派、合規原則

在配置合規原則時來顯示**檢視裝置指派**的頁面時，請在**指派**標籤上點選**檢視裝置指派**頁面。此頁面可確認指派的合規原則所影響 (或未影響) 的裝置。

View Device Assignment
✕

Assignment Status

All

Filter Grid

↻

Assignment Status	Friendly Name	User	Platform/OS/Model	Phone Number	Organization Group
Unchanged	gaurav Android Android ...	gaurav	Android / Android 8.1.0 / A...		laforge
Unchanged	g Android Android 8.0.0 ...	g	Android / Android 8.0.0 / A...		laforge
Unchanged	g Android Android 9.0.0 ...	g	Android / Android 8.1.0 / A...		laforge

Items 1-3 of 3

Page Size: 20

CANCEL

清單中所出現的裝置，會在**指派狀態**欄位中顯示下列項目。

- **已新增** – 已在列出的裝置中新增合規原則。
- **已移除** – 已從裝置中移除合規原則。
- **未變更** – 裝置不受合規原則的變更所影響。

點選**發佈**來完成變更，並在需要時重新發佈任何的合規原則。

使用健全狀況證明偵測遭破解裝置

健全狀況證明會在裝置啟動期間掃描裝置完整性是否有問題。由 Workspace ONE UEM powered by AirWatch 管理時，請使用健全狀況證明來偵測遭破解的 Windows 桌面裝置。

在 BYOD 和公司所屬的裝置部署中，存取公司資源時必須瞭解該裝置的健全狀況良好。Windows 健康情況證明服務會透過安全通訊，從雲端存取裝置開機資訊。系統會依據相關資料點來測量和檢查此資訊，此資訊測量，確保裝置是在預期情況下開機，而不受安全性漏洞或威脅之害。測量包括安全開機、程式碼完整性、BitLocker 及開機管理程式。

Workspace ONE UEM 可讓您設定 Windows 健康情況證明服務，以確保裝置合規性。如果任何啟用的檢查失敗，則 Workspace ONE UEM 合規原則引擎就會依據設定的合規原則套用安全措施。此功能可讓您保護企業資料免於遭破解裝置的侵害。由於 Workspace ONE UEM 會從裝置硬體提取必要資訊，而不是從作業系統，所以即使作業系統核心遭到破解，仍可偵測遭破解的裝置。

設定 Windows 桌上型電腦合規原則的健全狀況證明

透過 Windows 健康情況證明服務偵測遭破解的裝置以保護裝置安全。此服務可讓 Workspace ONE UEM 在開機期間檢查裝置完整性，並採取更正動作。

程序

- 1 導覽至**群組 & 設定 > 所有設定 > 裝置 & 使用者 > Windows > Windows 桌面版 > Windows 健康情況證明**。
- 2 (選擇性) 如果您使用執行健康情況證明的自訂內部部署伺服器，請選取**使用自訂伺服器**。輸入**伺服器 URL**。
- 3 配置健全狀況證明設定：

設定	描述
使用自訂伺服器	選取此選項可為「健康情況證明」配置自訂伺服器。 此選項需要執行 Windows Server 2016 或更新版本的伺服器。 啟用此選項會顯示伺服器 URL 欄位。
伺服器 URL	輸入自訂「健康情況證明」伺服器的 URL。
已停用安全開機的功能	啟用此選項可在裝置停用安全開機功能時，標記遭破解裝置的狀態。 「安全開機」功能會強制系統進行原廠的信任式開機。啟用「安全開機」功能後，用於啟動機器的核心元件必須具有 OEM 信任的正確加密編譯簽章。UEFI 韌體驗證信任後，才會允許機器啟動。如果偵測到任何遭篡改的檔案，安全啟動會禁止啟動。
證明識別金鑰 (AIK) 不存在	啟用此選項可在裝置沒有 AIK 時，標記遭破解裝置的狀態。 裝置上有證明識別金鑰 (AIK)，代表該裝置具有簽署金鑰 (EK) 憑證，比沒有 EK 憑證的裝置更受人信任。

設定	描述
已停用資料執行防止 (DEP) 原則	啟用此選項可在裝置停用 DEP 時，標記遭破解裝置的狀態。 資料執行防止 (DEP) 原則是內建於作業系統中系統層級的記憶體保護功能，主要作用是禁止從堆積、堆疊和記憶體集區等資料頁執行程式碼。DEP 是由硬體和軟體強制執行。
已停用 BitLocker	啟用此選項可在裝置停用 BitLocker 加密時，標記遭破解裝置的狀態。
已停用程式碼完整性檢查	啟用此選項可在裝置停用程式碼完整性檢查時，標記遭破解裝置的狀態。 程式碼完整性功能可在每次驅動程式或系統檔案載入記憶體時驗證其完整性。程式碼完整性功能會在未簽署的驅動程式或系統檔案載入核心之前先進行檢查。這項檢查也會掃描具有管理權限的使用者是否執行由惡意軟體修改的系統檔案。
已停用儘早啟動的反惡意程式碼原則	啟用此選項可在裝置停用儘早啟動的反惡意程式碼原則時，標記遭破解裝置的狀態。 初期啟動的反惡意程式碼 (ELAM) 可以在電腦啟動時或在第三方驅動程式初始化之前，為您網絡中的電腦提供保護。
程式碼完整性版本檢查	啟用此選項可在程式碼完整性版本檢查失敗時，標記遭破解裝置的狀態。
開機管理程式版本檢查	啟用此選項可在開機管理程式版本檢查失敗時，標記遭破解裝置的狀態。
開機 APP 安全性版本號碼檢查	啟用此選項可在開機管理程式版本號碼不符合輸入的數字時，標記遭破解裝置的狀態。
開機管理程式安全性版本號碼檢查	啟用此選項可在開機管理程式安全性版本號碼不符合輸入的數字時，標記遭破解裝置的狀態。
進階設定	啟用此選項可在「軟體版本識別碼」區段中進行進階設定。

4 選取儲存。

設定 Windows Phone 合規原則的健全狀況證明

透過 Windows 健康情況證明服務偵測遭破解的裝置以保護裝置安全。此服務可讓 AirWatch 在開機期間監控裝置完整性，並採取更正動作。

破解狀態合規性原則適用於具有可信賴平台模組 (TPM) 1.2 或更新版本的 Windows 10 行動裝置。

程序

- 1 導覽至**群組 & 設定 > 所有設定 > 裝置 & 使用者 > Windows > Windows Phone > Windows 健康情況證明**。
- 2 (選用) 如果您使用執行健康情況證明的自訂內部部署伺服器，請選取**使用自訂伺服器**。輸入**伺服器 URL**。

3 配置健全狀況證明設定：

表 4-8. 破解狀態的定義

設定	描述
使用自訂伺服器	選取此選項可為「健康情況證明」配置自訂伺服器。 此選項需要執行 Windows Server 2016 或更新版本的伺服器。 啟用此選項會顯示 伺服器 URL 欄位。
伺服器 URL	輸入自訂「健康情況證明」伺服器的 URL。
已停用安全開機的功能	啟用此選項可在裝置停用安全開機功能時，標記遭破解裝置的狀態。 「安全開機」功能會強制系統進行原廠的信任式開機。啟用「安全開機」功能後，用於啟動機器的核心元件必須具有 OEM 信任的正確加密編譯簽章。UEFI 韌體驗證信任後，才會允許機器啟動。如果偵測到任何遭篡改的檔案，安全啟動會禁止啟動。
沒有證明識別金鑰 (AIK)	啟用此選項可在裝置沒有 AIK 時，標記遭破解裝置的狀態。 裝置上有證明識別金鑰 (AIK)，代表該裝置具有簽署金鑰 (EK) 憑證，比沒有 EK 憑證的裝置更受人信任。
已停用資料執行防止 (DEP) 原則	啟用此選項可在裝置停用 DEP 時，標記遭破解裝置的狀態。 資料執行防止 (DEP) 原則是內建於作業系統中系統層級的記憶體保護功能，主要作用是禁止從堆積、堆疊和記憶體集區等資料頁執行程式碼。DEP 是由硬體和軟體強制執行。
已停用 BitLocker	啟用此選項可在裝置停用 BitLocker 加密時，標記遭破解裝置的狀態。
已停用程式碼完整性檢查	啟用此選項可在裝置停用程式碼完整性檢查時，標記遭破解裝置的狀態。 程式碼完整性功能可在每次驅動程式或系統檔案載入記憶體時驗證其完整性。程式碼完整性功能會在未簽署的驅動程式或系統檔案載入核心之前先進行檢查。這項檢查也會掃描具有管理權限的使用者是否執行由惡意軟體修改的系統檔案。
已停用儘早啟動的反惡意程式碼原則	啟用此選項可在裝置停用儘早啟動的反惡意程式碼原則時，標記遭破解裝置的狀態。 初期啟動的反惡意程式碼 (ELAM) 可以在電腦啟動時或在第三方驅動程式初始化之前，為您網絡中的電腦提供保護。
程式碼完整性版本檢查	啟用此選項可在程式碼完整性版本檢查失敗時，標記遭破解裝置的狀態。
開機管理程式版本檢查	啟用此選項可在開機管理程式版本檢查失敗時，標記遭破解裝置的狀態。
開機 APP 安全性版本號碼檢查	啟用此選項可在開機管理程式版本號碼不符合輸入的數字時，標記遭破解裝置的狀態。
開機管理程式安全性版本號碼檢查	啟用此選項可在開機管理程式安全性版本號碼不符合輸入的數字時，標記遭破解裝置的狀態。
進階設定	啟用此選項可在「軟體版本識別碼」區段中進行進階設定。

後續步驟

如需詳細資訊，請參閱有關健全狀況證明的 [Microsoft TechNet 文章](#)。

Workspace ONE UEM 中的自訂屬性可讓您從受管理裝置 (例如 IMEI、位置等等) 擷取特定值，並使用其作為產品的指派準則。您也可以設定第三方應用程式以建立自訂屬性，並將其顯示在啟動程式上。

什麼是自訂屬性？

自訂屬性是由 Workspace ONE Intelligent Hub 或第三方應用程式所收集之其他裝置資訊的預留位置。此預留位置能以多種不同方式使用。

- 其可用於指派佈建產品之類的內容。
 - ...例如，您可以將產品 XYZ 僅佈建至已簽出並在欄位中的裝置。
- 這可以提供資訊給在 UEM Console 上的管理員或裝置上的終端使用者。
 - ...例如，一位物流駕駛員可以查看內部開發的應用程式，以判斷下一站要到哪裡 (由收集裝置位置的自訂屬性提供)。
- 這可用於將新註冊的裝置移到特定的組織群組。
 - ...例如，您可以將其型號編號等於 Zebra VC80 的所有新註冊裝置，移至專為該特定型號所設計的組織群組。

備註 只有在「客戶」層級的企業群組中，才能配置和使用自訂屬性 (和規則產生器)。

如需進一步瞭解依準於自訂屬性之裝置指派規則的相關可用選項，請參閱[啟用裝置指派](#)。

建立自訂屬性

建立自訂屬性與值並推送至 Workspace ONE UEM 中的裝置。您可以根據這些屬性與其值，為要佈建的產品建立指派規則。

- 1 導覽至**裝置 > 佈建 > 自訂屬性**。
- 2 點選**新增**，然後選擇**新增屬性**。
- 3 在**設定標籤**下，輸入**屬性名稱**。
- 4 輸入可辨別此屬性之選擇性的**描述**。
- 5 輸入用於蒐集屬性之**應用程式**的名稱。此應用程式可為第三方應用程式或 Workspace ONE Intelligent Hub。

- 6 選擇**收集規則產生器的值**，讓使用者能夠在規則產生器的下拉式功能表中使用該屬性的值。
- 7 如果您要在規則生產器中使用屬性的話，請選擇**在規則生產器中使用**。
- 8 選取**保存**，以避免自訂屬性從 Workspace ONE UEM Console 中被移除 (除非管理員或 API 呼叫明確表示要將它移除)。

否則，屬性將依正常狀態被移除。如果您刪除裝置向 UEM 主控台所報告的自訂屬性，UEM 主控台仍會有保存的自訂屬性。自訂屬性的保存僅適用於 Android 和 Windows 堅固型裝置。

- 9 選擇**當查閱值使用**，即可在 UEM 主控台的任何地方都將自訂屬性當作查閱值使用。

範例：您可將自訂屬性當作是裝置暱稱的一部分，以簡化裝置命名。

- 10 選擇**值標籤**。
- 11 選擇**新增值**，將值新增至自訂屬性。

您不需要輸入屬性的所有可能值。此處輸入的屬性清單，並非裝置可報告之值的需求或限制，而是僅輸入用於事先定義企業群組指派規則的期望值。

- 12 選取**儲存**。

自訂屬性資料庫

自訂屬性會儲存為 XML 檔案，並儲存在 Workspace ONE Intelligent Hub 資料庫中，且每個資料庫都會儲存在裝置上。使用資料庫時，您可將自訂屬性當作樣本定期傳送至 Workspace ONE UEM，作為索引鍵/值組的資產追蹤。

如果裝置資料庫中的記錄設定為 'Create Attribute' = TRUE，那麼 Workspace ONE Intelligent Hub 會自動擷取與自訂屬性範例一起傳送的名稱和值。索引鍵/值組將會顯示在「自訂屬性」標籤下，該裝置的「裝置明細」頁面中。

備註 自訂屬性值不可傳回下列特殊字元：/ \ " * : ; < > ? |。如果指令碼傳回的值包含這類字元，就不會在主控台上報告該值。請修剪指令碼輸出中的這類字元。

使用自訂屬性來指派企業群組

設定裝置在 Workspace ONE UEM 中註冊後，要如何將裝置指派到企業群組的規則。每個企業群組 (OG) 只能有一個自訂屬性指派規則。

- 1 確認您目前位於客戶類型的企業群組。
- 2 導覽至**群組和設定 > 所有設定 > 裝置與使用者 > 一般 > 進階**。
- 3 將**裝置指派規則**設為**啟用**。
- 4 將**類型**設為**按自訂屬性編排的企業群組**。

如需進一步瞭解裝置指派規則的相關可用選項，請參閱[啟用裝置指派](#)。

- 5 選取**儲存**。
- 6 導覽至**裝置 > 佈建 > 自訂屬性 > 新增 > 新增屬性**，然後建立自訂屬性 (如果尚未建立)。

請參閱此頁面中標題為**建立自訂屬性**的區段。

- 7 導覽至**裝置 > 佈建 > 自訂屬性 > 自訂屬性指派規則 > 新增規則**。
- 8 選擇**企業群組**，規則會將裝置指派給此企群組。
- 9 選擇**新增規則**來配置規則的邏輯。

設定	描述
屬性/應用程式	裝置指派視此自訂屬性而定。從裝置型號、序號，以及您所在的客戶 OG 中所提供的任何自訂屬性或 XML 檔案中選取。
運算子	此運算子針對 屬性 與 值 做比較，來決定裝置是否符合產品。 當在規則中使用超過一個運算子時，每個 運算子 之間必須包含一個 邏輯運算子 。 備註 建立指派原則時，使用小於 (<) 和大於 (>) 運算子 (及其變體) 進行比較，僅能用於比較純數值，包括整數。 例外狀況為比較 OEM 組建編號版本時，可在非數字的 ASCII 字串使用 < 和 > 運算子。例如 OEM 更新檔案名稱內含有分隔線、小數點和其他字元與數字混雜。此類指派原則必須在原則邏輯中識別一個裝置製造商，當裝置上的格式符合伺服器上指定的格式時，比較結果即視為正確。
值	在所有適用的裝置中，為該規則所選的 屬性 值都列於此處。
新增邏輯運算子	選擇此項，以顯示邏輯運算子之下拉功能表，比如「和」、「或」、「非」和括弧。允許使用更複雜的規則。

- 10 在配置規則邏輯後，再選擇**儲存**。

結果：當具有指派屬性的裝置註冊後，規則會將裝置指派給已配置的企業群組。

自訂屬性匯入

Workspace ONE UEM 中的自訂屬性批次匯入功能可讓您將自訂屬性和相應值大量載入系統。在提供的範本中，每欄皆對應一個自訂屬性，每列則對應到自訂屬性的不同參數。

使用範本，可透過不同方法匯入自訂屬性，所含的資訊也不同。

注意 必須完全複製每個範本的第一欄語法。語法不正確，可能會導致資料庫發生問題，進而遺失資料。

範本類型

- 自訂屬性範本 – 可讓您定義自訂屬性及其設定。

	A	B	C	D	E	F	G
1	CustomAttributeName	Description	ApplicationName	UsedInRuleGenerator	CollectValuesForRuleGenerator	Persist	ShowOnDevicesGrid
2	AgentVersion1	Airwatch Agent Description	Services1.exe	1	0	1	0
3	AgentVersion2	Airwatch Agent Description	Services1.exe	1	0	1	0
4	AgentVersion3	Airwatch Agent Description	Services1.exe	1	0	1	0
5	AgentVersion4	Airwatch Agent Description	Services1.exe	1	0	1	0

- 自訂屬性值範本模板 – 可讓您定義預先定義的自訂屬性值。

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	SSID Bangalore	SSID Palo Alto	PreSharedKey AdminOffc	Custom Attributes									
2	Enterprise	PLTO_1	ADMIN\$										
3	BNG_Test	PLTO_Guest	ADM1N	Values									
4	AWT		#Dm1N										
5													

- 裝置自訂屬性值 – 可讓您根據交互參照 (Xref) 值為個別裝置定義預先定義的自訂屬性值。Xref 值判斷接收每個自訂屬性值的個別裝置。

	A	B	C	D	E	F	G	H	I
1	XRefType	XRefValue	SSID Cust1	USERNAME Cust	PASSWORD Cust3	SSID CXXX	Services1.exe AgentVersion1		
2	1	5263	AW_BNG	DEV1	XXXXXXXX	SS	5.3.56.147		
3									
4									
5									

- DeviceID (裝置註冊時 Workspace ONE UEM 指派的 DeviceID)
- 序號
- UDID (Unique Device Identifier)
- MAC 位址
- IMEI 號碼

匯入檔案前，請先另存為 .csv。

裝置動作

6

檢視可從 Workspace ONE UEM Console 遠端控制，並在裝置上執行的各種動作的詳細說明。此清單與平台無關。

導覽至**裝置 > 清單**視圖，然後選取每個裝置清單左側的核取方塊，以選取您要刪除的一或多個裝置。然後選擇**其他動作** 按鈕，以查看您可以在所選裝置上執行的動作。更多相關的資訊，請參閱 [裝置清單檢視中的大量動作](#)。

- **新增標記** – 將可自訂的標記指派給裝置，可以用來辨別您團隊中的特殊裝置。
- **APP (查詢)** – 將 MDM 查詢命令傳送給裝置，以傳回已安裝的應用程式清單。
- **書籍 (查詢)** – 將查詢指令傳送給裝置，以傳回已安裝的書籍清單。
- **憑證 (查詢)** – 將 MDM 查詢指令傳送給裝置，以傳回已安裝的憑證清單。
- **變更裝置密碼** – 用一組新密碼取代任何現有用來存取所選裝置之裝置密碼。新密碼會顯示在 [變更密碼] 畫面上。
 - 按一下**變更密碼**按鈕之前，請記下密碼。
 - 選取**變更密碼**按鈕以繼續。

- 您可以關閉視窗，或選取**取消**，然後稍後再試一次。亦即：如果您無法記下密碼或將密碼轉送給終端使用者，您可以稍後重新起始 [變更裝置密碼] 動作。
- **變更企業群組** – 將裝置的主企業群組變更為另一個現存 OG。包含可選取靜態或動態企業群組的選項。
 - 如果您想要一次變更多個裝置的企業群組，您必須使用區塊選取法 (使用 Shift 鍵)，而非使用 [全域] 核取方塊 (在 [裝置清單檢視] 中的 [最後上線時間] 欄位標題旁)，以進行大量動作選取裝置。
- **變更擁有權** – 在適用的情況下，變更裝置的擁有權設定。選項包括了公司專用、公司共用、員工自有的或是未分類等。
- **清除啟動鎖定** – 清除 iOS 裝置上之啟動鎖定。啟用 [啟動鎖定] 後，使用者需要使用 Apple ID 和密碼才能執行：停用「尋找我的 iPhone」、原廠抹除和重新啟動以使用裝置等的動作。
- **清除密碼 (Container)** – 清除 Container 專用的密碼。用在使用者忘記其裝置容器密碼的情況下。
- **清除密碼 (裝置)** – 清除裝置密碼。用在使用者忘記其裝置密碼的情況下。
- **清除密碼 (限制設定)** – 清除密碼命令會清除裝置上的登入密碼。裝置必須受到監督。
- **刪除裝置** – 從主控台中刪除裝置並解除裝置註冊。將企業抹除指令傳送到下次簽入時要接受抹除的裝置，並在主控台將該裝置標記為**正在刪除**。如果裝置已關閉抹除防護，則發出的指令會立即執行企業抹除，並在主控台中移除裝置表示。
- **裝置資訊 (查詢)** – 將 MDM 查詢命令傳送給裝置，以傳回裝置上的資訊，例如：暱稱、平台、型號、企業群組、作業系統版本和擁有權狀態等。
- **裝置抹除** – 傳送 MDM 指令，以將所有資料和作業系統中的裝置抹除。此動作無法復原。
 - iOS 裝置抹除考量事項
 - 針對 iOS 11 和較舊版本的裝置，裝置抹除指令也會抹除與裝置有關的 Apple SIM 卡的資料。
 - 針對 iOS 11 以上的裝置，您可以保留 Apple SIM 數據方案 (如果裝置中有此方案)。選取 [裝置抹除] 頁面上的**保留數據方案**核取方塊，然後再傳送裝置抹除命令。
 - 針對 iOS 11.3+ 裝置，您有一個額外的選項，能夠在傳送裝置抹除命令時略過**近距離感應設定**畫面。啟用此選項後，[設定輔助程式] 中將略過 [近距離感應設定] 畫面，讓裝置使用者不會看到 [近距離感應設定] 選項。
 - 若是 Windows 桌面裝置，您可以選取裝置抹除的類型。
 - **抹除** - 此選項會抹除裝置上所有內容。
 - **抹除受保護** - 此選項與一般裝置抹除相似，但裝置終端使用者無法規避動作。抹除受保護指令會持續嘗試重設裝置，直到成功為止。在某些裝置組態中，此命令會讓裝置無法開機。

- **抹除與存留佈建資料** - 此選項會抹除裝置，但會指定佈建資料應備份到固定的位置。抹除執行後，佈建資料會還原，並套用至裝置。已儲存佈建資料夾。若要找到資料夾，您可以在裝置上導覽至 %ProgramData%\Microsoft\Provisioning 。
- **編輯裝置** - 編輯裝置資訊，例如：**暱稱、資產編號、裝置擁有權、裝置群組和裝置類別**等。
- **啟用/停用遺失模式** - 使用此裝置動作即可鎖定裝置，並將一則訊息、一個電話號碼或一段文字傳送至鎖定畫面。裝置終端使用者無法停用遺失模式。當管理員停用遺失模式時，裝置會恢復正常功能。使用者會收到一則訊息，告訴他們系統已經開始共用裝置的位置資訊。(iOS 9.3 以上監督模式)
 - **要求裝置位置** - 進入遺失模式時查詢裝置，然後使用位置標籤來尋找裝置。(iOS 9.3 以上監督模式)
- **註冊** - 傳送訊息給裝置使用者，以便註冊其裝置。您也可以選擇使用有包含註冊資訊 (比如逐步說明和有用連結) 的訊息範本。此動作只用在未註冊的裝置。
- **企業重設** - 透過企業重設將裝置重設為原廠設定，只保留 Workspace ONE UEM 的註冊。
 - **僅限 Windows 桌面版**: 裝置損毀或內含故障的應用程式時，企業重設會將裝置還原至可供運作狀態。它會重新安裝 Windows 作業系統，同時保留使用者資料、使用者帳戶和受管的應用程式。裝置在重新同步後將會重新同步自動部署的企業設定、原則和應用程式，剩餘的則由 Workspace ONE 管理。
- **企業抹除** - 將裝置進行企業抹除，會解除註冊並移除所有受管的企業資源，包括應用程式和設定檔。此動作無法復原，而且必須要重新註冊後，Workspace ONE UEM 才能再次管理此裝置。此裝置動作包含可防止日後重新註冊的選項，以及一個**備註說明**文字方塊供您新增動作的相關資訊。
 - 雲端加入網域的裝置不支援企業抹除。
- **檔案管理員** - 在 UEM console 內啟動檔案管理員，讓您可以遠端檢視裝置內容、新增資料夾、進行搜尋和上傳檔案等。
- **搜尋裝置** - 將文字訊息傳送至適用的 Workspace ONE UEM 應用程式，連同可供使用者找到錯位裝置的音效。音效選項包括播放音效的次數，以及音效間隔的長度 (以秒為單位)。
- **強制 BIOS 密碼重設** - 強制裝置將 BIOS 密碼重設為自動產生的全新密碼。
- **Workspace ONE Intelligent Hub 查詢** - 傳送查詢指令至裝置上的 Workspace ONE Intelligent Hub，以確定該 Hub 已安裝並正常運作。
- **iOS 更新** - 將作業系統更新推送至一或多個 iOS 裝置。僅有受監督、透過 DEP 註冊且 iOS 版本為 9 以上的裝置可以使用此項。
- **位置** - 使用 macOS Workspace ONE Intelligent Hub 上啟用的 GPS 功能在地圖上顯示裝置，藉以指明裝置的位置。此裝置動作需要使用者核准，才能啟用 macOS 系統偏好設定中的功能。
 - 如果您想要一次顯示多個裝置的位置，您必須使用區塊選取法 (使用 Shift 鍵)，而非使用 [全域] 核取方塊 (在 [裝置清單檢視] 中的 [最後上線時間] 欄位標題旁)，以進行大量動作選取裝置。
- **鎖定裝置** - 傳送 MDM 指令以鎖定選取的裝置，使其呈現無法使用直至解除鎖定。
- **鎖定 SSO** - 將裝置使用者鎖在 Workspace ONE UEM Container 及所有相關的應用程式之外。
- **受管設定** - 啟用或停用語音漫遊、數據漫遊以及私人熱點。

- **管理標籤** – 檢視目前指派的裝置標籤，並查看可透過 [管理標記] 畫面指派的標籤清單。
 - 如果您想要一次管理多個裝置的標籤，您必須使用區塊選取法 (使用 Shift 鍵)，而非使用 [全域] 核取方塊 (在 [裝置清單檢視] 中的 [最後上線] 欄位標題旁)，以進行大量動作選取裝置。
- **標記為勿擾模式** – 將裝置標記為勿擾模式，禁止接收訊息、Email、設定檔，以及透過其他任何類型傳入的互動。僅有那些「標記為勿擾模式」的裝置可使用**清除勿擾模式**，用來移除該限制。
- **覆寫工作記錄層級** – 覆寫所選裝置之工作事件層級記錄的目前指定層級。此動作會設定藉由產品佈建推送的工作記錄詳細資訊，並覆寫目前在 Android Hub 設定中配置的記錄層級。若要清除工作記錄層級覆寫，您可以在 [動作] 畫面中選取下拉式功能表的**重設為預設**項目。您也可以在此 [Android Hub 設定] 中變更 [產品佈建] 類別下的工作記錄層級。
- **設定檔 (查詢)** – 將 MDM 查詢指令傳送到裝置，以傳回已安裝的裝置設定檔清單。
- **立即佈建** – 在裝置上佈建產品。佈建功能可以將有條理之檔案、動作、設定檔和應用程式的安裝程序建立為單一的产品，再推送給裝置。
- **全部查詢** – 將查詢命令傳送到裝置，以便傳回已安裝的應用程式 (如果適用的話，也包括 Workspace ONE Intelligent Hub)、書籍、憑證、裝置資訊、設定檔和安全措施等清單。
- **重新啟動裝置** – 從遠端重新啟動裝置，與關閉電源並重新開啟的效果一樣。
- **登錄管理員** – 在 UEM console 內啟動登錄管理員，讓您能夠遠端檢視裝置的作業系統登錄情形、新增金鑰、進行搜尋和新增內容等。
- **遠端協助** – 使用此動作來遠端控制可支援的裝置，可提供平台專屬工具，讓您能夠在裝置上執行支援動作與進行疑難排解。若是 Android 裝置，則必須將遠端控制服務安裝在裝置上。
- **遠端管理** – 使用此動作來遠端控制可支援的裝置，即可啟動主控台應用程式，並讓您能夠在裝置上執行支援動作與進行疑難排解。若是 Android 裝置，則必須將遠端控制服務安裝在裝置上。
- **遠端檢視** – 啟用裝置輸出的作用中串流至您選擇的目的地，讓您能夠看到使用者在操作裝置時所看到的內容。目的地參數包含 IP 位址、連接埠、音訊連接埠、密碼和掃描時間。
- **重新命名裝置** – 在 UEM console 中變更裝置的暱稱。
- **要求裝置記錄** – 要求所選裝置的偵錯記錄，然後選取**更多**索引標籤並選擇**附件 > 文件**，即可檢視記錄。您無法檢視 Workspace ONE UEM Console 內的記錄。此記錄以 ZIP 檔案格式傳遞，可用於疑難排解及提供支援。

要求記錄時，您可以選擇從**系統**或**Hub**接收記錄。**系統**提供系統層級記錄。**Hub**提供在裝置上執行的多個 Agent (代理程式) 的記錄。

僅限 Android 版：您可以從公司擁有的 Android 裝置擷取詳細記錄，並在主控台中加以檢視，以快速地解決裝置上的問題。

- **要求裝置簽入** – 要求所選裝置本身在 UEM 主控台中簽入。此動作會更新**最後上線時間**的欄位狀態。
- **重新啟動 Workspace ONE Intelligent Hub** – 重新啟動 Workspace ONE Intelligent Hub。此選項在註冊程序或子模組的安裝程序被中斷時，可用來執行疑難排解。
- **安全性 (查詢)** – 將 MDM 查詢命令傳送給裝置，以傳回使用中安全措施的清單 (裝置管理員、加密、密碼、憑證等)。
- **傳送訊息** – 傳送訊息給所選裝置之使用者。選擇**電子郵件**、**推送通知** (透過 AirWatch Cloud Messaging) 或是 **SMS**。推送通知需要如 Hub、Boxer 等至少必須啟動一次的 Airwatch 應用程式。
- **啟動 AirPlay** – 從裝置串流視聽內容至 AirPlay 鏡射目的地。必須提供目的地的 MAC 位址 (格式為「xx:xx:xx:xx:xx:xx」，不區分大小寫)。如有必要，也可以指定密碼。「掃描時間」用來定義搜尋目的地時所要花費的時間，以秒為單位 (10 至 300 秒)。需要使用 macOS 10.10 或更高版本。
- **啟動/停止 AWCM** – 啟動/停止所選裝置的雲端傳訊服務。VMware AirWatch Cloud Messaging (AWCM) 可簡化管理主控台傳送訊息和命令的功能。有了 AWCM，終端使用者不再需要存取公用網際網路或使用 Google ID 等取用者帳戶。
- **同步裝置** – 將所選裝置與 UEM 主控台進行同步處理，使其與**最後上線**狀態一致。
- **工作管理員** – 在 UEM console 內啟動工作管理員，讓您可以遠端檢視裝置目前運作中的工作，包括工作名稱、**程序 ID** 和您可以執行的適用**動作**。
- **檢視 BIOS 密碼** – 檢視 Workspace ONE UEM Console 自動產生之裝置的 BIOS 密碼。您會看到**上次套用的密碼**以及**上次提交的密碼**。
- **檢視資訊清單** – 以 XML 格式在 UEM 主控台上檢視裝置的**套件資訊清單**。在 Windows 堅固型裝置上的資訊清單，列出了小工具和應用程式的中繼資料。
- **暖開機** – 無須執行開機自我測試 (POST) 即可重新啟動作業系統。

裝置指派

7

裝置指派可讓您按照網際網路通訊協定 (IP) 位址範圍或自訂屬性，在跨企業群組 (OG) 和使用者名稱之中移動裝置。這是在 Workspace ONE UEM 中依使用者群組整理內容的替代方法。

與其需要管理員手動在 OG 之間移動裝置，您可以指導主控台在連接至定義的 Wi-Fi 時，自動移動裝置。您還可根據您定義的自訂屬性規則移動裝置。

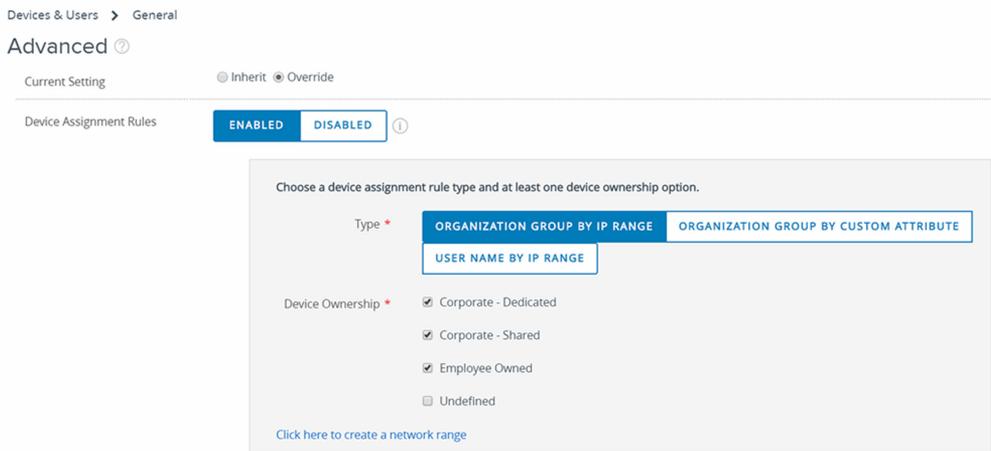
典型的裝置指派使用範例是：經常變更身份而且每個身份都需要有特殊的設定檔和應用程式的使用者。

若要移動裝置，您必須在施行**使用者群組**或是**裝置指派**之間做選擇，因為 Workspace ONE UEM 無法在一部裝置上同時支援這兩種功能。

啟用裝置指派

您必須先在 Workspace ONE UEM 中啟用裝置指派，才能以網際網路通訊協議 (IP) 或者自訂屬性作為基礎，在企業群組 (OG) 和使用者名稱之間移動裝置。裝置指派僅能在子企業群組中配置。

- 1 導覽至**群組 & 設定 > 所有設定 > 裝置 & 使用者 > 一般 > 進階**，然後依據您的需要來選擇**覆寫**或**繼承**目前的設定。



- 2 在**裝置指派規則**設定中選擇**啟用**。
- 3 選擇管理**類型**。從以下項目中選擇。
 - **依 IP 範圍的企業群組** – 裝置退出一個 Wi-Fi 網路範圍並進入另一個 Wi-Fi 網路範圍時，將裝置移到指定的 OG。此舉將自動推送設定檔、APP 原則和產品。

- **依自訂屬性的企業群組** – 依自訂屬性將裝置移到某企業群組。

自訂屬性讓管理員能夠從受管理裝置中摘錄特定的值，並將此值傳回 Workspace ONE UEM Console。您也可以將屬性值指派給裝置，以供產品佈建或裝置查閱值使用。

- 若已啟用**依自訂屬性的企業群組**，標題為**按一下這裡即可根據指派規則建立自訂屬性的連結**即會顯示。選取後，此連結將在瀏覽器中打開另一個分頁。此分頁顯示**自訂屬性指派規則**頁面，讓您建立自己的屬性指派規則。
- **依 IP 範圍的使用者名稱** – 若裝置退出一個網路並進入另一個網路，則裝置會變更使用者名稱，而不是移至另一個 OG。此使用者名稱變更會觸發的推送 (設定檔、APP 原則和產品)，與 OG 變更時的相同。此選項適用於那些只具有有限的權限來建立新企業群組的客戶；如此一來，這些客戶便可利用此替代方法的優勢來使用裝置指派的功能。

重要 如果您要在現有的指派配置變更指派**類型**，您必須刪除全部現有的已定義範圍。若要移除 IP 範圍指派，請導覽至**群組 & 設定 > 群組 > 企業群組 > 網路範圍**。若要移除自訂屬性指派，請導覽至**裝置 > 佈建 > 自訂屬性 > 自訂屬性指派規則**。

- 4 選擇**裝置擁有權**選項。僅指派具有某種已選之擁有權類型的裝置。從以下項目中選擇。

- 公司專用
- 公司共用
- 員工自有
- 未定義

- 5 您可以選取連結以新增網路範圍，請**按一下此處**建立網路範圍。

您也可以導覽至**群組與設定 > 群組 > 企業群組 > 網路範圍**來前往此頁面。前往這個位置時，您所屬企業群組的**裝置指派**必須已啟用，您才能看到 [網路範圍] 設定選項。

選取後，**網路範圍**頁面隨即顯示。

- 6 設好所有的選項後，請選擇**儲存**。

定義裝置指派規則或網路範圍

當您的裝置由 Workspace ONE UEM 管理且連線至 Wi-Fi 時，裝置會進行驗證，並針對您選取的 OG 自動安裝設定檔、APP、原則和產品佈建。

您也可依照自訂屬性來定義規則。當具有指派屬性的裝置註冊後，規則會將裝置指派給已配置的企業群組。裝置也可獲得指派，條件是裝置必須收到包含合格自訂屬性的產品佈建。

裝置指派僅能在子企業群組中配置。

- 1 導覽至**群組與設定 > 群組 > 組織群組 > 網路範圍**。

您必須啟用裝置指派，[網路範圍] 選項才會顯示。如果您在企業群組導覽路徑中找不到「網路範圍」，請參閱上方標題為**啟用裝置指派**一節。

- 2 若要新增單一的際網路通訊協定 (IP) 位址，請選擇**新增網路範圍**。在**新增/編輯網路範圍**頁面中，填妥下列的設定，然後選擇**儲存**。

表 7-1. 新增網路範圍

設定	描述
起始 IP 位址	輸入網路範圍的最上方結尾。
結束 IP 位址	輸入網路範圍的最底部結尾。
企業群組名稱	為輸入網路範圍時，輸入裝置移動的 OG 名稱。此設定只有在網路指派 類型 為「依 IP 範圍而定的企業群組」時才能看到。
使用者名稱	在輸入網路範圍時，輸入裝置登記的使用者名稱。此設定只有在網路指派 類型 為「依 IP 範圍區分的使用者名稱」時才能看到。
描述	選擇新增對網路範圍有助益的描述。

重疊網路範圍會出現「儲存失敗，網路範圍已存在」的訊息。

- 3 如果需要新增數個網路範圍，可以選擇**批次匯入**來節省時間。
- 在批次匯入頁面，選取**為此批次類型下載範本**連結，即可檢視並下載大量匯入的 CSV 範本。
 - 開啟 CSV 檔案。CSV 檔案有數個欄位，與**新增網路範圍**畫面上的選項相對應。在「OrganisationGroup」欄中輸入組織群組 ID，而不是組織群組名稱。

備註 您可以使用下列方式識別任何組織群組的群組 ID：1) 移至您想要識別的 OG，並 2) 將指標暫留在 OG 標籤上，其中會顯示包含群組 ID 的快顯視窗。



備註 CSV 檔案 (逗點分隔值) 只是一份副檔名從「TXT」變更為「CSV」的文字檔。此檔案會以純文字格式儲存表格式資料 (文字和數字)。檔案的每一行或每一列都是一筆資料記錄。每筆記錄都含有一或多個以逗號分隔的欄位。您可以使用任何文字編輯器開啟和編輯，也可以使用 Microsoft Excel 開啟和編輯。

- 開啟 CSV 範本時，您會注意到範例資料已新增至範本中的各個欄位。顯示的樣本資料旨在說明必須提供哪種資料，以及資料採用的格式。請勿偏離範例資料所示的格式。填寫您要新增的每個網路範圍的每個必要資料行，以完成此範本。
- 使用**批次匯入**頁面匯入完成的範本。
- 選取**儲存**。

Batch Import



Batch Name*

Batch Description*

Batch Type Network Ranges

Batch File (.csv) No file chosen

The Network Range Import feature can be used to load Network Ranges(s) into the system in bulk. The Network Ranges should be associated with a Organization Group.

Note: The file must be saved in .csv format.

For reference, click Download Template.

[Download template for this batch type](#)

裝置明細

8

您可以透過在 Workspace ONE UEM 中檢視 [裝置詳細資料] 頁面，查看單一裝置的資訊，並快速存取使用者和裝置的管理動作。

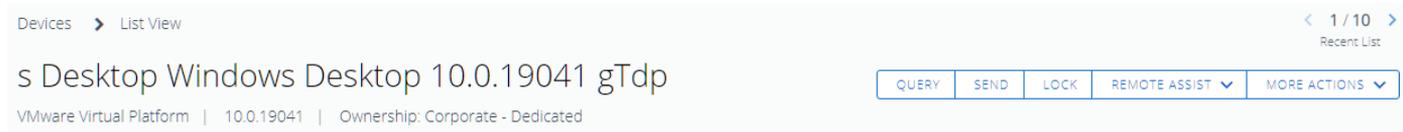
若要存取裝置詳細資料，可在任一個可用的儀表板上選取裝置暱稱，或是利用 Workspace ONE UEM Console 上可用的搜尋工具。**暱稱**是您指派給裝置的標籤，藉此協助您區分與其相同品牌和型號的裝置。

主要頁面主要區段

- **通知標誌** – 可顯示出遭破解狀態、違反合規、註冊日期、所選裝置上次顯示時間，以及 GPS/位置服務可用性 (僅限 Android 裝置)。
- **安全性** – 顯示安全性設定，例如使用哪種管理軟體註冊、密碼狀態和資料防護等。
 - 如果您使用 Web 應用程式或 Container 應用程式來註冊裝置，並在稍後下載及在裝置上執行 Workspace ONE Intelligent Hub 應用程式，則「由 Container 管理」指示器會變更為「已註冊的 Hub」，以反映 Workspace ONE Intelligent Hub 的存在。
- **使用者資訊** – 顯示基本使用者資訊，包括其全名和 Email。
- **裝置資訊** – 顯示裝置詳細資訊，例如組織群組、地點、智慧群組、序號與其他識別標籤、電源狀態、儲存空間容量、實體記憶體、保固資訊、上次重新開機時間 (僅 Android)，以及以英文字母順序排列的裝置標記。電池健全狀況僅適用於 Zebra Android 裝置。
- **設定檔** – 顯示所有設定檔，例如已安裝 (使用中)、已指派 (非使用中) 及未納管 (已側載)。
- **APP** – 顯示所有已安裝的 APP，包括自動化 APP 和隨選 APP。
- **內容** – 顯示 Workspace ONE UEM 所管理存放庫以及管理員存放庫中，由管理員標示為「必要」的內容。
- **憑證** – 列出所有已安裝的憑證，包括快要過期的憑證。
- **管理員應用程式** – 顯示已安裝的 Workspace ONE Intelligent Hub 資訊，包括版本編號。
- **Zebra 電池資訊** (僅適用於 Zebra Android 裝置) – 顯示詳細電池資訊，包括電池健康情形、製造日期、序號，以及零件編號。

裝置明細儀表板

儀表板會顯示基本裝置資訊，例如裝置暱稱。其他基本裝置資訊包括裝置類型、裝置型號、作業系統版本編號、擁有權類型、裝置動作按鈕叢集，以及近期清單指示器。



選擇**近期清單**顯示器的箭號按鈕，就會根據其在已篩選**清單檢視**中的位置，變更所選裝置。

您也可以合格的裝置上啟動**遠端協助**工作階段。如需詳細資訊，請參閱**遠端協助**。

功能表標籤

功能表標籤	描述
摘要	檢視一般統計資料，例如應用程式、可用作業系統更新、憑證、內容、裝置資訊、安全性、時間範圍和使用者資訊。
合規性	顯示狀態、原則名稱、過去和未來的合規性檢查日期，以及已在裝置上執行的動作。 合規性 標籤包括進階的疑難排解和各種便於使用的功能。 <ul style="list-style-type: none"> ■ 有各種可供違規裝置和合規狀態擱置中的裝置所使用的疑難排解功能。您可逐一檢視每台裝置以重新評估合規性 () 或取得裝置上合規狀態的相關詳細資訊 ()。 ■ 具有唯讀權限的使用者可以直接從合規性標籤中檢視特定的合規原則，管理員則可編寫合規原則。
設定檔	檢視裝置上目前所有已指派、已安裝及未納管的設定檔。
APP	檢視目前所有已指派和已安裝在裝置上的 APP。 APP 合規性 欄會列出不符合 SDK APP 合規性設定的 SDK 建置應用程式。如要檢視這些設定，請導覽至 群組與設定 > 所有設定 > 設定和原則 > SDK 應用程式合規性 。
內容	在 Workspace ONE UEM 受管理存放庫內，檢視由管理員標示為「必要」之裝置的狀態、類型、名稱、版本、優先順序、部署、上次更新時間、日期、檢視時間和內容。此標籤也提供管理動作的工具列 (安裝或刪除)。
位置	檢視裝置目前的位置或位置記錄。選取 期間 或者要在 搜尋 中回顧位置資料點的時間長度。請以 5 分鐘作為單位來選取自訂期間的長度。您也可以將游標移到地圖中的位置標記上方，藉此檢閱這些資料點的緯度和經度座標。 若要允許收集位置資料，請導覽至 群組 & 設定 > 所有設定 > 裝置 & 使用者 ，並依據特定平台來選取 Hub 設定 頁面。如需有關位置資料及其隱私權的進一步資訊，請參閱 隱私權最佳作法 。 若要編輯所要收集的位置資料點數量，以及兩位置間的最小距離，請導覽至 群組與設定 > 所有設定 > 安裝 > 地圖 。
使用者	存取有關裝置使用者的詳細資料，以及在此使用者之下註冊的其他裝置狀態。
時間範圍	檢視指派給裝置之時間範圍的相關詳細資訊，包括同步狀態、已套用的狀態、時間和排程詳細資料。 您可以引導終端使用者從 Workspace ONE Intelligent Hub 應用程式中選取 同步裝置 ，即會更新同步狀態。 當最低記錄層級設定為 資訊 或 偵錯 時，時間範圍事件便會由事件記錄器進行記錄。如需詳細資訊，請參閱 事件記錄 。

功能表標籤	描述
更多	<p>這些額外的功能表標籤會依據裝置平台而有所不同。</p> <ul style="list-style-type: none"> ■ 網路 – 檢視裝置目前的網路資訊 (行動、Wi-Fi、藍牙、IMEI)。 ■ 安全性 – 根據安全性設定，檢視裝置目前的安全狀態。 ■ 電信 – 檢視通話、資料以及訊息傳送與接收的數量。 ■ 備註 – 檢視並新增與裝置有關的備註。例如，備註說明運送狀態或該裝置是否已送修且不敷使用。 ■ 憑證 – 以名稱和發行者來辨別裝置憑證。此標籤也提供憑證到期日。 ■ 產品 – 檢視佈建於裝置上所有產品套件的完整歷程記錄和狀態，以及任何佈建錯誤。您也可以強制重新處理 (重新部署) 產品。 ■ 使用條款 – 檢視在裝置註冊時所接受的「終端使用者授權合約」(EULA) 清單。
多個，續上頁。	<ul style="list-style-type: none"> ■ 警示 – 檢視全部與裝置有關的警示訊息。 ■ 書籍 – 檢視裝置內的所有內部書籍。 ■ 共用裝置記錄 – 檢視共用裝置的歷程記錄，包括以往簽入和簽出的記錄，以及目前的狀態。 ■ 限制 – 檢視所有目前套用至裝置限制。此標籤也會依裝置、APP、評分和密碼顯示特定限制。 ■ 狀態記錄 – 檢視有關註冊狀態的裝置歷程記錄。 ■ 目標記錄 – 檢視主控台、目錄、裝置服務、裝置管理和自助入口網站之記錄。您必須在設定中啟用「目標記錄」，系統會提供此用途的連結。然後，您必須選取建立新的記錄按鈕，並選取收集記錄的時間長度。 ■ 疑難排解 – 檢視事件記錄和指令記錄資訊。此頁面具有匯出和搜尋功能，讓您能夠執行目標搜尋和分析。 <ul style="list-style-type: none"> ■ 事件記錄 – 檢視詳細的偵錯資訊和伺服器簽入，包括各種事件群組類型、各種日期範圍、各種嚴重性、各種模組與各種類別的篩選。 <p>在事件記錄清單中，事件資料欄位可能會顯示超連結，它會開啟另一個畫面，顯示與特定事件相關的詳細資料。這些資訊讓您能夠執行進階的疑難排解功能，例如決定無法安裝設定檔的原因。</p> ■ 指令 – 檢視已傳送到裝置，且處於擱置中、已佇列及已完成等狀態之指令的詳細清單。內含篩選器，供您依據類別、狀態及特定指令篩選指令。 ■ 附件 – 使用此伺服器上的儲存空間供螢幕擷取畫面、文件、顯示 Intelligent Hub 傳送的 Hub 記錄，以及用於疑難排解和其他目的的連結使用，且不會佔用裝置本身的空間。 ■ 入侵偵測 – 檢視關於裝置遭破解狀態的詳細資訊，包括狀態的特定原因和嚴重程度。

您必須先註冊裝置，才能透過 Workspace ONE UEM powered by AirWatch 管理該裝置。目前有多個註冊路徑，每個路徑亦提供不同的註冊選項。

不應在全域註冊裝置的原因

將裝置直接註冊到最上層企業群組 (OG) (通常稱為全域)，並不是好做法，原因如下。多租戶、繼承和功能。

多租戶

您可根據需要盡可能建立子企業群組，並配置為可獨立於其他群組。套用至子 OG 的設定不影響其他同層級。

繼承

對父層級 OG 所做的變更會套用至子層級。相反的，對子層級 OG 所做的變更，不會套用至父層級或同層級。

功能

有些設定和功能只能在客戶類型企業群組中配置，包括抹除保護、電信和個人內容。直接新增至最上層全域 OG 的裝置，會從這些設定和功能中排除。

全域企業群組 (OG) 旨在為客戶和其他類型的 OG 提供服務。鑑於繼承原理，若將裝置新增到全域，並根據該裝置所屬的設定配置全域，則將另外影響到以下所有客戶 OG。此舉將削弱多租戶和繼承的優點。

本章節討論下列主題：

- [透過 Workspace ONE Intelligent Hub 註冊裝置](#)
- [其他註冊工作流程](#)
- [其他註冊限制](#)
- [自動探索註冊](#)
- [基本註冊與目錄服務註冊](#)
- [自攜裝置 \(BYOD\) 註冊](#)
- [配置註冊選項](#)
- [封鎖清單和允許清單裝置登錄](#)

- 裝置登記
- 註冊狀態
- 自我註冊與裝置註冊預備
- 使用者註冊企業群組優先順序
- [Workspace ONE 直接註冊](#)

透過 Workspace ONE Intelligent Hub 註冊裝置

在 Workspace ONE Express 與 Workspace ONE UEM powered by AirWatch 中，透過 Workspace ONE Intelligent Hub 註冊裝置是 Android、iOS 與 Windows 等裝置的主要選項。

程序

- 1 從 Google Play 商店 (適用於 Android 裝置) 或從 App Store (適用於 Apple 裝置) 下載並安裝 Workspace ONE Intelligent Hub。

若要從公用的應用程式商店中下載 Workspace ONE Intelligent Hub，則必須有 Apple ID 或 Google 帳戶。

Windows 10 裝置必須將裝置上的預設瀏覽器指向 <https://getwsone.com> 以下載 Hub。

- 2 完成下載後，執行 Workspace ONE Intelligent Hub 或返回瀏覽器工作階段。

重要 若要確保 Workspace ONE Intelligent Hub 在 Android 裝置上安裝成功且順利執行，必須至少具有 60 MB 的可用空間。CPU 與執行時間記憶體會根據 Android 平台上的 APP 而配置。如果應用程式使用的資源多於配置的量，Android 裝置會結束這類應用程式以顧及整體的最佳化。。

- 3 出現提示時，請輸入您的電子郵件地址。Workspace ONE console 會檢查您先前是否曾把您的地址加入環境中。如果是，則表示系統已將您配置為終端使用者，而您的企業群組也已獲得指派。

如果 Workspace ONE console 無法依據您的電子郵件地址來識別您的終端使用者身份，就會提示您輸入**伺服器**、**群組 ID** 和**認證**。如果需要環境 URL 和群組 ID，您的 Workspace ONE 管理員可提供此類資訊。

- 4 依照所有剩餘的提示完成註冊。您可以使用電子郵件地址取代使用者名稱。如果兩個使用者擁有相同的電子郵件，註冊會失敗。

結果

裝置現在已透過 Workspace ONE Intelligent Hub 應用程式註冊。在此裝置的**裝置詳細資料視圖**的**摘要索引標籤**中，[安全性] 面板會顯示「已註冊的 Hub」以反映此註冊方法。

更多相關的資訊，請參閱 [第 8 章 裝置明細](#)。

其他註冊工作流程

在某些特殊情況下，Workspace ONE UEM powered by AirWatch 的註冊程序必須依照特定的企業和部署稍作調整。對於其他的每個註冊選項，終端使用者必須使用此指南在必要資訊的部分所敘述的認證。

- **多重網域環境** – 單一和多重網域環境的註冊登入在採用下列格式時可獲得支援。**網域\使用者名稱**。
- **Kiosk 模式和 Kiosk 設計工具** – Windows 桌面的終端使用者可以在 Kiosk 模式中設定桌面裝置。使用者也可使用 Kiosk 設計工具，在 Workspace ONE UEM 主控台中建立具有多項 App 的 Kiosk。
- **通知提示註冊** – 終端使用者收到含有註冊 URL 的通知 (Email 和 SMS)，然後輸入其群組 ID 和登入認證。當終端使用者接受使用條款 (TOU) 時，裝置會自動註冊並裝備所有 MDM 功能和內容。接受的內容包括 Workspace ONE UEM 伺服器的特定 APP 和功能。
- **單擊註冊** – 在此工作流程中，管理員會將 Workspace ONE UEM 所產生的 Token 以及註冊連結 URL 寄送給使用者；此流程也適用於 Web 式註冊。使用者只需選取所提供的連結，即可驗證和註冊裝置，對於終端使用者來說，此註冊程序可說是既簡單又快速。也可透過設定到期時間來確保此方法的安全。
 - **Web 註冊** – 管理員可以選擇性地在使用的環境中附加「/enroll/welcome」來為 Web 註冊叫用歡迎畫面。例如：為參與 Web 註冊的使用者提供 URL **https://<custenvironment > /enroll/welcome**，他們就會看到歡迎使用 Workspace ONE UEM 的畫面。此畫面包含使用 Email 地址或群組 ID 註冊的選項。Web 註冊選項適用於 Workspace ONE UEM 8.0 以上版本。
- **雙重要素驗證** – 在此工作流程中，管理員會將 Workspace ONE UEM 所產生的註冊 Token 傳送給使用者；但是，使用者還是需要輸入其登入認證。此執行方式就和單擊註冊一樣簡單，但安全性層級還要再提高一級。此額外的安全措施需要使用者輸入他們專用的認證。
- **終端使用者登記** – 使用者登入自助入口網站 (SSP)，並登記其個人所屬的裝置。登記完畢後，系統便會傳送一封含有註冊 URL 和登入認證的 Email 給終端使用者。此工作流程假設管理員尚未針對企業裝置團隊執行裝置登記，並也假設您規定企業裝置都必須註冊，這樣管理員才能追蹤註冊狀態。此外，終端使用者登記也表示企業裝置可與使用者購買的裝置搭配使用。
- **單一使用者裝置的註冊預備** – 管理員以某終端使用者的身份代理註冊裝置。當管理員需為整個團隊或團隊中的個別成員設定多個裝置時，本方法很實用。終端使用者若要註冊自己的裝置，使用此方法可說是省時又省力。管理員也可以先配置並註冊某個裝置，再將該裝置直接寄送給在外地的使用者。
- **多使用者裝置的註冊預備** – 管理員為多位使用者所使用的裝置進行註冊。每台裝置都會透過特定的一組功能來進行註冊與佈建，只有透過使用者專用的認證登入後才可存取這些功能。

其他註冊限制

您可以設定其他限制，以控管哪些人可以在 Workspace ONE UEM 註冊，以及允許的裝置類型。

其他裝置限制可套用至任何部署，無論是目錄服務整合、BYOD 支援、裝置登記還是其它配置。

您也可決定每個企業群組的最大註冊裝置數。配置註冊限制後，還可將這些限制另存為原則。

考量項目 #1：您是否會限制特定平台、OS 版本或允許裝置的最大數量？

- 您是否只會支援那些功能已內建於企業管理中的裝置，例如 Samsung SAFE/Knox、HTC Sense、LG Enterprise 和 Motorola 的裝置？如果是，您可以要求 Android 裝置必須具有支援的企業版本以作為註冊限制。
- 您是否要限制使用者允許註冊的裝置數量上限？如果是，您可以設定此數量，也可以明確指定公司專用裝置與員工自有裝置。
- 您的部署是否不支援特定平台？如果有，您可以建立一個清單，列出要封鎖的裝置平台並禁止他們註冊。

企業必須評估員工擁有的裝置數量和種類。還必須決定哪些裝置要在工作環境中使用。完成此工作後，可將這些註冊限制另存為原則。

考量項目 #2：您是否會將註冊限制為公司裝置的集合清單？

這些額外的登記選項能針對終端使用者所能註冊的裝置提供控制項。有助於容納 BYOD 部署，可防止列入封鎖清單的裝置註冊，或限制只有列入允許清單的裝置才能註冊。您可依類型、平台或特定裝置 ID 和序號，將裝置列入允許清單。更多相關的資訊，請參閱 [封鎖清單和允許清單裝置登錄](#)。

考量項目 #3：您是否會根據企業群組限制註冊裝置的數量？

您可以為特定的企業群組 (OG) 套用註冊裝置的數量限制。實施這樣的限制可以避免您超過有效的註冊數量，有助於管理部署。如需詳細資訊，請參閱此頁面中標題為**限制每個企業群組註冊的裝置數目**的區段。

配置註冊限制設定

整合 Workspace ONE UEM 與目錄服務時，您可以決定哪些使用者可以向您的企業部署註冊裝置。

您可以限制為只有已知的使用者或已配置的群組才能註冊。已知的使用者就是 UEM 主控台上現有的使用者。如果您選擇與使用者群組整合，則配置的群組指的就是與目錄服務群組關聯的使用者。您也可以根據企業群組來限制可註冊的裝置數量，並將限制儲存為可重複使用的原則。

若要使用這些選項，請導覽至**群組 & 設定 > 所有設定 > 裝置 & 使用者 > 一般 > 註冊**，然後選取**限制索引**標籤。限制標籤，讓您能夠按照企業群組和使用者群組身份來自訂註冊之限制原則。

- 使用「原則設定」來建立並指派現有的註冊限制原則。
- 在「群組指派設定」區域之下，將原則指派給一個使用者群組。
- 依照平台、作業系統、UDID、IMEI 等，將裝置列入封鎖清單或允許清單。

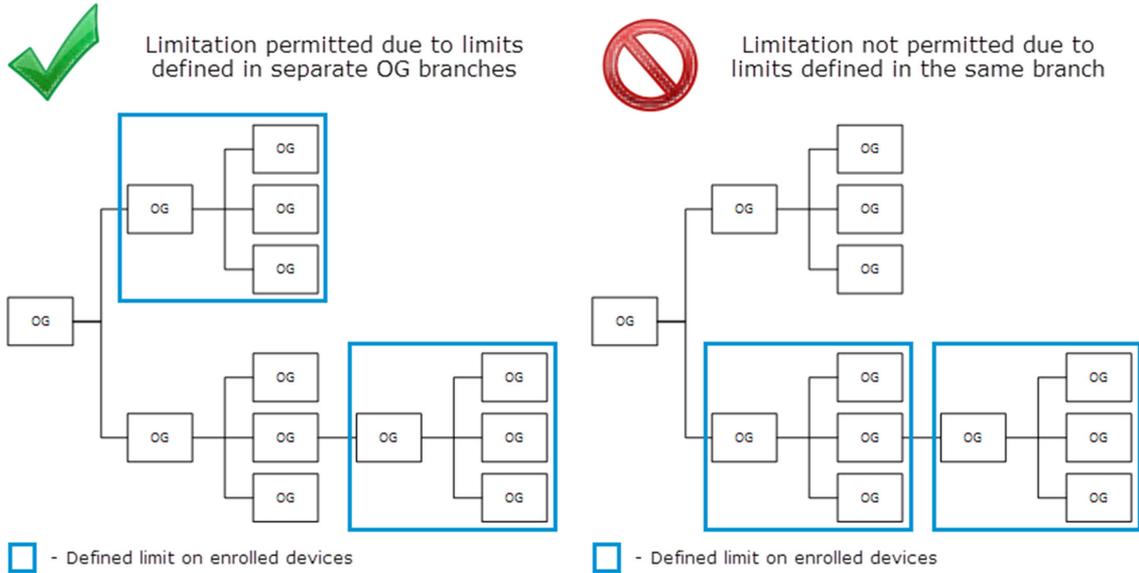
設定	描述
使用者存取控制	<p>Workspace ONE 直接註冊支援所有使用者存取控制選項。</p> <p>限制已知使用者才可註冊 – 啟用此選項會限制僅有 UEM 主控台中現有的使用者才可註冊。這個註冊選項適用於由您手動逐一加入或批次匯入 UEM 主控台目錄的使用者。當初始部署 (初始部署允許任何人註冊) 完成後，您也可利用此功能來鎖定註冊。此選項讓您可選擇能註冊的人員。</p> <p>您可以停用此選項，以允許沒有 UEM 主控台帳戶的所有目錄使用者向 Workspace ONE UEM 註冊。註冊時便會自動建立使用者帳戶。</p> <p>僅限已配置使用者註冊 – 啟用此選項，則僅有屬於「所有群組」或「所選群組」的使用者才可以註冊裝置 (如果您已與使用者群組進行整合)。如果您尚未與您的目錄服務使用者群組進行整合，請勿選取此項目。</p> <p>備註 僅在下列每個條件皆為 true 時，才支援 [限制讓已配置的群組註冊] 有 Just-In-Time (JIT) 使用者註冊：</p> <ul style="list-style-type: none"> ■ 若要將 Workspace ONE UEM 設定為 Workspace ONE Intelligent Hub 的驗證來源，請導覽至 群組 & 設定 > 所有設定 > 裝置 & 使用者 > 一般 > 註冊，然後選取 驗證 標籤。 ■ 註冊使用者用於驗證的 SAML 已停用。若要進行此設定，請導覽至 群組 & 設定 > 所有設定 > 系統 > 企業整合 > 目錄服務，並參考 目錄服務系統設定說明文件。 <p>停用讓所有目錄使用者註冊的選項，即可在註冊期間建立 Workspace ONE UEM 使用者帳戶。選取 對不屬於已配置群組中的使用者所擁有的裝置進行企業抹除，將會對相關裝置自動執行企業抹除。如果選取 所有群組，將會移除不屬於任何使用者群組的裝置。如果選取 所選的群組，則會移除不屬於特定使用者群組的裝置。</p> <p>與使用者群組整合的一個選項是建立「MDM 核准的」目錄服務群組，並將群組匯入 Workspace ONE UEM。執行此匯入步驟後，您可以將現有的目錄服務使用者群組新增到「MDM 核准的」群組，因為這些群組有資格使用 Workspace ONE UEM。</p>
設定此 OG 以下的註冊裝置上限	<p>啟用並輸入 裝置限制，即可限制可於目前企業群組中 (OG) 註冊的裝置數量。</p> <p>Workspace ONE 直接註冊支援此選項。</p>

備註 透過 Apple 的裝置註冊計劃 (DEP) 而註冊的 iOS 裝置，將無法套用這些限制，因為這些裝置只有在註冊後才能收到必要的裝置資訊。

限制每個企業群組註冊的裝置數目

您可以為特定的企業群組 (OG) 套用註冊裝置的數量限制。實施這樣的限制可以避免您在按裝置授權的環境中超過有效的註冊數量，有助於管理部署。

這項裝置限制可以施加於各類 OG (全域、客戶、夥伴)。為一個 OG 設定限制後，將無法在同一個 OG 分支的任何位置設定另一個限制。除非在單獨的 OG 分支中設定限制，否則無法為其他已註冊的裝置設定限制。



如果此選項不可使用，請檢查父系 OG (高於目前的 OG) 或子 OG (低於目前的 OG)。目前 OG 的上層或下層可能已定義了現有的限制。

- 1 導覽至**群組 & 設定 > 所有設定 > 裝置 & 使用者 > 一般 > 註冊**，然後選取**限制**索引標籤。
- 2 在設定此企業群組和其下的註冊裝置數目上限下啟用限制。

建立註冊限制原則

企業必須評估員工擁有的裝置數量和種類。他們還必須決定要在您工作環境中使用的裝置。完成此工作後，可將這些註冊限制另存為原則。

- 1 導覽至**裝置 > 裝置設定 > 裝置與使用者 > 一般 > 註冊**。
- 2 選擇**限制**標籤，然後選擇在**原則設定**區塊中的**新增原則**。
- 3 在**新增/編輯註冊限制原則**畫面中新增註冊限制原則。

設定	描述
註冊限制原則名稱	輸入您註冊限制原則之名稱。
OrganizationGroup	從下拉式功能表中選取企業群組。此為您新的註冊限制原則所要套用的企業群組。
原則類型	選擇「註冊限制原則」的類型，此類型可以是套用在所選企業群組上的 企業群組預設值 ；或是透過 限制 標籤中的群組指派設定，套用在特定使用者群組上的 使用者群組原則 。
AllowedOwnership 類型	選擇允許使用或禁用 公司 - 專用 、 公司 - 共用 和 員工自有 的裝置。 Workspace ONE 直接註冊僅支援 公司專用 和 員工自有 這兩種擁有權類型。
AllowedEnrollment 類型	選取要允許使用或禁用以 MDM (Workspace ONE Intelligent Hub) 和 AirWatch 容器 (適用 iOS/Android) 等 App 註冊裝置。

設定	描述
依據使用者設定裝置限制	<p>選取無限制來允許使用者註冊他們想要註冊的任何裝置數量。Workspace ONE 直接註冊支援設定每位使用者的裝置限制。</p> <p>取消勾選此方格，並於每位使用者的裝置限制區段中輸入數值，即可定義每種擁有權類型的裝置數量上限。</p> <ul style="list-style-type: none"> ■ 每個使用者可用的裝置數量上限 ■ 企業裝置數量上限 ■ 共用裝置數量上限 ■ 員工自有裝置數量上限
允許的裝置類型	<p>勾選依據特定平台、型號及作業系統來限制註冊的方格，加入其他特定裝置的限制。Workspace ONE 直接註冊支援此選項。</p>
裝置等級限制模式	<p>僅當您已於允許裝置類型選項中選取依據特定平台、型號或作業系統來限制註冊，才能使用此選項。決定要限制的裝置類型。</p> <ul style="list-style-type: none"> ■ 僅允許列出的裝置類型 (允許清單) – 選擇此項目，僅明確允許使用符合您所輸入參數之裝置，並封鎖其他所有裝置。 ■ 封鎖列出的裝置類型 (封鎖清單) – 選擇此項目，明確地封鎖所有符合您所輸入參數之裝置，並允許使用其他所有裝置。 <p>針對其中任一種裝置層級的限制模式，請選取新增裝置限制並選擇一個平台、型號、製造商 (Android 裝置限定) 或作業系統。您也可以根據定義好的裝置限制來新增裝置數量限制。您可以加入數種裝置限制。</p> <p>您也可依照裝置的 IMEI、序號或 UDID 來封鎖特定的裝置，請導覽至裝置 > 生命週期 > 註冊狀態，然後選取新增。這是封鎖單獨一個裝置的有效方法並且可以禁止該裝置重新註冊，此方法並不會影響到其他使用者的裝置。在執行企業抹除時，禁止重新註冊也是其中一種可用的選項。</p> <p>Workspace ONE 直接註冊支援此選項。</p>

4 選取**儲存**以儲存您的變更，並導覽回**裝置與使用者/一般/註冊**畫面。

自動探索註冊

Workspace ONE UEM powered by AirWatch 使用電子郵件式自動探索系統，向環境與企業群組 (OG) 註冊裝置，進而簡化註冊程序。自動探索功能也能讓終端使用者向自助入口網站 (SSP) 驗證。

備註 若要啟用內部部署環境的自動探索功能，請先確定您的環境能夠與 Workspace ONE UEM 自動探索伺服器進行通訊。

自動探索註冊登記

伺服器會檢查 Email 網域的獨特性，只允許企業群組在相同的環境中登記一個網域。由於有這項伺服器檢查，因此請在您最高層級的企業群組登記您的網域。

系統會為軟體即服務 (SaaS) 的新客戶，自動配置自動探索功能。

從父企業群組配置自動探索註冊

自動探索註冊能使用終端使用者的 Email 地址，來簡化裝置向預期的環境與企業群組 (OG) 註冊的程序。

若要從父級 OG 配置自動探索註冊，請執行以下步驟。

- 1 導覽至**群組 & 設定 > 所有設定 > 管理員 > 雲端服務**並啟用**自動探索**設定。在**自動探索 AirWatch ID**中輸入您的登入 Email 地址並選取**設定身份識別**。
 - a 如有需要，請導覽至 <https://my.workspaceone.com/set-discovery-password> 為自動探索服務設定密碼。一旦完成登記並選取了**設定身份識別**，系統便會自動填入 **HMAC Token**。按一下**測試連線**以確定連線能正常運作。
- 2 啟用**自動探索證書固定**選項以上傳您的證書，然後將之固定到自動探索功能。您可以檢閱現有憑證的有效日期及其他資訊，也可以選擇**取代**和**清除**這些現有的憑證。
- 3 選取**新增證書**及設定**名稱**及**證書顯示**。輸入您要上傳之憑證的名稱，選取**上傳**按鈕，然後選取位於您裝置上的憑證。
- 4 選擇**儲存**以完成自動探索設定。

下一步：指示自行註冊的終端使用者，選擇使用電子郵件地址選項進行驗證，不需輸入環境 URL 和群組 ID。若使用者使用 Email 地址註冊裝置，會順便在相關使用者帳戶的**註冊企業群組**所列的同一個群組中註冊。

從子企業群組配置自動探索註冊

您可以從註冊企業群組下方的子企業群組，配置自動探索註冊。要以這種方式啟用自動探索註冊，您必須要求使用者在註冊期間選擇群組 ID。

強制使用者在註冊期間選擇群組 ID。

- 1 導覽至**裝置 > 裝置設定 > 一般 > 註冊**，然後選取**群組標籤**。
- 2 選取**提示使用者選取群組 ID**。
- 3 選取**儲存**。

基本註冊與目錄服務註冊

您可以註冊現有的使用者，以及 Active Directory (AD)、Lotus Domino 和 Novell e-Directory 等目錄服務群組。如果沒有該等基礎結構，或是選擇不與之整合，則必須在 Workspace ONE UEM 中執行基本註冊。

基礎註冊會參考手動建立使用者帳戶的程序，以及企業中各個使用者所屬的使用者群組。若您的企業未整合 Workspace ONE UEM 與目錄服務，則基本註冊是您建立使用者帳戶的方法。

如果您有多個基本帳戶需要建立，請按照[建立基本使用者帳戶](#)中所述的步驟，每次建立一個帳戶。

如果是包含較多終端使用者的基本註冊，為節省時間，您可以填寫並上傳 CSV (逗號分隔值) 範本檔案。這些檔案包含您新增的所有使用者資訊，並透過批次匯入功能引入 UEM。如需詳細資訊，請參閱[批次匯入使用者或裝置](#)主題。

備註 由於 Workspace ONE UEM 支援混用基本使用者與目錄式使用者，通常只需要使用其中一種，就能為使用者與裝置進行第一次註冊。

優點與缺點

	優點	缺點
基本註冊	<ul style="list-style-type: none"> ■ 可用於任何的部署方式。 ■ 不需任何技術整合。 ■ 不需任何企業基礎結構。 ■ 可以向潛在多個企業群組註冊。 	<ul style="list-style-type: none"> ■ 認證僅存在於 Workspace ONE UEM，而且未必符合現有的企業認證。 ■ 不提供聯合安全性。 ■ 不支援單一登入。 ■ Workspace ONE UEM 會儲存所有使用者名稱和密碼。 ■ 無法用於 Workspace ONE 直接註冊。
目錄服務註冊	<ul style="list-style-type: none"> ■ 終端使用者可以利用現有的企業憑證來進行驗證。 ■ 可自動偵測目錄系統的變更並同步至 Workspace ONE UEM。例如，停用 AD 中的使用者時，Workspace ONE UEM Console 中對應的使用者帳戶會標記為停用狀態。 ■ 能提供安全的方法來與現有的目錄服務整合。 ■ 標準的整合作法。 ■ 可用於 Workspace ONE 直接註冊。 ■ 使用 AirWatch Cloud Connector 的 SaaS 部署無需變更防火牆，並可為其他的基礎結構提供安全的組態，如 Microsoft ADCS、SCEP 和 SMTP 伺服器。 	<ul style="list-style-type: none"> ■ 需要現有的目錄服務基礎結構。 ■ 由於 AirWatch Cloud Connector 安裝在防火牆後方或 DMZ 之中，因此 SaaS 部署需要額外的組態。

註冊考量：基本與目錄比較

考量終端使用者註冊時，除了基本與目錄使用者的現有利弊之外，還要考量其他問題。

考量項目 #1：誰可以註冊？

回答這個問題時，請先考量下列事項。

- 為企業的所有使用者管理裝置而採用的 MDM 部署，其目的是否符合您配置的基本 DN*？如果是，那麼要達成這個目的，最簡單的方式就是不要勾選「限制註冊」方格，好讓所有的使用者都能註冊。
您可以允許所有使用者在初始部署推出期間註冊，之後再限制註冊，以防未知的使用者註冊。企業在現有的使用者群組新增新員工或成員時，這些變更將同步並合併。
- 是否未將某些使用者或群組加入 MDM？如果有的話，您就要逐一新增使用者，或是只將 CSV (逗號分隔值) 檔案中的合格使用者批次匯入。

* 基本 DN (「辨別名稱」的縮寫) 是伺服器搜尋使用者的起點。辨別名稱是專用來辨識目錄中某項目的唯一名稱。目錄中的每個項目都有一個 DN。

考量項目 #2：要在哪裡指派使用者？

整合 Workspace ONE UEM 環境與目錄服務時，還有另一件事情需要考量。那就是在註冊時，您打算如何將目錄使用者指派至企業群組。回答這個問題時，請先考量下列事項。

- 您是否已建立了在邏輯上與目錄服務群組相互對應的企業群組結構？您必須先完成此任務，才能編輯使用者群組指派。

- 如果使用者註冊自己的裝置，從清單選擇群組 ID 的選項很簡單。但在這種簡單的情況中，卻容易發生人為錯誤，並導致產生錯誤的群組指派。

您可以根據使用者群組來自動選取群組 ID，也可以允許使用者從清單中選取。若要選取上述的**群組 ID 指派模式**選項，請導覽至**裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 註冊**，然後選取**組成群組**標籤。

啟用目錄服務型註冊

目錄服務註冊是指整合 Workspace ONE UEM 與企業目錄服務基礎結構的程序。以這種方式整合目錄服務代表您可自動匯入使用者，以及像安全性群組和通訊群組清單的使用者群組 (選擇性)。

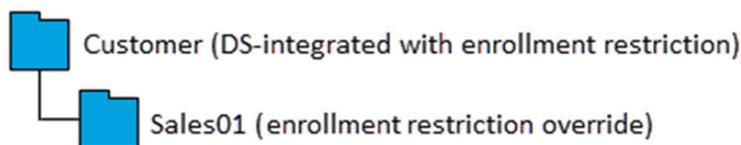
與 Active Directory (AD) 這類的目錄服務整合時，可以進一步選擇匯入使用者的方法。

- **允許所有目錄使用者註冊** – 您可以允許您目錄服務內的所有使用者進行註冊。此外，您可以根據使用者的 Email 自動探索使用者，以便設置環境。接著再於他們執行註冊時，為他們建立 Workspace ONE UEM 使用者帳戶。
- **逐一新增使用者** – 與目錄服務整合後，可個別新增使用者，方法如同建立基本 Workspace ONE UEM 使用者帳戶。唯一的區別在於，您只需要為其輸入使用者名稱，並選取**檢查使用者**，即可從您的目錄服務中將剩下的資訊自動填入。
- **批次上傳 CSV 檔案** – 使用此選項，您就可以使用 CSV (逗號分隔值) 範本檔案來匯入目錄服務帳戶的清單。該檔案具有特定欄位，有些不能留空。
- **透過使用者群組整合 (可選)** – 透過這個方法，您就能使用現有使用者群組成員資格來指派設定檔、APP、合規原則等等。

備註 如需 Workspace ONE UEM 環境與目錄服務之整合方法 (包括 SAML 提供者整合) 的相關資訊，請參閱[整合目錄服務指南](#)。

目錄服務整合和註冊限制

在 Workspace ONE UEM 配置目錄服務整合時，目錄服務帳戶會從經過配置的目錄服務中繼承企業群組 (OG) 的註冊設定。不過基本帳戶必須遵守本機設定，包括覆寫設定。



以上述企業群組模型為例，假設在名為「客戶」的 OG 上啟用**對自己配置群組移除之使用者所擁有的裝置進行企業抹除**的選項。

在此情況下，無論該 OG 配置的註冊限制覆寫設定為何，退出已配置之群組的 Sales01 子 OG 中的**目錄**註冊使用者皆會看到其裝置遭到抹除。雖然這些帳戶已經在其他 OG 註冊裝置，上述規則依然適用，因為註冊設定以使用者為依據，而非以裝置為依據。

但是，在相同例子中，裝置如果屬於 Sales01 OG 的**基本**註冊使用者，該使用者離開已配置的群組後，上述裝置並不會遭到抹除。這是因為 Sales01 中的基本註冊使用者並不屬於目錄服務整合後的 OG，因此可辨識並遵守覆寫的註冊限制。

自攜裝置 (BYOD) 註冊

管理 Workspace ONE UEM 中的使用者個人裝置時，最大的挑戰就是要去辨識與區分員工自有的裝置與公司專用的裝置，還要限制為只有核准的裝置才能註冊。

Workspace ONE UEM 讓您可配置各種選項，並針對註冊個人裝置自訂終端使用者體驗。但是在您開始前，您需要先考慮到自己如何在部署中識別出員工自有的裝置，以及是否要為員工自有的裝置強制實施註冊限制。

註冊注意事項

假設您允許員工在 Workspace ONE UEM 環境中註冊個人裝置，在進行下一步前，有許多因素必須考量。

考量項目 #1: BYOD 使用者會使用 VMware Workspace ONE 還是 Workspace ONE Intelligent Hub 註冊?

VMware Workspace ONE 是安全的企業平台，可在各種裝置上傳送並管理任何 APP。從自助式和單一登入存取，到雲端、行動和 Windows APP，甚至包含了完全整合的 Email、行事曆、檔案和協作工具等等。

有了 Workspace ONE，使用者不需註冊個人裝置也能夠存取服務。Workspace ONE APP 本身可從 Apple App Store、Google Play 或 Microsoft Store 下載並安裝。然後使用者登入並根據建立的原則存取應用程式。Workspace ONE APP 在安裝時就會配置好 MDM 管理設定檔，以便自動註冊裝置。

考量項目 #2: 您是否會為員工自有的裝置套用其他註冊限制?

回答這個問題之前，請先考量下列事項。

- 您的 MDM 部署是否只支援特定的裝置平台？如果是，則您可以指定這些平台，並僅允許執行這類平台的裝置註冊。
- 您是否會限制員工所能註冊的個人裝置數量？如果會，您可以指定每位員工所能註冊的個人裝置數量上限。

您可以設定其他限制，以進一步控管可以允許哪些人和裝置類型進行註冊。例如，您可以選擇只支援具有內建企業管理功能的 Android 裝置。在貴企業做完評估，並且決定哪種員工自有裝置適用於工作環境後，您便可配置這些設定。

識別企業裝置與指定預設的裝置所有權

如果您擁有公司專用裝置和員工自有裝置 (員工自己註冊)，準備一張裝置清單將非常實用。註冊開始後，您識別為公司專用的裝置將根據您選擇的內容自動配置其所有權類型。然後，您可配置員工自有的所有裝置 (不在清單中)，並將所有權類型註冊為員工自有。

以下程序將說明如何匯入預先核准的公司裝置清單。即使您對自動套用員工自有所有權類型設定限制，仍可在自動註冊後，套用企業專用所有權類型。

相反的，開放註冊的限制會明確地允許或封鎖符合您所辨識之參數的裝置註冊，包含平台、型號和作業系統。

- 1 導覽至**裝置 > 生命週期 > 註冊狀態**，選取**新增**，然後再選取**批次匯入**以便顯示**批次匯入**畫面。
或者，您也可以選取**新增**，然後選取**允許清單裝置**，按 IMEI、UDID 或序號輸入要加入允許清單的裝置，一次最多可以輸入 30 個裝置。您也可將**所有權類型**選為公司專用或公司共用。
- 2 輸入**批次名稱**和**批次描述**，然後選取**新增允許清單裝置**作為**批次類型**。
- 3 選取標題為「下載範本 (含有允許清單裝置的範例)」的連結，並將這份逗點分隔值 (CSV) 範本儲存到您可存取的位置。使用 Excel 編輯此 CSV 檔案，以便新增所有想列入允許清單的裝置，然後儲存檔案。
- 4 選取**選擇檔案**，然後選取已儲存的 CSV 檔案。
- 5 選取**匯入**，將此裝置資訊匯入至允許清單。
- 6 針對所有開放的註冊，將**預設裝置所有權類型**設定為員工自有。
 - a 導覽至**裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 註冊**，然後選取**分組**標籤。
 - b 選取**員工自有**作為**預設裝置所有權**。
 - c 選取要指派給使用者的**預設身份**，用來決定使用者對自助入口網站 (SSP) 的存取層級。
 - d 為**非使用中使用者**選取**預設動作**，以決定當使用標示為非使用中時應採取什麼動作。
 - e 選取**儲存**。

提示使用者識別所有權類型

如果部署有企業群組，其中具有多種擁有權類型，您可提示使用者在註冊期間識別自己的擁有權類型。允許使用者選擇自己的擁有權類型之前，請務必審慎考慮。

雖然簡單，但這個方法會假設每位使用者都會正確為其裝置選取合適的擁有權類型。如果個人裝置使用者錯誤選取公司專用類型，則其裝置將受到通常不適用於個人裝置的原則和設定檔約束。這類錯誤選擇可能對使用者的隱私權，造成嚴重的法律問題。

您可在日後隨時更新個人裝置的所有權類型，但是列出公司裝置將更加安全有保障。然後分別註冊企業專用裝置，之後所有權類型預設值設為員工自有。

- 1 導覽至**裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 註冊**，然後選取**選取性提示**標籤。
- 2 選取**提示裝置擁有權類型**。註冊期間，系統會提示使用者選取其擁有權類型。
- 3 選取**儲存**。

配置註冊選項

您可以透過結合 Workspace ONE UEM 中可用的進階選項，自訂您的註冊工作流程。

若要存取更多註冊選項，請導覽至**裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 註冊**。

使用入門

設定	描述
新增電子郵件網域	此按鈕用來設定自動探索服務，向您的環境註冊 Email 網域。
驗證模式	<p>選取允許的驗證類型，包括：</p> <ul style="list-style-type: none"> ■ 基本 – 基本使用者帳戶 (您在 UEM 主控台中手動建立的帳戶) 可進行註冊。 ■ 目錄 – 目錄使用者帳戶 (您已匯入或允許使用目錄服務整合的帳戶) 可進行註冊。Workspace ONE 直接註冊支援具有或不具 SAML 的目錄使用者。 ■ Authentication Proxy – 可讓使用者使用 Authentication Proxy 使用者帳戶進行註冊。使用者會向 Web 端點進行驗證。 <ul style="list-style-type: none"> ■ 輸入 Authentication Proxy URL、Authentication Proxy URL 備份和驗證方法類型 (從 HTTP Basic 和 Exchange ActiveSync 之間加以選擇)。
Intelligent Hub 的驗證來源	<p>選擇使用 Intelligent Hub 服務做為其使用者和驗證原則來源的系統。</p> <ul style="list-style-type: none"> ■ Workspace ONE UEM – 如果您想要讓 Hub 服務使用 Workspace ONE UEM 作為使用者和驗證原則的來源，請選取此設定。 <p>設定 Hub 服務適用的 Hub 組態 頁面時，請輸入 Hub 服務租用戶 URL。</p> <ul style="list-style-type: none"> ■ Workspace ONE Access – 如果您想要讓 Hub 服務使用 Workspace ONE Access 作為使用者和驗證原則的來源，請選取此設定。 <p>設定 Hub 服務適用的 Hub 組態 頁面時，請輸入 Workspace ONE Access 租用戶 URL。</p> <p>如需 Workspace ONE Intelligent Hub 的相關詳細資訊，請參閱 VMware Workspace ONE Hub 服務說明文件。</p> <p>如需 Workspace ONE Access 的相關詳細資訊，請參閱 VMware Workspace ONE Access 說明文件。</p>
裝置註冊模式	<p>選取偏好的裝置註冊模式，其中包括：</p> <ul style="list-style-type: none"> ■ 開放式註冊 – 基本上允許符合其他註冊準則 (驗證模式、限制等) 的任何人進行註冊。Workspace ONE 直接至冊支援開放式註冊。 ■ 僅限已登錄的裝置 – 僅允許使用者使用已由您或他們登錄的裝置進行註冊。裝置登錄是在公司裝置註冊之前新增至 UEM 主控台的程序。Workspace ONE 直接註冊支援僅允許已登錄裝置進行註冊，但前提是此情況不需要提供登錄 Token。
需要註冊 Token	<p>只有在已選取僅限已登錄的裝置時，才會顯示。</p> <p>若您僅限已登錄的裝置進行註冊，則您還可以選擇要求使用登錄 Token 進行註冊。此選項可藉由確認特定使用者有權進行註冊，而提升安全性。您可以透過 Workspace ONE UEM 帳戶，將附加了註冊 Token 的 Email 或 SMS 訊息傳送給使用者。</p>
要求 iOS 使用 Intelligent Hub 註冊	選取此核取方塊，會要求 iOS 裝置使用者必須先下載並安裝 Workspace ONE Intelligent Hub，才可以註冊。若停用，將使用 Web 註冊。
要求 macOS 使用 Intelligent Hub 註冊	選取此核取方塊，會要求 macOS 裝置使用者必須先下載並安裝 Workspace ONE Intelligent Hub，才可以註冊。若停用，將使用 Web 註冊。

在 Hub 整合上配置註冊選項

「Hub 整合」可讓使用者在 OG 樹狀結構的任何子系 OG 層級上啟用或停用 Hub 服務體驗。

如需詳細資訊，請參閱 [Workspace ONE Hub 服務說明文件](#)。

設定	描述
在 Intelligent Hub 中使用 Hub 服務功能	啟用以允許此 OG 中的裝置連結至 Workspace ONE Hub 服務 ，以使用統一應用程式目錄、支援、終端使用者通知、 People 和首頁索引標籤等功能。 停用以使裝置在管理模式 (僅代理程式模式) 下運作。例如，使用 Intelligent Hub 和 Workspace ONE Access 進行驗證，但不使用業務線堅固裝置中使用的 Hub 服務功能 。

在 [使用條款] 索引標籤中配置註冊選項

使用條款索引標籤可讓您新增並檢閱與註冊相關的使用條款。導覽至 **裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 註冊**，即可找到使用條款標籤。

設定	描述
必須接受註冊使用條款	啟用此設定，即可要求使用者在註冊時接受使用條款合約。
新增註冊使用條款	選取以開始新增註冊時必須接受的使用條款合約。

重要 如果您啟用 **必須接受註冊使用條款**，則必須建立使用條款，否則 **Windows** 桌面的裝置可能無法註冊。

在分組標籤上配置註冊選項

分組的標籤，讓您可以檢視並指定有關終端使用者之企業群組和群組 ID 的基本資訊。啟用 **群組 ID 指派模式**，讓您可以選取 **Workspace ONE UEM powered by AirWatch** 環境如何將群組 ID 指派給使用者。

導覽至 **裝置 > 裝置設定 > 裝置與使用者 > 一般 > 註冊**，即可找到分組索引標籤。

設定	描述
群組 ID 指派模式	<p>Workspace ONE 的直接註冊支援所有指派模式。</p> <ul style="list-style-type: none"> ■ 預設 - 如果您將提供使用者一個註冊用的群組 ID，請選取此項。群組 ID 會用來決定使用者將被指派到哪個企業群組。 ■ 提示使用者選取群組 ID - 啟用此選項來允許目錄服務使用者在註冊時，從清單上選取群組 ID。群組 ID 指派 區段，列出了可供使用的企業群組和相關的群組 ID。此清單不需要您執行群組指派對應動作，但的確意味著使用者有可能會選擇不正確的群組 ID。 ■ 依照使用者群組自動選取 - 此選項只適用在您與使用者群組進行整合的情況下。啟用此選項可以確保使用者能根據其目錄服務群組指派內容，而被自動指派給企業群組。 <p>群組指派設定 區段，列出了環境中的所有企業群組及其相關的目錄服務使用者群組。</p> <p>選取 編輯群組指派 按鈕以修改企業群組/使用者群組關聯性，並且設定每個群組應有的優先順序排名。</p> <p>舉例來說，您有三種以工作身份來排序之群組：高階主管、業務和全域。每個人都是「全域」之成員，所以如果您要將該使用者群組排名在第一順位，就會將您所有的使用者都置放在單一企業群組中。</p> <p>如果您將「高階主管」排名在第一順位，您可確保屬於該群組的少數成員可以置放在其專屬的企業群組中。如果您將「業務」排名在第二順位，您可確保所有業務員工可以置放在業務特定的企業群組中。將「全域」排名在第三順位，代表尚未指派給群組的任何人，都會置放在一個獨立的企業群組中。</p>

表 9-1. 預設值

設定	描述
預設裝置擁有權	選取註冊到目前企業群組之裝置的預設裝置擁有權。 Workspace ONE 直接註冊支援設定預設裝置擁有權。
預設身份	選取為目前企業群組中的使用者指派的預設身份，這會影響對自助入口網站的存取。 <ol style="list-style-type: none"> 完整存取權 – 授予使用者更高級 SSP 功能的存取權限，例如安裝/移除設定檔和 APP、重設密碼、傳送裝置訊息和內容寫入權限。 基本存取權 – 授予使用者影響較小的存取權限。使用者可登錄自己的裝置、單純檢視 (但不可安裝) 設定檔和 APP、檢視自己的帳戶，以及查詢及尋找自己的裝置。 外部存取權 – 擁有外部存取權的使用者可使用所有基本存取權使用者的功能。另外，若 SSP 內有明確與他們共用的內容，他們也會擁有這些內容的唯讀存取權限。 Workspace ONE 直接註冊支援設定預設角色。
非使用中使用者的預設動作	選取在 Active Directory 使用者的裝置變成非使用中狀態時，會對這些使用者造成影響的預設動作。 帳戶處理永遠以使用者為中心，而非以裝置為中心。這表示套用至裝置的處理行為是根據 OG 的設定，其中管理的是 使用者 ，不是裝置。 Workspace ONE 直接註冊支援設定非使用中使用者的預設動作。

表 9-2. 使用者群組：同步

設定	描述
為 Workspace ONE 即時同步使用者群組	Workspace ONE 可在指定的使用者透過 UEM 主控台進行登錄時同步其使用者群組。 此功能預設為啟用，在使用者群組經常用於 APP 指派、設定檔指派、原則指派或使用者對應時最有效用。 此功能會使用大量 CPU 資源，因此，除非您的使用案例類似於前述作業，否則請停用此設定，以改善效能，以及防止在啟動 Workspace ONE 應用程式時出現延遲問題。

表 9-3. 使用者身份關係對應

設定	描述
啟用目錄群組型的對應	選取此方塊，可啟用將目錄使用者群組連結至特定 Workspace ONE UEM 角色的排名式指派。系統會指派相關聯角色給屬於特定群組的使用者。屬於多個群組的使用者將會獲得最高排名配對。 您可以選取 編輯指派 按鈕，以編輯為已導入身份的使用者群組排名的順序。 Workspace ONE 的直接註冊支援目錄群組型的對應。

在選擇性提示標籤上配置註冊選項

在**選擇性提示**標籤上，可決定請求額外的裝置資訊，或向使用者顯示有關註冊和 MDM 資訊的選擇性訊息。

導覽至**裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 註冊**，然後選取**選取性提示**標籤。

配置訊息、範本和通知的特定指示列於下表之後。

設定	描述
提示裝置擁有權類型	您可提示終端使用者選取其裝置擁有權類型。或者，您也可以為目前的企業群組配置預設的裝置擁有權類型。 Workspace ONE 直接註冊支援裝置擁有權類型的提示。
顯示歡迎訊息	在裝置註冊過程之初，可顯示歡迎訊息來歡迎您的使用者。若要配置此歡迎訊息的標題和正文，請導覽至 系統 > 當地語系化 > 當地語系化編輯器 。接著，分別選取「EnrollmentWelcomeMessageHeader」和「EnrollmentWelcomeMessageBody」標籤。
顯示 MDM 安裝訊息	在裝置註冊過程中，可向您的使用者顯示訊息。若要配置此 MDM 安裝訊息的標題和正文，請導覽至 系統 > 當地語系化 > 當地語系化編輯器 。接著，分別選取「EnrollmentMdmInstallationMessageHeader」和「EnrollmentMdmInstallationMessageBody」標籤。 如果您選擇使用當地語系化編輯器來自訂您的標題和內文訊息，請記得在 目前的設定 中選取「覆寫」的選項。如此一來，便可確保系統會使用您的自訂訊息，而非預設的訊息。 除了進行單次性的當地語系化變更，您也可以藉由上傳已編輯的逗點分隔值 (CSV) 檔案，大量進行當地語系化變更。請導覽至 系統 > 當地語系化 > 當地語系化編輯器 ，然後選取 修改 按鈕，以下載此當地語系化範本 CSV 檔案。依據您的喜好編輯檔案以影響大規模的當地語系化變更，並使用相同的畫面上傳檔案。
啟用註冊 Email 提示	您可提示使用者在註冊過程中輸入其 Email 認證。 「註冊 Email 提示」會向終端使用者請求提供 Email 地址，以在使用者記錄中自動填入該選項。此資料對使用 {EmailAddress} 查閱值來將 Email 部署到裝置中的企業特別實用。
啟用裝置資產編號提示	您可提示使用者在註冊時輸入裝置資產編號。 Workspace ONE 直接註冊支援註冊電子郵件提示，但僅在啟用 設備所有權提示 類型且僅適用於公司所有設備時。
顯示註冊轉換訊息 (僅適用於 Android)	您可在 Android 裝置中顯示或隱藏註冊訊息。
啟用 OOBE 的狀態追蹤頁面	啟用此設定以顯示「可立即使用的註冊」(OOBE) 期間的狀態追蹤頁面，此頁面顯示裝置的佈建狀態，並告知使用者已安裝的應用程式、資源和原則。
啟用 Windows 的 TLS 相互驗證	您可強制 Windows 裝置使用受 TLS 相互驗證所保護的端點。這種方式需要額外設定和組態。請聯絡支援部門以取得協助。
顯示驗證畫面訊息 (僅限 Windows)	您可以為裝置終端使用者提供自訂記錄，以提示他們註冊至 Workspace ONE UEM Console 時必須使用的項目。例如，如果他們的 UEM 的註冊驗證與 Active Directory 認證相同，則您可以將其作為提示。也可以包含連結，讓使用者可以點選取得說明協助。此功能目前僅支援 Windows 裝置。 您必須藉由在同一個文字方塊中納入提示的翻譯，來進行自身的本地化作業。

建立自訂註冊訊息

您可自訂有關裝置註冊的訊息，以及任何未來傳送到裝置的行動裝置管理 (MDM) 提示。

- 1 導覽至 **裝置 > 裝置設定 > 一般 > 註冊**，然後選取自訂標籤。
- 2 選取為每個平台使用特定的訊息範本，然後從每個平台的下拉式功能表中選取一個裝置啟動訊息範本。按照本節下的 **建立訊息範本** 一節中的步驟來建立新訊息範本。
- 3 針對 iOS 裝置，可以選擇性設定以下內容。
 - a 輸入 iOS 裝置的 **後置註冊登陸 URL**。
 - b 輸入 iOS 裝置的 **MDM 設定檔訊息**，也就是在註冊時 MDM 設定檔所顯示的安裝提示訊息。
- 4 選取 **儲存**。

建立訊息範本

您可以依平台自訂的訊息範本建立您專屬的資料庫，以涵蓋您可能遇到的各種情況，包含註冊。

- 1 導覽至 **裝置 > 裝置設定 > 一般 > 訊息範本** 然後選取 **新增**。
- 2 設定 **類別** 下拉式功能表以符合您範本所屬的類別。選項包括 **管理員、應用程式、合規性、內容、裝置生命週期、註冊和使用條款**。
- 3 設定最能呼應子類別之 **類型**。**類型** 下拉式功能表的選項，將取決於 **類別** 設定。
- 4 設定 **選取語言** 下拉式功能表。僅會根據目前的使用中地區來顯示語言。選取 **新增** 按鈕來新增語言。
- 5 如果要將某範本作為所選 **類別** 的預設範本，請勾選 **預設** 勾選方格。
- 6 選取範本的 **訊息類型**。這些選項包括 **電子郵件、SMS* 和推播通知**。
- 7 將文字輸入 **訊息內文** 文字方塊中，來撰寫您的 **電子郵件** 訊息。
 - **純文字** 選項只有等寬並有襯線的字型 (Courier)，也沒有任何格式的選項。
 - **HTML** 選項讓您能夠使用 **RTF 文字** 的編輯環境，包括字型、格式、標題層級、項目符號、縮排、段落對齊、下標、上標、圖像和超連結等功能。HTML 環境支援基本的 HTML 編碼，您可以使用 **顯示來源** 鍵在 **RTF 文字** 與來源檢視畫面之間作切換。
- 8 點選 **儲存** 按鈕來儲存範本。

* 為了讓您的裝置機群能夠使用 SMS 通知，您必須具備第三方閘道提供者的帳戶並配置閘道設定。導覽至 **群組與設定 > 所有設定 > 系統 > 企業整合 > SMS**，然後完成 **SMS 設定** 中說明的選項。

配置生命週期通知

您可使用生命週期通知，在裝置生命週期中發生任何的特定事件後傳遞自訂的訊息。

若要配置此選擇性設定，請導覽至 **裝置 > 生命週期 > 設定 > 通知**，然後在下列區塊中輸入以下選項。

- **已取消裝置註冊** – 當裝置取消註冊時傳送 Email 通知。
- **裝置註冊成功** – 當裝置註冊成功時傳送 Email 通知。
- **裝置因註冊限制遭封鎖** – 如果註冊限制封鎖裝置，會傳送 Email 通知。若要設定此行為，請導覽至 **群組 & 設定 > 所有設定 > 裝置 & 使用者 > 一般 > 註冊**，然後選取 **限制** 索引標籤。

設定	描述
將 Email 傳送至。	<ul style="list-style-type: none"> ■ 無 – 在成功地封鎖裝置、註冊或取消註冊後，不會傳送確認的 Email。 ■ 使用者 – 將確認的 Email 傳送給裝置使用者，通知他們系統已成功地完成了裝置封鎖、註冊或取消註冊的動作。 <ul style="list-style-type: none"> ■ 副本 – 將相同的確認 Email 傳送給單一 Email 地址，或是傳送給數個以逗號分開的 Email 地址。 ■ 訊息範本 – 從下拉式清單中選取您要的訊息範本。若要新增訊息範本或編輯現有範本，請選取「按一下這裡...」超連結，您隨即前往 裝置 & 使用者 > 一般 > 訊息範本 設定頁面。 ■ 管理員 – 將確認 Email 傳送給 Workspace ONE UEM 管理員，通知他們系統已成功地完成裝置封鎖、註冊或取消註冊的動作。 <ul style="list-style-type: none"> ■ 收件者 – 將相同的確認 Email 傳送給單獨一個 Email 地址，或是傳送給數個以逗號分開的 Email 地址。

在自訂標籤上配置註冊選項

若要提供額外終端使用者支援層級，包括 Email 和電話號碼，請配置自訂標籤。使用者基於任何原因而無法註冊裝置時，這類支援層級就很有價值。

導覽至 **裝置 > 裝置設定 > 裝置與使用者 > 一般 > 註冊**，即可找到自訂索引標籤。

設定	描述
為各平台使用特定的訊息範本	如果啟用，就能為每個平台選取唯一訊息範本。 此提供的連結將顯示訊息範本頁面，允許您立即開始建立範本。 Workspace ONE™ 直接註冊支援特定平台訊息範本。
註冊支援 Email	輸入支援 Email 地址。
註冊支援電話	輸入支援電話的號碼。
註冊後的登陸 URL (僅用於 iOS)	您可提供後置註冊登陸 URL，在終端使用者註冊成功後，系統便會導向該處。此 URL 可能會連結至公司資源，例如：公司網站或導向其他資源的登入畫面。 Workspace ONE 直接註冊支援註冊後的登陸 URL。
MDM 設定檔訊息 (僅用於 iOS)	只有在 iOS 裝置上，系統才會在註冊過程中顯示此文字方塊中的訊息。您所指定的訊息，長度不得超過 255 個字元。 Workspace ONE 直接註冊支援僅限 iOS 的 MDM 設定檔訊息。
使用自訂 MDM 應用程式	顯示可開啟 APP 群組清單頁面的連結。此連結標示為 應用程式群組 。 Workspace ONE 直接註冊支援自訂 MDM APP。

封鎖清單和允許清單裝置登錄

封鎖清單會明確列出禁止使用的裝置或應用程式。而允許清單會列出僅能使用的裝置或應用程式。將此概念套用至登錄，您可以控制哪些裝置可以在 Workspace ONE UEM powered by AirWatch 中註冊。

舉例來說，在部署公司的專用裝置時，您可以建立一份已核准的 iOS 裝置允許清單。您可以依據國際行動裝置識別碼 (IMEI)、序號或獨特裝置辨別碼 (UDID) 來建立此裝置清單。如此一來，只有經您識別的裝置才能進行註冊，而員工的個人裝置均不得註冊。

此外，在裝置遺失或遭竊的情況下，您即可將裝置的 IMEI、序號或 UDID 資料，列入裝置的封鎖清單中。將裝置列入封鎖清單將會取消裝置該註冊、移除所有 MDM 設定檔並禁止註冊，直到您將它從封鎖清單中移除。

註冊後，系統會使用裝置資訊更新使用者的登錄記錄。當裝置取消註冊時，任何其他嘗試註冊相同裝置的使用者都會遭封鎖而無法進行註冊，直到先前使用者的登錄記錄刪除。

新增封鎖清單或允許清單裝置

您可以根據裝置的各種屬性，將其加入封鎖清單 (禁止註冊的裝置) 或允許清單 (可以註冊的裝置)。

備註 在裝置註冊計劃 (DEP) 中登錄的封鎖清單裝置，會限制在未來指派 DEP 設定檔給那些裝置。

1 導覽至 **裝置 > 生命週期 > 註冊狀態**，然後選取 **新增**。

- 2 從**新增**下拉式功能表選取**封鎖清單裝置**或**允許清單裝置**，並完成相關設定。

設定	描述
封鎖清單/允許清單裝置	輸入要加入封鎖清單或允許清單的裝置 (按裝置屬性選項)，一次最多輸入 30 個裝置。
裝置屬性	相取相應的裝置屬性類型。選取 IMEI、序號或 UDID。
企業群組	確認要將哪些企業群組的裝置加入封鎖清單或允許清單。
擁有權	您可以僅允許具有所選擁有權類型的裝置。 此選項僅在裝置列入允許清單時才能使用。
其他資訊	允許您選取要套用允許清單或封鎖清單的平台。
平台	您可以將整個平台上的所有裝置都列入封鎖清單或允許清單。 此選項僅在您已勾選 其他資訊 方格時才能使用。

- 3 點選**儲存**來確認此設定。

裝置登記

您可以選擇登錄公司裝置，這麼做的主要優點在於可限制為只有已登錄的裝置才能在 Workspace ONE UEM 中註冊。

登錄的優點

除了可限制為僅供已登錄的裝置進行註冊之外，另一個優點是可以追蹤註冊狀態，讓您知道哪些使用者已經註冊及哪些使用者尚未註冊。接著您就可以通知這些還沒註冊的使用者。

即使在輸入裝置資料的階段，使用者或管理員就已遺失裝置識別碼，Workspace ONE UEM 還是能夠成功地登記裝置。

安全性則是在註冊前先登錄裝置的第三個優點。已登記的裝置會認為第一個登入的使用者與登記裝置的使用者為同一人。如果其他使用者嘗試登入已登記的裝置，裝置將遭到鎖定，且無法進行註冊。

註冊注意事項

如果要在註冊之前繼續登記裝置程序，請考量下列項目。

誰會登記裝置？

登記裝置時，決定由誰來執行登記裝置的實際動作，是十分值得考量的重點。

- 您的部署中共有多少部裝置？大量部署數以千計的裝置時，您可以將此資訊新增到 CSV (逗點分隔值) 檔案中。接著，在裝置佈建之前上傳此檔案。請參閱本頁面中標題為**登錄個別裝置**和**登錄多個裝置**的區段。
- 您是否打算採用 BYOD 方案，好允許員工們使用自己的個人裝置？若要將註冊限制為只有已登錄的裝置才能進行，您可以指示員工如何為各自的裝置進行註冊。請參閱本頁面中下一個標題為**透過 SSP 登錄終端使用者的裝置**的區段。

透過 SSP 登錄終端使用者的裝置

如果您支援 BYOD，您可以引導終端使用者登錄自己的裝置，接著再註冊到 Workspace ONE UEM 中。如果想要追蹤註冊或使用登錄 Token，您也可以要求那些使用公司專用裝置的使用者進行登錄。無論是哪種情況，您都需要向其告知終端使用者須遵循的程序。

下列說明假設終端使用者具有 Workspace ONE UEM 憑證，可能是來自他們現有的目錄服務憑證，或來自先前已啟動的使用者帳戶。若您之前選擇使用目錄服務來註冊，而不是手動新增使用者，此時便不會擁有任何已建立好的使用者帳戶。

在這種情況下，如果想允許終端使用者登錄裝置，您將需要透過 Email 或內部網路通知，將登錄說明傳送給 Workspace ONE UEM 之外的每個使用者。請透過下列途徑，確認已啟用 Active Directory 或驗證代理伺服器的註冊驗證：**裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 註冊 > 驗證**。

若要確認**拒絕未知使用者**設定是否已取消勾選，請導覽至**裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 註冊 > 限制**。

- 向 Workspace ONE UEM 外部的使用者傳送內含登記說明的 Email 或內部網路通知。
- 先為所有的終端使用者建立使用者帳戶讓他們可以自行登記裝置，然後再將內含登記說明的使用者帳戶啟動訊息傳送給每位使用者。

在傳送給終端使用者的註冊訊息中包含這五個步驟，他們將會獲得所需的內容以便登錄自己的裝置。

- 1 導覽至自助入口網站 (SSP) 的 URL: **https://<UEM_Environment>/MyDevice**，其中 <UEM_Environment> 是您環境專用的註冊 URL。
- 2 輸入**群組 ID** 和**認證** (Email 地址或使用者名稱和密碼) 以便登入。
這些認證可以與目錄使用者的目錄服務認證互相配對。
- 3 選取**新增裝置**來開啟**登記裝置**的表格。
- 4 完成**登記裝置**的表格中之必要的文字方塊來輸入裝置資訊。
- 5 透過選取**儲存**來提交並註冊裝置。

僅限已登記裝置進行註冊

此時，無論管理員和終端使用者是否已經登記裝置，您都可以將註冊限制為只有已登記的裝置才能進行。若要執行此操作，請導覽至**裝置 > 裝置設定 > 裝置與使用者 > 一般 > 註冊**，然後選取**僅限已登記裝置**。

Devices Enrollment Mode Open Enrollment Registered Devices Only

追蹤註冊狀態

您偶爾也需要為裝置登錄進行疑難排解，或者追蹤整個階段的註冊過程。終端使用者也許會不小心刪除含有登錄指示的訊息，或是未在規定效期內兌換驗證。

裝置經登記後，若要追蹤其註冊狀態，只需要瀏覽至**裝置儀表板**頁面並選取**註冊**圖表，並根據裝置的註冊狀態來進行篩選即可。您也可以存取 Monitor，其中列出最近註冊的所有裝置。

若要管理註冊狀態，請前往**裝置 > 生命週期 > 註冊狀態**存取 [註冊狀態] 頁面。只要將清單的**註冊狀態**欄加以排序，或者根據**註冊狀態**來篩選清單檢視，都能夠追蹤裝置的登記狀態。

使用「註冊狀態」頁面，您可以產生已登記 (但為註冊) 裝置的自訂清單、選取此自訂清單中的所有裝置，並重新傳送註冊說明。如果經過足夠的時間，但裝置仍無法註冊，您可以選擇以重設 (或甚至撤銷) 其登錄 Token。

如需詳細資訊，請參閱[註冊狀態](#)。

註冊期間執行使用者群組同步處理

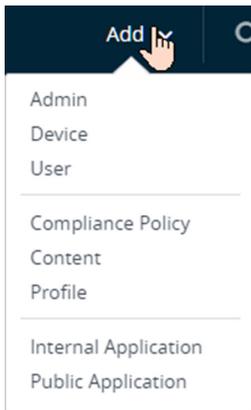
如果您想要整理應用程式、裝置設定檔、合規原則的指派項目，或整理使用者群組的相關使用者對應，不妨將使用者群組同步處理設定維持為啟用 (此為預設設定)。此設定會使 Workspace ONE 在每次建立裝置記錄時對驗證伺服器進行即時呼叫。

如需詳細資訊，請參閱在[分組標籤上配置註冊選項](#)中的**使用者群組同步**區段。

登記個別裝置

當您有少量裝置要登錄時，可以個別登錄這些裝置。

- 1 選取**新增**按鈕；您可在 Workspace ONE UEM Console 絕大多數畫面的右上象限中找到此按鈕。選取後，此按鈕會顯示有多個選項的下拉式功能表。



- 2 選取**裝置**。
新增裝置頁面即會出現。
- 3 根據您的需求，從**使用者索引**標籤開始完成選項。

設定	描述
使用者區段	
搜尋文字	輸入搜尋參數並選取 搜尋使用者 按鈕，以搜尋使用者。 搜尋成功時，請選取要登錄裝置的使用者帳戶。此時會顯示數個預先填入的文字方塊，包括 [安全性類型]、[使用者名稱]、[密碼] 和 [電子郵件地址]。您可以顯示進階使用者詳細資料，以編輯這些欄位。
裝置區段	

設定	描述
預期的暱稱	輸入裝置的暱稱。此文字方塊接受經由您點選加號來嵌入的 查閱值 。如需詳細資訊，請參閱第 12 章 查閱值 。
企業群組	選擇裝置所屬的企業群組。
擁有權	選擇裝置的擁有權層級。
平台	選擇裝置平台
顯示進階裝置資訊選項	顯示進階裝置資訊設定。
型號	選擇裝置型號。此下拉式功能表的選項將依所選的 平台 而定。
作業系統	選擇裝置的操作系統。此下拉式功能表的選項將依所選的 平台 而定。
UDID*	輸入該裝置的唯一識別碼。
序號* ‡	輸入裝置的序號。
IMEI*	輸入裝置的國際行動裝置識別碼 (International Mobile Station Equipment Identity)。
SIM*	輸入裝置的訂閱者識別模組。
資產編號*	輸入裝置的資產編號。
訊息區段	
訊息類型	新增裝置後，傳送給使用者的通知之類型。選取 無 、 電子郵件 或 SMS* 。 Email 的選項需要有效的 Email 地址。同時也必須選取一個電子郵件訊息範本。 SMS 選項則需要電話號碼，包括國碼和區碼。可能需要 SMS 的費用。同時也必須選取一個 SMS 訊息範本。
Email 地址	Email 訊息類型所需。
Email 訊息範本	Email 訊息類型所需。從下拉式功能表中選取一個範本。透過 訊息預覽 按鈕來檢視 Email 訊息。
電話號碼	SMS* 訊息類型所需。
SMS 訊息範本	SMS* 訊息類型所需。從下拉式清單中選取一個範本。透過 訊息預覽 按鈕來檢視 SMS 訊息。

* 為了讓您的裝置機群能夠使用 SMS 通知，您必須具備第三方閘道提供者的帳戶並配置閘道設定。導覽至**群組與設定 > 所有設定 > 系統 > 企業整合 > SMS**，然後完成 **SMS 設定**中說明的選項。

* 若要登記裝置，請至少填妥其中一個具有此標記的欄位。

§ Windows Desktop 裝置必須輸入序號才能登記。

4 (選用) 完成自訂屬性索引標籤。

設定	描述
新增	選取這個按鈕，可以新增自訂的 屬性 及其對應的 應用程式 和 值 。 若要在新增裝置時使用自訂屬性功能，您必須已建立好自訂屬性。若要完成此作業，請造訪第 5 章 自訂屬性 。
應用程式	選取收集屬性的應用程式。
屬性	從下拉式功能表中選擇自訂屬性。
值	從下拉式功能表中選擇自訂屬性值。

- (選用) 完成**標記索引**標籤。

設定	描述
新增	新增 標記 至裝置。
標記	從現有標記的下拉式功能表中，選擇所要的標記。

- 點選**儲存**來完成裝置的登記程序。

結果：裝置現已登錄至步驟 3 中指定的選定 Workspace ONE UEM 使用者帳戶。

下一步：請將此裝置傳遞給該使用者，以使其登入並完成註冊程序。如果有其他使用者嘗試在已登錄的使用者之前登入此裝置，裝置將會鎖定，且無法註冊。

登記多個裝置

如果您有數百個或數十個裝置要註冊，可以採用批次匯入的方式進行。

- 導覽至**帳戶 > 使用者 > 清單檢視**，或是**裝置 > 生命週期 > 註冊狀態**。

- 選取**新增**，然後選取**批次匯入**以顯示**批次匯入**畫面。

- 完成每個必要選項：**批次名稱**、**批次描述**和**批次類型**。

批次檔 (.csv) 選項內有一份以工作為基礎的範本清單，您可以利用該清單大量載入使用者及其裝置。

- 選取適當的下載範本，然後將逗點分隔值 (CSV) 檔案儲存至可供存取之處。

- 導覽至儲存 CSV 檔案的位置，使用 Excel 加以開啟，並輸入您要匯入之各項裝置的所有相關資訊。

每個範本都會預先填入樣本項目，以示範每個欄位中所應填入的資訊類型 (和資訊格式)。CSV 檔案中標示星號 (*) 的欄位為必填欄位。

- 以 CSV 檔的形式來儲存完成的範本。在 UEM 主控台中，從**批次匯入**畫面中選取**選擇檔案**按鈕，導覽至您已完成的 CSV 檔案儲存所在的路徑，並選取該檔案。

- 點選**儲存**以完成所有列出的使用者和相關裝置的登記工作。

登記 Token

若您僅限已登記的裝置註冊，則您還可以進一步透過選項來要求登記 Token。此選項能確認特定使用者是否經過授權而允許註冊，從而提升安全性。

您可以透過 Workspace ONE UEM 帳戶，將附加了註冊 Token 的 Email 或 SMS 訊息傳送給使用者。

備註 為了讓您的裝置機群能夠使用 SMS 通知，您必須具備第三方閘道提供者的帳戶並配置閘道設定。導覽至**群組與設定 > 所有設定 > 系統 > 企業整合 > SMS**，然後完成 **SMS 設定**中說明的選項。

啟用登錄 Token

- 若要啟用 Token 型註冊，請選擇相應的企業群組。導覽至**裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 註冊**，並務必選擇**驗證**標籤。
- 向下捲動至**使用入門**區段，並將**裝置註冊模式**選取為**僅限已登記的裝置**。

出現標有**需要登記 Token**的切換選項。啟用此選項，即可將限制只有登記過 Token 的裝置才能註冊。

Authentication Mode(s) Basic Directory Authentication Proxy

Source of Authentication for Intelligent Hub **WORKSPACE ONE UEM** **IDENTITY MANAGER** ⓘ

Devices Enrollment Mode* Open Enrollment Registered Devices Only

Require Registration Token **ENABLED** **DISABLED**

Registration Token Type* Single-Factor Two-Factor

Registration Token Length* ⓘ

Token Expiration Time (hours)*

3 選取**登記 Token 類型**。從以下項目中選擇。

- **單一要素** – 只需要 Token 即可註冊。
- **雙重要素** – 除了 Token，也需要登入使用者憑證才能註冊。

4 設定**登記 Token 長度**。

此必要設定能指出登記 Token 的複雜度，其數值長度必須包括 6 至 20 個英數字元。

5 設定**Token 到期時間** (以小時為單位)。

此必要設定是終端使用者能用來選取連結並註冊的時間長度。一旦到期，您就必須傳送另一個連結。

產生 Token

您必須產生和傳送登錄 Token，此 Token 是註冊行動裝置的高度安全方法。有兩種方式可以產生 Token：透過 **UEM 主控台**或透過**自助入口網站**。

UEM 主控台	自助入口網站
<ol style="list-style-type: none"> 1 導覽至帳戶 > 使用者 > 清單檢視，然後為使用者選擇編輯使用者。新增/編輯使用者的畫面便會顯示。 2 向下捲動並選取訊息類型。從以下項目中選擇。 <ul style="list-style-type: none"> ■ 適用於目錄使用者的電子郵件 ■ 適用於基本使用者帳戶的SMS 3 選取訊息範本。接下來請選取儲存並新增裝置。即會出現新增裝置畫面。 若要使用預設範本或建立新範本，請在新的索引標籤中，選取訊息範本頁面下方的連結。 4 檢閱裝置的一般資訊，確認訊息本身的資訊。完成後，點選儲存即可使用所選的訊息類型來將 Token 傳送給使用者。 <p>備註 基於安全性考量，您無法透過 UEM 主控台存取 Token。</p>	<ol style="list-style-type: none"> 1 登入自助入口網站。 如果您使用單一登入或智慧卡驗證，您可以從裝置或電腦登入。目錄使用者可使用目錄服務憑證來登入。 2 選取新增裝置。 3 若要輸入裝置資訊 (暱稱與平台) 以及其他詳細資料，請完成登記裝置表單中的設定。由於系統可能不會自動填入電子郵件地址與電話號碼，請務必提供這些資訊並確保其正確無誤。 4 選擇儲存即可使用所選的訊息類型來將註冊 Token 傳送給使用者。 <p>備註 Token 不會顯示在此頁面上，只會出現在傳送的訊息中。</p> <p>作為安全功能，已對使用 token 註冊的帳戶進行了以下更改。</p> <ul style="list-style-type: none"> ■ 新增裝置畫面和帳戶畫面上的電子郵件地址和電話號碼皆設為唯讀。 ■ 「檢視註冊訊息」動作已移除。

終端使用者使用 Token 註冊之相關指示

您的終端使用者可以使用登錄 Token 來註冊裝置，登錄 Token 是一種高度安全的驗證方法。

- 1 在裝置上開啟 SMS 或 Email 訊息，並選取包含了註冊 Token 的連結。當註冊頁面提示您輸入群組 ID 或 Token 時，直接輸入 Token。
- 2 如使用雙因素驗證，請輸入使用者名稱或密碼。
- 3 繼續照常註冊。

結果：完成後，裝置便會與使用您所建立之 Token 的使用者建立關聯。

下一步：MDM 設定檔一旦安裝至裝置，系統便會將該 Token 視為「已使用」，且無法再用於註冊其他裝置。如果註冊未完成，則 Token 仍可於另一個裝置使用。如果 Token 已根據您所設定的時限而到期，就需要再產生另一個註冊 Token。

登記時缺少裝置識別碼

如果在登錄期間未指定任何裝置識別碼 (例如 UDID、IMEI 和序號)，Workspace ONE UEM 就會自動使用這些屬性來比對註冊的裝置及其登錄記錄。

提供的登錄資訊不足時，可利用下列順序讓 Workspace ONE UEM 成功登錄裝置。

- 1 登錄裝置的使用者。
- 2 平台 (如果已指定)。
- 3 型號 (如果已指定)。
- 4 擁有權類型 (如果已指定)。
- 5 最早比對登錄記錄的日期。

註冊狀態

藉由檢視註冊狀態，您可以在 Workspace ONE UEM powered by AirWatch 中存取個別裝置的註冊狀態資訊、大量匯入和登錄裝置、將裝置列入允許清單/封鎖清單，以及撤銷/重設裝置 Token。

選取**裝置 > 生命週期 > 註冊狀態**，透過目前所選的企業群組中之裝置狀態，來查看整個裝置的清單。

Devices > Lifecycle

Enrollment Status

Filters << ADD

LAYOUT EXPORT Search List

Enrollment Status	First Seen	General Info	Platform	User	Enrollment Status	Token Status	Source
	10d ago	user1_device1 Ramesh_01 Corporate - Dedicated	Android	vm2 vm2 test	Unenrolled	Registration Expired	Batch Import 9/24/2019 7:40:50 AM
	10d ago	c's Device mtog Corporate - Dedicated	Unknown	c c c	Registered	Registration Active	Console 9/23/2019 5:05:40 PM
	10d ago	mtog's Device mtog Corporate - Dedicated	Unknown	mtog mtog mtog	Registered	Registration Active	Console 9/23/2019 4:27:37 PM
	11d ago	inam Device inam Corporate - Dedicated	Android Android RZ8K90AAR6E	inam md inam	Registered	Registration Active	Console 9/23/2019 1:20:45 AM
	20d ago	Test_iphone Test_P Corporate - Shared	Apple iOS iOS 12.4.0 iPhone	test_pg	Registered	Registration Active	Self-Service Portal 9/13/2019 3:49:05 PM
	24d ago	IMEI # 3522 Sreejith	Unknown		Blacklisted	Non-Compliant	Console 9/9/2019 3:37:38 PM
	36d ago	f1's Device f1 Corporate - Dedicated	Unknown	f1 f1 f1	Registered	Registration Expired	Console 8/28/2019 12:34:44 PM Registration Expired
	38d ago	test123 cdvivi Corporate - Dedicated	Apple iOS	sakshis Sakshis ss	Registered	Registration Active	Self-Service Portal 8/27/2019 2:29:17 AM
		wrf					API

Items 1 - 50 of 576 Page Size: 50

依照特定的資訊，透過欄位和配置資訊篩選條件來檢視裝置的活動。例如，按照 **Token 狀態** 的欄位來排序，僅檢視登記不適用的裝置，並只對這些特定的裝置採取行動。搜尋所有裝置的暱稱或使用者名稱，來隔離某台裝置或某位使用者。

設定	描述
篩選條件	若要篩選整個裝置類別，可使用篩選條件，只查看您感興趣的裝置。 <ul style="list-style-type: none"> ■ Email 狀態 ■ 平台 ■ 擁有權 ■ Token 狀態 ■ Token 類型 ■ 來源 ■ 首次上線時間
新增按鈕	<ul style="list-style-type: none"> ■ 登記裝置 - 您可以登記或新增要註冊的單一裝置。 ■ 將裝置列入允許清單或封鎖清單 - 您可以只允許已識別或已列入允許清單的裝置進行註冊。或者您也可以將裝置列入封鎖清單，禁止這些裝置註冊。 ■ 批次匯入 - 利用批次匯入畫面匯入多個裝置或多名使用者。
重新傳送訊息	將原始訊息重新傳送給使用者，包括自助入口網站的 URL、群組 ID 和登入認證。
更多動作	
變更企業群組	將所選的裝置移到您選定的企業群組。
變更所有權	變更所選裝置的所有權類型。
刪除	永久刪除所選裝置的登記資訊。此動作會強制使用者預先登記才能註冊。在適用情況下，您必須先撤銷 Token，才能刪除裝置登記。
重設 Token	重新設定已撤銷或失效的 Token 狀態。
撤銷 Token	迫使所選裝置的登記 Token 失效，以從根本阻斷不歡迎的使用者或裝置的存取權。 針對 重設 Token 和 撤銷 Token 動作，您可選取停用 通知使用者 設定，以防止系統傳送預設的電子郵件通知。

設定	描述
登記多個裝置	若要對個別裝置或多台裝置採取動作，請勾選每個裝置旁邊的勾選方格並使用動作按鈕。 套用篩選條件以顯示特定一組裝置後，您就能對多個選定的裝置執行批次動作。若要執行此動作，請選擇裝置，並從 重新傳送訊息 和 更多動作 按鈕選擇一個動作。 您可各別勾選方格。若要選取經過篩選的所有裝置組，可勾選位於勾選方格欄上方的全域勾選方格。 當您為一或多台裝置選擇某項動作時，便會顯示確認畫面，讓您能夠 儲存 或 取消 動作。
版面配置按鈕	選取 自訂 選項，即可顯示可看到的欄位完整清單，或根據您的喜好設定顯示或隱藏欄位。 您也可以選擇將您自訂的欄位檢視，套用在現有企業群組與其下層群組中的所有管理員。 您可以隨時回到 版面配置 按鈕設定，調整您的欄位顯示喜好。
匯出按鈕	您可以使用 註冊狀態 清單檢視的預設 Excel 格式 (XLSX) 或逗號分隔值格式 (CSV) 下載報告。

您可以從**明細檢視**，透過點選**重新傳送訊息**鍵來重新傳送註冊的訊息。您也可以透過選擇**編輯登記**鍵並且完成**進階裝置資訊**的區段來編輯裝置的登記資訊。

明細檢視顯示一系列的標籤，每個都包含有關裝置註冊的資訊。

- **摘要** – 檢視登記日期、自從裝置首次出現後的時間、基本的裝置和使用者資訊。
- **使用者** – 檢視使用者詳細資料。
- **訊息** – 檢視傳出的啟動裝置的 Email 訊息，包括認證資訊和 QR 碼。提供您一個「使用者登錄訊息」的資源，它可在裝置成功註冊後，讓管理員隱藏**訊息**索引標籤。
- **自訂屬性** – 檢視有關裝置之自訂屬性。
- **標籤** – 檢視有關裝置之標籤。
- **離線註冊** – 如果可用，此標籤會允許您在裝置離線時也能將其註冊。當您想要在離線時使用裝置時 (例如旅行時)，此功能相當實用。

自我註冊與裝置註冊預備

Workspace ONE UEM 支援兩種註冊企業裝置的方式。您可以讓使用者自行註冊裝置，也可以由管理員透過一種叫作**裝置註冊預備**的程序來代替使用者註冊。

在裝置註冊預備期間，管理員會先將裝置註冊，再加以指派並發佈給終端使用者。若有管理員必須設定整個企業中多個使用者的裝置，這個方法非常實用。

Android、iOS 和 macOS 的裝置都能執行裝置註冊預備。

考量項目 #1: 裝置所有權

- 您是否已為終端使用者指派了企業裝置？如果是的話，重新收集這些裝置並為其進行註冊預備顯然很不切實，最好還是讓使用者自行註冊。
- 終端使用者是共享裝置，還是擁有專用裝置？如果終端使用者未共享裝置，那麼您可以讓裝置的單一擁有者負責自行註冊裝置。

此外，裝置註冊預備也很適合用於剛佈建的裝置，因為此時員工仍未收到這些裝置。如果終端使用者已經擁有企業裝置，那麼允許他們自行註冊是最合理不過了。裝置總數多到讓管理員無法執行裝置註冊預備時，讓使用者註冊自己的裝置也是好事。

考量項目 #2：自動探索

您會在企業的 Email 網域與 Workspace ONE UEM 環境之間建立關聯嗎？此程序稱為**自動探索**，代表終端使用者只需輸入 Email 地址和認證。就會自動輸入註冊 URL 和群組 ID。

另請參閱[自動探索註冊](#)。

考量項目 #3：Workspace ONE 直接註冊

不支援透過 Workspace ONE 直接註冊進行裝置註冊預備。如果您必須為單一或多個使用者進行裝置註冊預備，您必須使用 Workspace ONE Intelligent Hub 註冊裝置，而不是使用 Workspace ONE 直接註冊。

Workspace ONE 直接註冊是一項適合用於自我註冊的功能。啟用後，所有符合資格的裝置在登入註冊企業群組時都能立即註冊。且完整安裝後，終端使用者可以同意安裝公司選取的 APP，也可以選擇不安裝 APP。

如需詳細資訊，請參閱[Workspace ONE 直接註冊](#)。

考量項目 4：您是否參與 Apple 的裝置註冊計劃？

為了將在行動裝置管理 (MDM) 中註冊 Apple 裝置的好處最大化，Apple 推出了裝置註冊計劃 (DEP)。使用 DEP，您可以執行以下操作。

- 在裝置上安裝不可移除的 MDM 設定檔，可避免終端使用者將其刪除。
- 在監督模式下佈建裝置 (僅適用於 iOS)。監督模式中的裝置能存取額外的安全性與配置設定。
- 為所有終端使用者執行註冊。
- 自訂並簡化註冊程序以滿足企業的需求。
- 若要避免 iCloud 備份，請在產生 DEP 設定檔時，停用讓使用者以其 Apple ID 登入的功能。
- 為所有終端使用者強制升級 OS。

考量項目 5：Apple Configurator 的使用

Apple Configurator 允許 IT 管理員有效部署並管理 Apple iOS 裝置。對零售店、教室和醫院等企業會特別實用，尤其是預先註冊裝置讓多個終端使用者共用時。

支援使用 Configurator 為單一使用者註冊預先登記裝置，只要在主控台將序號/IMEI 資訊新增到使用者的登記裝置即可。Apple Configurator 還有個最重要的好處，那就是您可以使用 USB Hub 或 iOS 裝置圖表來佈建多個裝置，且耗時不過數分鐘。

考量項目 6：該選擇單一使用者註冊預備還是登錄？

如果您想針對單一使用者進行裝置註冊預備，採取登錄方式可能是較佳的選項。單一使用者註冊預備和登記裝置之間的差異儘管細微，卻相當重要。

登記 – 登記裝置的方式適合針對已命名的個別使用者採用。這個程序代表裝置認為第一個登入的使用者與登錄裝置的使用者將為同一人。如果其他使用者嘗試登入已登記的裝置，基於安全考量，該裝置將遭到鎖定，且無法進行註冊。

單一使用者註冊預備 – 裝置註冊預備的方式適合針對任何有資格在 Workspace ONE UEM 中註冊的使用者採用。理論上，您可以將已經完成註冊預備的裝置交給任何符合使用資格的使用者，該使用者也可以成功登入裝置並在 Workspace ONE UEM 中註冊。

透過註冊預備工作流程，您可以先行準備所需裝置，然後啟動所有合格註冊使用者都能登入的 Workspace ONE Intelligent Hub，接著讓 Workspace ONE UEM 執行一次性的重新指派，以便使裝置建立與該使用者的關聯。

考量項目 7：裝置註冊預備的使用

除非使用 Apple Configurator，否則管理員必須逐一註冊預備裝置。對於大型部署，請考慮這項工作所需的時間和人力。

管理員可輕鬆註冊預備新裝置，但是已使用公司專用裝置的員工必須將裝置送到現場，或是在現場收集裝置，才能註冊預備裝置。

如果有上千台裝置要預先註冊，裝置註冊預備可能需要一段時間。因此，如果有一批新的裝置需要佈建，最好使用此方法，因為您可在員工收到裝置前，先取得裝置的存取權。

請按照下列方法來為 Android 和 iOS 執行裝置的註冊預備。

- **單一使用者 (標準)** - 在註冊預備任何使用者都可以註冊的裝置時使用。

備註 根據指示，此註冊流程適用於無人看管的裝置。若您使用此流程進行零接觸使用者註冊，則您需負責確保完成註冊預備的裝置交付給預期的使用者。

- **單一使用者 (進階)** – 此法可用來註冊預備您要代替某特定使用者來註冊的裝置。

備註 註冊預備使用者/管理員必須確保將裝置簽出給已登錄的使用者。

- **多使用者** – 此法可用來註冊預備將供多位使用者所使用的裝置。

如需詳細指示，請參閱[建立多使用者註冊預備帳戶以進行註冊](#)。

註冊預備單一使用者裝置

Workspace ONE UEM Console 上的「單一使用者裝置註冊預備」允許由單一管理員代表其他使用者配置其裝置，這對於佈建大量裝置群的 IT 管理員特別有用。

不支援透過 Workspace ONE 直接註冊進行裝置註冊預備。如果您必須為單一或多個使用者進行裝置註冊預備，您必須使用 Workspace ONE Intelligent Hub 註冊裝置，而不是使用 Workspace ONE 直接註冊。

重要 建立註冊預備使用者的能力，屬於較高級的管理員權限。應僅限特定可信任的管理員擁有建立註冊預備使用者的權限。此外，請像處理其他任何管理員權限一樣處理註冊預備使用者認證，且請勿揭露使用者認證。

目前，具有建立使用者權限的任何管理員，也可以建立註冊預備使用者。您可透過編輯指派給管理員的角色，來限制此能力。導覽至 **帳戶 > 管理員 > 角色**。僅識別您想要限制的角色，然後透過清除「新增/編輯」權限中的 **編輯** 核取方塊，**編輯** (✎) 在類別路徑中的每個角色：**所有 > 帳戶 > 使用者 > 帳戶**。

備註 進行裝置註冊預備時，必須要有 LDAP 繫結。若要建立此裝載，請參閱本指南中的「將裝置繫結至目錄服務」。

- 1 導覽至 **帳戶 > 使用者 > 清單檢視**，然後針對要啟用裝置註冊預備的使用者帳戶選取 **編輯**。
- 2 在 **新增/編輯使用者** 頁面上，選擇 **進階** 標籤。
 - a 向下捲動至 **註冊預備** 的區段。
 - b 在 **啟用裝置註冊預備** 部分，選取 **已啟用** 滑桿。註冊預備選項隨即顯示。
 - c 在 **單一使用者裝置** 部分，選取 **已啟用** 滑桿。
 - d 將單一使用者之裝置註冊預備的模式切換為 **標準** 或 **進階**。
 「標準」註冊預備會在完成此預備動作後，要求終端使用者輸入登入資訊；而「進階」註冊預備則表示執行預備的使用者可代表另一位使用者註冊裝置。
 - e 確保 **多使用者裝置** 已設為 **停用**。
 - f 在 **Android 共用裝置模式** 部分，為簽入和簽出模式選取 **原生** 或 **啟動程式**。原生 Android 支援較簡單且不需要執行自訂的使用情境。啟動程式支援用於複雜使用情境的 UI 自訂。
 - g 在 **系統應用程式** 部分，您可以讓終端使用者存取系統應用程式。
 - h 在 **管理員模式密碼** 部分，指定在管理員模式中疑難排解裝置使用的英數密碼。在登入畫面上點選 Hub 圖示 5 次，以存取管理員模式。
結果：單一使用者裝置 可以為單一使用者註冊預備裝置。
- 3 註冊裝置。從以下項目中選擇。
 - 輸入伺服器 URL 與群組 ID，即可透過 Workspace ONE Intelligent Hub 來進行註冊。
 - 開啟裝置的網際網路瀏覽器、瀏覽至註冊 URL，然後輸入適當的群組 ID。
- 4 在註冊時，請輸入您的註冊預備使用者認證。
 - a 有必要的話，也可指明您是為 **單一使用者裝置** 執行註冊預備。
 只有在您同時為註冊預備使用者啟動多使用者裝置註冊預備時，才需執行上述動作。

5 完成進階或標準的註冊預備程序。

- a 若是執行「進階」註冊預備，系統將提示您輸入要使用此裝置之終端使用者裝置擁有者的名稱。安裝行動裝置管理 (MDM) 設定檔繼續進行註冊，並接受所有的提示和訊息。
- b 若是執行「標準」註冊預備，在終端使用者完成註冊時，系統便會在登入視窗中通知這些終端使用者輸入其認證。

結果：此後，裝置已備妥並隨時可供新使用者來使用。如果已有註冊使用條款協議，則註冊預備單一使用者在登入其 SSP 帳戶前，將無法查看此 TOU 協議提示。

註冊預備多使用者裝置

「多使用者裝置/共享裝置註冊預備」，讓 IT 管理員能夠佈建那些即將提供給多位使用者所使用的裝置。多使用者註冊預備能允許裝置在不同網路的使用者登入時，動態變更其指派的使用者。

不支援透過 Workspace ONE 直接註冊進行裝置註冊預備。如果您必須為單一或多個使用者進行裝置註冊預備，您必須使用 Workspace ONE Intelligent Hub 註冊裝置，而不是使用 Workspace ONE 直接註冊。

- 1 導覽至 **帳戶 > 使用者 > 清單檢視**，然後針對要啟用裝置註冊預備的使用者帳戶選取 **編輯**。
- 2 在 **新增/編輯使用者** 頁面上，選擇 **進階** 標籤。
 - a 向下捲動至 **註冊預備** 的區段。
 - b 在 **啟用裝置註冊預備** 部分，選取 **已啟用** 滑桿。註冊預備選項隨即顯示。
 - c 確保 **多使用者裝置** 已設為 **啟用**。
 - d 在 **Android 共用裝置模式** 部分，為簽入和簽出模式選取 **原生** 或 **啟動程式**。原生 Android 支援較簡單且不需要執行自訂的使用情境。啟動程式支援用於複雜使用情境的 UI 自訂。
 - e 在 **系統應用程式** 部分，您可以讓終端使用者存取系統應用程式。
 - f 在 **管理員模式密碼** 部分，指定在管理員模式中疑難排解裝置使用的英數密碼。在登入畫面上點選 Hub 圖示 5 次，以存取管理員模式。
- 3 使用下列一或兩個方法來註冊裝置。
 - 輸入伺服器 URL 與群組 ID，即可透過 Workspace ONE Intelligent Hub 來進行註冊。
 - 開啟裝置的網際網路瀏覽器、瀏覽至註冊 URL，然後輸入適當的群組 ID。
- 4 在註冊時，請輸入您的註冊預備使用者認證。有必要的話，也可指明您是為 **單一使用者裝置** 執行註冊預備。

只有在您同時為註冊預備使用者啟動多使用者裝置註冊預備時，才能執行上述動作。

結果：裝置已備妥並隨時可供新使用者來使用。

自我註冊程序

終端使用者可能必須知道自己的正確群組 ID 和登入認證才能自我註冊。若您已與目錄服務整合，那麼此處的憑證與使用者的目錄服務憑證是一樣的。

您也可以使用一種叫做自動探索的程序，為企業的電子郵件網域建立與 Workspace ONE UEM 環境的關聯。啟用自動探索後，支援的平台裝置會提示終端使用者輸入 Email 地址。如果 Email 網域 (@ 之後的文字) 相符，這些裝置將自動完成註冊，不需輸入群組 ID 或註冊 URL。如需詳細資訊，請參閱[自動探索註冊](#)。

- 1 終端使用者可導覽至 AWAgent.com，自動偵測是否已安裝 Workspace ONE Intelligent Hub。
如果未安裝 Workspace ONE Intelligent Hub，則網站將重新導向至行動 App Store。
- 2 AirWatch Container 使用者可從 APP 商店下載 AirWatch Container。
- 3 啟動 Workspace ONE Intelligent Hub 或 Container APP 後，使用者須輸入自己的認證，以及電子郵件地址或 URL/群組 ID，接著繼續註冊。

監督模式

管理員可以允許那些透過 Apple Configurator 註冊的裝置使用監督模式，從而啟用更多增強的安全性功能。但此模式也會為裝置帶來許多限制。

優點

一旦裝置在 Workspace ONE UEM 中註冊完成並獲得監督，比起一般裝置，管理員還會獲得下列可用於配置作業的增強功能。

- **可在 MDM 上提高限制**
 - 可禁止使用者移除應用程式。使用系統配置下的限制選項，即可在裝置本機限制應用程式的移除作業。
 - 禁止 AirDrop。
 - 禁止使用者修改 iCloud 與郵件帳戶設定，從而避免帳戶遭到竄改。
 - 停用 iMessage。
 - 為 iBookstore 設定內容分級限制。
 - 停用遊戲中心與 iBookstore。
- **增強的安全性**
 - 禁止終端使用者使用 Safari 造訪具有成人內容的網站。
 - 限制哪些裝置可以連線至特定 AirPlay 目的地，例如 Apple TV。
 - 禁止安裝憑證或未受管的配置設定檔。
 - 強制所有裝置的網路流量經過全域 HTTP 代理伺服器傳送。
- **Kiosk 模式**
 - 使用單一 APP 模式並停用首頁按鈕即可將裝置鎖定於單一 APP。
- **自訂裝置上的底色圖案與文字**
- **啟用或清除啟動鎖定**

限制

- 監管裝置只能透過監管用的 Mac 來使用 USB 存取。
- 如果是使用 iTunes 的裝置，則除非已在裝置上安裝 Apple Configurator 身份識別憑證，否則無法從該裝置複製資料、亦無法複製資料至該裝置。
 - 無法將相片或影片等媒體從裝置複製到 PC 或 Mac。若要傳輸這類資料，請使用 VMware Content Locker 來將內容同步至使用者的個人文件區段。此外，透過共享檔案用的應用程式，也能用 WLAN/WWAN 來將資料傳輸至伺服器。
- 監督模式雖能禁止使用者透過 iPhone Configuration Utility (IPCU) 來存取裝置側的記錄。
 - 此模式使得疑難排解任何應用程式或裝置問題變得難上加難。原因是裝置的日誌只能在連接到監管用的 Mac 才能取得。要克服這樣的挑戰，請使用 Workspace ONE SDK 將日誌與邏輯從應用程式傳送至 UEM 主控台。
- 您無法簡單地使用原廠設定重設裝置。
 - 裝置一旦還原成出廠設定，就必須與監管用的 Mac 重新連接，才能還原成監督模式。如果 Mac 不在裝置附近，則此程序可能會有問題。

決定是否要啟用監督模式前，請考量下列事項。雖然這能為裝置啟用更多增強的安全性功能，但 USB 限制值得您深思。

因此裝置與監督用 Mac 之間的距離，應是決定時的重要考量。由於 USB 限制可避免任何人存取裝置側的記錄，因此裝置發生問題，都得要回收才能還原功能。

事先決定監督至關重要，因為監督或「不監督」的程序，影響了裝置是要運送到 IT 位置或是倉庫的決定。

使用者註冊企業群組優先順序

成為使用者註冊 OG 的企業群組 (OG)，在裝置和其使用者的管理中扮演著特殊角色。選擇階層可決定哪些 OG 會成為使用者的註冊 OG。

依據下列優先順序，選取作為使用者註冊 OG 的企業群組。

1. 使用者所屬使用者群組的 OG

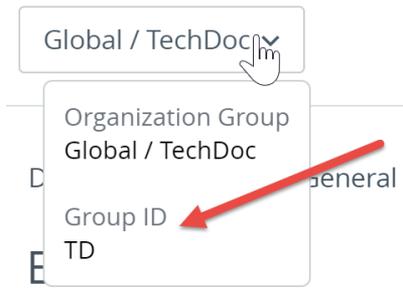
- 若要設定此選項，請導覽至 **群組與設定 > 所有設定 > 裝置與使用者 > 一般 > 註冊**，然後在分組索引標籤下方，選取 **依照使用者群組自動選擇** 作為 **群組 ID 指派模式**。更多相關的資訊，請參閱 [在分組標籤上配置註冊選項](#)。

如果未選取上述選項或使用者不屬於某一使用者群組，則註冊 OG 會變成...

2. 註冊期間提供的 OG

- 若要設定此選項，請導覽至 **群組與設定 > 所有設定 > 裝置與使用者 > 一般 > 註冊**，然後在分組索引標籤下方，選取 **預設** 作為 **群組 ID 指派模式**。
 - 接著，您必須提供使用者在註冊時必須輸入的群組 ID 名稱。通常，此作業會透過含有註冊 URL 的電子郵件與使用者通訊。

- 您可以將指標移到 OG 選取器上並查看產生的快顯視窗，以取得目前所處 OG 的群組 ID。



- 或者，您也可以讓使用者從群組 ID 清單中選擇。若要啟用此選項，請導覽至**群組與設定 > 所有設定 > 裝置與使用者 > 一般 > 註冊**，然後在分組索引標籤下方，選取**提示使用者選擇群組 ID** 作為**群組 ID 指派模式**。
 - 註冊時，系統會向使用者顯示子系 OG 清單 (屬於您所處的父亲系 OG)，使用者可以從中選取其群組 ID (註冊 OG)。此選項不需要您執行群組指派對應，且使用者可任意從清單中選取任何子系 OG。

如果未在註冊前與使用者通訊群組 ID，且使用者不屬於某一使用者群組，則註冊 OG 會變成...

3. 以自動探索群組 ID 為基礎的 OG

- 若要設定此選項，請導覽至**群組與設定 > 所有設定 > 裝置與使用者 > 一般 > 註冊**，然後在**驗證索引標籤**下方，新增與使用者工作電子郵件地址相對應的電子郵件網域。如需**驗證索引標籤**的詳細資訊，請參閱**配置註冊選項**。
 - 註冊時，系統會提示使用者輸入其工作電子郵件地址。系統會根據輸入的電子郵件地址網域，自動將使用者的裝置註冊到適當的 OG。

如果未設定上述任何選項，則註冊 OG 會變成...

4. 新增使用者時選取的 OG

- 當您在 Workspace ONE UEM Console 中新增使用者時，若要設定此選項，請導覽至**帳戶 > 使用者 > 清單視圖**，然後依序選取**新增**、**新增使用者**。在顯示的**新增/編輯使用者**畫面中，向下捲動並開啟**註冊區段**。完成**註冊企業群組**選項。
- 或者，如果您在**新增/編輯使用者**畫面的**註冊區段**中選取無 OG，則該使用者的註冊 OG 將成為您在新增使用者時所處的 OG。

Workspace ONE 直接註冊

在 Workspace ONE UEM 中直接註冊可讓您盡快地註冊裝置。

直接註冊是公司所屬與個人啟用之裝置 (COPE) 的最平穩註冊方式。COPE 型號可為企業提供方式，讓企業可在裝置消費以及 IT 需要的安全性和控制之間取得平衡。

身為管理員，您可以使用想要的選項來設定直接註冊。這些選項包含選擇性提示、依裝置類型限制、依使用者群組限制，以及延遲使用者安裝應用程式。

啟用 Workspace ONE 的直接註冊

您可針對完成偏好設定的企業群組 (OG) 啟用 Workspace ONE™ 直接註冊。啟用後，所有符合資格的裝置在第一次登入 Workspace ONE UEM 後都會直接註冊。不合資格的裝置，如果與您定義的條件不符，則會註冊為不受管理或容器狀態。

直接註冊預設為停用。若要啟用 Workspace ONE 直接註冊，請採取以下步驟。

- 1 切換到您想要啟用 Workspace ONE 直接註冊的企業群組。
- 2 導覽至 **群組 & 設定 > 所有設定 > 裝置 & 使用者 > 一般 > 註冊**，然後選取**限制索引標籤**。
- 3 如有必要，請選取為覆寫父級 OG 設定。
- 4 向下捲動至 **Workspace ONE 管理需求**，然後選取您的配置選項。

設定	描述
Workspace ONE 需要 MDM	登入 Workspace ONE 時，提示符合資格的裝置和使用者必須立即註冊。 不符定義條件的裝置能夠以不受管理的狀態註冊，且之後可能會變更為受管理的狀態 (可調式管理)。
指派的使用者群組	此設定會指定您想要納入直接註冊程序的使用者群組。您也可以選取 所有使用者 ，此為啟用 Workspace ONE 需要 MDM 時的預設選取項目。
iOS	啟用此設定以納入 iOS 裝置。停用時，iOS 裝置不符合直接註冊的資格，不過仍能夠以不受管理的狀態註冊至 Workspace ONE UEM。
Android 舊版	啟用此選項以納入舊版 Android 裝置。停用時，舊版 Android 裝置不符合直接註冊的資格，不過仍可以不受管理的狀態註冊至 Workspace ONE UEM。
Android Enterprise	啟用此設定以納入 Android 企業裝置。停用時，Android Enterprise 裝置不符合直接註冊的資格，不過仍可以不受管理的狀態註冊至 Workspace ONE UEM。

結果：只有在其他註冊索引標籤中配置的支援選項，可套用到已儲存的直接註冊組態。

下一步：Workspace ONE 直接註冊啟用後，下一步就是**使用 Workspace ONE 直接註冊來註冊裝置**。如需 Workspace ONE 直接註冊選項和註冊選項的相關資訊，請參閱此頁面的其他區段。

使用 Workspace ONE 直接註冊來註冊您的裝置

啟用 Workspace ONE™ 直接註冊後，只要透過 Workspace ONE APP 使用符合資格的裝置和使用者登入註冊企業群組，您就能立即完成註冊。

您的使用者也可以立即安裝公司認為實用的 APP。如果他們想要稍後再安裝應用程式，也可以略過此步驟。若要使用 Workspace ONE 直接註冊來註冊裝置，終端使用者必須採取下列步驟。

- 1 從平台專用的 APP 商店或貯存器下載、安裝並執行 Workspace ONE APP。
- 2 輸入伺服器網址或電子郵件地址。
- 3 輸入目錄服務使用者名稱和密碼。
- 4 選取平台特定的確認步驟，以安裝或啟用 **Workspace Services**。
 - a **iOS** – 允許伺服器開啟**設定**，輸入裝置密碼，安裝未簽署的裝置設定檔，並在 Workspace 中開啟畫面。

- b **Android 舊版** – 安裝 Workspace ONE Intelligent Hub，允許其建立與管理通話，利用輸入裝置資產編號的選項來選取裝置擁有權，啟動裝置管理員應用程式，然後登入 Workspace ONE。
 - c **Android 企業版** – 接受 (或拒絕) 使用協議條款，設定工作設定檔，並建立 Workspace ONE 密碼。
- 5 Workspace ONE 完成安裝例行工作時，您就可以**繼續安裝 APP**。
 - 6 您可以安裝選取自清單的個別 APP、**全部安裝**，或完全**略過**此步驟。

Workspace ONE 直接註冊支援的選項

Workspace ONE 直接註冊功能可用於許多在此功能開發之前即推出的現有註冊選項和平台。

Workspace ONE™ 的直接註冊支援以下平台和註冊選項。

支援的平台

- iOS。
- Android 舊版。
- Android Enterprise。

導覽至**群組 & 設定 > 所有設定 > 裝置&使用者 > 一般 > 註冊**，選取每個適用的標籤，然後根據與 Workspace ONE 直接註冊的相容性進行選取。

驗證

以下是與 Workspace ONE 直接註冊相容的驗證選項。

- 目錄使用者。
- SAML 和 Active Directory 使用者受到「即時」支援。只要在初次登入時有使用者記錄存在於 Workspace ONE UEM 中，即支援未使用 LDAP 的 SAML 使用者。
目前不支援基本使用者、註冊預備使用者、未使用目錄的 SAML 使用者，以及 Authentication Proxy 使用者。
- 開放式註冊。
- Workspace ONE 不會稽核「要求 iOS 或 macOS 使用 Workspace ONE Intelligent Hub」設定；這些設定可用來封鎖其各自平台上的 Web 註冊。

使用條款

所有使用條款選項皆與 Workspace ONE 直接註冊相容。

分組

所有分組選項皆與 Workspace ONE 直接註冊相容。

限制

以下是與 Workspace ONE 直接註冊相容的限制選項。

- 已知的使用者和已配置的群組。
- 已註冊的裝置數上限。
- 原則設定受到部分支援。
 - 允許的擁有權類型 – Workspace ONE 只會對員工擁有和公司專用的類型發出提示。如果您不想看見兩者的提示，請停用選擇性提示，並使用預設的擁有權類型。
 - 不支援「允許的註冊類型」。
- 支援裝置平台、裝置型號和作業系統限制。
- 使用者群組限制。

選擇性提示

以下是與 Workspace ONE 直接註冊相容的選擇性提示選項。

- 裝置擁有權提示。
- 資產號碼提示 (只有在 [裝置擁有權提示] 已啟用時才支援)。
- 不支援其他所有的選擇性提示。

自訂

以下是與 Workspace ONE 直接註冊相容的自訂選項。

- 為各平台使用特定的訊息範本。
- 註冊後的登陸 URL (僅限 iOS)。
- MDM 設定檔訊息 (僅限 iOS)。
- 使用自訂 MDM 應用程式。
- 不支援「註冊支援電子郵件」和「註冊支援電話」。

註冊預備

不支援透過 Workspace ONE 直接註冊進行裝置註冊預備。如果您必須為單一或多個使用者進行裝置註冊預備，您必須使用 Workspace ONE Intelligent Hub 註冊裝置，而不是使用 Workspace ONE 直接註冊。

裝置設定檔是您在 Workspace ONE UEM powered by AirWatch 中管理裝置的主要方式。在設定檔與合規原則合併時，它們可協助您強制執行公司規則和程序的設定及規定。

先為每種平台類型建立設定檔，然後再為每種平台類型配置具有您所配置之個別設定的裝載。

建立設定檔的程序包括依序指定**一般**設定與**裝載**設定。

- **一般**設定會決定如何部署設定檔，以及誰可接收此設定檔。
- 而設定檔的**裝載**實際上包含了限制本身，以及會在設定檔安裝後套用至裝置的其他各項設定。

本章節討論下列主題：

- [設定檔處理](#)
- [新增一般設定檔設定](#)
- [裝置設定檔清單檢視](#)
- [技術預覽：工作流程中使用的設定檔和設定檔資源](#)
- [裝置設定檔編輯](#)
- [合規設定檔](#)
- [設定檔資源](#)
- [地理柵欄區域](#)
- [時間排程](#)
- [檢視裝置指派、裝置設定檔](#)

設定檔處理

裝置設定檔為 Workspace ONE UEM 的裝置管理提供標準化基礎。請務必瞭解處理裝置設定檔的方法 (包括設定檔安裝失敗時的重試邏輯)。

將裝置設定檔指派給裝置後，其會經歷以下程序。

- 1 設定檔會排入安裝佇列。
- 2 裝置會與裝置服務連線，以便接收安裝設定檔。
 - 若連線成功，則設定檔安裝狀態會變成「擱置中」。

- 若連線失敗，則在下一個裝置簽入時，設定檔會再次排入安裝佇列 (步驟 1)。

3 裝置會安裝設定檔。

- 若安裝成功，則設定檔安裝狀態會變成「已處理」。
- 若安裝失敗，則在下一個裝置簽入時，設定檔會再次排入安裝佇列 (步驟 1)。

效能微調

處理和發佈裝置設定檔，例如與憑證相關的設定檔，將對伺服器造成巨大壓力，必須加以管理才能緩減。針對最耗處理器資源的裝置設定檔類型，Workspace ONE UEM Console 會使用批次處理邏輯。

此批次處理邏輯可透過導覽至 **群組 & 設定 > 所有設定 > 安裝 > 效能微調** 進行調整。

設定	描述
大量發佈交付頻率	設定檔會推送到各交易在此處輸入的裝置數目。最小值為 1000。最大值為 50000。預設值為 40000。
取樣排程器間隔 (分鐘)	此設定會決定排程器從裝置中提取樣本的頻率，以分鐘為單位。最小值為 1。最大值為 1440 (24 小時)。預設值為 5。
最小取樣時間間隔 (小時)	
iOS 裝置每秒邀請次數	這是每秒受邀請透過 APNs 輸出訊息簽入裝置服務的 iOS 裝置數。最小值為 4。預設值為 30。建議最大值為 120。
憑證設定檔發佈的頻率	這是整個環境中，可在任何時間點發布的憑證設定檔安裝命令數上限。預設值為 50。
佇列命令數量 (上限)	這是佇列允許的最大命令數。命令會根據憑證設定檔發佈頻率進行發佈，直到達到此限制。裝置耗用命令後，會排入更多命令至佇列。 您在此處輸入的值乘以「憑證設定檔發佈頻率」，即為最大數目。可增加此數目以改善憑證批次，不過，您應考慮密切監控 CA 和 DS 伺服器效能。預設值為 10。
憑證佇列節流	如果裝置未耗用根據憑證設定檔發佈頻率新增的命令，依預設，下一批次會在 15 分鐘內排入佇列。可減少此時間間隔以改善憑證批次，不過，您應考慮密切監控 CA 和 DS 伺服器效能。
憑證設定檔手動安裝臨界值	這是每個管理員、每個設定檔版本可從儀表板排入佇列的憑證設定檔安裝命令數上限。預設值為 100。
每秒最大 Apple API Calls 的限制 (適用於邀請 VPP 使用者)	指定對 Apple VPP 伺服器的每秒呼叫數上限。最小值為 1。最大值為 1000。預設值為 30。
執行即時合規性	
允許以分鐘為最小合規性間隔來計算	啟用以建立合規性原則，並設定以分鐘基礎為間隔來進行合規性向上提報動作。依照在此環境下已註冊裝置的數量，系統效能可能會受影響。在啟用此選項前請考慮這些可能要素。
內部用應用程式部署的批次大小	此值指定內部應用程式部署的批次所包含的裝置數量。最小值為 1。最大值為 10000。預設值為 100。
此時間過後將應用程式 UEM 指令標記為過時:	此依據平台的時間限制會定義在命令被視為「過時」之前最後一個 UEM 命令 (裝置已確認但尚未執行) 之後的時間長度。發佈應用程式後，會重新觸發過時命令。 應用程式目錄將不再向終端使用者顯示「處理中」狀態的應用程式，而是改為重新啟用「安裝」或「更新」動作。
MDM 應用程式清單取樣間隔 (分鐘)	最小值為 1。預設值為 480。
Windows 應用程式清單取樣基本輪詢時間 (分鐘)	最小值為 1。最大值為 1440。預設值為 5。

設定	描述
同步 VPP 應用程式授權的批次大小	此設定會指定每個批次與 VPP 雲端同步時所包含的應用程式數量。最小值為 1。最大值為 250。預設值為 250。
失敗的應用程式安裝重設間隔 (分鐘)	此設定會指定嘗試重新安裝失敗的應用程式安裝前所需等待的時間。最小值為 15。最大值為 10000。預設值為 60。
應用程式 (Windows) 安裝失敗後，可以再重試的次數上限	指定重試失敗安裝的次數上限。最小值為 0。最大值為 8。預設值為 5。
安裝失敗後，再重試之裝置批次的大小	此設定指定嘗試重新安裝失敗的應用程式安裝時包含的最大裝置數量。最小值為 1。最大值為 15000。預設值為 10000。
以裝置為基礎的 VPP 應用程式自動更新的頻率 (小時)	您可以自動更新以裝置為基礎的 VPP 應用程式。此設定會控制這些更新發生的頻率，以小時為單位。最小值為 1。最大值為 24。預設值為 1。
要用於檢查應用程式版本更新的應用程式清單大小	當系統檢查應用程式的新版本時，此設定會指定要檢查的應用程式清單大小。最小值為 20。最大值為 100。預設值為 20。
在註冊時不批次處理即安裝憑證設定檔	決定憑證設定檔命令是否以批次傳送。 若啟用，新註冊的憑證設定檔安裝命令將略過批次邏輯。 若停用，新註冊的憑證設定檔安裝命令將套用批次邏輯。
企業群組的 VPP 授權計數同步間隔 (小時)	這是排程器選擇企業群組來執行同步授權計數所花的最小時間量 (以小時為單位)。最小值為 2。最大值為 24。預設值為 6。
在同步 VPP 授權計數時每個批次的企業群組數量	此為排程器每次執行同步 VPP 授權計數工作時可以選擇的企業群組數量。最小值為 1。最大值為 50。預設值為 10。
自動刪除原廠 PPKG	啟用時，會自動刪除已上傳至裝置的產品佈建套件，以節省裝置儲存空間。 停用時，會在裝置上保留 PP 套件。
刪除 PPKG 前的天數	僅當自動刪除原廠 PPKG 啟用時，才能使用此設定。 此設定可決定從裝置移除 PPKG 檔案之前的天數。最小值為 0 (立即刪除)。最大值為 90。預設值為 5。
產品佈建 AWCM 節流速率	代表 AirWatch 雲端傳訊程式 (AWCM) 每秒傳送的通知數。根據隨附的 產品佈建大小 表格，使此節流速率與 產品佈建命令發行批次大小 一致。 最小值為 1。最大值為 100。預設值為 2。
產品佈建命令發行批次大小	產品佈建命令會以擱置狀態建立。此設定代表每個批次發行工作時間間隔中，從裝置命令佇列發行的命令數。 名為「產品佈建批次發行工作」的排程器工作 (位於 群組 & 設定 > 所有設定 > 管理員 > 排程器) 可控制命令佇列的發行頻率。 此設定可控制每個間隔發行的命令數，並與 產品佈建 AWCM 調節速率 保持一致。這兩項設定都是以您環境中的裝置服務 (DS) 伺服器數目為基礎，如 產品佈建大小 表格中所述。 最小值為 1。最大值為 10000。預設值為 200。
Apple 設定檔安裝批次大小	此值會設定每批次新增至命令佇列的設定檔命令數。此設定的目的是管理所要處理的命令流程，以防程式逾時。最小值為 300。最大值為 1000。預設值為 300。

產品佈建大小

DS 伺服器數	AWCM 節流速率	命令發行批次大小
1	2	200
2	4	400

3	6	600
4	8	800
5	10	1000

新增一般設定檔設定

以下這些設定檔的設定和選項，可套用於 Workspace ONE UEM powered by AirWatch 管理下的大部分平台，並可作為一般參考之用。然而，有些平台會提供一些不同的選項。以下的步驟和設定可套用至任何設定檔。

程序

1 導覽至資源 > 設定檔與基準 > 設定檔 > 新增。

您可以選取下列任一選項來新增設定檔。

- **新增設定檔** – 執行單次新增裝置設定檔。
- **上傳設定檔** – 在您的裝置上傳一個已簽署的設定檔。
- **批次匯入** – 透過以逗點分隔值 (.csv) 的檔案，大量匯入新的裝置設定檔。輸入一個特殊名稱和描述，以便同時分組和統整多重設定檔。

2 選擇新增設定檔。

3 為您所要部署的設定檔，選擇適當的平台。

裝載設定可能依平台而異。

4 請完成下列設定以完成一般標籤。

設定	描述
名稱	Workspace ONE UEM Console 所顯示的設定檔名稱。
版本	回報設定檔目前版本的唯讀文字方塊，依 新增版本 而定。
描述	簡短描述設定檔的使用目的。
OEM 設定 (僅限 Android)	啟用 OEM 設定以為 Zebra 和 Samsung 裝置設定專屬設定檔。啟用後，設定檔會附上 Knox 符號，表示該設定檔是 Knox 專屬的可用設定。系統會顯示兩個新的設定檔： 日期/時間 和 APN ，且這兩個設定檔為 Knox 專屬。此選項只會在設定 Android 設定檔時顯示。
選取 OEM (僅限 Android)	選取 OEM Samsung 或 Zebra 。此選項只會在設定 Android 設定檔時顯示。
部署	決定是否在取消註冊時，也同時自動移除該設定檔 (不適用於 Android 設定檔)。 <ul style="list-style-type: none"> ■ 納管 – 移除設定檔。 ■ 手動 – 除非終端使用者手動移除設定檔，否則會維持安裝狀態。
設定檔範圍 (僅限 Android 或 Windows Rugged)	判斷使用設定檔的方式。從下列方式中選取。 <ul style="list-style-type: none"> ■ 生產 – 設定檔將被用於產品佈建。 ■ 註冊預備 – 設定檔將被用於註冊預備設定。 ■ 兩者皆選 – 設定檔將被同時用於註冊預備和佈建。

設定	描述
指派類型	<p>判斷設定檔部署到裝置的方式。</p> <ul style="list-style-type: none"> ■ 自動 - 設定檔會自動部署到所有裝置。 ■ 選用 - 終端使用者可選擇從自助入口網站 (SSP) 安裝設定檔，也可由管理員自行決定部署至個別裝置。 <p>終端使用者也可以使用 Web Clip 或書籤裝載來安裝代表 Web 應用程式的設定檔。如果您配置裝載以在 APP 目錄中顯示，那麼您就可以從 APP 目錄中安裝。</p> <ul style="list-style-type: none"> ■ 互動式 - (不適用於 iOS 或 Android)。此設定檔為終端使用者透過自助入口網站安裝的獨特類型。安裝完畢後，這些特殊類型的設定檔會與外部系統進行互動，以產生要傳送到裝置上的資料。只有依以下的步驟啟用後，才能使用此選項：群組 & 設定 > 所有設定 > 裝置 & 使用者 > 進階 > 設定檔選項。 ■ 合規 - 若使用者未能採取補救措施使得裝置合規，設定檔將由合規引擎套用於裝置。如需進一步資訊，請參閱合規設定檔。
允許移除	<p>(只適用於 iOS 7 及更早版本) 判斷終端使用者是否能移除設定檔。</p> <ul style="list-style-type: none"> ■ 始終允許 - 終端使用者可隨時手動移除設定檔。 ■ 經過授權 - 終端使用者必須經過管理員授權才能移除設定檔。選取此項目會新增一個帳戶密碼文字方塊。 ■ 永不允許 - 終端使用者無法從裝置移除設定檔。
管理者	具備設定檔管理存取權的企業群組。
已指派的群組	<p>指派的群組指的是要加入裝置設定檔的群組。其中包括建立新的智慧群組之選項，您可以利用最低作業系統的規格要求、裝置型號、擁有權類別和企業群組等來進行配置。</p> <p>雖然「平台」是智慧群組的一項準則，但是在裝置設定檔或合規原則中所配置的平台，其重要性始終都比智慧群組的平台優先。舉例來說，如果某裝置設定檔是為 iOS 平台所建立的，即使智慧群組中含有 Android 裝置，設定檔還是只會指派到 iOS 裝置上。</p>
排除項目	如果選取 是 ，畫面就會顯示新的文字方塊 排除的群組 。此文字方塊可讓您選取要從裝置設定檔的指派中排除的群組。
檢視裝置指派	在您選取 指派群組 後，您可以預覽所有指派裝置的清單，並將智慧群組指派項目和排除項目列入考量。
其他指派標準	<p>這些勾選方格可提供額外的設定檔限制。</p> <ul style="list-style-type: none"> ■ 僅在選定選區域內的裝置上進行安裝 - 輸入世界上任何地方的地址，以及以公里或英里計算的半徑，即可設定「設定檔安裝週界」。如需詳細資訊，請參閱地理柵欄區域。 ■ 啟用排程，並只在選定的時間內安裝 - 指定配置的時間排程，讓裝置只在該時間範圍內接收設定檔。選取此項即會新增一個必要的指派的排程文字方塊。如需進一步資訊，請參閱時間排程。
移除日期	從裝置上移除設定檔的日期。必須是未來的日期，且格式為 MM/DD/YYYY。

- 為裝置平台配置**裝載**。您可以在裝載清單上方的**尋找裝載**文字方塊中輸入關鍵字，依名稱搜尋裝載。有關配置某平台之特定**裝載**的逐步說明，請參閱 docs.vmware.com 上適用的**平台指南**。
- 選取**儲存並發佈**。

裝置設定檔清單檢視

在 Workspace ONE UEM 中建好並指派設定檔後，您還必須能夠從遠端的單一來源，個別管理這些設定。資源 > 設定檔與基準 > 設定檔可讓您集中整理並針對設定檔採取動作。

您也可以使用**篩選條件**、**版面配置**和**欄位排序**來量身訂做自己的清單，使其根據您所指定的準則來列出所有裝置設定檔。您也可將這些清單匯出為 CSV 檔案，以便使用 Excel 來檢視，並查看裝置設定檔的狀態。

Filters	ADD	LAYOUT	EXPORT	Search List			
Status	Profile Details	Payloads	Managed By	Assignment Type	Assigned Groups	Installed Status	Status
Active	Apple iOS VPN	1	perapp_vac	Auto		Not Assigned	✓
All	bookmark Android (Legacy) Bookmarks	1	Android	Auto	All Devices	0 16 16	✓
Any	SofiaGer Apple iOS Passcode	1	i18n	Auto	All Corporate Dedicated Devices	2 0 2	✓
	lpulse Android VPN	1	qalady	Auto	qalady	0 0 0	✓
	lpupda Windows Desktop Windows Updates	1	bandi	Auto	All Devices	0 0 0	✓
	lcvetest Apple iOS Credentials	1	TechDoc	Auto		Not Assigned	✓
	ltest Apple iOS - Device Passcode, Restrictions	2	hedu	Optional	child test	0 0 0	✓
	lpupda Windows Desktop - Device Windows Updates	1	bandi	Auto	All Devices	0 0 0	✓
	lpupda Windows Desktop - Device Windows Updates	1	bandi	Auto	All Devices	0 0 0	✓

裝置設定檔暫留快顯視窗

設定檔詳細資料欄位中每個裝置設定檔的右上方都有一個工具提示圖示。若輕觸此圖示 (行動觸控裝置) 或滑鼠游標暫留在圖示上 (PC 或 Mac)，將會顯示暫留快顯視窗。

此快顯包含設定檔資訊，例如**設定檔名稱**、**平台**和所包含的裝載**類型**。



在**設定檔清單**檢視中的**指派的群組**欄位，可以找到一個類似的工具提示圖示，具有「暫留快顯視窗」功能並顯示**指派的智慧群組**和**部署類型**。

裝置設定檔唯讀檢視

當一個企業群組 (OG) 建立並管理某「裝置設定檔」時，另一個層級較低的管理員登入系統後，僅可以唯讀狀態存取該設定檔。該設定檔視窗會透過新增下列特殊註解來反映此唯讀狀態：「此設定檔為階層較高的企業群組所管理，無法進行編輯。」

這項唯讀限制也會套用至所有智慧群組指派。若在父級 OG 建立設定檔並指派給智慧群組，則子 OG 管理員可以查看但不能編輯設定檔。

此舉除了促進管理員之間交流，還可以維持階層式的安全性。

清單檢視選項

設定	描述
篩選條件	<p>使用下列篩選條件即可僅檢視您想要的設定檔。</p> <ul style="list-style-type: none"> ■ 狀態 - 透過使用中、非使用中或所有裝置來篩選出要檢視的裝置。 ■ 平台 - 依據來 13 種不同類型的平台，或所有平台來透過篩選出要檢視的裝置。 ■ 智慧群組 - 依據下拉式功能表中所選擇的智慧群組來篩選出要檢視的裝置。
版面配置	<p>讓您自訂清單的欄位配置。</p> <ul style="list-style-type: none"> ■ 摘要 - 利用預設欄位和檢視設定來查看清單檢視。 ■ 自訂 - 在清單檢視中僅選擇您要的資訊。您也可以將所選欄位套用至目前所有的企業群組及其下層的所有管理員。
匯出 	<p>儲存完整清單檢視的 XLSX 或 CSV (逗點分隔值) 檔案，可在 MS Excel 中檢視及分析。如果您已在清單檢視套用篩選條件，匯出的清單也反映篩選結果。</p>
欄位排序	<p>選取欄位標頭即可切換清單的排序方式。</p>
設定檔詳細資料	<p>在摘要和自訂視圖中，皆會於設定檔詳細資料欄位中顯示名稱、平台和裝載類型。</p>
裝載	<p>顯示裝置設定檔中指定的裝載數目。</p>

設定	描述
安裝狀態	<p>該欄位會藉由三種圖示指示器來顯示設定檔安裝狀態，每種指示器都有超文字數字連結。選擇此連結會顯示 檢視裝置 頁面，也就是在所選類別中受到影響的裝置清單。</p> <ul style="list-style-type: none"> ■ 安裝擱置中 (🕒) - 此指示器會顯示已排程安裝設定檔的裝置數。 ■ 已安裝 (✅) - 此指示器會顯示受指派並成功安裝設定檔上的裝置數量。 ■ 未安裝 (❌) - 此指示器會顯示受指派卻未安裝設定檔的裝置數量。 ■ 已指派 (👤) - 此指示器會顯示已安裝或未安裝的受指派設定檔總數。 ■ 移除擱置中 (⊕) - 此指示器會顯示已排程移除的設定檔總數。 ■ 已移除 (✖) - 此指示器會顯示已移除的設定檔總數。 ■ 過時 (⚠) - 已安裝的設定檔有更新版本可供使用時，即會顯示此指示器。 ■ 待處理的資訊 (⚠) 設定檔處於「擱置」狀態時，即會顯示此指示器。此狀態的一般範例包括保持需要來自第三方伺服器資訊的設定檔為擱置狀態 (例如，涉及 Websense 和 zScaler 的 VPN 設定檔，以及需要 CA 資料的憑證設定檔)，直到與這些伺服器聯絡及取得先決資訊。 ■ 未指派 - 在設定檔已定義和儲存但尚未指派給裝置時，會顯示此純文字指示器。 ■ 不適用 - 已定義、已儲存和已指派設定檔，但其組態中的詳細資料會讓設定檔無法適用於所指派的裝置時，會顯示這個純文字指示器。 ■ 安裝失敗 - 已定義、已儲存和已指派設定檔，但發生錯誤而無法成功安裝時，會顯示這個純文字指示器。
選項按鈕和編輯圖示	<p>清單檢視中，在每個設定檔的左側有一個選項按鈕和編輯圖示。選取編輯圖示 (✎)，可讓您對設定檔組態進行基本變更。選擇單一選項按鈕，裝置 按鈕、XML 按鈕以及 更多動作 按鈕將出現在清單上方。</p> <ul style="list-style-type: none"> ■ 裝置 - 檢視可供該設定檔使用的裝置、設定檔是否已安裝，若未安裝，則查看原因。審查您的團隊中已有哪些裝置，並在需要時手動推播設定檔。 ■ </> XML - 顯示設定檔建立後 Workspace ONE UEM 產生的 XML 程式碼。檢視並儲存 XML 碼，以便在主控台外重新使用或進行變更。 ■ 更多動作 <ul style="list-style-type: none"> ■ 複製 - 複製現有的設定檔並調整該複本之配置內容，以便開始使用裝置設定檔。 ■ 啟動/停用 - 切換裝置設定檔之使用與停用狀態。 ■ 刪除 - 透過移除不必要的設定檔，來維護您的設定檔名冊。

確認裝置設定檔安裝

在設定檔未安裝於目標裝置的罕見案例中，**檢視裝置** 畫面讓您能夠查看特定原因。

設定檔安裝狀態

- 1 導覽至 **資源 > 設定檔與基準 > 設定檔**，然後查看顯示的清單。
- 2 檢閱 **安裝狀態** 欄位，然後選取在指示器圖示右側顯示的號碼連結，以開啟 **檢視裝置** 畫面。如需指示器圖示的詳細資訊，請參閱 **裝置設定檔清單視圖** 中的 **安裝狀態** 定義。

View Devices - 3rd_Party_VPN

Last Update: Friday, March 9, 2018 2:50 PM

Installed  

Status	Friendly Name	C/E/S	User	Platform/OS/Model	Organization Group	Updated
✔ Installed	192.168.191.3Android Android 5.1.1		ws1supportdevs...	Android / 5.1.1 / Android	Android Garnet Integration	Monday, February 26, 2018 2:02 AM
✔ Installed	sakshis Android Android 8.0.0 4REJ		ws1supportdevs...	Android / 8.0.0 / Android	afwchild	Monday, February 5, 2018 10:42 AM

Items 1-2 of 2

Page Size: 50

結果：即會顯示**檢視裝置 - <設定檔名稱>**畫面。

- (選用) 選取**匯出圖示** ().Excel 可用來閱讀和分析 CSV 檔案。
- (可選) 選取**可用欄圖示** ()，以自訂要在**檢視裝置**頁面中顯示哪些欄。

檢視 iOS 裝置命令狀態欄位

iOS 裝置在**檢視裝置**畫面上有**指令狀態**欄位，其中包含與選取的 iOS 裝置有關的安裝狀態。[指令狀態] 欄位會顯示下列狀態。

- **錯誤** – 顯示為連結，當選取該連結時，會顯示適用於裝置的特定錯誤碼。
- **擱置** – 當裝置列入進行中的憑證批次處理程序時，會顯示此訊息。
- **不適用** – 如果設定檔指派沒有影響裝置，但仍屬於智慧群組或部署的一部分，就會顯示。例如，當該設定檔類型不受到管理時。
- **不是現在** – 當裝置為鎖定或使用中，會顯示此訊息。
- **擱置中** – 當安裝指令已排入佇列並且會按時完成時，就會顯示此訊息。
- **成功** – 當設定檔安裝成功時，會顯示此訊息。

技術預覽：工作流程中使用的設定檔和設定檔資源

若要查看多少 Freestyle 工作流程包含設定檔或設定檔資源，請從清單檢視中選取設定檔，然後選取**檢視工作流程**連結。對裝置設定檔和設定檔資源所做的變更會反映在使用該設定檔和資源的工作流程中。

備註 Workspace ONE UEM 提供 Freestyle Orchestrator 工作流程作為提供給 SaaS 客戶的技術預覽功能。如需詳細資訊，請參閱[什麼是 Freestyle Orchestrator](#)。

技術預覽功能尚未經過完整測試，某些功能可能無法如預期般運作。但是，這些預覽可協助 Workspace ONE UEM 改善目前的功能並開發未來的增強功能。本節中的內容僅適用於參與技術預覽的客戶。如果您參與技術預覽功能，且想要在工作流程中使用應用程式或特定版本的應用程式，請考慮下列內容：

設定檔通知

導覽至**資源 > 設定檔與基準 > 設定檔**。當您選取在 Freestyle 工作流程中使用的裝置設定檔時，會看到下列通知。

 This profile is used in workflows, updating it will have some effect on devices in the workflows as well. [View Workflow](#)

 Workflows that include this profile, use the assignment and deployment settings defined in that workflow.

當您選取**檢視工作流程**連結時，**設定檔的工作流程**畫面會顯示使用所選設定檔的所有 **Freestyle** 工作流程，包括工作流程說明、指派的群組，以及建立工作流程的日期。

正在處理

屬於智慧群組指派的設定檔也可用於 **Freestyle** 工作流程。若有任何裝置是智慧群組和工作流程指派所共用，以工作流程為先。

工作流程優先順序的例外狀況是當**指派類型**設「自動」時，此時直接指派為先。導覽至**資源 > 設定檔與基準 > 設定檔 > 新增 > 新增設定檔**，選取平台後，**指派類型**選項即會出現在**一般**裝載畫面中。

變更設定檔

如果您變更工作流程中使用的設定檔，這些變更會自動推送至工作流程。

您不能刪除工作流程中使用的設定檔。必須先透過編輯工作流程的方式，從工作流程中移除設定檔。如需詳細資訊，請參閱 [Freestyle Orchestrator 指南](#)。

設定檔資源

與裝置設定檔變更會影響工作流程的情況類似，如果您變更工作流程中使用的 **Windows** 設定檔資源，這些變更會以相同的方式推送至工作流程。

可以在**編輯資源**畫面的**指派**索引標籤，識別含有該設定檔資源的工作流程名稱。

如需有關設定檔資源的詳細資訊，請參閱[設定檔資源](#)。

裝置設定檔編輯

透過 **Workspace ONE UEM powered by AirWatch**，您可以編輯已經在您團隊裝置上安裝的某個裝置設定檔。您可以對任何裝置設定檔進行下列兩種變更。

- **一般** – 一般設定檔設定可用於管理設定檔的發佈事宜：以何種方式指派設定檔、由哪個企業群組所管理、指派到哪個智慧群組以及從哪個智慧群組中排除。
- **裝載** – 裝載設定檔設定會影響裝置本身：密碼要求、裝置限制 (比如使用相機或擷取畫面功能)、Wi-Fi 設定、VPN 等等。

既然裝置本身的操作不會受到影響，您通常可以不需要重新發佈該設定檔來進行**一般**變更。儲存此變更僅會將設定檔推播至未指派給該設定檔的裝置。

然而**裝載**變更因為會影響裝置本身的操作，一定得重新發佈到所有新的及現有裝置上才行。

編輯一般裝置設定檔設定

一般設定檔設定包括僅可管理其分發的變更。此分發包括如何指派設定檔，由哪個企業群組 (OG) 管理，以及指派給哪個指派群組/在哪個指派群組中排除。

- 1 導覽至 **資源 > 設定檔與基準 > 設定檔**。
- 2 找出您要編輯的設定檔，並選取其 **編輯** 圖示 (✎)。
唯一可編輯的設定檔是企業群組 (或其下的子群組企業群組) 所管理的。
- 3 在 **一般** 類別中，進行任何您想要的變更。
- 4 在完成 **一般** 之中的變更後，您可以選取 **儲存並發佈**，將該設定檔套用在任何您已增加或移除的新裝置。

已有指派設定檔的裝置將會再次收到重新發佈的設定檔。**檢視裝置指派** 的畫面會顯示出來，讓您確認目前指派的裝置清單。

編輯裝載裝置設定檔設定

裝載設定檔設定包括了會影響裝置本身的變更：密碼要求、裝置限制 (比如使用相機或擷取畫面功能)、Wi-Fi 設定、VPN 等等。

新增版本 按鍵讓您可以建立設定檔的遞增版本，並能夠修改 **裝載** 設定。

- 1 若要啟用 **裝載** 編輯，影響裝置的操作，請選擇 **新增版本** 按鈕。
選取 **新增版本** 按鈕並儲存您的變更，即會重新發佈裝置設定檔至所有指派的裝置上。此重新發佈包含已有該設定檔的裝置。
有關配置特定 **裝載** 的逐步說明，請參閱 docs.vmware.com 所提供之適用的 **平台指南**。
- 2 在完成 **裝載** 的變更後，您可選擇 **儲存並發佈** 來將該設定檔套用到所有被指派的裝置上。

結果：系統會顯示 **檢視裝置指派** 畫面，讓您可以確認目前指派的裝置清單。

合規設定檔

要瞭解 Workspace ONE UEM powered by AirWatch 中的合規性設定檔，必須充分瞭解裝置設定檔和合規原則。裝置設定檔是裝置管理和安全性的基礎，而合規原則是防護閘，專門保護企業內容。

裝置設定檔可讓您控制各種裝置設定。這些設定包括密碼複雜性、地理柵欄，時間排程、裝置硬體功能、Wi-Fi、VPN、Email、憑證等等。

合規引擎會監視規則、強制執行動作並套用升級 (上述全都是您定義的)。但是合規設定檔會向合規引擎提供通常僅適用於裝置設定檔的所有選項和設定。更多相關的資訊，請參閱 [第 4 章 合規原則](#)。

例如，您可以建立與一般裝置設定檔相同的特殊裝置設定檔，但設定更嚴格。然後在定義合規原則時，將此特殊裝置設定檔套用至動作標籤。透過這種安排，如果使用者無法使其裝置合規，將可以套用更為嚴格的合規設定檔。

新增合規設定檔

您可以新增合規設定檔，結合同合規原則和裝置設定檔，同時享有這兩項功能的最佳優點。新增合規設定檔的程序分為兩部分：1) 建立裝置設定檔，然後 2) 在合規原則內指派視為「動作」的裝置設定檔。

合規性設定檔是以與「自動」和「可選的」裝置設定檔相同的方式來建立和儲存。

- 1 導覽至 **資源 > 設定檔與基準 > 設定檔**，然後依序選取**新增**和**新增設定檔**，接著選取一個平台。
- 2 為合規設定檔選擇**名稱**，以便稍後識別。
- 3 在**一般**設定檔標籤中，在**指派類型**下拉式設定中選擇「合規」。
- 4 完成剩餘的一般和裝載設定。
- 5 完成後，選擇**儲存 & 發佈**。
- 6 在合規原則中選取此設定檔。
- 7 導覽至 **裝置 > 合規原則 > 清單檢視**，選取**新增**，然後選取平台。
- 8 定義**規則**，然後選取**下一步**。
- 9 在**動作**標籤中選取以下項目。
 - a 將第一個下拉式功能表設定為「設定檔」。
 - b 將第二個下拉式功能表設定為「安裝合規設定檔」。
 - c 將第三個下拉式功能表設定為您命名的裝置設定檔。
- 10 選擇**下一步**，然後繼續配置剩餘的設定，包括指派和摘要標籤。
- 11 若要儲存合規原則，請選擇**完成**或**完成並啟用**。

如需完成裝置設定檔的逐步指示，請參閱[裝置設定檔編輯](#)。

如需完成合規原則的逐步說明，請參閱[新增合規原則](#)。

設定檔資源

設定檔資源在同時支援 iOS、Android 與 Windows 等多種裝置平台的 Workspace ONE UEM 部署中，能夠簡化 Wi-Fi、VPN 與 Exchange 裝載的佈建程序。

請為上述的任何裝載建立設定檔資源，並定義各裝置平台所接收的一般設定。接著您便可以選擇性地配置特定裝置的設定，而這些設定將僅套用至上述裝置。

設定檔資源可在裝置設定檔中個別定義、管理與部署。部署設定檔資源與裝置設定檔，可為您部署中支援的所有平台提供既深又廣的裝置管理選項。

您不必使用設定檔資源來部署 Wi-Fi、VPN 或 Exchange 設定。您仍能選擇為上述各平台的裝載各自建立裝置設定檔。若您希望能在各平台之間使用相同或類似的 Wi-Fi、VPN 或 Exchange 設定，請考慮部署設定檔資源。之後如常建立其他裝置設定檔即可進一步管理各平台的功能。

設定檔資源清單檢視

使用 Workspace ONE UEM 中的設定檔資源清單檢視來為您的設定檔資源集合進行新增與管理，包括個別資源組態的檢視、刪除和編輯等等。

新增設定檔資源

您可以新增設定檔資源，並藉此使用相同的 Exchange、Wi-Fi 和 VPN 設定來佈建您的多平台裝置機群。導覽至 **裝置 > 設定檔資源**，然後選取**新增資源**。您必須選取下列任一選項來新增資源。

- **Exchange** – 配置 Email 設定，以便與 Exchange Email 伺服器保持連線。
- **Wi-Fi** – 配置 Wi-Fi 連線設定，以便維持網路連線。
- **VPN** – 配置虛擬的私人網路設定，以便保有安全連線。

各設定檔資源均有三個不同的組態步驟。藉由指定**資源明細**、適用的**平台**，並將資源**指派**給裝置，即可建立設定檔資源。

- **資源明細**包含資源的名稱、說明、伺服器依存性，以及其他決定設定檔資源操作方式的重要設定。
- **平台**定義執行設定檔資源的裝置。
- **指派**決定設定檔資源的部署方式，包括企業群組、使用者群組和智慧群組。

管理資源

一旦設定檔資源收集到了一定程度，即可導覽至 **裝置 > 設定檔資源**，透過「篩選」、「檢視」、「編輯」和「刪除」資源來管理資源。

- **篩選**設定檔資源清單檢視，即可選擇顯示使用中、非使用中或全部的資源。
- 選取**平台**欄位中的超連結號碼，即可**檢視**設定檔資源所包含的不同平台。
 - 若要開啟設定檔資源的**進階設定**，請選取超連結平台名稱。
 - 若要開啟**檢視裝置**頁面，請在平台頁面的**已安裝/已指派**欄位選取超連結編號。此頁面會顯示指派至設定檔資源的裝置清單。
 - 若要檢視並匯出 XML 代碼並上傳憑證，請在平台頁面的 XML 欄中按一下**檢視**超連結。
- 若要**編輯**設定檔資源，請在**編輯資源**頁面中，針對顯示著**資源明細**區段的資源，選取其名稱連結。
 - 透過按一下資源清單左側的編輯鉛筆來編輯設定檔資源詳細資料 (✎)。若要繼續編輯**編輯資源**頁面中的其他區段，只需選取**下一個**按鈕即可。
 - 若要編輯設定檔資源的指派內容，請選取 [設定檔資源] 清單左側的選項按鈕，然後按一下**編輯指派**按鈕。
- 若要**刪除**設定檔資源，請選取資源清單左側的選項按鈕，然後按一下**刪除**按鈕。刪除資源會將資源設定為非使用中，直到從裝置中加以移除為止。

新增 Exchange 資源

您可以新增一項專用的資源，好讓裝置在受到 Workspace ONE UEM powered by AirWatch 管理的同時，具有收發安全性電子郵件通訊的方法。

如需查看概覽，請參閱[設定檔資源](#)。

程序

- 1 導覽至 **裝置 > 設定檔 & 資源 > 資源**，再依序選取**新增資源**和 **Exchange**，並完成下列設定。

設定	描述
資源明細	
資源名稱	Workspace ONE UEM Console 所顯示的設定檔名稱。
描述	簡短描述設定檔的使用目的。
連線資訊	
郵件用戶端	選取要與資源搭配使用的 Email 用戶端。
Exchange 主機	為 Email 帳戶輸入要包含在資源中的 Exchange 主機。
使用 SSL	為此郵件用戶端啟用安全通訊端層。
進階	
網域*	為電子郵件網域輸入查閱值。
使用者名稱*	為電子郵件使用者名稱輸入查閱值。
電子郵件地址*	為電子郵件地址輸入查閱值。
密碼	為 Email 帳戶輸入密碼。勾選 顯示字元 方格即可顯示未編輯的密碼。
身份識別憑證	選取 新增憑證 按鈕，上傳並附加憑證授權單位至 Email 帳戶。
要同步過去多少天的郵件	選取要同步的 Email 記錄長度。請從 3 天 、 1 週 、 2 週 、 1 個月 和 無限制 中加以選取。
同步行事曆	選取此項即可將您的裝置行事曆與 Exchange 行事曆同步。在 iOS 和 macOS 裝置上，此設定預設為啟用。
同步聯絡人	選取此項即可將您的裝置聯絡人與 Exchange 聯絡人同步。在 iOS 和 macOS 裝置上，此設定預設為啟用。

* 如需詳細資訊，請參閱[第 12 章 查閱值](#)。

- 2 按一下**下一步**，繼續選擇**平台**。請從下列項目中選擇支援的平台，並選擇使用**預設設定**或**進階設定**。

■ iOS。

設定	描述
使用 S/MIME。	使用安全多用途網際網路郵件延伸，一種公開金鑰加密和簽署標準。
S/MIME 憑證	僅當 使用 S/MIME 啟用時才能使用此項。若要在 Email 新增簽署憑證，選擇 新增憑證 。
S/MIME 加密憑證	僅當 使用 S/MIME 啟用時才能使用此項。若要新增加密憑證和經過數位簽署的 Email，選擇 新增憑證 。
啟用每個訊息切換。	僅當 使用 S/MIME 啟用時才能使用此項。允許終端使用者透過 iOS 本機郵件用戶端來選擇哪些個別 Email 訊息需要簽署並加密 (僅支援 iOS 8 以上版本的受監督裝置)。

設定	描述
設定與安全性	
禁止移動訊息。	禁止在 Exchange 信箱中，將郵件移到裝置的另一個信箱中。
禁止在第三方 APP 中使用。	禁止其他 APP 使用 Exchange 信箱來傳送訊息。
禁止同步處理最近使用的地址。	禁止系統在您使用 Exchange 傳送 Email 時提出聯絡人建議。
禁止 Mail Drop 功能。	禁止使用 Apple 的 Mail Drop 功能。

■ macOS。

設定	描述
內部的 Exchange 主機	供 EAS 使用的安全伺服器名稱。當您選擇了 本機郵件用戶端 ，便會出現此選項與下列各項。
連接埠	為指派來與內部 Exchange 主機溝通用的連接埠輸入埠號。
內部伺服器路徑	供 EAS 使用的安全伺服器位置。
內部 Exchange 主機使用 SSL。	若要與內部 Exchange 主機通訊，請啟用安全通訊端層 (SSL)。
外部 Exchange 主機。	供 EAS 使用的外部伺服器名稱。
連接埠	為指派來與外部 Exchange 主機溝通用的連接埠輸入埠號。
外部伺服器路徑	供 EAS 使用的外部伺服器位置。
外部 Exchange 主機使用 SSL。	若要與外部 Exchange 主機通訊，請啟用安全通訊端層 (SSL)。

■ Android。

設定	描述
設定	
要同步過去多少天的行事曆	在裝置行事曆上同步選取的過去天數。
允許同步工作	允許工作與裝置同步。
Email 截斷大小上限 (KB)	指明在將 Email 訊息同步到裝置時，在多大的額度後 Email 訊息即會被截斷 (以 kb 為單位)。
Email 簽名	輸入 Email 的簽名，此簽名將顯示在傳出的 Email 上。
略過 SSL 錯誤	允許裝置在 Agent 程序中略過 SSL 錯誤。
限制	
允許附件	允許在 Email 中加上附件。
附件大小上限	指定附件大小 (MB) 的上限。
允許轉寄 Email	允許轉寄 Email。

設定	描述
允許 HTML 格式	指定與裝置同步的 Email 是否可為 HTML 格式。 如果停用此設定，所有 Email 都將轉換為文字。
停用螢幕擷取畫面	不允許在裝置上擷取螢幕畫面。
同步間隔	輸入同步的間隔時間 (分鐘)。
同步排程的尖峰日期	<ul style="list-style-type: none"> ■ 排定同步的尖峰日期，以及在指定日期進行同步的開始時間和結束時間。 ■ 設置同步排程尖峰日期和同步排程離峰日期的頻率。 <ul style="list-style-type: none"> ■ 選取自動，則可在每次更新時自動同步電子郵件。 ■ 選取手動，則只在選取此項時才會同步電子郵件。 ■ 選取一個時間值，可在指定的排程時間同步電子郵件。 ■ 啟用使用 SSL、使用 TLS 和預設帳戶。
S/MIME 設定	<p>選擇使用 S/MIME，從這裡您可以在認證裝載上，選擇和您有關聯的 S/MIME 憑證作為使用者憑證。</p> <ul style="list-style-type: none"> ■ S/MIME 憑證 - 選擇要使用的憑證。 ■ 需要加密的 S/MIME 訊息 - 需要加密的 S/MIME 訊息。 ■ 需要簽署的 S/MIME 訊息 - 需要經過數位簽署的所有 S/MIME 訊息。 <p>如果您使用 S/MIME 憑證來加密，請提供移轉主機。</p>

■ **Windows 桌面。**

設定	描述
設定	
下一次同步時間間隔 (分鐘)	選擇裝置與 EAS 伺服器同步的頻率 (分鐘)。
診斷性記錄	記錄資訊，供進行疑難排解時使用。
內容類型	
允許 Email 同步	允許同步 Email 訊息。

3 按一下下一步，繼續進行**指派**。

4 若要將資源指派至裝置，請完成下列設定。

設定	描述
指派類型	決定設定檔部署到裝置的方式。 <ul style="list-style-type: none"> ■ 自動 - 資源會自動部署到所有裝置。 ■ 選用 - 終端使用者可選擇從自助入口網站 (SSP) 安裝資源，也可由管理員自行決定部署至個別裝置。
管理者	具備資源管理存取權的企業群組。
已指派的群組	指派的群組指的是要加入裝置資源的群組。其中包括建立新的智慧群組之選項，您可以利用最低作業系統的規格要求、裝置型號、擁有權類別和企業群組等來進行配置。

設定	描述
排除項目	如果選擇 是 ，就會顯示一個新的 已排除的群組 的文字方塊，讓您選擇想要從此資源的指派中排除的群組。
檢視裝置指派	在 指派的群組 文字方塊中做出選擇後，可選擇此按鈕預覽會指派此資源的所有裝置清單，並將智慧群組指派項目和排除項目列入考量。

新增 Wi-Fi 資源

您可以新增一個資源，專門用來為裝置提供與無線網路連線的方法，好讓裝置在受到 Workspace ONE UEM powered by AirWatch 管理的同時，能夠安全地收發資料。

如需查看概覽，請參閱[設定檔資源](#)。

程序

- 1 導覽至**裝置 > 設定檔 & 資源 > 資源**，再依序選取**新增資源**和 **Wi-Fi**，並完成下列設定。

設定	描述
資源明細	
資源名稱	Workspace ONE UEM Console 所顯示的設定檔名稱。
描述	簡短描述設定檔的使用目的。
連線資訊	
服務組識別元	輸入與所需 Wi-Fi 網路名稱 (SSID) 有關聯的識別元。
隱藏網路	如果網路沒有要開放廣播，請啟用此項。
自動加入	自動引導裝置加入網路的設定。
加密	使用下拉式功能表欄指定使用 Wi-Fi 連線來傳輸的資料是否要加密。 依據 安全性類型 而顯示。
密碼	為 Email 帳戶輸入密碼。勾選 顯示字元 方格即可顯示未編輯的密碼。

- 2 按一下下一步，繼續選擇平台。請從下列項目中選擇支援的平台，並選擇使用預設設定或**進階設定**。

- 為 **Wi-Fi 代理伺服器配置進階設定**。

設定	描述
代理伺服器類型	請在 無 、 手動 或 自動 間擇一。
代理伺服器 URL	僅當 代理伺服器類型 設為 自動 時，才能使用此項。為裝置輸入要用來連線的 Wi-Fi 代理伺服器 URL。
無法到達 PAC 時允許直接連線	僅當 代理伺服器類型 設為 自動 時，才能使用此項。若要在代理伺服器自動配置檔案無法存取時允許裝連線，請啟用此項。
代理伺服器	僅當 代理伺服器類型 設為 手動 時，才能使用此項。輸入要讓裝置連線的代理伺服器名稱。
代理伺服器連接埠	僅當 代理伺服器類型 設為 手動 時，才能使用此項。包括代理伺服器的埠號，裝置將透過這個埠號來與代理伺服器連線。

設定	描述
代理伺服器使用者名稱	僅當代理伺服器類型設為 手動 時，才能使用此項。輸入使用者名稱以供代理伺服器辨識。
代理伺服器密碼	僅當代理伺服器類型設為 手動 時，才能使用此項。輸入與使用者名稱對應的密碼。

■ 為 **Android Wi-Fi** 配置進階設定。

設定	描述
Fusion	
包含 Fusion 設定	顯示 Fusion 功能的主要設定。
設定 Fusion 802.11d/啟用 802.11d	使用 802.11d 無線規格在法規適用的其他網域中進行作業。
設定國碼 (地區碼)/國碼 (地區碼)	設定可使用 802.11d 規格的國碼 (地區碼)。
設定 RF 頻帶	顯示所有無線電頻率的規格選項，包括 2.4 GHz 與 5 GHz 的頻道遮罩在內。
設定 2.4 GHz/啟用 2.4 GHz	使用 2.4 GHz 無線頻率。
2.4 GHz 頻道遮罩	套用 2.4 GHz 頻率左右的頻道遮罩或頻譜遮罩，從而減少相鄰頻道的干擾。
設定 5 GHz/啟用 5 GHz	使用 5 GHz 無線頻率。
5 GHz 頻道遮罩	套用 5 GHz 頻率左右的頻率遮罩或頻譜遮罩，從而減少相鄰頻道的干擾。
代理伺服器	
啟用手動代理伺服器	顯示代理伺服器設定。
代理伺服器	請輸入代理伺服器網域名稱。
代理伺服器連接埠	請輸入要供代理伺服器使用的埠號。
排除清單	輸入要避免由代理伺服器進行路由的主機名稱。請在網域中使用星號作為萬用字元。例如： *.air-watch.com。

3 按一下下一步，繼續進行指派。

4 若要將資源指派至裝置，請完成下列設定。

設定	描述
指派類型	決定設定檔部署到裝置的方式。 <ul style="list-style-type: none"> ■ 自動 - 資源會自動部署到所有裝置。 ■ 選用 - 終端使用者可選擇從自助入口網站 (SSP) 安裝資源，也可由管理員自行決定部署至個別裝置。
管理者	具備資源管理存取權的企業群組。
已指派的群組	指派的群組指的是要加入裝置資源的群組。其中包括建立新的智慧群組之選項，您可以利用最低作業系統的規格要求、裝置型號、擁有權類別和企業群組等來進行配置。

設定	描述
排除項目	如果選擇 是 ，就會顯示一個新的 已排除的群組 的文字方塊，讓您選擇想要從此資源的指派中排除的群組。
檢視裝置指派	在 指派的群組 文字方塊中做出選擇後，可選擇此按鈕預覽會指派此資源的所有裝置清單，並將智慧群組指派項目和排除項目列入考量。

新增 VPN 資源

Workspace ONE UEM powered by AirWatch 可讓您新增資源，專用於提供虛擬私人網路 (VPN)。VPN 可讓使用者在公用網絡上傳送和接收資料，就像直接連線到私用網路一樣。

如需查看概覽，請參閱[設定檔資源](#)。

程序

- 1 導覽至**裝置 > 設定檔 & 資源 > 資源**，再依序選取**新增資源**和**VPN**，並完成下列設定。

設定	描述
資源明細	
資源名稱	Workspace ONE UEM Console 所顯示的設定檔名稱。
描述	簡短描述設定檔的使用目的。
連線資訊	
連線類型	從下拉式清單中選取安全連線類型。
伺服器	輸入伺服器 URL。

- 2 按一下**下一步**，繼續選擇**平台**。請從下列項目中選擇支援的平台，並選擇使用**預設設定**或**進階設定**。

■ iOS

設定	描述
連線資訊	
帳戶	輸入 VPN 帳戶名稱。
閒置時中斷連線 (以分鐘為單位)。	允許 VPN 在經過了特定的時間後自動中斷連線。此值的支援與否取決於 VPN 提供者。
傳送所有流量。	選取此項即可強制使用特定網路來傳送所有流量。
按個別 APP 配置的 VPN 規則	選取此項即可按個別 APP 啟用並配置 VPN 規則。
自動連接。	選取此項以允許 VPN 自動連線至 Safari 網域。若勾選 個別 App VPN 規則 勾選方格，將顯示此選項。
提供者類型	選取個別 APP VPN 提供者類型。選取 AppProxy 或 PacketTunnel，以決定要在應用程式層或是 IP 層透過通道傳送流量。若勾選 個別 App VPN 規則 勾選方格，將顯示此選項。
Safari 網域	請為個別 APP 配置的 VPN 輸入要自動連線的各個網域。這些網域均為內部站台，且均能觸發 VPN 自動連線。若勾選 個別 App VPN 規則 勾選方格，將顯示此選項。
驗證	

設定	描述
使用者驗證	若要驗證終端使用者，可上傳 憑證 或要求 VPN 存取 密碼 。
群組名稱	輸入 Workspace ONE UEM 群組名稱。
密碼	僅當 使用者驗證 設為「密碼」時才能使用。輸入 Workspace ONE UEM 群組名稱的密碼。
身份識別憑證	僅當 使用者驗證 設為「憑證」時才能使用此設定。選取 新增憑證 即可為憑證命名或上傳憑證檔，也可以使用憑證範本來選擇現有的憑證授權機構。
啟用「隨選即用 VPN」。	僅當 使用者驗證 設為「憑證」時才能使用此設定。啟用隨選 VPN 即可使用憑證來自動建立 VPN 連線。
使用新的隨選鍵。	僅當 使用者驗證 設為「憑證」時才能使用此設定。啟用此項，即可在終端使用者存取任何所指定的網域時啟動 VPN 連線。
配對網域或主機。	僅當 使用者驗證 設為「憑證」時才能使用此設定。輸入網域或主機名稱，當終端使用者存取這些網域或主機時，觸發 VPN 連線。
隨選動作	僅當 使用者驗證 設為「憑證」時才能使用此設定。為特定網域選取隨選動作，當終端使用者啟動 VPN 連線時，這些動作便會發生。可選取 [始終建立]、[從不建立] 或 [視需要建立]。
代理伺服器	
代理伺服器	選取 無 、 手動 或 自動 。
代理伺服器自動配置 URL	僅當 代理伺服器 設為 自動 時，才能使用此項。為裝置輸入要用來連線的 Wi-Fi 代理伺服器 URL。
伺服器	僅當 代理伺服器 設為 手動 時，才能使用此項。輸入要讓裝置連線的代理伺服器名稱。
連接埠	僅當 代理伺服器 設為 手動 時，才能使用此項。包括代理伺服器的埠號，裝置將透過這個埠號來與代理伺服器連線。
使用者名稱	僅當 代理伺服器 設為 手動 時，才能使用此項。輸入使用者名稱以供代理伺服器辨識。
密碼	僅當 代理伺服器 設為 手動 時，才能使用此項。輸入與使用者名稱對應的密碼。
廠商組態	
廠商鍵	使用廠商配置字典建立自訂鍵。
鍵	輸入廠商所提供的特定鍵。
值	輸入各鍵的 VPN 值。

■ Android

設定	描述
驗證	
身分識別憑證。	選取 新增憑證 即可輸入要用於驗證連線的憑證認證。
認證來源	選擇認證來源。選取 [上傳]、[定義的憑證授權機構] 或 [使用者憑證]。
認證名稱	當 認證來源 已設為「上傳」時，即可使用此項。輸入已上傳認證的名稱。
憑證	當 認證來源 已設為「上傳」時，即可使用此項。按一下上傳，從您的裝置選取憑證檔案。
憑證授權單位	當 認證來源 已設為「已定義的憑證授權單位」時，即可使用此項。從下拉式清單中選取憑證授權單位。
憑證範本	當 認證來源 已設為「已定義的憑證授權單位」時，即可使用此項。此設定會根據您在憑證授權單位設定中的選擇而自動填入內容。

設定	描述
S/MIME	當 認證來源 已設為「使用者憑證」時，即可使用此項。選取使用者中心的 [S/MIME 簽署憑證]，或者 [S/MIME 加密憑證]。
啟用隨選即用 VPN	
啟用「隨選即用 VPN」。	啟用隨選 VPN 即可使用憑證來自動建立 VPN 連線。 輸入 APP 名稱並選取放大鏡圖示左側的加號，即可啟用 VPN。您可輸入多個應用程式。

- 按一下下一步，繼續進行指派。
- 若要將資源指派至裝置，請完成下列設定。

設定	描述
指派類型	決定設定檔部署到裝置的方式。 <ul style="list-style-type: none"> ■ 自動 – 資源會自動部署到所有裝置。 ■ 選用 – 終端使用者可選擇從自助入口網站 (SSP) 安裝資源，也可由管理員自行決定部署至個別裝置。
管理者	具備資源管理存取權的企業群組。
已指派的群組	指派的群組指的是要加入裝置資源的群組。其中包括建立新的智慧群組之選項，您可以利用最低作業系統的規格要求、裝置型號、擁有權類別和企業群組等來進行配置。
排除項目	如果選擇 是 ，就會顯示一個新的 已排除的群組 的文字方塊，讓您選擇想要從此資源的指派中排除的群組。
檢視裝置指派	在 指派的群組 文字方塊中做出選擇後，可選擇此按鈕預覽會指派此資源的所有裝置清單，並將智慧群組指派項目和排除項目列入考量。

地理柵欄區域

Workspace ONE UEM 可讓您使用地理柵欄區域定義設定檔，可將裝置的使用限制在特定區域。您可以將「地理柵欄」區域想像成一個為真實世界所劃分的虛擬邊界。

舉例來說，您可將方圓 1 英里的地理柵欄區域套用至您的公司，也可將更大規模的地理柵欄區域套用至整個州/省。一旦您定義好地理柵欄區域的範圍，便可將其套用到設定檔、SDK 應用程式及 Workspace ONE UEM 應用程式。

- 啟用地理柵欄區域有兩個步驟。
 - 新增地理柵欄區域。
 - 將地理柵欄套用至設定檔。
- Android 和 iOS 裝置皆可使用「地理柵欄」。
- 請切記，雖然地理柵欄需要和其他裝載合併使用才能根據位置啟用安全性設定檔，請考慮只為每個設定檔賦予一個裝載項目。

如需關於 Workspace ONE UEM 如何追蹤 GPS 位置的詳細資訊，請參閱下列 VMware 知識庫文章：

<https://support.workspaceone.com/articles/115001663108>。

新增地理柵欄區域

您必須先定義地理柵欄區域才能套用至裝置。

- 1 若要存取區域設定頁面，請導覽至 **資源 > 設定檔與基準 > 設定 > 區域**。

結果：系統設定隨即顯示。

- 2 選取**地理柵欄區域**按鈕。
- 3 輸入地理柵欄的**地址**和**半徑** (公里或英里)。您可以在地圖上的任何區域連接兩下，來設定中心位置。
- 4 選取**點選以搜尋**，以將輸入的位址作為搜尋參數傳送至 Bing 地圖。如果搜尋成功，地圖檢視會更新以顯示輸入的位置，並以該位址作為地理柵欄的中心。

備註 與 Bing 地圖之整合，需要在此頁面載入「不安全的內容」。如果無法順利載入位置搜尋，您可能需要允許瀏覽器「顯示所有內容」。

- 5 輸入**區域名稱** (在 Workspace ONE UEM Console 主控台中顯示的區域名稱)，然後選取**儲存**。

下一步：接下來，您必須將地理柵欄套用至設定檔。

將地理柵欄套用至設定檔

新增地理柵欄區域後，便可套用在設定檔，並與其他裝載合併使用，以建立更強固的設定檔。

如果使用者手動停用 iOS 裝置上的位置服務，Workspace ONE UEM 將無法再收集位置更新。Workspace ONE UEM 會認為裝置處於停用服務的位置。

- 1 導覽至 **資源 > 設定檔與基準 > 設定檔**，然後找出您要套用地理柵欄的設定檔。
- 2 選取設定檔的 [編輯] 鉛筆圖示 (✎)。
- 3 在**一般**標籤上，選擇**僅安裝在所選區域內的裝置**。如果已停用此核取方塊，請選取**新增版本**按鈕。建立新的版本表示重新發佈設定檔。

便會顯示**指派的地理柵欄區域**的方格。如果您尚未定義地理柵欄區域，功能表就會將您導回到「地理柵欄區域」之建立功能表。

- 4 請在此設定檔輸入一個或多個「地理柵欄」區域。
- 5 配置一項您要裝置在所選的地理柵欄區域內才能套用的裝載，例如密碼、限制或 Wi-Fi 等。
- 6 選取**儲存並發佈**。

例如，您可以在每個辦公室周圍定義地理柵欄區域。然後新增限制裝載，禁止存取遊戲中心、多人遊戲、YouTube 內容和其他設定。啟動此限制後，這些企業群組中適用此設定檔的員工，將無法在辦公室內存取上述的功能。

iOS 裝置上的地理柵欄支援

APP 的地理柵欄功能，只有在運行**位置服務**的 iOS 裝置上才能使用。為了讓位置服務能正常運作，裝置必須與行動網路或 Wi-Fi 熱點連線。否則，裝置必須具備內建 GPS 功能。

對僅使用 Wi-Fi 的裝置來說，只有在開啟並解鎖裝置，而且也開啟並使用 Workspace ONE Intelligent Hub 時，才會呈報 GPS 資料。對行動裝置來說，但裝置改換行動塔台時，便會回報 GPS 資訊。

裝置在「飛航模式」時，系統便會停用位置服務 (和地理柵欄) 功能。

裝置	Wi-Fi	行動網路	內建 GPS
iPhone	✓	✓	✓
iPad Wi-Fi + 3G/4G	✓	✓	✓
iPad Wi-Fi	✓		
iPod Touch	✓		

必須符合下列的所有要求，GPS 位置才能更新。

- 裝置必須執行 Workspace ONE Intelligent Hub。
- 隱私權設定必須允許收集 GPS 位置資料 (群組與設定 > 所有設定 > 裝置與使用者 > 一般 > 隱私權)。
- Apple iOS 的 Workspace ONE Intelligent Hub 設定必須啟用「收集位置資料」(群組與設定 > 所有設定 > 裝置與使用者 > Apple > Apple iOS > Hub 設定)。

將 Workspace ONE Intelligent Hub SDK 設為預設的 SDK 設定，而非設為 [無]。

iBeacon

iBeacon 是一種由 Apple 開發的藍牙式近接感通訊協定，因此只適用於特定 Apple 產品。

iBeacon 是專屬於 iOS 的功能，用來管理定位知悉。如需詳細資訊，請參閱 [Apple iBeacon 概觀](#)。

時間排程

雖然 Workspace ONE UEM powered by AirWatch 底下的設定檔決定了裝置可用性的限制或權限程度，但時間排程會將設定檔的強制執行置於排程上。您可以將時間排程套用到新的設定檔或現有的設定檔。您也可以刪除未使用的時間排程。

啟用時間排程有兩個步驟。

- 1 定義時間排程。
- 2 將時間排程套用於新的或現有的設定檔。

定義時間排程

- 1 導覽至 **資源 > 設定檔與基準 > 設定 > 時間排程**。
- 2 選取 **新增排程** 按鈕。即會出現 **新增排程** 畫面。
- 3 選取 **星期幾** 欄位下方的 **+新增排程** 按鈕，完成下列設定。

設定	描述
排程名稱。	為出現在清單中的時間排程輸入名稱。
時區	為容納管理裝置的企業群組選取時區。

設定	描述
星期幾	若要套用已排程設定檔安裝，請選擇星期幾。
全天	請設定為在所選星期幾的午夜安裝設定檔。勾選此方格以移除開始時間欄與結束時間欄。
開始時間。	為該日選取要安裝設定檔的時間。
結束時間。	為該日選取要將設定檔解除安裝的時間。
動作	若要移除排程的日期，請按一下 X 。

- 4 選取儲存。

將時間排程套用至設定檔

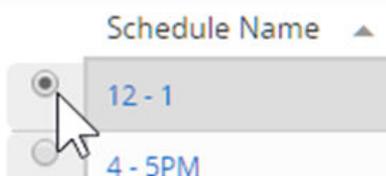
- 1 導覽至資源 > 設定檔與基準 > 設定檔 > 新增，然後選取您的平台。
- 2 在一般標籤上，選取啟用排程，並只在選定的時間內安裝。
- 3 在指派的排程方格中，將一或多個「時間排程」輸入此設定檔。
- 4 配置裝置必須在特定的時間範圍內才套用的裝載，例如密碼、限制或 Wi-Fi 等。
- 5 選取儲存並發佈。

將間排程套用至現有的設定檔

- 1 導覽至資源 > 設定檔與基準 > 設定檔，然後從清單中找出要編輯的設定檔。若要編輯設定檔，請選取鉛筆圖示 (✎)，或按一下設定檔名稱。
- 2 前往設定檔頁面的一般索引標籤中，並將啟用排程，並只在選定的時間內安裝設定啟用。
- 3 指派的排程設定隨即出現，此時請在下拉式功能表中選擇先前所儲存的時間排程。
- 4 選取儲存並發佈。

刪除時間排程

- 1 導覽至資源 > 設定檔與基準 > 設定 > 時間排程。
- 2 在要刪除的時間排程旁邊選擇選項按鈕。



- 3 選擇刪除按鈕。

檢視裝置指派、裝置設定檔

在設定裝置設定檔時，選取儲存並發佈按鈕則會顯示檢視裝置指派畫面。此畫面可預覽由 Workspace ONE UEM powered by AirWatch 管理且受到裝置設定檔指派影響 (或未受影響) 的裝置。

指派狀態欄位會反映出各種狀態，取決於您對裝置設定檔所進行的變更。

- **新增的** – 該設定檔會被新增和發佈至裝置。
- **移除的** – 該設定檔會被從裝置上移除。
- **不變更的** – 指出不會排程該設定檔並重新發佈至裝置。
- **更新的** – 指出該設定檔會被重新發佈至已指派設定檔的裝置。

選擇**發佈**來完成變更，並在需要時重新發佈任何必要的設定檔。

在 Workspace ONE UEM powered by AirWatch 中的裝置標籤可讓您辨識特定裝置，不需透過裝置設定檔、智慧群組或合規性原則，也不需要建立備註。

您可以依標籤篩選裝置清單檢視、將標籤指派給一或多個裝置、取消指派標籤，以及刪除未指派的標籤。

舉例來說，若裝置有老化的電池或螢幕有損壞時，您可在主控台中利用標籤來識別這些裝置。另外一種用途是以較明顯的方式來辨識硬體的差異，而不靠型號或描述來分辨裝置。

舉例來說，即使兩台 Windows 桌面裝置具有相同型號，但其 CPU 也許會有些差異，或是已有自訂的記憶體容量或視訊卡。標記經過強化的硬體，可以讓您輕鬆識別主控台內這些裝置。

標記和智慧群組

標籤功能已與智慧群組整合。此整合表示可使用標籤來定義智慧群組。

例如，如果已將裝置團隊中外觀有損壞的裝置都標記出來，則可針對這些裝置建立智慧群組。接著可將智慧群組從暫時指派到網站訪客的裝置集區中排除。

另一個範例是標記出效能不佳的裝置。您可為這些已標記的裝置建立一個智慧群組並將其排除，以避免在指派關鍵任務時誤用這些裝置。

裝置標記和角色權限

與裝置標記功能相關的所有活動都需要您指派給管理員的角色相關權限。如果您想要管理員擁有建立標記的責任，您必須將該權限（在主控台中稱為「資源」）新增至您指派給該管理員的角色。檢視標記、編輯標記、刪除標記、指派標記，甚至搜尋標記也是同樣的做法。

按照標記來篩選裝置

- 1 導覽至 **裝置 > 清單檢視**，然後點選 **篩選條件**，顯示裝置清單左側的 **篩選條件** 欄位。
- 2 從篩選器類別的清單中選取 **進階**，然後選取 **標記**。
- 3 按一下搜尋文字方塊的任意處，然後從顯示的裝置標記清單中選取。

結果：未被選取標記的裝置便會從結果清單中被排除。在選好第一個標記後，**裝置清單檢視**便會自動更新。

從系統設定建立新標記

開始之前：您必須擁有正確權限才可以建立標記。您可以查看管理員身份的所有指派資源 (或權限) 以檢查這些權限，修改具有「建立標記」權限的角色，如果尚未指派，則將修改後的角色指派至您的管理員帳戶。如需詳細資訊，請參閱主題[檢視管理員角色的資源](#)。

- 1 導覽至**群組 & 設定 > 所有設定 > 裝置 & 使用者 > 進階 > 標記**。
- 2 點選**建立標記**按鈕。**建立標記**畫面即會顯示。
- 3 輸入標記的**名稱**。您選取的標記名稱會決定該標記是否可用。請選取可一眼識別裝置的名稱。
- 4 選取所需標記的**類型**：**裝置**、**一般**或**影片**。
- 5 選取**儲存**。

現在可以將裝置標記指派給裝置。導覽至**裝置 > 清單檢視**，然後選取一或多個要指派此標記的裝置。

在單一裝置上指派標記

您可以為裝置指派標記以便於識別，而無需使用註解、設定檔、原則，也無需為裝置賦予特別的暱稱。您是否需要以管理員身分授與權限，而這個管理員身分包含 (或不包含) 為裝置指派標記的能力？請參閱主題[檢視管理員角色的資源](#)。

- 1 導覽至**裝置 > 清單檢視**，然後選取您要標記的裝置。在這兩個選取方法之間選擇一個，以選取您要標記的裝置。
 - a 從清單中選取裝置暱稱，以顯示**明細檢視**。
 - b 選取裝置旁鉛筆圖示上方的勾選方格。
- 2 選取**更多動作**按鈕，然後選擇**指派標記**。**標記指派**的畫面會隨著可用的標記清單一起顯示，讓您套用在選定的裝置上。
- 3 選擇每個要指派給裝置的標記。您可選取數個標記。如果您從裝置**明細檢視**中選取了**指派標記**，就會取得**管理標記**連結，選取此連結即會開啟「標記系統設定」頁面，您可以在此頁面建立新標記。

將標記指派至多個裝置

您必須擁有權限，才能將標記指派給多個裝置。您可以查看管理員身份的所有指派資源 (或權限) 以檢查這些權限，修改具有「裝置大量管理指派標記」權限的角色，如果尚未指派，則將修改後的角色指派至您的管理員帳戶。

您可以設定允許指派或取消指派標籤的裝置數量上限，請導覽至**群組 & 設定 > 所有設定 > 裝置 & 使用者 > 進階 > 大量管理**，然後向下捲動到**指派/取消指派標籤**選項。

- 1 導覽至**裝置 > 清單檢視**。
- 2 勾選每個您要指派標記的裝置所適用的勾選方格。
- 3 選取**更多動作**，然後選取**管理標籤**。

管理標籤頁面會顯示多項資訊。可從中確認從清單視圖選取的裝置數目，其中會顯示目前指派的標籤，以及可指派的所有標籤。您也可以在此 [管理標籤] 頁面右上角的搜尋文字方塊中輸入標記標籤的搜尋參數。

- 4 選擇您要指派給所有選定的裝置之標記。您可選取數個標記。您可以採用相同步驟指派一些標籤，也可以取消指派其他標籤。
- 5 選取**儲存**。

編輯現有的裝置標記

您必須擁有正確權限才能編輯標記。您可以查看管理員身份的所有指派資源 (或權限) 以檢查這些權限，修改具有「編輯標記」權限的角色，如果尚未指派，則將修改後的角色指派至您的管理員帳戶。

- 1 導覽至**群組 & 設定 > 裝置 & 使用者 > 進階 > 標記**。
- 2 在清單中識別要編輯的標記。
- 3 選取您要編輯的標記旁邊的鉛筆圖示 (✎)。即會顯示「編輯標記」畫面。
- 4 編輯標籤的**名稱**。
- 5 選取**儲存**。

結果：編輯後的標籤具備新的名稱。系統已經使用編輯後的標記更新以先前的標記指派的裝置。

從多個裝置中取消指派標記

您必須擁有正確的權限，才能取消指派多個裝置的標記。您可以查看管理員身份的所有指派資源 (或權限) 以檢查這些權限，修改具有「大量管理取消指派標記」權限的角色，如果尚未指派，則將修改後的角色指派至您的管理員帳戶。如需詳細資訊，請參閱主題**檢視管理員角色的資源**。

您可以設定允許指派或取消指派標籤的裝置數量上限，請導覽至**群組 & 設定 > 所有設定 > 裝置 & 使用者 > 進階 > 大量管理**，然後向下捲動到**指派/取消指派標籤**選項。

若要從多個裝置中解除指派標記，請執行下列步驟。

- 1 導覽至**裝置 > 清單檢視**，然後搜尋您要取消指派的標籤。或是您可以根據一或多個標記篩選裝置。
- 2 在 [裝置清單檢視] 中，於您要取消指派標記的裝置左側選取核取方塊。
- 3 在清單上方選擇**更多動作**按鈕。
- 4 選取**管理標籤**。

管理標籤頁面會顯示多項資訊。可從中確認從清單視圖選取的裝置數目，其中會顯示目前指派的標籤，以及可指派的所有標籤。您也可以在此 [管理標籤] 頁面右上角的搜尋文字方塊中輸入標記標籤的搜尋參數。

- 5 在每個您要移除的已指派標籤旁邊，點選小「x」。您可以取消指派數個標籤。您可以採用相同步驟指派一些標籤，也可以取消指派其他標籤。
- 6 選取**儲存**。

結果：已從您選取的所有裝置中取消指派標籤。如果該標籤已指派給任何其他裝置，則不能將其刪除。

刪除取消指派 (未使用) 的裝置標籤

只要標籤處於取消指派狀態且您不打算再使用該標籤，就可以刪除標籤。

您必須擁有正確權限才能刪除標記。您可以查看管理員角色的所有指派資源 (或權限) 以檢查這些權限，修改具有「刪除標記」權限的角色，如果尚未指派，則將修改後的角色指派至您的管理員帳戶。如需詳細資訊，請參閱主題[檢視管理員角色的資源](#)。

您想要刪除的標記不得指派給任何裝置。

若要從裝置取消指派標籤，請參閱前一節。

- 1 標記完全取消指派後，導覽至**群組 & 設定 > 裝置 & 使用者 > 進階 > 標記**。
- 2 識別您要從清單中刪除的標記。
- 3 在要刪除的標記旁選擇選項按鈕。**刪除**按鈕會顯示在清單的上方。
- 4 選取**刪除**。畫面上會出現確認訊息，詢問「永久刪除標記嗎？」
- 5 在確認畫面中選取**確定**。如果標記已指派給裝置，則您不能刪除該標記。請參閱上面的指示，從裝置中取消指派標記。

如果在您刪除標籤時，該標籤未指派給任何裝置，則現在就會移除。

查閱值是一個變數，用來代表 Workspace ONE UEM 和 Workspace ONE Express 中裝置、使用者或管理員帳戶的特定資料元素。對於完成程序或填寫表單而言，查閱值至關重要。

在 Workspace ONE UEM Console 和 Workspace ONE Express 的多個不同文字方塊中，您可新增查閱值取代手動輸入的值或靜態值。大多數情況下，您可用查閱值充當一段未知資訊或無法存取的資訊。

例如，**新增裝置**畫面是用來新增裝置到您的裝置團隊，而此畫面上可使用查閱值填入的其中一個文字方塊可以是**預期的暱稱**。

暱稱代表 UEM 主控台中多個不同畫面上的裝置，包括**裝置清單檢視**和**詳細資訊檢視**。雖然可在新增裝置時手動輸入靜態暱稱，但您也可使用查閱值將暱稱標準化，使其成為有實用價值的識別碼。

常用的暱稱格式架構如下查閱值所示：

```
{EnrollmentUser} {DeviceModel} {DeviceOperatingSystem} {DeviceSerialNumberLastFour}
```

如果您在**預期的暱稱**文字方塊中輸入此字串，便會產生如**裝置清單檢視**中所呈現的暱稱。

```
jsmith iPad iOS GHKD
```

此暱稱可直接提供您至少三項實用的資訊；在結尾處的裝置序號之最後四碼則幾乎可確保暱稱的唯一性。

資料額外負荷

使用查閱值不會造成裝置記憶體額外的額外負荷。查閱值本身就是主控台架構的一部分，因此不會轉移任何負載到裝置上。

靜態字串與查閱值

一旦在文字方塊中輸入靜態字串，便無法套用查閱值。

例如，假設您有 100 台要註冊的裝置，新增前 50 個裝置的**預期的暱稱**時，您可使用手動輸入的靜態字串；而接下來 50 個裝置，您可改用查閱值填入**預期的暱稱**。這 100 台裝置有一半使用靜態暱稱，一半使用查閱值，在此設定下彼此可理想共存。混合使用靜態字串和查閱值並不會造成任何問題。

不過，您就無法再回到前 50 個裝置，以查閱值取代靜態字串。

自訂查閱值

您可使用自訂屬性功能製作專屬的查閱值。接著，您即可按照使用一般查閱值的方式來使用這些自訂查閱值。

BYOD 終端使用者的最大顧慮是 Workspace ONE UEM 所管理裝置上的個人內容隱私權。您的組織必須確保這些個人資料不在公司的監管範圍內。

使用 Workspace ONE UEM，您可以依據裝置擁有權類型建立不收集個人資料的自訂隱私權政策，以確保個人資料的隱私。此外，還可以定義細微的隱私權設定，以停用收集可識別個人身分的資訊，且不允許對員工自有裝置執行某些遠端動作，以確保員工隱私權。

請務必通知終端使用者，並說明當他們向 Workspace ONE UEM 註冊時，將如何收集與儲存他們的資料。

如需關於 VMware 如何處理經由 Workspace ONE UEM 收集之資訊 (例如分析) 的詳細資訊，請參閱 VMware 隱私權政策：<https://www.vmware.com/help/privacy.html>。

重要 各個國家/地區和管轄區域有不同的規則，管理可以從終端使用者處收集的資料。設定 BYOD 和隱私權政策之前，您的組織必須徹底瞭解適用的法規。

配置隱私權設定

終端使用者的隱私權您與您的使用者需關注的重要事項。Workspace ONE UEM 可提供最細微的控制方案，決定要從使用者收集何種資訊，而管理員又能查閱哪些收集而來的資訊。配置隱私權設定，同時滿足使用者的需求和您的和商務需求。

- 根據裝置擁有權來檢視並調整隱私權原則，讓您可以遵守其他國家的資料隱私權法規或法律所定義的各種限制。
- 確保某 IT 的檢查與平衡性都已到位，以避免伺服器與系統超載。

重要 每個管轄權皆有其本身的規則，可管理能向終端使用者收集的資料。必須通盤研究這些資訊，才能開始配置您的隱私權政策。

- 1 導覽至 **裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 隱私權**。

- 2 為 **GPS 資料**、電信資料、應用程式資料、設定檔和網路資料的收集選取合適的設定。



收集並顯示 - 使用者資料會收集至 Workspace ONE UEM 主控台並從中顯示。



收集但不顯示 - 收集使用者資料並用於報告中，但不在 Workspace ONE UEM 主控台中顯示。



不收集 - 不收集使用者資料，因此無法顯示。

- 3 為可在裝置上執行的**指令**選取合適的設定。請考慮在所有的員工自攜裝置上停用遠端指令，特別是完全抹除指令。停用後可以防止不小心刪除或抹除終端使用者的個人內容。如果您停用特定 iOS 所有權類型的抹除功能，使用者不會在註冊期間看到「清除所有內容和設定」權限。



允許 - 指令在沒有使用者同意下在裝置上執行。



經使用者同意允許 - 只有在使用者同意下，才能在裝置上執行該指令。



禁止 - 不在裝置上執行指令。

- 4 如果您允許 Android/Windows 和堅固型裝置使用遠端控制或登錄管理員的存取權限，請考慮使用**經使用者同意允許**的選項。在執行此選項前，管理員必須透過訊息提示來取得終端使用者同意才能存取其裝置。如果您要允許使用任何指令，請在使用條款協議中明確地指出這些指令。
- 5 對於**使用者資訊**，請選擇是否要在主控台的資訊中**顯示或不顯示**姓氏名字、電話號碼、**Email 帳戶**和**使用者名稱**等資料。
- 6 如果**使用者名稱**以外的任一選項設為**不顯示**，那麼無論該資料出現在 UEM 主控台的任何地方，都會顯示為「私人」。主控台無法搜尋設為**不顯示**的選項。設為**不顯示**的使用者名稱，在裝置清單檢視與裝置明細頁面中都只會顯示為「私人」而已。UEM 主控台的其他頁面都會顯示已註冊使用者的使用者名稱。
- 7 您可以將名字、姓氏、Email 地址和電話號碼等個人識別資訊予以加密。在您要設定加密的全域或客戶層級企業群組內，導覽至**群組 & 設定 > 所有設定 > 系統 > 安全性 > 資料安全**。若要啟用加密功能，請選擇您要加密的使用者資料，然後選取**儲存**來加密使用者的資料。此動作會限制 UEM 主控台上的某些功能，譬如搜尋、排序和篩選等。
- 8 選擇是否要在裝置上**啟用或停用勿擾模式**。此設定允許使用者裝置在特定時間內略過 MDM 指令。啟用後，您可選擇**勿擾模式**到期前的寬限期或啟動時間 (以分鐘、小時或天為單位)。
- 9 選擇在裝置上**啟用或停用方便使用的隱私權通知**。
- 10 **啟用**後，您便可在下列各個擁有權層級上選擇**是** (顯示隱私權注意事項) 或**否** (不顯示隱私權注意事項)：**員工自有、公司專用、公司共用和未知**。
- 11 按一下**儲存**。隱私權設定是受限動作，因此您必須輸入四位數主控台 PIN 碼以便繼續。

隱私權聲明部署

隱私權聲明會依照裝置所連接之企業群組和裝置擁有權而自動傳送。您可以為各個擁有權類型選擇是否要顯示隱私權聲明：**員工自有**、**公司專用**、**公司共用**和**未知**。

當您指派某個將要接收隱私權聲明的擁有權類型時，所有符合所選之擁有權類型的使用者，都會立即收到具有 **Web Clip** 形式的隱私權聲明。如果您在訊息範本中插入隱私權聲明的查閱值 `PrivacyNotificationUrl`，那麼該訊息便會包含一條 URL，可供使用者閱讀隱私權聲明之用。

每當下列情形發生時，使用者便會自動收到隱私權聲明：

- 當使用者註冊新裝置，而您已為其擁有權類型啟用了隱私權通知。
- 使用者目前正在使用已註冊的裝置；而在註冊後，其擁有權已變成要指派 **Web Clip** 的類型。

若要瞭解如何將隱私權聲明部署為裝置啟用程序的一部分，請參閱[登記個別裝置](#)。

為 BYOD 使用者建立隱私權通知

自訂隱私權聲明來告知使用者，說明您的公司將會從他們所註冊的裝置中收集何種資料。請與您的法律部門合作，決定應使用何種訊息來與終端使用者溝通資料的收集事宜。

- 1 導覽至**群組與設定 > 所有設定 > 裝置與使用者 > 一般 > 訊息範本**。
- 2 選取**新增**即可建立範本。如果您已建立隱私權通知範本，請從可用的範本清單中選擇此範本加以使用或編輯。
- 3 完成**新增/編輯訊息範本**的設定。

設定	描述
名稱	輸入通知範本的名稱。
描述	輸入您所建立的範本描述。
類別	選取 註冊 。
類型	選取 MDM 裝置啟動 。
選擇語言	選取您範本的預設語言。在需要多語言表達的情況下，選擇 新增 按鍵來新增其他的預設語言。
預設值	將此範本指派為預設訊息範本。
訊息類型	選取一種或多種訊息類型： Email 、 SMS 或 推播 訊息。

- 4 建立通知內容。您在上方的**訊息類型**選取項目中所選的訊息類型，將會決定即將顯示哪種範本供您配置。

元素	描述
Email	
Email 內容格式化	選擇您的 Email 通知是要以 純文字 或 HTML 格式傳送。
主題	輸入您 Email 通知中的主旨列。
訊息內文	撰寫 Email 訊息以傳送給您的使用者。出現在此文字方塊的編輯和格式化工具取決於您在 Email 內容格式 選取項目中所選的格式。 如果您已啟用視覺隱私權聲明，請在訊息內文中附上查閱值 <code>PrivacyNotificationUrl</code> 。

元素	描述
SMS 簡訊	
訊息內文	撰寫 SMS 訊息以傳送給您的使用者。 如果您已啟用視覺隱私權聲明，請在訊息內文中附上查閱值 PrivacyNotificationUrl。
推播	
訊息內文	撰寫推播通知以傳送給您的使用者。 如果您已啟用視覺隱私權聲明，請在訊息內文中附上查閱值 PrivacyNotificationUrl。

5 選取儲存。

隱私權最佳作法

要在商務需求與員工的隱私考量之間取得平衡可說是個挑戰。有幾個簡單的做法可讓隱私設定管理達到最佳平衡。

重要 每個部署都不盡相同。請洽詢您的法律、人力資源和管理團隊，以最適合您企業的方式量身制訂這些設定和原則。

使用者資訊的隱私權最佳作法

一般而言，您會在員工自有和公司擁有的裝置上，顯示使用者資訊，例如姓氏、名字、電話號碼與 Email 地址。

應用程式資訊的隱私權最佳作法

一般而言，您應該將員工自有裝置中應用程式資訊的收集設為**不收集**或是**收集但不顯示**。此設定至關重要，因為公用 APP 已安裝在裝置上，若經檢視則會被視為可辨識個人身份的資訊。針對公司擁有的裝置，Workspace ONE UEM 會將所有已安裝的應用程式記錄在裝置上。

選擇「不收集」時，只有個人應用程式的資訊不會被收集。Workspace ONE UEM 會收集所有受管理的應用程式，無論其為公用、內部，或是被購入。

遠端指令的隱私權最佳作法

請考慮停用所有員工自有裝置上的遠端指令。然而，如果允許使用遠端的動作和指令，請在使用條款協議中明確指出所用的遠端動作和指令。

GPS 座標收集隱私權的最佳做法

收集 GPS 座標基本上存有侵犯隱私權的疑慮。收集員工自有裝置的 GPS 資料雖然不適當，但下列附註可適用於所有在 Workspace ONE UEM 中註冊的裝置。

- 只有 Workspace ONE Intelligent Hub 會將裝置 GPS 位置資料轉送到 UEM 主控台。
 - VMware Browser、Content、Boxer 等其他使用 Workspace ONE SDK 的應用程式並不會將 GPS 資料傳回 UEM console。
 - GPS 通常用於尋找遺失或遭竊的裝置。此外，如果 Workspace ONE UEM Console 原本就有 (例如地理柵欄) 得知裝置位置的功能，也會使用 GPS。
 - 回報 GPS 資料時，Workspace ONE UEM 會針對目前位置定義出一個 1 公里的範圍。當裝置在區域外移動時，它就會報告位置資訊。

私人電信資料的最佳作法

只有手機費用獲得津貼補助時，才可收集員工自用裝置的電信數據。針對上述情況或公司專用的裝置，請考慮使用以下方式來處理您所收集的資料。

- **電信業者/國家代碼** – 電信業者和國家代碼都會被記錄下來，並且可以用在電信追蹤上。您可以依據所使用的電信業者和國家位置來設定電信計劃，並將裝置指派到適當的計劃中。您可利用這些資訊，並依電信業者和居住國家，或是目前所處國家和目前所用的電信業者追蹤裝置。
- **漫遊狀態** – 此狀態可用來追蹤哪些裝置處於「漫遊」或「非漫遊」狀態。當裝置處於漫遊狀態時，您可以設置合規原則來停用語音和數據的使用，或套用其他的合規原則。此外，如果裝置指派給某個電信方案，Workspace ONE UEM 便可追蹤漫遊時的數據使用量。收集和監控漫遊狀態，有效地避免因過度使用而導致電信業者收取龐大超額費用的情況。
- **行動電話數據使用量** – 數據使用量指的就是傳送和接收數據的總位元組。您可收集每台行動裝置的該項資料。如果已將該裝置指派給某項電信方案，您便可依據計費週期內總數據的百分比來監控數據的使用量。此功能讓您能夠依據數據的使用比率來建立合規原則，有助於防止電信業者收取龐大的超額費用。
- **行動裝置使用量** – 指的是可從每台行動裝置上收集的通話時間 (分鐘)。正如數據使用量，如果該裝置已指派給某電信方案，您就可以根據計費週期的分鐘百分比來監控使用量。此方式可讓您能依據分鐘的使用百分比來建立合規原則，有助於避免支付龐大的超額電信費用。
- **SMS 使用量** – 每台行動裝置可被收集的短訊服務 (SMS) 數據。正如數據使用量，如果該裝置已指派給某電信方案，您就可以根據計費週期的訊息百分比來監控 SMS 使用量。此方法可讓您藉由已使用訊息的百分比來建立合規性原則。監控 SMS 的使用量，有助於防止電信業者收取龐大超額費用。

從 BYOD 終端使用者收集使用者資料

Workspace ONE UEM 的基礎結構會收集並儲存多種使用者產生的資料。下表會對照每一種資料類型與該資料收集來源的作業系統。

請使用此表格來決定您的部署需要收集哪些資料。Workspace ONE UEM 也會定義您可以收集的選用資料，例如藍牙 MAC。您可以按照下列擁有權類型來設定這些選項及指派隱私權設定：公司專用、公司共用和員工自有。

如需關於 VMware 如何處理經由 Workspace ONE UEM 收集之資訊 (例如分析) 的詳細資訊，請參閱 VMware 隱私權政策：<https://www.vmware.com/help/privacy.html>。

✓ - 可以收集。

X - 不能收集。

✓* - 可以在 Workspace ONE Intelligent Hub 部署中收集。

✓** - 可以在 Workspace ONE Intelligent Hub 或 iOS 9.3+ 監督模式部署中收集。

	Android	Apple iOS	macOS	Windows Rugged	Windows 桌面
應用程式追蹤					
檢視已安裝的內部應用程式。	✓	✓	✓	X	✓
檢視應用程式版本	✓	✓	✓	X	✓
擷取應用程式狀態	✓	X	✓	X	✓
憑證					
檢視已安裝的憑證清單	✓	✓	✓	X	✓*
資產追蹤					
裝置名稱	✓	✓	✓	✓	✓
裝置 UDID	✓	✓	✓	✓	✓
電話號碼	✓	✓	X	✓	✓
IMEI/MEID 號碼	✓	✓	X	✓	✓
裝置序號	✓	✓	✓	✓	✓
IMSI 號碼	✓	X	X	✓	✓
裝置型號	✓	✓	✓	✓	X
裝置型號名稱 (暱稱)	X	✓	✓	✓	X
製造商	✓	✓	✓	✓	✓
作業系統版本	✓	✓	✓	✓	✓
作業系統組建編號	✓	X	✓	✓	✓
韌體/核心版本	X	X	✓	X	X
追蹤裝置錯誤	X	X	✓	✓	✓
裝置狀態					
可使用電池	✓	✓	✓	✓	✓
電池電量	✓	✓	✓	✓	X
有記憶體可用	✓	✓	✓	✓	X
記憶體容量	✓	✓	✓	✓	X

	Android	Apple iOS	macOS	Windows Rugged	Windows 桌面
位置					
GPS 追蹤	✓	✓**	✓	✓	✓
藍牙資料	✓	✓**	✓	✓	✓
USB 資料	X	✓**	✓	✓	✓
網路					
Wi-Fi IP 位址	✓	✓	✓	✓	✓
Wi-fi MAC	✓	✓	✓	✓	✓
Wi-Fi 訊號強度	X	X	✓	✓	✓
電信業者設定版本	✓	✓	X	X	X
手機訊號強度	✓	X	X	X	X
手機技術 (無、GSM、CDMA)	✓	✓	X	X	X
目前的 MCC	✓	✓	X	X	X
目前的 MNC	✓	✓	X	X	X
SIM 卡號碼	✓	✓	X	X	✓
SIM 卡電信業者網路	✓	✓	X	X	X
訂閱者 MNC	✓	✓	X	X	X
藍牙 MAC	✓	✓	✓	X	X
顯示 IP 位址。	✓	✓	✓	X	X
顯示 LAN 介面卡。	X	X	✓	X	X
顯示 MAC 位址。	✓	✓	✓	X	X
漫遊					
偵測漫遊狀態。	✓	✓	X	X	X
漫遊時停用推送通知。	X	✓	X	X	X
啟用語音漫遊 (允許)。	X	✓	X	X	X
數據使用量					
透過行動網路追蹤數據使用量	✓	✓	X	X	X
透過 Wi-fi 網路追蹤數據使用量	X	X	X	X	X
通話					
追蹤通話記錄	✓	X	X	X	X
訊息					
追蹤 SMS 歷程記錄	✓	X	X	X	X
行動電話通訊狀態					
目前的電信業者網路	✓	✓	X	X	X
目前的網路狀態	✓	✓	X	X	X

	Android	Apple iOS	macOS	Windows Rugged	Windows 桌面
遠端檢視					
遠端控制裝置	✓	×	✓	✓	✓
螢幕擷取 (儲存、電子郵件、列印等)	✓	×	✓	✓	✓
螢幕共享 (在應用程式中遠端檢視)	✓	✓	×	✓	✓
檔案管理員					
存取裝置檔案管理員	✓	×	✓	✓	✓
存取裝置登錄管理員	×	×	×	✓	✓
複製檔案	✓	×	✓	✓	✓
建立資料夾。	✓	×	✓	✓	✓
從裝置下載檔案。	✓	×	✓	✓	✓
移動檔案	✓	×	✓	✓	✓
重新命名資料夾和檔案。	✓	×	✓	✓	✓
將檔案上傳到裝置	✓	×	✓	✓	✓

BYOD 終端使用者的使用條款

基於責任，您必須通知員工所擷取的資料，以及允許在 Workspace ONE UEM 中註冊的裝置上執行的動作。為了協助傳達您的策略，請在 Workspace ONE UEM 中建立使用條款合約。

系統會提示使用者閱讀並接受您所設定的使用條款，然後才能在其個人裝置上啟用 MDM。依據擁有權類型指派使用條款合約，您就可以為企業和 BYOD 使用者建立及散佈不同的合約。

在您的組織撰寫其使用條款合約後，請考慮省略不必要的法律用語後，以一到兩頁白皮書的形式將此合約提供給終端使用者。此白皮書並不是終端使用者同意的官方使用條款，而是用來傳達您的企業政策。理想情況下，終端使用者在第一次註冊其裝置時，不會看到員工自有裝置的使用條款。請坦白說明您收集哪些終端使用者資訊，以及 BYOD 原則所造成的影響。

BYOD 裝置的限制

Workspace ONE UEM 允許您將不同的安全性原則和限制部署到員工自有和公司專用的裝置。

使用限制設定檔，您可以為公司專用裝置設定嚴格限制，並為員工自有裝置設定較寬鬆的限制。例如，YouTube 或原生 App Store 之類應用程式的限制通常不會部署到員工自有裝置。但是，您可以建立安全設定檔和限制，以提高裝置安全等級，而不會對功能造成負面影響。

適用於多種裝置的限制

Workspace ONE UEM 設定的下列限制適用於每一種裝置和平台：

- **加密備份** – 在有權存取公司內容的 BYOD 裝置中使用資料加密功能保護所有備份。

- 在支援的瀏覽器中強制使用詐騙警告 - 此功能會在偵測到可疑網站時，要求使用者確認所有由瀏覽器發出的警告。
- 停用移動電子郵件 - 將公司電子郵件轉寄至個人帳戶的功能，或在第三方應用程式中開啟此功能，以防止曝露公司的機密資料。

平台特定限制

每個平台都有一組專用的強制限制。請分別評估這些限制，以判定這些限制對部署的影響。有些限制 (例如，限於受監督裝置的 iOS 限制) 並不適用，因為無法在 Apple Configurator 中註冊員工自有裝置。

- 若要建立安全設定檔和限制，請導覽至 **資源 > 設定檔與基準 > 設定檔**，選取 **新增**，然後選取適當的平台。
- 如果要專為員工自有裝置建立設定檔，只需將設定檔指派給「擁有權類型」為「員工自有」的智慧群組。如需詳細資訊，請參閱 [智慧群組](#)。

如需建立安全設定檔和限制的詳細資訊，請參閱 [新增合規原則](#)。

BYOD 裝置的企業抹除

部署 BYOD 最重要的一點，就是在員工離職，或是裝置遺失或遭竊時，能夠移除公司內容。Workspace ONE UEM 可讓您在裝置上執行企業抹除，以移除所有公司內容和存取權限，但仍保留個人檔案和設定。

裝置抹除會將裝置還原到最初的原廠狀態，但在處理無法明確界定屬於公司裝置或員工自有裝置的公用與購買 VPP 應用程式時，您可以使用 Workspace ONE UEM 的企業抹除功能，並決定要套用至這些應用程式的抹除範圍廣度。企業抹除也能從 Workspace ONE UEM 取消註冊裝置，並去除透過 MDM 啟用的所有內容，包括電子郵件帳戶、VPN 設定、Wi-fi 設定檔、安全內容，以及企業應用程式。

如果您將 Apple 大量採購方案兌換碼用於 iOS 6 及更舊版本的裝置，將無法回收該應用程式的任何已兌換授權。一旦安裝完成後，應用程式便會與使用者的 App Store 帳戶產生關聯。此關聯無法復原，但您可兌換用於 iOS 7 及更新版本的授權碼。

- **裝置抹除** - 傳送 MDM 指令，以將所有資料和作業系統中的裝置抹除。此動作無法復原。
 - iOS 裝置抹除考量事項
 - 針對 iOS 11 和較舊版本的裝置，裝置抹除指令也會抹除與裝置有關的 Apple SIM 卡的資料。
 - 針對 iOS 11 以上的裝置，您可以保留 Apple SIM 數據方案 (如果裝置中有此方案)。選取 [裝置抹除] 頁面上的 **保留數據方案** 核取方塊，然後再傳送裝置抹除命令。
 - 針對 iOS 11.3+ 裝置，您有一個額外的選項，能夠在傳送裝置抹除命令時略過 **近距離感應設定** 畫面。啟用此選項後，[設定輔助程式] 中將略過 [近距離感應設定] 畫面，讓裝置使用者不會看到 [近距離感應設定] 選項。
 - 若是 Windows 桌面裝置，您可以選取裝置抹除的類型。
 - **抹除** - 此選項會抹除裝置上所有內容。
 - **抹除受保護** - 此選項與一般裝置抹除相似，但裝置終端使用者無法規避動作。抹除受保護指令會持續嘗試重設裝置，直到成功為止。在某些裝置組態中，此命令會讓裝置無法開機。

- **抹除與存留佈建資料** - 此選項會抹除裝置，但會指定佈建資料應備份到固定的位置。抹除執行後，佈建資料會還原，並套用至裝置。已儲存佈建資料夾。若要找到資料夾，您可以在裝置上導覽至 %ProgramData%\Microsoft\Provisioning 。
- **企業抹除** - 將裝置進行企業抹除，會解除註冊並移除所有受管的企業資源，包括應用程式和設定檔。此動作無法復原，而且必須要重新註冊後，Workspace ONE UEM 才能再次管理此裝置。此裝置動作包含可防止日後重新註冊的選項，以及一個備註說明文字方塊供您新增動作的相關資訊。
 - 雲端加入網域的裝置不支援企業抹除。

執行 BYOD 裝置的企業抹除

企業抹除會從 Workspace ONE UEM 裝置取消註冊裝置，並去除其所有企業內容，包括 Email 帳戶、VPN 設定、設定檔及應用程式。

- 1 在 Workspace ONE UEM Console 中，選取適當的組織群組。
- 2 導覽至**裝置 > 清單檢視**，然後從清單選取一或多個裝置。
- 3 「裝置明細」視圖顯示您可以在右上角的**更多**下拉式功能表中執行的動作清單。選取**企業抹除**。
- 4 在確認對話方塊中，選取**防止重新註冊**以防止重新註冊此裝置。
- 5 輸入安全 PIN 碼 (如果有的話)，然後選取**企業抹除**以完成動作。

停用 BYOD 裝置的完全抹除功能

基於安全性和隱私權原因，您可以停用 BYOD 裝置上執行完全抹除的功能。

如果您為特定 iOS 擁有權類型停用完全抹除，則註冊為該擁有權類型的使用者就無法在設定檔安裝期間看見「抹除所有內容與設定」權限。

- 1 導覽至**裝置 > 裝置設定 > 裝置 & 使用者 > 一般 > 隱私權**。
- 2 向下捲動到**指令**區段，並尋找**員工自有**欄位。
- 3 將**完全抹除**選項設為**防止**，並選取**儲存**。

Workspace ONE UEM powered by AirWatch 中的資源類似拼圖碎，代表您在裝置上安裝或設定的個別元素。資源包括應用程式與書籍、設定檔、更新、感應器、指令碼、時間範圍和安裝順序。整合在一起時，成果即是行動團隊安全且可靠的運作。

APP & 書籍

存取並管理 APP 目錄、書籍目錄、以及大量採購方案 (VPP) 的訂單。同時還可檢視應用程式的分析和記錄，以及包括應用程式類別、智慧群組、應用程式群組、精選應用程式、地理柵欄和與應用程式有關聯的設定檔等的各種設定。如需詳細資訊，請參閱[應用程式生命週期管理簡介](#)。

設定檔與基準

設定檔 – 裝置設定檔是您在 Workspace ONE UEM 中管理裝置的主要方式。在設定檔與合規原則合併時，它們可協助您強制執行公司規則和程序的設定及規定。更多相關的資訊，請參閱 [技術預覽：工作流程中使用的設定檔和設定檔資源](#)。

基準 – 維持裝置符合最佳做法的組態是一項非常耗時的處理程序。您可以使用業界建議的設定和組態來保護所有的裝置。Workspace ONE UEM 將這些最佳做法歸納成稱為基準的組態。這些組態可大幅減少設定和配置 Windows 裝置所需的時間。如需詳細資訊，請參閱[使用基準](#)。

裝置更新

在一個位置管理所有裝置更新檔案，包括每次更新的完整安裝狀態記錄。裝置更新是平台特有功能。如需詳細資訊，請參閱適用於 [Windows 桌面](#)、[Android](#) 及 [iOS](#) 的平台指南。

感應器

感應器是一種特殊的指令碼。指令碼是隨需執行的可程式設計命令。

感應器也是可程式設計，但其可程式設計條件更優。感應器名稱可變成金鑰，而該金鑰的值是根據外部觸發器 (例如代理程式動作、排程或事件) 的執行動作所產生。此動作也可以隨需產生。然後，感應器金鑰及其產生值將用作指派的條件。

如需詳細資訊，請參閱[建立適用於 Windows 桌面裝置的感應器](#)及[適用於 macOS 裝置的感應器](#)。

指令碼

指令碼是一種可程式設計資源，執行目的是為了收集值或影響裝置變更。裝置上的指令碼會依感應器條件、隨需執行或透過 Freestyle 工作流程來觸發。

如需詳細資訊，請參閱[適用於 Windows 桌面的指令碼](#)及[適用於 macOS 裝置的指令碼](#)。

時間範圍

使用已佈建和其他可下載內容更新裝置，可能需要很長的時間。時間範圍的功能可讓您使用裝置的本機時間，在尖峰工作時間之外排程這些下載項目。您不再需要選擇要讓您的裝置保持最新狀態或保持生產力。

更多相關的資訊，請參閱 [技術預覽：建立時間範圍並指派給裝置](#)。

訂單

訂單會參照透過 Apple Business Manager 大量採購方案 (VPP) 所購買的內容，然後使用兌換碼和受管理的散發來分送該內容。如需有關訂單和 VPP 的詳細資訊，請參閱 [Apple Business Manager 指南中的大量採購方案主題](#)。

本章節討論下列主題：

- [技術預覽：建立時間範圍並指派給裝置](#)

技術預覽：建立時間範圍並指派給裝置

您可在考量工作與維護時間後，在 [時間範圍] 內排程於 Workspace ONE UEM 中更新與傳遞內容的時間。排程開始與結束日期、持續時間和重複選項，以完成您的 [時間範圍]。

目前，Windows 桌面裝置僅支援時間範圍。

如果您有要使用的已定義時間範圍，請直接跳至步驟 2 進行指派。

備註 Workspace ONE UEM 以技術預覽方式提供時間範圍功能。技術預覽功能尚未經過完整測試，某些功能可能無法如預期般運作。但是，這些預覽可協助 Workspace ONE UEM 改善目前的功能並開發未來的增強功能。若要使用技術預覽功能，請連絡您的 VMware 代表。

必要條件

在檢視、建立或指派時間範圍之前，您的管理員帳戶角色必須具備這些活動的角色權限。如需進一步資訊，請參閱 [〈管理員角色〉](#)。

權限類別路徑	權限名稱
裝置管理 > 時間範圍。	管理時間範圍 (新建、編輯及指派)
	檢視時間範圍
	檢視裝置詳細資料頁面上的時間範圍

程序

1 建立時間範圍。

- a 導覽至**資源 > 時間範圍**，然後選取**新建**按鈕。
- b 完成**名稱、說明、類別**以及**時間**選項。

類別 – 您可以建立一個維護時間專用的時間範圍，然後另外為工作時間建立一個時間範圍，這樣就能針對各類別調整合適的排程。在高流量、高可用性的環境中，這樣的安排非常有用。

時間 – 您可以選取時間範圍的時間參照標準。如果您的更新主要仰賴工作時間和非工作時間之間的時間差，則可以為 [時間範圍] 選取 [裝置時間]。但是，若更新需要同步化至所有裝置 (無論當地時間為何)，則您可以為該特定的時間範圍選取 UTC。

- c 完成**重複、開始日期、結束日期**以及**持續時間**選項。最短持續時間長度為 1 小時。

您可以在每個定義的時間範圍內新增多個排程，方法是選取**新增新排程**按鈕，然後再建立另一組**重複、開始日期、結束日期**以及**持續時間**選取項目。

每個時間範圍內需要多個排程的原因可能有所不同：您在維護時間可能有多個活動尖峰，而您的工作時間可能有多個山谷等等。

有多個排程時，您可以選取視窗右上角的垃圾桶圖示，刪除特定的排程。

- d 完成時間範圍。
 - **儲存** – 儲存時間範圍，但不進行指派。
 - **儲存並指派** – 儲存並立即指派時間範圍。

2 將時間範圍指派給裝置。

- a 導覽至**資源 > 時間範圍**。時間範圍清單檢視隨即顯示。
- b 選取清單中欲套用至裝置之時間範圍左側的選項按鈕，以將其選出。
- c 選取清單上方顯示的**指派**按鈕。

指派畫面隨即顯示。

- d 使用**智慧群組**搜尋列，將時間範圍指派給智慧群組。如需詳細資訊，請參閱[建立智慧群組](#)。請記住，時間範圍目前僅適用於 Windows 桌面裝置。如果在這裡選取的任何智慧群組所含的裝置不是使用 Windows 桌面，則不會將時間範圍指派給該些裝置。
- e 在**智慧群組**搜尋列中選取智慧群組後，請選取**指派**按鈕以完成此步驟。
- f 在 [工作流程條件] 中使用 [時間範圍]。請遵循[使用時間範圍條件建立工作流程](#)中所說明的步驟進行。

後續步驟

導覽至**詳細資料 > 清單檢視**，然後從清單中選取特定裝置，以檢視該裝置的**詳細資料檢視**並追蹤它的時間範圍。更多相關的資訊，請參閱 [第 8 章 裝置明細](#)。

您可以引導終端使用者從 Workspace ONE Intelligent Hub 應用程式選取**同步裝置**，更新**詳細資料檢視**中報告的同步狀態。

當最低記錄層級設定為**資訊**或**偵錯**時，時間範圍事件便會由事件記錄器進行記錄。如需詳細資訊，請參閱[事件記錄](#)。

Workspace ONE UEM 中的共用裝置/多使用者裝置功能，可確保每名獨特終端使用者都有安全性和驗證。共用裝置也可以僅允許特定的終端使用者存取機密資訊。

要在特定企業內將某項裝置發放給每位員工可能所費不貲。Workspace ONE UEM 可讓您以兩種方法與其他的終端使用者共用行動裝置：讓所有終端使用者都使用單一固定配置，或者讓個別的終端使用者擁有獨特的配置設定。

在管理共享裝置時，您必須先透過適用的設定和限制來佈建裝置，再將這些這些部署給終端使用者。部署之後，Workspace ONE UEM 將使用共用裝置的簡易登入或登出程序，此時終端使用者只需輸入其目錄服務或專屬的認證，即可登入。終端使用者角色將決定他們對公司資源 (例如內容、功能和應用程式) 的存取層級。此身份可確保使用者登入後能夠自動配置各項功能與資源。

登入或登出功能已內含在 Workspace ONE Intelligent Hub 中。這種獨立性可確保註冊狀態絕對不會受到影響，且不論裝置是否正在使用，都會受到管理。

也可以在與 Apple Business Manager 整合的 Apple iPad 本機上以原生方式使用共用裝置功能。這個稱為「適用於商務的共用 iPad」的功能，能以使用者的受管理 Apple ID 進行登入，而不會在 Workspace ONE Intelligent Hub 進行登入和登出。若要深入瞭解如何透過 Apple Business Manager 設定「適用於商務的共用 iPad」，以及執行此功能的步驟，請參閱 Apple Business Manager 指南簡介中的**適用於商務的共用 iPad** (可從 docs.vmware.com 取得)。

共用裝置功能

共享裝置有需多基本功能，這些功能都涉及跨使用者共享裝置時的功能和安全性。這些功能會提供充份的理由，說明共享裝置為何算是符合成本效益的解決方案，又能如何協助您發揮企業的行動性。

功能

- 在不失去企業的設定之下，為每位終端使用者提供個人化的體驗。
- 登入裝置後，系統便會透過公司存取權和特定設定、應用程式，以及根據終端使用者角色和企業群組 (OG) 的內容來配置裝置。
- 允許內含在 Workspace ONE Intelligent Hub 或 Workspace ONE Access 內的登入/登出程序。
- 當終端使用者登出裝置後，工作階段的配置設定就會抹除。然後裝置就可以讓另一名終端使用者登入。

安全性

- 先透過共用裝置設定來佈建裝置，再將裝置提供給終端使用者。
- 登入/登出裝置而不影響 Workspace ONE UEM 中的註冊。

- 使用目錄服務或專屬的 Workspace ONE UEM 憑證登入時，進行終端使用者的驗證。
- 使用 Workspace ONE Access 驗證終端使用者。
- 即便裝置尚未登入也可以管理裝置。

支援共用裝置的平台

下列裝置支援共享裝置/多使用者裝置功能。

- Android 4.3 或更新版本
- 具有 Workspace ONE Intelligent Hub 4.2 或更新版本的 iOS 裝置。
 - 如需有關登入和登出共用的 iOS 裝置的詳細資料，請參閱 **iOS 平台指南** 中的登入和登出共用的 iOS 裝置主題，可於 docs.vmware.com 取得。
- 具有 Workspace ONE Intelligent Hub 2.1 或更新版本的 MacOS 裝置。

定義共享裝置階層

雖然可選性嚴格，由於多重租用和繼承裝置的設定，為共用裝置指定企業群組 (OG) 可提供許多好處。

如果您團隊中有大量的共用裝置，且您想要將其與單一使用者裝置分別進行管理，您可以建立共用裝置專用的 OG。在您的 OG 結構中建立共用裝置階層是選擇性的。利用智慧群組和使用者群組等功能，代表您不需要嚴格仰賴 OG 階層設計來簡化裝置管理。

但是，擁有共用裝置的 OG (或巢狀的 OG) 可簡化裝置管理，讓您透過設定檔、原則和裝置繼承將裝置功能標準化，不須處理智慧群組或使用者群組所需的額外負荷。

1 導覽至群組與設定 > 群組 > 企業群組 > 企業群組明細。

您可以在此處看到代表您公司的 OG。

- 請確認所顯示的**企業群組明細**正確無誤，並且利用可用的設定來做必要的修改。如果您做了任何變更，請點選**儲存**。
- 選取**新增子企業群組**。
- 為最高層 OG 下的第一個 OG，輸入以下的資訊。

設定	描述
名稱	請為子企業群組 (OG) 輸入要顯示的名稱。只能使用英數字元。請勿使用奇怪的字元。
群組 ID	請為 OG 輸入識別碼，以供終端使用者在裝置登入期間使用。在註冊過程中，利用群組 ID 來將裝置分配到正確的 OG。 請確定共用裝置的使用者都收到該 群組 ID ，因為依據您「共用裝置」的配置，系統可能會要求裝置必須透過該群組 ID 才能登入。 若您未處於內部部署環境，則群組 ID 會在整個共用的 SaaS 環境中識別您的組織群組。因此，所有群組 ID 皆必須使用唯一的名稱。
類型	選擇預先配置的 OG 類型，以反映其子 OG 的類別。
國家	選擇 OG 所在國家。
地區設定	為所選國家選擇語言分類。

設定	描述
客戶產業	僅當 類型 為客戶時才能使用此設定。從客戶產業清單中加以選取。
時區	選擇 OG 的時區。

5 選取儲存。

共用 macOS 裝置的登入與登出

多位使用者可以登入和登出 macOS 共用裝置，啟用裝置設定檔的自動推送。

登入 macOS 裝置 – 使用指派的網路認證，登入已暫存的 macOS 裝置，並在 Workspace ONE UEM 中接收指派給您帳戶的設定檔。

登出 macOS 裝置 – 標準 macOS 登出程序也會將裝置登出指派的 Workspace ONE UEM 使用者設定檔。

共享 Android 裝置的登入與登出

若要在 Android 裝置上使用共用裝置功能，請使用 Workspace ONE Intelligent Hub 註冊裝置，然後將 VMware Workspace ONE Launcher 設為預設的主畫面。在註冊期間，系統會自動下載 Workspace ONE Launcher。

一旦應用程式安裝完成並設為預設主畫面，裝置就會進入簽到狀態。處於此狀態時，終端使用者的瀏覽範圍僅限於此頁面，且裝置會提示使用者簽出。若要移除設定檔並讓整個裝置都可再次提供存取，請透過 Workspace ONE UEM Console，在註冊預備的使用者裝置上執行企業抹除。

- 1 在 Workspace ONE Launcher 登入頁面中，使用者必須輸入其群組 ID、使用者名稱及密碼。如果在主控台上啟用**提示使用者輸入企業群組**功能，則終端使用者必須輸入**群組 ID** 才能登入。
- 2 若適用，請選取**登入**然後接受使用條款。

裝置已配置。登入後，系統會根據智慧群組和使用者群組關聯將使用者設定檔向下推播。

下一步：若要登出 Android 裝置，請選取**啟動程式設定**，然後選取**登出**（門圖示）。

共享 iOS 裝置的登入與登出

您可以從多個使用者所共用的 iOS 裝置登入和登出。

- 1 在裝置上執行 Workspace ONE Intelligent Hub。
- 2 輸入終端使用者認證。

如果裝置已登入 Workspace ONE Intelligent Hub，則系統會提示使用者輸入 SSO 密碼。如果裝置尚未登入，則系統會提示使用者輸入使用者名稱及密碼。登入後，系統會根據智慧群組和使用者群組關聯，將指派給每位使用者的設定檔向下推送。

備註 如果啟用**提示使用者提供組織群組 ID**功能，則終端使用者必須輸入**群組 ID** 才能登入裝置。

3 選取登入，並接受使用條款。

備註 如果系統提示輸入密碼，使用者可以在自助入口網站中建立一個密碼。這些密碼會有到期時間。即將到期時，Workspace ONE Intelligent Hub 會提示使用者變更裝置上的密碼。如果使用者並未在到期時間前變更其密碼，使用者將必須返回自助入口網站建立另一個密碼。

下一步：若要登出 iOS 裝置，請執行 Workspace ONE Intelligent Hub 並選取底部的**登出**。

從 UEM 主控台簽入共用裝置

您可以直接從 Workspace ONE UEM Console 簽入裝置，略過終端使用者必須使用安裝的 Workspace ONE Intelligent Hub 簽入裝置的步驟。

使用 UEM 主控台簽入裝置時，您可以使用指定的企業群組、設定檔、應用程式等資訊，有效地將註冊重設為多個註冊預備使用者。裝置端的 Workspace ONE Intelligent Hub 會重新啟動，並顯示簽出畫面。

此功能目前僅適用於 iOS 裝置。不支援使用 Workspace ONE Intelligent Hub 以外方式 (例如：直接註冊、Workspace ONE 或 Container) 註冊的裝置。不支援從主控台大量簽入裝置。

- 1 導覽至**裝置 > 清單檢視**，然後找到您要簽入的共用 iOS 裝置。
- 2 選取裝置的**暱稱**以顯示**裝置明細**。
- 3 選取畫面右上角的**更多動作**按鈕。
- 4 在**管理**區段選取**簽入裝置**。

配置共享裝置

多使用者裝置 (「共用裝置」) 註冊預備與單一使用者裝置註冊預備相似，讓 IT 管理員能夠佈建那些即將提供給多人使用的裝置。

- 1 導覽至**群組與設定 > 所有設定 > 裝置與使用者 > 一般 > 共享裝置**。

2 選取覆寫，然後填寫群組區段。

設定	描述
群組指派模式	<p>設定裝置的方法有三種：</p> <ul style="list-style-type: none"> ■ 選取提示使用者輸入企業群組，讓終端使用者在登入時輸入企業群組的群組 ID。 使用此方法，您可以針對設定、應用程式和企業群組輸入的內容靈活提供存取權。使用此方法，終端使用者可存取的內容，不只限於設定、應用程式和他們註冊的企業群組所輸入的內容。 ■ 選取固定的企業群組可對受管理裝置的設定和內容設定限制，讓裝置只適用於單一企業群組。 登入裝置的每個終端使用者都可以存取相同的設定、應用程式和內容。如果應用在零售的案例，員工為了檢查庫存等類似用途必須使用共用裝置，這種方法可能就非常實用。 ■ 選取使用者群組企業群組可根據階層中的使用者群組和組織群組啟用功能。 終端使用者登入裝置時，他們可根據在階層內獲派的角色權限存取特定設定、應用程式和內容。舉例來說，某終端使用者是「銷售」使用者群組的成員，而該使用者群組對應至「標準存取」企業群組。該終端使用者登入裝置後，裝置的設定、應用程式和內容會配置為適合「標準存取」企業群組使用的狀態。 您可以在 UEM 主控台上將使用者群組對應到企業群組。導覽至群組 & 設定 > 所有設定 > 裝置 & 使用者 > 一般 > 註冊。選取群組標籤並填寫所需的詳細資料。
不斷提示使用條款	提示終端使用者必須同意 使用條款 協議才能登入裝置。

3 按照適用情況，填寫安全性區段。

設定	描述
需要共享裝置密碼	(僅適用於 iOS 設備) 要求使用者在「自助入口網站」中建立「共享裝置」密碼才能簽出裝置。此密碼不同於單一登入密碼或裝置層級密碼。
需要使用特殊字元	共享裝置密碼必須使用特殊字元，包括 @、%、& 等等。
共享裝置密碼的最短長度	設定共享密碼的最短字元長度。
共享裝置密碼即將到期天數	設定共享密碼多久 (以天為單位) 到期。
保持共享裝置密碼的最短時間 (天數)	設定使用者必須在多短的時間內 (以天為單位) 變更共享設備密碼。
在到期前，提示使用者變更他們的共享裝置密碼 X (天)	(僅適用於 iOS 設備) 設定要在密碼到期幾天前提醒使用者變更共享裝置密碼。 為了達到最佳效果，設定的值請小於「到期時間」和「保持共享裝置密碼的最短時間」之間的差值。
密碼歷程記錄	設定系統記憶的密碼數目，避免使用者重複使用舊密碼，藉此打造更安全的環境。
自動登出	設定要讓系統在經過特定時間後自動登出。
以下時間後自動登出:	設定必須經過多久時間 (分鐘、小時或天)， 自動登出 功能才能啟用。
iOS 單一應用程式模式	<p>選取此核取方塊可設定「單一 APP 模式」，該模式可在終端使用者登入裝置時將裝置限制在單一應用程式中。</p> <p>若要簽出處於「單一 APP 模式」的 iOS 裝置，終端使用者必須使用認證登入。重新簽入裝置後，將返回「單一 APP 模式」。</p> <p>啟用「單一 APP 模式」也會停用裝置上的 [首頁] 按鈕。</p> <p>備註 「單一 APP 模式」僅適用於受監督的 iOS 裝置。</p>

4 按照適用情況，設定登出設定。

設定	描述
清除 Android 應用程式資料	使用者登出共享裝置 (簽入裝置) 時，清除 APP 資料。
重新安裝 Android 應用程式	使用下拉式功能表選取是否一律在不同使用者間重新安裝應用程式，或永不在不同使用者間重新安裝應用程式。針對 Android (舊版) 部署，如果 Hub 無法清除不同使用者間的應用程式資料，您可以選擇重新安裝應用程式。
清除 Android 裝置密碼	此設定在使用者登出 (簽入) 多個使用者共用的裝置時，控制是否清除目前的 Android 裝置密碼。
在啟動時允許 PIN 碼	啟用或停用 Android 安全啟動，需要輸入初始 PIN 碼來啟動裝置。如果已停用，使用者將無法在密碼設定期間啟用安全啟動功能。如果已在裝置上停用安全啟動功能，則裝置必須進行原廠重設，才能將其啟用。此功能僅適用於沒有以檔案為基礎進行加密的 Android 裝置。
清除 iOS 裝置密碼	此設定在使用者登出 (簽入) 多個使用者共用的裝置時，控制是否清除目前的 iOS 裝置密碼。

5 選取儲存。

下一步：有關為單一使用者和多使用者裝置註冊預備而佈建裝置的特定資訊，請參閱主題：[註冊預備單一使用者裝置](#)和[註冊預備多使用者裝置](#)。

您可以在 Workspace ONE UEM 中設定抹除臨界值，以保護您的裝置不受過度抹除和企業抹除。

從遠端抹除公司權限內容的裝置被稱為「企業抹除」，是一種當裝置遺失或失竊時才會考慮採取的步驟。這是一種避免公司內容落入競爭者手中的保障措施。裝置抹除可能更具破壞性，會移除所有內容直到裝置恢復其原廠狀態為止。

- **裝置抹除** – 傳送 MDM 指令，以將所有資料和作業系統中的裝置抹除。此動作無法復原。
 - iOS 裝置抹除考量事項
 - 針對 iOS 11 和較舊版本的裝置，裝置抹除指令也會抹除與裝置有關的 Apple SIM 卡的資料。
 - 針對 iOS 11 以上的裝置，您可以保留 Apple SIM 數據方案 (如果裝置中有此方案)。選取 [裝置抹除] 頁面上的**保留數據方案**核取方塊，然後再傳送裝置抹除命令。
 - 針對 iOS 11.3+ 裝置，您有一個額外的選項，能夠在傳送裝置抹除命令時略過**近距離感應設定**畫面。啟用此選項後，[設定輔助程式] 中將略過 [近距離感應設定] 畫面，讓裝置使用者不會看到 [近距離感應設定] 選項。
 - 若是 Windows 桌面裝置，您可以選取裝置抹除的類型。
 - **抹除** - 此選項會抹除裝置上所有內容。
 - **抹除受保護** - 此選項與一般裝置抹除相似，但裝置終端使用者無法規避動作。抹除受保護指令會持續嘗試重設裝置，直到成功為止。在某些裝置組態中，此命令會讓裝置無法開機。
 - **抹除與存留佈建資料** - 此選項會抹除裝置，但會指定佈建資料應備份到固定的位置。抹除執行後，佈建資料會還原，並套用至裝置。已儲存佈建資料夾。若要找到資料夾，您可以在裝置上導覽至 %ProgramData%\Microsoft\Provisioning 。
- **企業抹除** – 將裝置進行企業抹除，會解除註冊並移除所有受管的企業資源，包括應用程式和設定檔。此動作無法復原，而且必須要重新註冊後，Workspace ONE UEM 才能再次管理此裝置。此裝置動作包含可防止日後重新註冊的選項，以及一個**備註說明**文字方塊供您新增動作的相關資訊。
 - 雲端加入網域的裝置不支援企業抹除。

然而，有時候如合規引擎等排定時間的程序，以及其他自動化指示詞，會抹除多個裝置。除了自動抹除，管理員啟動的意外抹除也可能會發生問題。身為管理員，您應事先瞭解這類動作會於何時啟動，這樣才有機會介入。

可藉由定義抹除閾值，也就是在特定時間內可抹除的最小裝置數量，來配置抹除保護設定。例如，如有超過 10 個以上的裝置在 20 分鐘內遭到抹除，您便能將未來的抹除程序自動擱置，直到您驗證抹除命令為止。

您可檢閱「抹除記錄」，來查看裝置抹除的時間與原因。在檢閱完資訊後，您可以選擇接受或拒絕保留中的抹除指令，以及解鎖系統來重設抹除的閾值計數器。

為受管理的裝置配置抹除保護設定

為受管裝置設定抹除閾值，並於抵達閾值時透過 Email 通知管理員。您僅可在全域或客戶層級的企業群組上配置這些設定。

- 1 導覽至**裝置 > 生命週期 > 設定 > 受管裝置抹除防護**。
- 2 配置下列各項設定。

設定	描述
抹除裝置	輸入抹除的裝置的數量，當作觸發抹除防護的閾值。
在幾分鐘內	輸入在幾分鐘內的值，此值表示抹除動作必須在此時限內發生，才會觸發抹除防護功能。
Email	選擇透過 Email 寄給管理員的訊息範本。 若要建立抹除防護的訊息範本，請導覽至 群組 & 設定 > 所有設定 > 裝置 & 使用者 > 一般 > 訊息範本 ，然後選取 新增 ，再選取 裝置生命週期 作為 類別 ，並選取 抹除防護通知 作為 類型 。您可將下列的查閱值當作是訊息範本的一部分。 <ul style="list-style-type: none"> ■ {EnterpriseWipeInterval} – 設定頁面中，在幾分鐘內的數值。 ■ {WipeLogConsolePage} –將您帶入「抹除記錄」頁面的連結。
收件者	輸入必須收到通知之管理員的電子郵件地址。這些管理員必須具有「抹除記錄」頁面的存取權。

如需詳細資訊，請參閱[第 12 章 查閱值](#)。

- 3 選取**儲存**。

檢視抹除記錄

您可以檢視**抹除記錄**頁面，來查看裝置遭抹除的時間與原因。在檢閱完資訊後，您可以選擇接受或拒絕任何保留中的抹除指令，以及解鎖系統來重設抹除的閾值計數器。

如果系統已被鎖定，頁面最上方便會顯示一個橫幅來指明此狀況。

- 1 導覽至**裝置 > 生命週期 > 抹除記錄**。

[抹除記錄] 頁面的存取權由**報告裝置抹除記錄**資源所管理，且該資源依預設可供系統管理員、SaaS 管理員和 Workspace ONE UEM 管理員使用。您可以利用**建立管理員身份**頁面來將此資源新增至任何自訂管理員身份。

- 2 使用下列參數來**篩選**抹除記錄。從以下項目中選擇。
 - 日期範圍
 - 抹除類型
 - 狀態

- 來源
- 擁有權

3 檢視裝置清單並決定抹除目前所顯示的裝置是否正確。

裝置擱置動作會顯示「保留中」狀態。達到臨界值限制之前，遭抹除的裝置會顯示為「已處理」。

- a 如果是有效的抹除，請選取每個裝置，然後從指令清單中選取**同意抹除**。其狀態就會變為「已核准」。
- b 如果是無效的抹除，請選取每個裝置，然後從指令清單中選取**拒絕抹除**。其狀態就會變為「已拒絕」。

4 若要重設裝置閾值計數器，並允許抹除指令通過，請選取**解鎖系統**。

系統會允許未來的自動抹除命令，直至臨界值再次超過上限為止。您僅可以在全域或客戶層級的企業群組上執行這項動作。