Windows 應用程式管理

VMware Workspace ONE UEM

vmware by Broadcom

您可以在 VMware by Broadcom 網站上找到最新的技術說明文件，網址如下：

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

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

目錄

Workspace ONE UEM 中 Windows 的應用程式管理

1

使用 Workspace ONE UEM 將 Windows 應用程式推送至 Windows 桌面 (Windows 10) 裝置。檢視系統針對每個應用程式類型所支援的檔案類型。

應用程式類型和支援的 Windows 平台

Workspace ONE UEM 將應用程式以內部用、公用和 Web 來分類，您可以依據這些類型來上傳應用程式。本主題說明每種應用程式類型所支援的平台和部署。

有關如何使用 Workspace ONE UEM 管理 Windows Desktop 應用程式的詳細資訊，請參閱位於 https://techzone.vmware.com/deploying-traditional-win32-applications-windows-devices-workspace-one-operational-tutorial#overview 的操作教學。

表 1-1. 應用程式類型和支援的 Windows 平台

應用程式類型	支援的平台
內部用	Windows 桌面 (Windows 10) ■ APPX **備註** 上傳 APPX 檔案，可為 x86、x64 或 ARM。然而，APPX 僅會安裝於使用相同架構的裝置上。舉例來說，如果您使用 ARM，Workspace ONE UEM 便不會將 x64 和 x86 架構的安裝命令排入佇列。不會將應用程式推播至使用 x64 或 x86 架構的裝置。 ■ EXE：上傳適用於 Windows 10 的 Win32 應用程式 EXE 套件。 ■ MSI：MSI 檔案 (亦稱為 Windows Installer) 為一組含有安裝、維護及移除軟體所需工具的套件。 ■ ZIP：上傳適用於 Windows 10 的 Win32 應用程式 ZIP 套件。
公用 (免費和付費)	商務用 Microsoft Store 讓您能夠取得、管理和散佈大量應用程式。如果您使用 Workspace ONE UEM 來管理 Windows 10 裝置，您便可同時整合這兩個系統。整合之後，即可從商務用 Microsoft Store 取得並散佈應用程式，並且利用 Workspace ONE UEM 來管理該應用程式的更新版本。 您可以指派從商務用 Microsoft Store 匯入的公用應用程式，利用彈性部署功能將這些應用程式套用到裝置上。您也可以根據您的授權管理策略來指派線上和離線授權。
Web 連結	Workspace ONE UEM Console 支援 Windows 桌面 (Windows 10) 以推送和管理 Web 連結應用程式。Web 剪輯設定檔可讓您將 URL 推送到終端使用者裝置上，以輕鬆存取重要的網站。 您可使用兩種方法來新增 Web 連結應用程式。 ■ 做為 Workspace ONE UEM console **資源**區段中的應用程式。 ■ 做為 UEM console [裝置] 區段中的 Web 剪輯裝置設定檔。

使用商務用 Microsoft Store 管理應用程式 2

商務用 Microsoft Store 讓您能夠取得、管理和分發大量應用程式。如果您使用 Workspace ONE UEM 來管理 Windows 10+ 裝置，便可與兩個系統整合。整合之後，即可從商務用 Microsoft Store 取得並散佈應用程式，並使用 Workspace ONE UEM 來管理其更新版本。如需商務用 Microsoft Store 程序的資訊，請參閱 https://technet.microsoft.com/itpro/windows/manage/windows-store-for-business。

離線和線上授權模式有共同的需求

- Windows 10+ 裝置 - 指派應用程式時，請使用 Windows 桌面 (Windows 10 裝置)。您選取的 OG 必須是**客戶**類型。
- Azure Active Directory 服務 - 在 Workspace ONE UEM 中設定 Azure Active Directory 服務以啟用系統間的通訊。此組態會啟用 Workspace ONE UEM 以在這些裝置上管理 Windows 裝置和應用程式。

  您不需要有 Azure AD Premium 帳戶，即可與商務用 Microsoft Store 整合。此整合與自動 MDM 註冊是各自獨立的程序。

  重要 只有在目標組織群組 (OG) 是客戶類型 OG，且您會在此設定 Azure Active Directory 服務時，整合才會有效。
- 商務用 Microsoft Store 管理員帳戶與全域權限 - 使用商務用 Microsoft Store 管理員帳戶取得應用程式。全域權限讓管理員能夠存取所有系統，以便獲取、管理和分發應用程式。
- 針對內部部署 Workspace ONE UEM 啟用的檔案儲存空間會在安全的檔案儲存系統上，儲存商務用 Microsoft Store 應用程式。內部部署環境必須在 Workspace ONE UEM Console 的 [目錄服務] 頁面中，新增租用戶識別碼和租用戶名稱方可啟用此功能。此為配置 Azure AD 服務程序的必要條件之一。

線上授權模式的需求

Azure Active DirectoryDevice 使用者必須使用 Azure Active Directory 以驗證內容。

離線授權模式的需求

程序進行期間，Workspace ONE UEM 會匯入所有的應用程式套件，並停用指派動作。當您為更新等目的重新匯入套件時，Workspace ONE UEM 僅會下載有所變更的套件。如果您沒有限制使用裝置上的 APP 商店，應用程式的更新項目就會從商務用 Microsoft Store 推播到裝置上。如果您限制使用裝置上的 App Store，則需在 Workspace ONE UEM 中匯入更新的應用程式。然後再通知裝置使用者，從 AirWatch Catalog 中上傳更新的版本。

比較商務用 Microsoft Store 的線上與離線授權模式

商務用 Microsoft Store 的線上與離線模式可提供不同的功能。根據您要管理部署的方式來選取模式。功能包括以何種系統來管理授權、應用程式套件的儲存位置，以及以何種系統驗證資源。

表 2-1. 線上與離線模式比較 – 不同功能

功能	線上授權模式	離線授權模式
授權控制	由商務用 Microsoft Store 管理的授權。 使用者可以在 Workspace ONE UEM 部署之外接收應用程式並要求授權。	由企業管理的授權。 使用離線授權方式來掌控應用程式的套件和更新。 雖然此模式可以提供您彈性，但是您必須隨時注意以確保即時更新應用程式和續訂授權。
APP 套件代管	由商務用 Microsoft Store 代管的 APP 套件。	由 Workspace ONE UEM 檔案儲存以進行內部部署，或在 Workspace ONE UEM SaaS 環境中代管的應用程式套件。
Azure Active Directory	裝置必須使用您的 Azure Active Directory 系統以進行驗證。 啟用 Azure Active Directory 系統，以便讓 Workspace ONE UEM 和商務用 Microsoft Store 進行通訊。	裝置不需要使用 Azure Active Directory 系統以進行驗證。 然而，您必須啟用 Azure Active Directory 系統，才能讓 Workspace ONE UEM 和商務用 Microsoft Store 進行通訊。
限制 App Store	裝置無法安裝應用程式，因為限制會導致商務用 Microsoft Store 無法在裝置上運作。	裝置仍可安裝應用程式，因為應用程式套件是在 Workspace ONE UEM 環境中代管。

表 2-2. 線上與離線模式比較 – 相同功能

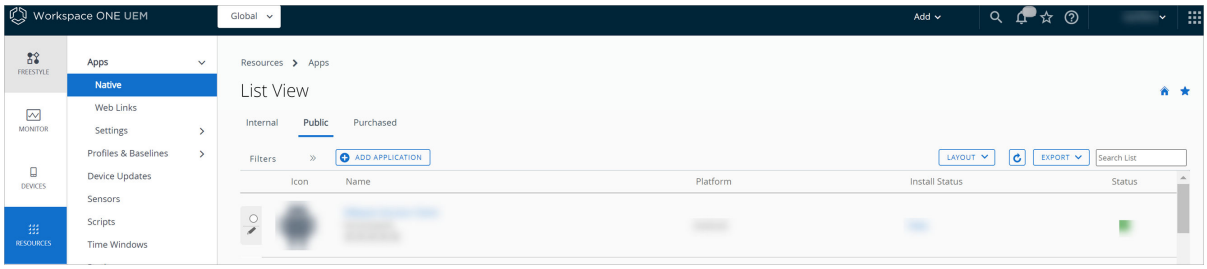
功能	線上授權模式	離線授權模式
要求授權的層級	在使用者層級中由應用程式的 Workspace ONE UEM 要求授權。	在使用者層級中由應用程式的 Workspace ONE UEM 要求授權。
授權重複使用	管理員可透過 Workspace ONE UEM 撤銷授權並重複使用授權。	管理員可透過 Workspace ONE UEM 撤銷授權並重複使用授權。

匯入從商務用 Microsoft Store 取得的公用應用程式

您可以將從商務用 Microsoft Store 取得的公用應用程式匯入 Workspace ONE UEM console 中。線上與離線授權模式的適用流程皆相同。針對離線授權模式，會規劃在您企業網路處於非忙碌狀態時匯入這些應用程式。由於涉及的應用程式數量很多，匯入的過程可能會使用比其他 Workspace ONE UEM 系統更多的頻寬。

1 前往您設定 Azure Active 目錄服務的企業群組。

2 導覽至**資源** > **應用程式** > **原生** > **公用**，然後選取**新增應用程式**。



3 選擇**平台**。

4 選擇**從 BSP 匯入**，然後選擇**下一步**。

5 檢視 Workspace ONE UEM 從您的商務用 Microsoft Store 帳戶匯入的應用程式清單。您無法在 Workspace ONE UEM console 中編輯此清單。

6 選擇**完成**。

- 離線授權模式 - 系統會將應用程式下載至遠端檔案儲存系統。
- 線上授權模式 - 系統會將應用程式儲存於商務用 Microsoft Store 中並等候安裝指令。

部署從商務用 Microsoft Store 取得的公用應用程式

您可以指派從商務用 Microsoft Store 取得的公用應用程式，利用彈性部署功能將這些應用程式套用到裝置上。您可以根據您的授權管理策略來指派線上和離線授權。

1 導覽至**資源** > **應用程式** > **原生** > **公用**。

2 選取應用程式並選擇**指派**。

3 完成**新增指派**選項以新增規則。

設定	描述
指派 – **線上授權**	透過線上授權將群組指派至應用程式。 若裝置為 Azure Active Directory 系統的一部分，且部署具有可用的線上授權，裝置即可接收應用程式。 若您為裝置同時指派線上與離線授權，則系統會優先採用線上授權。
指派 – **離線授權**	透過離線授權將群組指派至應用程式。 若部署具有可用的離線授權，裝置即會接收應用程式。 若您為裝置同時指派線上與離線授權，則系統會優先採用線上授權。

設定	描述
部署 – **APP 遞送方法**	檢視交付方式。隨選會將內容部署到部署代理程式，並讓裝置使用者自行決定是否要安裝該內容以及何時安裝。
部署 – **DLP**	使用**限制**設定檔配置裝置設定檔，以設定應用程式專用的資料遺失防護原則。 選擇**配置**。系統會導覽至**設定檔**區域。選取 **新增 > 新增設定檔 > Windows > Windows 桌面 > 裝置設定檔 > 限制**。啟用可套用至您要保護之資料的選項

4 如果您有多個指派規則，選取**新增**並排列指派的優先順序。

5 透過**儲存並發佈**來部署應用程式。

重新宣告和重新指派應用程式授權

將商務用 Microsoft Store 應用程式指派給裝置時，指派程序會在系統啟動應用程式安裝之前要求相應的授權。[詳細資料檢視] 可為您提供使用者裝置清單，以及相關聯的已宣告授權。您也可以刪除應用程式指派，以重新宣告和重新指派授權。在 [應用程式詳細資料檢視] 中同步離線與線上授權，可為您提供授權的對應使用者。

您可以導覽至**資源** > **應用程式** > **清單檢視** > **公用**，然後選取商務用 Microsoft Store 應用程式。此動作會顯示明細顯示。在此檢視中，使用**同步授權**動作，以匯入對應至要求授權的使用者清單。若要查看要求的授權，請選取**授權**標籤。

備註 在初次匯入商務用 Microsoft Store 應用程式之際，選擇 [從 BSP 匯入] 選項時，Workspace ONE UEM 也會匯入授權關聯。此同步與應用程式套件同步執行不同步。

您可以藉由刪除對使用者裝置的應用程式指派，以回收並重複使用**授權**標籤上顯示的授權。Workspace ONE UEM 包括刪除指派的數種方式。刪除會造成應用程式從裝置中移除。

表 2-3. 回收授權的方法

方法	描述
明細檢視	在應用程式的明細檢視中，選擇**刪除應用程式**功能。 此動作會將應用程式從指派至應用程式的群組中移除。
裝置	從主控台刪除適合的裝置。
企業群組	刪除組織群組。此動作會影響組織群組中的資產和裝置。
指派群組	刪除指派給應用程式的智慧或使用者群組。此動作會影響群組中的每部裝置。
使用者	從主控台刪除適合的使用者帳戶。

設定 Azure AD 整合

若要設定您的 Azure AD，請使用 Azure 管理員帳戶來登入商店，並啟用 Workspace ONE UEM 管理工具。

1 針對 Workspace ONE UEM 建立 Azure 管理員帳戶。在您的 Microsoft Azure 預設目錄中，配置具有全域管理員身份的管理員帳戶。使用此帳戶，在商務用 Microsoft Store 中取得應用程式。您不需要 Azure Premium 帳戶即可建立商務用 Microsoft Store 的管理員帳戶。

   a 在 Azure 中導覽至您的 Azure Active Directory。

   b 選擇**使用者及群組**和 **+ 新增使用者**。

   c 將**目錄角色**配置為**全域管理員**。

   d 建立暫時性密碼，這樣您就可登入商務用 Microsoft Store。

2 在商務用 Microsoft Store 中啟動 Workspace ONE UEM，並取得應用程式。使用您的 Azure 管理員帳戶認證，在商務用 Microsoft Store 中啟用 Workspace ONE UEM 管理工具。若您使用離線授權，請啟用取得離線授權應用程式。

   a 導覽至商務用 Microsoft Store，並使用您的 Azure 管理員帳戶登入。

   b 導覽至**管理** > **設定** > **散佈** > **管理工具**，然後啟用 VMware Workspace ONE UEM 工具。

   c 若要使用離線授權，請前往**管理** > **設定** > **商店** > **購物體驗**，並啟用**向在商店中購物的使用者顯示離線授權的應用程式**。

   d 在 Store for Business 中，新增應用程式至您的庫存清單。您可根據授權管理策略，使用離線或線上授權來新增應用程式。

Flexera Software Vulnerability Manager 整合

3

Flexera Software Vulnerability Manager (有時以縮寫 SVM 顯示) 包含許多功能，其中一項功能是為數以千計的應用程式提供弱點分數與精選修補程式清單。您可以在 Workspace ONE UEM 中根據 Flexera Software Vulnerability Manager 所報告的 Windows 10 應用程式分數來檢視、驗證和指派所管理的 Windows 10 應用程式。

需求

- 使用 Flexera Software Vulnerability Manager v7.6.1.16 或 2021 R1。
- 使用 Workspace ONE UEM Console v2101 或更新版本。
- 使用已搭配 Workspace ONE UEM 註冊，且同時執行 Flexera Software Vulnerability Manager 代理程式的 Windows 10 裝置。
- 使用 SVM 修補程式精靈 v5.0.381 或更新版本。

如何設定整合？

設定 SVM 修補程式精靈，並在 Workspace ONE UEM 中使用需要的應用程式。

1 使用您的 Workspace ONE UEM 認證來設定 SVM 修補程式精靈。

   a 啟動 SVM 修補程式精靈，然後選取 **Workspace ONE** 索引標籤。

   b 輸入您的 Workspace ONE UEM 執行個體認證。

   c 選取驗證類型。

   d 提供您要發佈修補程式之租用戶階層的 REST API 金鑰。

   SVM 修補程式精靈會顯示 Workspace ONE UEM 組織群組的清單。

   e 為您的整合選取適用的 Workspace ONE UEM 組織群組。

   f 測試連線，並在 **SVM** 索引標籤上驗證記錄層級。

2 識別並發佈 Software Vulnerability Manager 中的弱點。

   a 在 Software Vulnerability Manager 中，檢閱 **SPS** 區段或**廠商修補程式**模組中的重要修補程式。

b 識別需要修補的弱點，然後在選項上按一下滑鼠右鍵以建立套件。

c 使用套件精靈設定封裝弱點。選取**修補程式精靈**作為發佈模式。

d 在**修補程式部署狀態**頁面上發佈套件，並監控其狀態。

e 確認 Workspace ONE 環境詳細資料。

3 檢視、驗證和指派 Workspace ONE UEM 中的應用程式。

備註 將此整合推送至生產裝置之前，請考慮推送至裝置測試群組。

a 在 Workspace ONE UEM Console 中，移至 **資源 > 應用程式 > 原生**，然後選取應用程式類型以查看應用程式**清單檢視**。

b 使用 **Flexera SVM** 屬性篩選**清單檢視**以查看應用程式及其指派的嚴重度 (弱點分數)。

c 驗證應用程式的中繼資料。中繼資料包含從 Software Vulnerability Manager 中應用程式適用性規則轉換的安裝不確定因素和偵測準則。

d 將彈性化部署指派新增至應用程式以推送至裝置。整合只會將 **Flexera SVM** 應用程式安裝到符合中繼資料 (轉換適用性規則) 的裝置。

Microsoft Intune 應用程式防護原則整合

4

Workspace ONE UEM 與 Microsoft Intune® 應用程式防護原則整合後，將在兩個控制台中移除 Microsoft Intune 應用程式防護原則的資料遺失防護 (DLP) 原則管理。

您可以在 Workspace ONE UEM 中為 Microsoft Intune 應用程式防護設定 DLP 應用程式原則。整合這兩個系統之後，請在 Workspace ONE UEM Console 中管理 DLP 應用程式原則，讓整合保持最新狀態。

大多數 Microsoft Intune 應用程式防護原則可在 Android 平台和 iOS 平台上使用。

在 Workspace ONE UEM Console 中管理以保持同步

整合這兩個系統之後，請在 Workspace ONE UEM Console 中管理 DLP 應用程式原則，讓整合保持最新狀態。Workspace ONE UEM 不會收到在整合的其他部分中所做的變更。DLP 應用程式原則或安全性群組指派可能會不同步。

Android 和 iOS 上的使用者體驗

與 Intune 成功整合後，使用者首次存取應用程式時，iOS 和 Android 平台會提供不同和類似的使用者體驗。

iOS 上的體驗

當裝置使用者向 iOS 裝置上的 Microsoft Office 365 應用程式進行驗證，且成功推送設定檔時，系統會出現快顯視窗，說明您的組織管理應用程式。組態中沒有其他步驟。

Android 上的體驗

要管理 Android 和 Android Enterprise 裝置，使用者必須安裝 Intune 公司入口網站應用程式。此應用程式可做為 Intune App SDK 的代理程式，這跟 Workspace ONE Intelligent Hub 做為 Workspace ONE UEM 應用程式的代理程式一樣。

iOS 和 Android 上的常見體驗

兩個平台都必須將 Intune 設定為裝置上的 MDM 授權單位。您可以在 **Azure 租用戶 > 所有資源 > Intune** 中為此裝置進行這項設定。從**開始使用**通知啟用 **Intune MDM 授權單位**。

在 Azure 中執行這些動作，來整合 Microsoft Intune

進行整合前，請建立使用者帳戶，並為使用者指派列出的 Microsoft 授權。

未在 Workspace ONE UEM Console 的目錄服務中整合 Azure AD 的環境，您必須在 Azure 中新增 **AirWatch by VMware** 應用程式。如需詳細資訊，請存取設定 Workspace ONE UEM 以使用 Azure AD 作為識別服務。

重要 如果您已使用 Workspace ONE UEM 以外的任何其他 MDM 提供者設定可立即使用的註冊 (OOBE)，請新增 **AirWatch by VMware**，且不要在 Azure 中輸入或編輯任何其他設定。如果您輸入或編輯組態，可能會中斷目前的註冊流程。

- 在 Azure 建立服務帳戶 (使用者)，然後為使用者指派適當的角色。

  備註 這些步驟是一般步驟。如需有關設定 Azure 的最新詳細資料，請參閱 Microsoft 說明文件。

  a 在瀏覽器中輸入 **`portal.azure.com`**，前往 Azure 入口網站。

  b 建立使用者，或將使用者與內部部署 Active Directory 同步。

  停用此使用者網域的 MFA (多重要素驗證)。

  c 將列出的角色指派給此使用者。

  - **Intune 管理員**
  - **應用程式管理員**
  - **目錄讀取者**
  - **目錄寫入者**

- 如果您已在 Azure AD 中建立使用者，請使用此帳戶在 **`portal.azure.com`** 登入 Azure。確認密碼有效，且不需要更新。
- 您必須為使用者指派 Azure 中列出的授權。
  - Microsoft Intune 應用程式防護原則
  - Microsoft Enterprise Mobility + Security E3 或 E5

配置 Intune 設定

在 Workspace ONE UEM Console 中設定資料遺失防護 (DLP) 應用程式原則，並套用至 Microsoft Intune® 應用程式防護應用程式和資料。請先設定 [驗證] 索引標籤，讓系統能夠進行通訊。接著配置 DLP 設定，並將其指派給群組。

Workspace ONE UEM 不會直接在應用程式上強制執行原則。Microsoft SDK 會控制並強制執行原則。

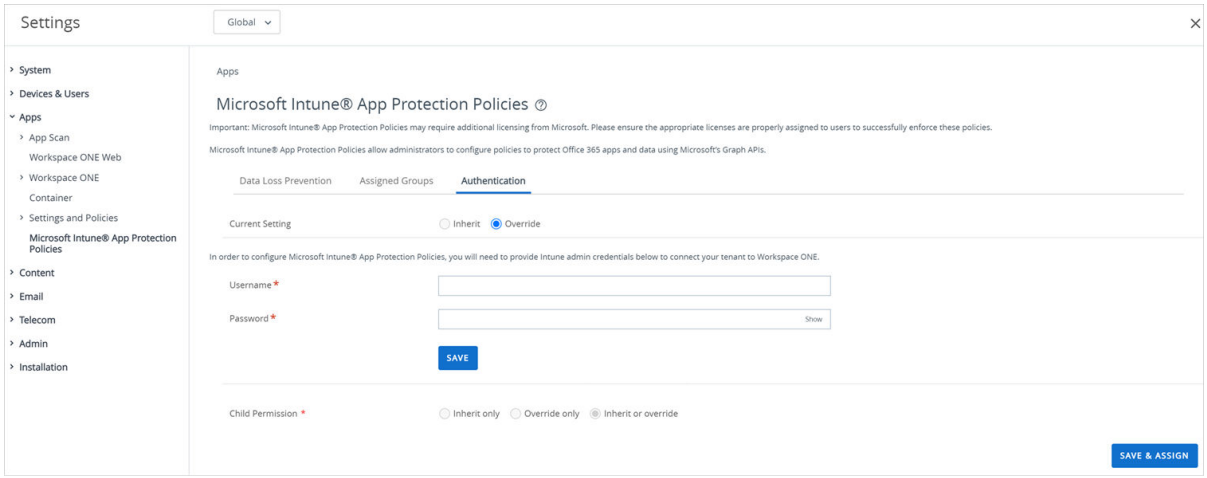
備註 警告會因作業系統版本與應用程式版本而異。Android 修補程式版本只會以警告訊息通知使用者。不過，警告警示並不會阻止終端使用者使用應用程式。

必要條件

若要設定 DLP 應用程式原則，並將其套用至 Intune 應用程式，您必須具有在 Intune 中設定應用程式原則的權限。

操作程序

1 導覽至**群組與設定 > 所有設定 > 應用程式 > Microsoft Intune® 應用程式防護原則**。



2 選取**驗證**索引標籤，然後輸入 Azure 管理員的使用者名稱和密碼。

管理員可以使用 Office 365 DLP 應用程式原則，透過 Microsoft Graph API 保護 Office 365 應用程式和資料。若要設定 Office 365 DLP 原則，您需要管理員認證才能將租用戶連線至 Workspace ONE UEM。

設定	描述
使用者名稱	輸入將租用戶設定至 Workspace ONE UEM 的使用者名稱。
密碼	輸入將租用戶設定至 Workspace ONE UEM 的密碼。

Workspace ONE UEM 會使用這些認證來搜尋 DLP 應用程式原則，並將其指派給 Microsoft 安全性群組。

3 選取 [資料遺失防護] 索引標籤，並設定偏好的 Microsoft Intune 應用程式防護原則 DLP 應用程式原則。為受管理 Microsoft Intune 應用程式防護原則應用程式和資料設定 DLP 應用程式原則。

資料重新配置的設定	描述
禁止備份	防止使用者備份來自受管理應用程式的資料。
允許應用程式將資料傳輸到其他應用程式	■ **全部** - 使用者可以將資料從受管理應用程式傳送至任何應用程式。 ■ **受限制** - 使用者可以將資料從受管理應用程式傳送至其他受管理應用程式。 ■ **無** - 避免使用者將資料從受管理應用程式傳送至任何應用程式。
允許應用程式接收從其他應用程式傳來的資料	■ **全部** - 使用者可以接收從應用程式傳來的資料，並放至其受管理應用程式。 ■ **受限制** - 使用者可以接收從其他受管理應用程式傳來的資料，並放至其受管理應用程式。 ■ **無** - 防止使用者接收從所有應用程式傳來的資料，並放至其受管理應用程式。

資料重新配置的設定	描述
禁止「另存新檔」	防止使用者將受管理 Microsoft Intune 應用程式防護原則應用程式資料儲存到另一個儲存系統或區域。
限制與其他應用程式之間進行剪下、複製與貼上	■ **任何應用程式** - 使用者可以在其受管理應用程式與任何應用程式之間進行剪下、複製與貼上資料。 ■ **已封鎖** - 防止使用者在受管理應用程式與所有應用程式之間進行剪下、複製和貼上資料。 ■ **原則管理應用程式** - 使用者可以在受管理 Microsoft Intune 應用程式防護原則應用程式之間進行剪下、複製和貼上資料。 ■ **原則管理應用程式可貼入** - 使用者可以從其受管理應用程式中剪下和複製資料，以及將資料貼入其他受管理應用程式。 使用者也可以將任何應用程式的資料剪下並複製到其受管理應用程式中。
限制在受管理瀏覽器中顯示 Web 內容	強制受管理應用程式中的連結在受管理瀏覽器中開啟。
加密應用程式資料	當裝置處於所選狀態時，加密與受管理應用程式相關的資料。系統會加密儲存在任何位置的資料，包括外部儲存磁碟機和 SIM 卡。
停用內容同步	防止受管理應用程式將聯絡人儲存到本機通訊錄。
禁止列印	防止使用者列印與受管理應用程式相關聯的資料。
允許的資料儲存位置	管理員可以控制使用者儲存受管理應用程式資料的位置。

存取的設定	描述
需要使用 PIN 碼以進行存取	需要使用者輸入 PIN 碼才能存取受管理應用程式。 使用者會在初始存取期間建立 PIN 碼。
重設 PIN 碼前嘗試的次數	設定使用者在系統重設 PIN 碼之前嘗試的輸入次數。
允許簡單的 PIN 碼	使用者可以建立包含重複字元的四位數 PIN 碼。
PIN 碼長度	設定使用者必須為其 PIN 碼設定的字元數。
允許的 PIN 碼字元	設定使用者必須為其 PIN 碼設定的字元。
允許使用指紋而不是 PIN 碼	使用者可以使用指紋而非 PIN 碼存取受管理應用程式。
要求使用公司認證存取	使用者可使用其企業認證存取受管理應用程式。
封鎖在破解或刷機過的裝置上執行受管理應用程式。	防止使用者存取遭破解裝置上的受管理應用程式。
(分鐘) 後重新檢查存取要求	設定系統，以便在存取工作階段達到其中一個時間間隔時，驗證存取 PIN 碼、指紋或認證資訊。 ■ **逾時** - 受管理應用程式的存取工作階段閒置分鐘數。 ■ **離線寬限期** - 搭載受管理應用程式裝置的離線分鐘數。
抹除應用程式資料前的離線間隔 (天)	設定系統在裝置離線達一定天數時，從裝置上移除受管理應用程式資料。

Android 的設定	描述
封鎖螢幕擷取和 Android Assistant	如果選取**是**，則使用 Office 應用程式時，無法使用螢幕擷取和 Android Assistant 應用程式掃描。
要求的最低作業系統版本	輸入要求使用者應具備的最低 Android 作業系統版本編號，以取得對應用程式的安全存取。
要求的最低作業系統版本 (僅為警告警示)	輸入要求使用者應具備的最低 Android 作業系統版本編號，以取得對應用程式的安全存取。
要求的最低應用程式版本	輸入要求使用者應具備的最低應用程式版本編號，以取得對應用程式的安全存取。
要求的最低應用程式版本 (僅為警告警示)	輸入使用者應具備的最低應用程式版本編號，以取得對應用程式的安全存取。
要求的最低 Android 修補程式版本	輸入要求使用者應具備的最舊 Android 安全性修補程式層級，以取得對應用程式的安全存取。
要求的最低 Android 修補程式版本 (僅為警告警示)	輸入使用者可擁有的最舊 Android 安全性修補程式層級，以取得對應用程式的安全存取。

4 選取**指派群組**索引標籤，然後將 DLP 應用程式原則指派給 Microsoft 安全性群組。先前已在 Azure 中設定安全性群組。

設定	描述
所有安全性群組	輸入安全性群組的名稱，並將其指派給 DLP 應用程式原則。從輸入後顯示的清單中選取。 選取**新增群組**，並將 DLP 應用程式原則指派給安全性群組。
指派給 O365 原則的安全性群組	列出指派給 DLP 應用程式原則的安全性群組。 選取**移除群組**，然後從安全性群組中移除指派。

已刪除和已修改原則的警告訊息

載入 Microsoft Intune 應用程式防護原則後，Workspace ONE UEM Console 會在 Azure 入口網站的 Intune 中檢查刪除和修改。受管理原則可能會與已部署原則不同步。為了警告管理員可能的刪除和修改，Workspace ONE UEM Console 會根據案例顯示警告訊息。

- 已在 Microsoft Intune 入口網站上刪除原則。按一下 [刪除設定]，從 UEM 刪除原則設定。

  某人刪除部署在 Intune 中的 iOS 和 Android 原則 (其中一個，或兩個都刪除) 後，Workspace ONE UEM Console 會顯示此訊息。選取**刪除設定**會從 Workspace ONE UEM Console 移除這兩個原則的設定，無需修改 Azure 端的任何內容。主控台頁面不會自動重新整理。

  使用者可以將新的 iOS 和 Android 原則部署至 Azure，而不會發生錯誤。

  備註 如果在 Azure 中僅刪除了其中一個原則 (iOS 或 Android)，另一個原則仍會保留在 Azure 中。如果使用者選擇不保留過去的設定，則必須手動刪除另一個原則。

- 已在 Microsoft Intune 入口網站上更新原則設定，並且不與 Workspace ONE UEM 同步。按一下 [同步設定]，以在 UEM 中更新此原則。

某人在 Azure 入口網站中修改 Intune 的 iOS 和 Android 原則後，Workspace ONE UEM Console 會顯示此訊息，且兩個原則之間的原則設定仍相符。選取**同步設定**會更新 Workspace ONE UEM 中這兩個原則的設定，以符合從 Azure 原則中提取的設定。主控台頁面不會自動重新整理。

備註 此案例會排除 iOS 或 Android 專用的設定，例如 iOS SDK 設定和 Android Assistant 設定。

- 在 Azure 入口網站中，Android 原則和 iOS 原則的「接收其他應用程式之間的資料」原則有所不同。此設定必須相同，Workspace ONE UEM 才能同步 Android 和 iOS 原則。請聯絡 IT 管理員以解決此問題。

  在 Azure 入口網站中，Android 原則和 iOS 原則的「接收其他應用程式之間的資料」和「將組織資料傳送至其他應用程式」的原則各有不同。這些設定必須相同，Workspace ONE UEM 才能同步 Android 和 iOS 原則。請聯絡 IT 管理員以解決此問題。

  在 Azure 入口網站中，Android 原則和 iOS 原則的「禁止備份」、「接收其他應用程式之間的資料」和「將組織資料傳送至其他應用程式」原則有所不同。這些設定必須相同，Workspace ONE UEM 才能同步 Android 和 iOS 原則。請聯絡 IT 管理員以解決此問題。

  若某人在 Azure 入口網站中修改 Intune 的這兩個原則，但兩個原則之間的原則設定不相同，則 Workspace ONE UEM Console 會顯示這些訊息。這些訊息會列出 Azure 中兩個原則之間的設定不一致狀況。此外也會列出 Azure 中所列原則名稱，而不是由 Workspace ONE UEM Console 使用的原則名稱。

  請先解決訊息中列出的衝突，再使用 Workspace ONE UEM Console 中的**同步設定**功能表項目。

  備註 此案例會排除 iOS 或 Android 專用的設定，例如 iOS SDK 設定和 Android Assistant 設定。

刪除設定功能表項目和**同步設定**功能表項目不會修改 Azure 入口網站中 Intune 的任何設定。