

# 行動內容管理

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](http://www.vmware.com)

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

# 目錄

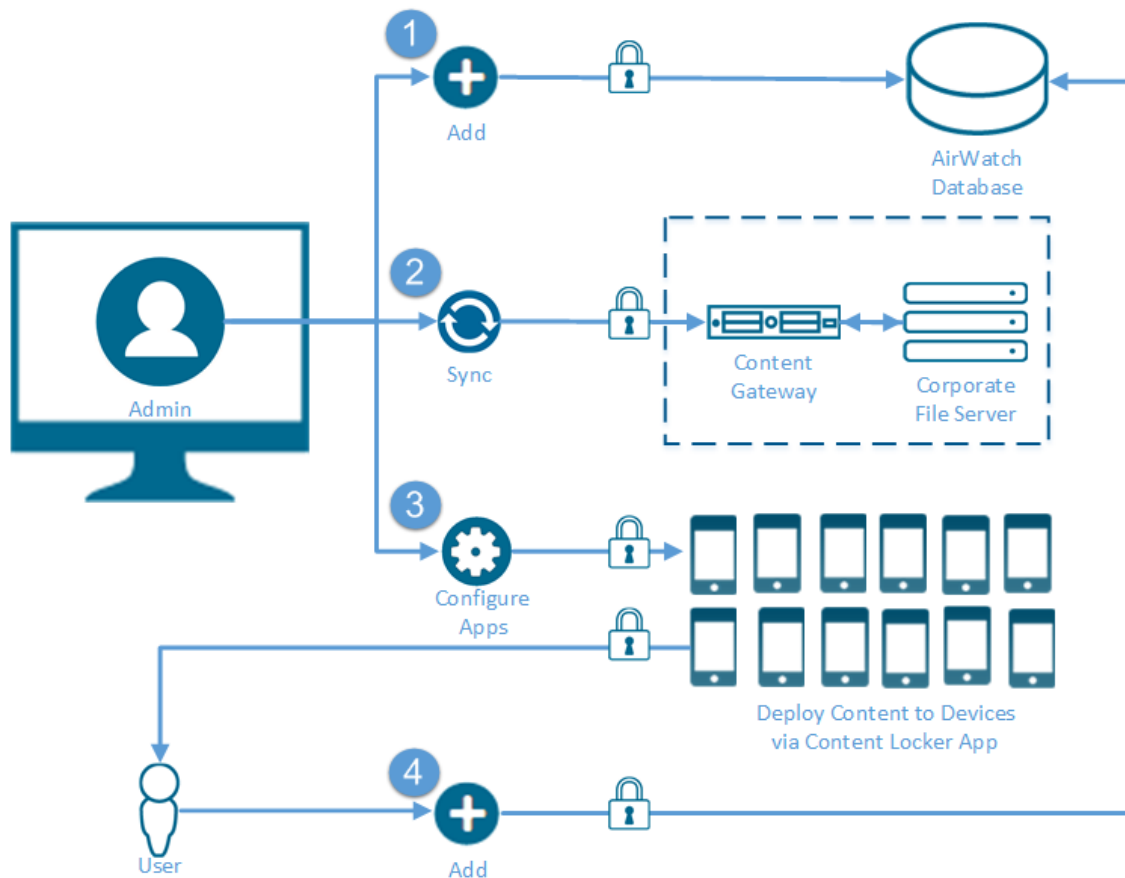
- 1** 行動內容管理介紹 4
- 2** 企業檔案伺服器 8
- 3** Workspace ONE UEM 受管理內容存放庫 18
- 4** APP 套件 SDK 配置 23
- 5** VMware Workspace ONE Content 29
- 6** Workspace ONE Smartfolio 47
- 7** 使用 Workspace ONE 主控台管理內容 55

# 行動內容管理介紹

# 1

Workspace ONE UEM powered by AirWatch 提供行動內容管理™ (MCM) 解決方案，能利用幾個關鍵動作，協助您的組織克服將內容安全地部署至各種裝置時所面臨的挑戰。使用 Workspace ONE UEM Console 來建立、同步或啟用檔案儲存機制，也稱為存放庫。一旦設定完成，就能使用 VMware Workspace ONE Content 應用程式將內容部署至終端使用者的裝置上。

若要瞭解內容管理的運作方式，請檢閱下列大綱。



- 1 **UEM 所管理內容存放庫** – 是指用來儲存檔案的存放庫，Workspace ONE UEM 管理員如具有合適的權限，便能完全控管儲存於此處的檔案。
- 2 **企業檔案伺服器** – 是指組織的內部網路中已存在的存放庫。根據組織結構的不同，Workspace ONE UEM 管理員可能已擁有企業檔案伺服器的管理權限，也可能沒有。

- 3 **VMware Workspace ONE Content** – 一種應用程式，可部署至終端使用者的裝置上，允許使用者在所設定的參數集內存取內容。

## 行動內容管理需求

行動內容管理 (MCM) 具有一系列靈活的服務可供您實作。每個服務本身都有獨特的需求。配置 MCM 前，先檢閱您要配置的服務並滿足其基本需求十分重要。

元件	需求與說明
軟體與硬體需求	
支援的瀏覽器	<p>Workspace ONE 統一端點管理 (UEM) 主控台支援下列網頁瀏覽器最新的穩定組建。</p> <ul style="list-style-type: none"> <li>■ Chrome</li> <li>■ Firefox</li> <li>■ Safari</li> <li>■ Internet Explorer 11</li> <li>■ Microsoft Edge</li> </ul> <p><b>備註</b> 如果使用 IE 來存取 UEM 主控台，請導覽至 <b>控制面板 &gt; 設定 &gt; 網際網路選項 &gt; 安全性</b>，並確認您的安全性層級或自訂的安全性層級包含設定為 [啟用] 的 [字型下載] 選項。</p> <p>如果您使用比上述還舊的瀏覽器版本，請升級您的瀏覽器，以確保 UEM 主控台的效能。系統已執行完整的平台測試，以確定在使用這些 Web 瀏覽器時，所有的功能都能正常運作。如果您選擇在未經認證的瀏覽器中執行 UEM 主控台，可能會有某些問題。</p>
平台需求	<p>iOS 7.2 和更新版本</p> <p>Android 3.2 和更新版本</p> <p>Windows 7</p> <p>Windows 8</p> <p>Windows 10</p> <p>10.9 Mavericks 和更新版本</p>
架構需求	<p>.NET 4.0.3 和更新版本</p> <p>.NET 4.5 和更新版本</p> <p>Mono</p>
Visual Studio 需求	<p>Visual Studio 2010 v10.0.50903</p> <p>Visual C++ 2008</p>
其他	<p>已啟用連結共享</p> <p>Microsoft Outlook 2007 以上版本 (32 位元或 64 位元)</p>
角色需求	
管理員身分	<p><b>選取一個預設啟用 Content、Content Device Install 和 Content Device Remove 的角色。</b></p> <p>授與內容管理頁面及內容散發控制項的存取權。</p> <p>欲取得有關如何建立身分的資訊，請參閱《身分與新增資源指南》。</p>

元件	需求與說明
終端使用者角色	啟用管理內容，並授與完整的存取權 欲取得有關如何建立身分的資訊，請參閱《 <a href="#">身分與新增資源指南</a> 》。
存放庫需求	
UEM 管理內容	上傳內容前先配置類別結構。 您不能將子類別加入已含有內容的類別中。
企業檔案伺服器內容	安裝 Content Gateway 安裝內容閘道，即可在 Workspace ONE UEM 伺服器網域無法存取企業檔案伺服器的執行個體中建立連線。如需檢閱哪些 Workspace ONE UEM 支援的存放庫需要、支援或不支援 Content Gateway，請參閱 <a href="#">支援企業檔案伺服器</a> 。 如需完整的安裝說明，請參閱《 <a href="#">Content Gateway 安裝指南</a> 》。
檔案儲存空間替代方案的需求	
本機檔案儲存空間	判斷最適合企業的解決方案 如需可用選項的詳細資訊，請參閱 <a href="#">Workspace ONE UEM 受管理內容的本機檔案儲存空間</a> 。
選用安全性元件的需求	
入門培訓	滿足 APP 與 OS 的最低需求。 <ul style="list-style-type: none"> <li>■ iOS VMware Workspace ONE Content v2.4 以上版本</li> <li>■ iOS 7 以上版本的裝置</li> </ul>
APP 需求	
Workspace ONE Content	

## Content Gateway

Workspace ONE UEM powered by AirWatch 提供內容管理解決方案，可連同其他企業整合元件使用，解決在行動裝置上保護內容的獨特挑戰。Content Gateway 就是這類可協助終端使用者安全存取內容的元件。

將 Content Gateway 與 VMware Workspace ONE Content 應用程式搭配使用，可讓您的終端使用者從內部存放庫安全地存取內容。這表示您的使用者可直接從內容存放庫或內部檔案共享遠端存取文件、財務文件、紙本書籍等等。當檔案新增或更新至您現有的內容存放庫時，所有變更都會即時反應至 VMware Workspace ONE Content 應用程式，而系統僅會根據您於內部存放庫中定義的現有存取控制清單，來為使用者賦予獲准存取的檔案與資料夾的存取權限。將 Content Gateway 與 VMware Workspace ONE Content 應用程式搭配使用，可讓您為企業內容提供無與倫比的存取層級，而無需犧牲安全性。

## 檔案儲存空間

您可以在 Workspace ONE UEM Console 中設定各種內容類型，以便在終端使用者裝置上部署至 VMware Workspace ONE Content 應用程式。雖然內容類型並不影響部署位置，後端儲存空間也因內容類型而異。

若要深入瞭解每個內容類型可用的儲存空間選項，請檢閱表格。瞭解每個儲存空間選項的其他配置與元件需求。

	配置	元件	備註
Workspace ONE UEM 受管內容			
Workspace ONE UEM 資料庫	X	X	
本機檔案儲存空間	√	√	於全域層級組織群組修改 僅限內部部署
企業檔案伺服器			
Workspace ONE UEM 資料庫	X	X	同步的內容僅將中繼資料儲存在 Workspace ONE UEM 資料庫。
網路存放庫	√	√/X	有些存放庫需要內容閘道。需求 依存放庫類型而異。

# 企業檔案伺服器

# 2

內容管理解決方案支援與企業檔案伺服器 (CFS) 整合。企業檔案伺服器是指組織的內部網路中現有的存放庫。

## 功能

企業檔案伺服器整合支援下列功能：

- 安全整合
- 保護企業內部網路的存取權限
- 使用 Content Gateway 的進階整合選項

## 安全

內容管理解決方案提供下列安全性功能：

- SSL 加密，可用於資料傳輸
- 控制 Workspace ONE UEM 管理員的存取權和下載權限
- 在企業網路內儲存的内容
- 只有儲存在 Workspace ONE UEM 資料庫中的中繼資料。支援所儲存之中繼資料的檢閱和管理。

## 部署

根據組織結構的不同，Workspace ONE UEM 管理員可能已擁有 CFS 的管理權限，也可能沒有。內容管理解決方案與 CFS 整合之後，終端使用者裝置即可使用 VMware Workspace ONE Content 從伺服器同步内容。

## 支援企業檔案伺服器

Workspace ONE UEM 支援與各種企業檔案伺服器進行整合。所支援的同步方法以及 Content Gateway 元件的各種需求均因存放庫的類型而異。



## 可用的同步方法

請檢閱各存放庫可用的同步方法：

- **管理員** – 已由管理員在 UEM 主控台中完全配置且同步的存放庫。每個指派的使用者會接收到檔案存放庫的相同靜態連結。
- **自動** – 已由管理員在 UEM Console 中設定的存放庫，但允許管理員使用動態查閱值。該存放庫由終端使用者在其裝置上進行同步。每個指派的使用者會收到檔案存放庫的唯一或半唯一連結。這是連結到使用者主目錄的實用選擇。
- **手動** – 已在 UEM Console 中設定的存放庫，但允許管理員設定連結的靜態和萬用字元部分。每位終端使用者可以手動新增符合管理員所設定格式的存放庫連結，並將其裝置上的存放庫同步。

**備註** 無論存放庫資料夾中有多少檔案，只有在任何資料夾中按字母排序的一千個檔案會同步至裝置。

## 企業檔案伺服器矩陣

使用此矩陣以判斷各存放庫類型所支援的同步方法與 Content Gateway 需求：

	管理員	自動	手動
可用的存放庫			
Box	✓	✓	✓
CMIS	✓	✓	✓
Google 雲端硬碟	✓	-	-
網路共享	✓	✓	✓
OneDrive	✓	-	-
商務用 OneDrive	✓	-	-
ADFS 商務用 OneDrive	✓	-	-
業務用 OneDrive OAuth	✓	-	-
SharePoint	✓	✓	✓
SharePoint ADFS	✓	✓	✓
SharePoint O365	✓	✓	✓
SharePoint O365 ADFS	✓	✓	✓
SharePoint O365 OAuth	✓	-	-
SharePoint - 個人 (我的網站)	✓	-	-
SharePoint WebDAV	✓	-	-
SharePoint Windows 驗證	✓	✓	✓

	管理員	自動	手動
WebDAV	✓	✓	✓
透過 Content Gateway 存取			
Box	-	-	-
CMIS	✓+	✓+	✓+
Google 雲端硬碟	-	-	-
網路共享	✓+	✓+	✓+
OneDrive	-	-	-
商務用 OneDrive	✓	-	-
ADFS 商務用 OneDrive	✓	-	-
SharePoint	✓	✓	✓
SharePoint ADFS	✓	✓	✓
SharePoint O365	✓	✓	✓
SharePoint O365 ADFS	✓	✓	✓
SharePoint - 個人 (我的網站)	✓	-	-
SharePoint WebDAV	✓	-	-
SharePoint Windows 驗證 (Linux 專用 Content Gateway)	-	-	-
SharePoint Windows 驗證 (Windows 專用 Content Gateway)	✓	✓	✓
WebDAV	✓	✓	✓
文件副檔名			
Box	✓	✓	✓
CMIS	✓	✓	✓
Google 雲端硬碟	✓	-	-
網路共享	✓*	✓*	✓*
OneDrive	✓	-	-
商務用 OneDrive	✓	-	-
ADFS 商務用 OneDrive	✓	-	-
業務用 OneDrive OAuth	✓	-	-

	管理員	自動	手動
SharePoint	✓**	✓**	✓**
SharePoint ADFS	✓**	✓**	✓**
SharePoint O365	✓**	✓**	✓**
SharePoint O365 ADFS	✓**	✓**	✓**
SharePoint O365 OAuth	✓	-	-
SharePoint - 個人 (我的網站)	✓**	-	-
SharePoint WebDAV	✓**	-	-
SharePoint Windows 驗證	✓**	✓**	✓**
WebDAV	✓*	✓*	✓*

**圖例：**

¥ = Linux 伺服器上的 VMware Content Gateway 僅支援 SMB v2.0 和 SMB v3.0。預設支援的版本為 SMB v2.0。

✓+ = 必要

✓ = 支援

- = 不支援

✓\* = 有限支援。僅限於存取先前已於 VMware Workspace ONE Content 中開啟過的存放庫中的檔案。

✓\*\* = 有限支援。僅限於存取先前已於 Workspace ONE Content 中下載過的檔案。

## 允許終端使用者存取企業檔案伺服器的內容

藉由配置管理員存放庫、自動使用者新增存放庫，或者手動使用者新增存放庫，將您網路的現有企業檔案伺服器與 Workspace ONE UEM 同步。可用配置會影響將內容同步至裝置的觸發程序。

使用此巨集層級的配置概覽，以深入瞭解允許終端使用者存取企業檔案伺服器內容的整個過程。

- 1 在 UEM 主控台中配置存放庫。
- 2 下載並執行已配置的 Content Gateway 安裝程式。
- 3 驗證 UEM 主控台與 Content Gateway 之間的連線能力。
- 4 為您的組織評估是否需要使用多個內容閘道節點。  
全域企業如需考量地域分隔所造成的延遲，可使用此功能。
- 5 在 UEM 主控台中配置管理員存放庫或同步企業檔案伺服器 (CFS)。  
若要配置管理員存放庫，請選取**測試連線**以確保連線能力。
- 6 在 UEM 主控台中設定 VMware Workspace ONE Content。
- 7 將 Workspace ONE UEM 應用程式部署至您的裝置團隊。

## 配置管理員存放庫

配置管理員存放庫以將您網路上現有的企業檔案伺服器與 Workspace ONE UEM 同步。同步之後，終端使用者可以從其裝置存取「企業檔案伺服器」內容。

- 1 導覽至 UEM 主控台中的 **內容 > 存放庫 > 管理員存放庫**。
- 2 選取**新增**。
- 3 為出現的設定進行設定。

設定	描述
名稱	標記內容目錄
類型	從下拉式功能表中選取企業檔案伺服器。
連結	不是只提供根網域，而是提供整個目錄位置的路徑。 <b>範例：</b> <a href="http://SharePoint/Corporate/Documents">http://SharePoint/Corporate/Documents</a> 直接使用從 Web 瀏覽器中複製下來的 URL，可能不具特定存放庫類型的伺服器存取權限。
企業群組	將企業檔案伺服器的存取權限指派給選取的使用者群組。
使用 PIV-D 衍生認證	僅在將 SharePoint 選取為存放庫類型時，才能使用此設定。 選取核取方塊以使用 PIV-D 憑證驗證來驗證使用者，而不使用使用者名稱和密碼進行驗證。 PIV-D 憑證驗證，適用於驗證要從其裝置存取內部部署 SharePoint 存放庫的使用者。  <b>備註</b> 需要在 Content Gateway 設定中使用 Kerberos 組態，才能啟用 PIV-D 衍生認證的使用。  如需 Content Gateway 憑證驗證設定的相關資訊，請參閱 Content Gateway 說明文件中的〈在 UEM Console 上設定 Content Gateway〉主題。
透過 Content Gateway 存取	如果 Workspace ONE UEM 伺服器的網域無法存取「企業檔案伺服器」，請使用「內容閘道」來存取。
Content Gateway	從下拉式功能表中識別出合適 Content Gateway 節點的獨特名稱。
允許繼承	允許子組織群組繼承與其父組織群組相同的存取權限。
允許寫入	允許終端使用者建立並上傳檔案和資料夾、編輯文件，以及將檔案簽入或簽出至其裝置上的外部存放庫。
允許檔案動作	需要將 SharePoint O365 OAuth 或 OneDrive for Business OAuth 選取為存放庫類型，才能使用此設定。 選取此核取方塊，可允許 Workspace ONE Content 應用程式使用者重新命名、移動和刪除雲端存放庫上的檔案。

設定	描述
允許刪除	允許網路共享存放庫進行遠端內容刪除。使用此功能時，終端使用者可使用 <b>Workspace ONE Content</b> 應用程式，將其內容從網路共用存放庫永久刪除。
驗證類型	<p>在 <b>UEM</b> 主控台中，選取管理員對於企業檔案伺服器所擁有的存取層級。</p> <ul style="list-style-type: none"> <li>■ <b>無</b> – 禁止管理員在 <b>UEM</b> 主控台檢視及下載企業檔案伺服器的內容。</li> <li>■ <b>使用者</b> – 允許在 <b>UEM</b> 主控台中瀏覽存放庫檔案結構。在所出現的<b>使用者名稱</b>與<b>密碼</b>文字方塊中輸入憑證。</li> </ul> <p><b>備註</b> 如果已選取使用 <b>PIV-D</b> 衍生認證核取方塊，則不會顯示密碼文字方塊。在使用者名稱文字方塊中，為使用者提供使用者主體名稱。</p>

- 4 選擇**測試連線**以確認連線狀況。測試結果成功表示企業檔案伺服器已成功整合。
- 5 填妥 [安全性]、[指派] 和 [部署] 索引標籤下的詳細資料。
  - a 在 [安全性] 索引標籤上填妥文字方塊，以控制終端使用者共用機密文件並將其移出公司媒體的方式。

自 **Workspace ONE UEM Console 9.5** 版起已移除強制加密設定。**VMware Workspace ONE Content** 應用程式預設為加密所有檔案，不論是否可使用該設定均同。

設定	描述
文件共享	停用共用設定可確保最大的安全性。您可以為了配置終端使用者協作而啟用共用設定。
存取控制	設為 <b>允許離線檢視</b> 時，可以讓終端使用者擁有最高度自由來檢視文件。配置 <b>僅允許線上檢視</b> ，以確保所有存取內容的裝置都合規，因為 <b>Workspace ONE UEM</b> 無法離線掃描裝置的合規性。
允許在 <b>Email</b> 中開啟	<p>允許在 <b>Email</b> 中開啟內容。</p> <p>使用者無法開啟大於 <b>10 MB</b> 的檔案。若要允許使用者開啟大於 <b>10 MB</b> 的檔案，您必須在 <b>UEM Console</b> 上編輯此類檔案，並啟用此選項。無法編輯使用者存放庫中的檔案。</p>
允許在第三方 <b>APP</b> 中開啟	給予可在其他應用程式中開啟此內容的權限。您可以在 <b>SDK</b> 設定檔中設定一份已被核准的 <b>APP</b> 清單。停用此選項，也會停用終端使用者從 <b>iOS VMware Workspace ONE Content</b> 中列印 <b>PDF</b> 文件的權限。
允許儲存到其他的存放庫	選擇此項，允許終端使用者將檔案儲存到「個人內容」中。
啟用浮水印	<p>選擇此項，將「浮水印重疊」加印在檔案上。</p> <p>設置浮水印之「重疊文字」作為 <b>SDK</b> 設定檔的一部分。</p>

設定	描述
允許列印	授權終端使用者利用 AirPrint 伺服器，從 iOS VMware Workspace ONE Content 中列印 PDF 文件。列印完畢後，內容即不再受 Workspace ONE UEM 管理員的控制。只有在啟用「允許在第三方 APP 中開啟」時，才支援列印。
允許編輯	此設定僅可用於「已啟用寫入」的存放庫中。

- b 在 [指派] 索引標籤上，配置設定以控制哪些使用者可以存取內容。此功能可確保只有獲授權的員工才能存取機密或敏感的資料，並可讓您設定內容存取的分層階層。

設定	描述
裝置所有權	定義為：任何、公司專用、公司共用、員工自有或是未分類。
企業群組	若要將內容指派至新的群組，請在文字方塊中開始輸入。
使用者群組	若與「目錄服務」或「自訂使用者群組」整合，請在此指明所要委派的群組。

- c 在 **部署** 索引標籤上，配置設定以掌控終端使用者存取內容的方式和時間。

設定	描述
傳輸方式	從下拉式功能表指定 <b>任何</b> 方式或 <b>僅限 Wi-Fi</b> 方式。對 Wi-Fi 傳輸設立限制，強制裝置必須使用 Workspace ONE UEM 簽入，以確保裝置的合規性。
漫遊時下載	啟用此項，允許您的終端使用者在漫遊時下載內容。
下載類型	使用下列其中一種方法來部署內容： <ul style="list-style-type: none"> <li>■ <b>自動</b> - 在內容變為可用時安裝在裝置上。</li> <li>■ <b>隨選</b> - 只有在終端使用者要求時，才會安裝在裝置上。</li> </ul>
下載優先順序	將此下載內容定義為 <b>中</b> 、 <b>高</b> 或 <b>低</b> ，以使終端使用者明瞭其優先順序。
必要	在 VMware Workspace ONE Content 中選取此項，將內容標記為「必要」。終端使用者必須下載並檢閱必要內容，才能確保其裝置持續符合 Workspace ONE UEM 的合規性。
生效日	指明此項來配置內容的有效期間。
到期日	指明此項來配置內容的有效期間。

- 6 選取**儲存**。

## 存取正確的連結

確保以正確連結設定 Content Gateway。這些特殊規則適用於 SharePoint 2013、Office 365 及更新版本。有些 URL 無法使用應用程式與服務來存取，而只能使用 Web 瀏覽器。配置內容閘道時，如果在連結中輸入了「僅限使用瀏覽器」的 URL，連線就會失敗。

- 1 在瀏覽器中輸入 URL。

- 2 導覽至 **頁面 > 編輯屬性 > 檢視屬性**。
- 3 按一下右鍵並複製連結位址。
- 4 在 UEM 主控台的 **連結** 文字方塊中貼上該位址。

## 允許使用者將企業檔案伺服器功能

配置終端使用者可從其裝置進行同步的自動或手動範本，來將 Workspace ONE UEM 與現有的內容存放庫整合。同步之後，終端使用者可以從其裝置存取「企業檔案伺服器」內容。將 Content Gateway 與企業檔案伺服器搭配使用，可讓終端使用者安全地新增、編輯和上傳內容至企業檔案伺服器。

這些步驟在配置自動與手動範本時會有不同。

- 1 導覽至 UEM Console 中的合適頁面。

企業檔案伺服器類型	位置
自動範本	內容 > 存放庫 > 範本 > 自動
手動範本	內容 > 存放庫 > 範本 > 手動

- 2 選取 **新增**。
- 3 填妥出現的文字方塊。這些文字方塊在配置「管理員存放庫」、「自動範本」與「手動範本」時會有不同。

設定	描述
名稱	標記內容目錄。
使用者存放庫名稱 (僅限自動範本)	使用查閱值，以 VMware Workspace ONE Content 中終端使用者的名稱來命名存放庫。
類型	從下拉式功能表中選取企業檔案伺服器。
連結	直接使用從 Web 瀏覽器中複製下來的 URL，可能不具特定存放庫類型的伺服器存取權限。
連結 (僅限自動範本)	使用查閱值，在終端使用者存取 VMware Workspace ONE Content 時建立存放庫。 <b>範例:</b> https://sharepoint.acme.com/share/{EnrollmentUser}
連結 (僅限手動範本)	使用 * 作為網域連結的萬用字元，以提供目錄位置的路徑。 <b>範例:</b> http://*.sharepoint.com 您可以將新連結新增至現有手動範本，但無法編輯或刪除現有連結。在封鎖清單中新增新連結時請務必小心，因為如果有任何錯誤，則無法編輯或刪除這些連結。要針對連結進行任何修正都需要刪除整個範本。
已遭拒的連結	在檔案路徑中指定萬用字元 (*) 的值。 在檔案路徑的開頭與結尾指定的 * 值能夠阻止您的使用者使用手動範本建立手動存放庫與子資料夾。
企業群組	將企業檔案伺服器的存取權限指派給特定群組的使用者。

設定	描述
使用衍生認證	<p>僅在將 SharePoint 選取為存放庫類型時，才能使用此設定。選取核取方塊以使用 PIV-D 憑證驗證來驗證使用者，而不使用使用者名稱和密碼進行驗證。</p> <p>PIV-D 憑證驗證，適用於驗證要從其裝置存取內部部署 SharePoint 存放庫的使用者。</p> <p><b>備註</b> 需要在 Content Gateway 設定中使用 Kerberos 組態，才能啟用 PIV-D 衍生認證的使用。</p> <p>如需 Content Gateway 憑證驗證設定的相關資訊，請參閱 Content Gateway 說明文件中的〈在 UEM Console 上設定 Content Gateway〉主題。</p>
透過 Content Gateway 存取	如果 Workspace ONE UEM 伺服器的網域無法存取「企業檔案伺服器」，請使用「內容閘道」來存取。
允許繼承	允許子組織群組繼承與其父組織群組相同的存取權限。
允許寫入	允許終端使用者建立並上傳檔案和資料夾、編輯文件，以及將檔案簽入/簽出至其裝置上的外部存放庫。

## PIV-D 憑證驗證支援

在使用者使用 PIV-D 衍生認證進行驗證後，內部部署 SharePoint 存放庫的存取權，即會授與 Workspace ONE Content 的應用程式使用者。以憑證為基礎的驗證可消除對使用者名稱和密碼的需求。

諸如 SharePoint 的內部部署存放庫，可配置為使用 PIV D 衍生認證進行驗證。將 SharePoint 存放庫配置為使用 PIV-D 衍生認證時，需要在 VMware Content Gateway 設定中具備 Kerberos 組態。

若要設定 PIV-D 憑證驗證，則必須考慮下列必要條件：

- 必須使用適當的 SPN (服務主體名稱) 來設定 Kerberos Constrained Delegation (KCD) 伺服器。
- Active Directory 必須以使用者主體名稱 (UPN) 做為屬性來與 Workspace ONE UEM 同步。
- 服務帳戶必須可同時用於 Workspace ONE UEM 和 VMware Content Gateway，以作為 Kerberos 驗證工作流程的一部分。
- 必須由發出使用者憑證的憑證授權機構 (CA)，為 Content Gateway 提供可信賴的憑證。根據 CA 的驗證需求，這些憑證可能只是中繼憑證或整個憑證鏈結。

## 快取效能

當整個企業存放庫已快取，裝置服務伺服器可能會由於內部記憶體不足而出現記憶體峰值情況。每次都必須停用快取，以解決裝置服務伺服器上的負載。

**備註** 從 Workspace ONE UEM 1904 版開始，無法再使用資料庫指令碼來停用快取。可以在 API `https://<host>/api/system/featureflag/<FeatureFlagName>/<OG_GUID>/false` 將 `ContentCacheFeatureFlag` 切換為 `false` 以停用快取。

Just-in-Time 快取策略能夠僅快取使用者存取的資料夾和內容記錄，以解決記憶體不足的問題。不需要的資料夾和內容會從快取中移除。



使用 **folderId** 快取索引鍵快取個別資料夾，而非使用 **RepoId** 快取索引鍵快取整個存放庫。

當快取遺失時，裝置服務伺服器僅會從資料庫載入目前資料夾的中繼資料，然後將其儲存在快取。當快取命中時，裝置服務伺服器僅會從快取中讀取根層級的資料夾結構。

# Workspace ONE UEM 受管理內容 存放庫

# 3

UEM 受管理內容存放庫是一種用來儲存檔案的位置，管理員如具有合適的權限，便能完全控管儲存於此處的檔案。使用 VMware Workspace ONE Content 應用程式，終端使用者可以從標有「UEM 管理」的存放庫存取新增的內容，但無法編輯內容。

## 功能

所管理內容存放庫提供下列功能：

- 手動上傳檔案
- 配置個別檔案並提供其權限的選項
- 同步選項可控制在終端使用者裝置上存取的內容
- 進階檔案管理選項的清單檢視

## 安全

若要保護從存放庫儲存並同步到終端使用者裝置的內容，可使用下列安全性功能：

- SSL 加密可保護 UEM console 和終端使用者裝置之間的傳輸資料。
- 具有安全釘選的角色可用於受到控制的內容存取權限。

## 部署

UEM 所管理存放庫內容儲存在 Workspace ONE UEM 資料庫中。您可以選擇將資料庫存放於 Workspace ONE UEM 雲端或內部部署中，視您的部署模型而定。

## 為 UEM 所管理內容設定類別結構

內容類別有助於 UEM 所管理存放庫內容在 UEM console 與 Workspace ONE Content 應用程式中維持條理。先針對 UEM 所管理內容設定類別結構，然後再將內容上傳至 UEM console。

- 1 導覽至 [內容 > 類別 > 新增類別](#)。

## 2 配置出限的設定並儲存。

設定	描述
管理者	選擇某個企業群組，或者您要套用此類別的群組。
名稱	輸入一個易於辨識的名稱，再將它套用到一組明確的內容。
描述	提供簡短的類別描述。

## 3 依需要將子類別新增至您的類別結構中。

- a 從 [動作] 功能表中選取**新增**。
- b 配置出限的設定並**儲存**。

設定	描述
管理者	檢閱組織群組依預設而填入的父類別。
名稱	輸入一個易於辨識的名稱，再將它套用到一組明確的內容。
描述	提供簡短的子類別描述。

## 將內容上傳至 UEM 所管理存放庫

您可從 UEM console 手動上傳並設定檔案，以將檔案新增至 UEM 所管理內容存放庫。根據預設，存放庫會將其內容儲存於 Workspace ONE UEM 資料庫，並與 VMware Workspace ONE Content 應用程式同步，將內容傳遞到終端使用者的裝置。但是，終端使用者無法編輯已同步的管理內容。

- 1 導覽至 **內容 > 清單檢視**。
- 2 選取**新增內容**並選擇**選取檔案**。
- 3 選取要從對話方塊上傳的個別檔案。
- 4 配置內容**資訊**設定。

設定	描述
名稱	檢閱自動填入此文字方塊中的檔案名稱。
企業群組	檢閱將要部署此內容的企業群組。
檔案	檢閱自動填入此文字方塊中的檔案。
儲存類型	確保此文字方塊顯示為「UEM 所管理」。
版本	這是您初次將此內容加入 UEM 主控台，所以請把此版本的編號設為 1.0。您可以在 [UEM 所管理的清單檢視] 中，使用 [動作] 功能表來上傳新版本。
描述	提供有關上傳檔案的描述。
重要性	將內容的重要性設為： <b>高</b> 、 <b>中</b> 或 <b>低</b> 。
類別	將已上傳的內容對應到已配置的類別。

- 5 在**詳細資料**的設定中，提供其他有關內容的中繼資料。

設定	描述
作者	檔案作者的名稱。
備註	提供檔案備註。
主題	提供主題。
關鍵字	列出此檔案所涵蓋的關鍵字和主題。

**備註** 無論 UEM Console 上新增的檔案數量有多少，只有前一萬個按字母排序之檔案的中繼資料會同步至使用者的裝置。

## 批次上傳 Workspace ONE UEM 受管理內容

在專用 SaaS 或帶有強化網路的內部部署中，使用批次匯入功能來繞過外部檔案共享的整合程序。

- 1 瀏覽至**內容 > 批次狀態**。
- 2 選取**批次匯入**。
- 3 輸入批次名稱和批次描述。
- 4 若要下載 .csv 範本檔案，請選取資訊圖示 (i)。
- 5 填入 CSV 檔的檔案路徑，以及其他要上傳的內容資訊。
- 6 點選 **Choose File** (選擇檔案) 來選擇您所要建立的 .csv 檔。
- 7 點選**開啟**來選擇此 .csv 檔。
- 8 點選**儲存**來上傳您所填入的批次檔。

## 設定內容儲存空間容量

儲存區容量是指在企業群組及其子群組中，為受管理內容配置的空間量。

**備註** 您必須確認您擁有檢視和使用儲存空間設定所需的管理員權限。

- 1 導覽至客戶或全域組織群組層級的**群組與設定 > 所有設定 > 管理員儲存空間**。
- 2 從**儲存類型**下拉功能表中，選取**內容**。
- 3 針對適當的企業群組，選取**編輯**圖示。即會顯示 [儲存區管理] 視窗。完成設定。

設定	描述
企業群組名稱	指定您要套用內容儲存限制的群組。
容量	以 MB 為單位，為儲存於 Workspace ONE UEM 資料庫中的內容設定要分配的儲存空間上限。VMware Workspace ONE UEM 為 SaaS 客戶提供的 Workspace ONE Content 預設儲存空間為 5 GB。
允許超出的用量	輸入可超額使用的用量 (如果允許的話)。SaaS 客戶無法配置此值。

設定	描述
檔案大小上限	使用預設值 200 MB 作為上傳的上限。如果操作時不想遵照此建議，請記得上限為 2 GB。
加密	使用 AES - 256 檔案層級加密，對內容進行加密。啟用加密將會觸發檔案加密移轉排程器，使其開始移轉任何所發現的未加密資料。

#### 4 選取儲存。

## 限制檔案副檔名

為企業檔案伺服器以及受管理內容建立允許清單與封鎖清單，以指定檔案類型權限。此限制會按照副檔名在 UEM console 中或在 Workspace ONE Content 應用程式中隱藏封鎖的檔案類型，因此不會下載或上傳到內容存放庫。

- 1 導覽至內容 > 設定 > 進階 > 副檔名。
- 2 設定允許的副檔名。

設定	描述
允許清單	輸入您想要包含的副檔名。使用換行、逗號或空格來分隔副檔名。
拒絕清單	輸入您想要排除的副檔名。使用換行、逗號或空格來分隔副檔名。
全部	選取此項可允許上傳或同步任何類型的檔案。

#### 3 點選儲存以套用此配置。

一旦套用了限制，便能預期下列回應。

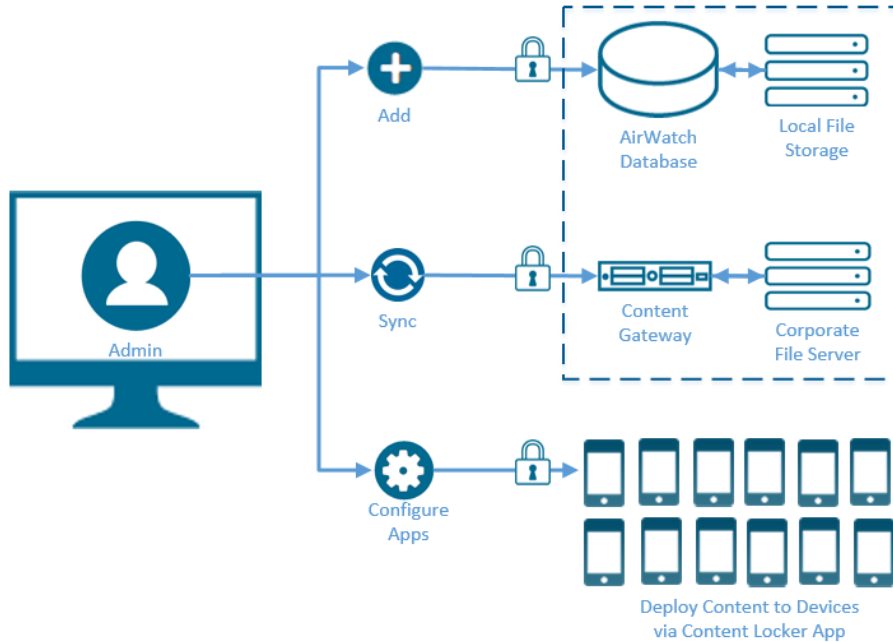
回應	人物	事物	位置	存放庫
錯誤訊息	管理員	將限制的檔案手動新增至內容存放庫	Console	已納管的 UEM
無訊息互動	管理員	與包含著限制檔案的企業檔案伺服器進行同步	Console	企業檔案伺服器
無訊息互動	終端使用者	與包含著限制檔案的企業檔案伺服器進行同步	裝置 (透過 Workspace ONE Content 應用程式)	企業檔案伺服器

## Workspace ONE UEM 受管理內容的本機檔案儲存空間

本機檔案儲存空間會將管理內容從 Workspace ONE UEM 資料庫獨立出來，並將其儲存在與 Workspace ONE UEM 執行個體連線的專用內部部署位置。

依預設，管理內容儲存在 Workspace ONE UEM 資料庫中。然而，上傳大量管理內容會造成資料庫的效能問題。此時，內部部署客戶可將管理內容移至已整合的本機檔案儲存空間解決方案中，從而釋出資料庫中的空間。

**備註** 內部部署客戶可以手動設定檔案儲存空間，而 SaaS 客戶的檔案儲存空間則會自動設定。



如需設定檔案儲存空間的相關資訊，請參閱系統設定說明文件中的安裝/檔案路徑。

## 自訂報告

使用 Workspace ONE UEM Console 上的 Workspace ONE Intelligence，您可以產生自訂報告，以收集和檢視安裝在終端使用者裝置上之受管理內容的詳細資料。此自訂報告不同於**依裝置顯示內容詳細資料**報告或是從**內容 > 清單檢視**主控台頁面匯出的報告。

若要產生內容的自訂報告，請存取 Workspace ONE Intelligence 介面，然後選取**裝置內容**範本類別。使用可用於識別裝置的元素(例如裝置 ID) 做為篩選器參數。

您可以產生受管理內容或使用者特定的報告。

您可以檢視的內容詳細資料如下：

- 依存放庫，在特定日期範圍的一個月內，內容下載的總數和唯一數目。
- 內容的檢視次數。

您可以檢視的特定使用者詳細資料如下：

- 依存放庫，使用者在特定日期範圍內的內容下載總數。
- 使用者尚未檢視的內容清單。
- 內容的上次下載日期。
- 缺少文件特定 (通常為最近) 版本的使用者清單。

如需有關使用 Workspace ONE Intelligence 產生報告的詳細資訊，請參閱 Workspace ONE Intelligence 說明文件中的 Workspace ONE Intelligence 報告。

# APP 套件 SDK 配置

# 4

配置應用程式時，您可以選擇自訂或預設的應用程式設定檔。此動作會將一個 SDK 設定檔套用到應用程式，使現已部署的 Workspace ONE UEM 應用程式擁有其他功能。

為確保應用程式的配置可以順利執行，建議您應：

- 瞭解自訂和預設 SDK 設定檔之間的差異。
- 判斷您的應用程式較適合自訂還是預設的 SDK 設定檔。
- 確定您已配置即將要套用的 SDK 設定檔類型。

利用以下表來決定要將**預設**或是**自訂**的 SDK 設定檔套用到您的應用程式，並將您導入您所使用之設定檔的配置說明。

定義 SDK 設定檔時可使用下列兩種不同的設定檔類型：**預設**或是**自訂**的 SDK 應用程式設定檔。

	預設值	自訂
實行	在特定的企業群組 (OG) 或其下群組所設置的所有應用程式中，共用 SDK 設定檔的設定。	將 SDK 設定檔套用到特定的應用程式中，並覆寫預設的 SDK 設定檔。
優點	為特定群組或其子群組中所有的 APP，提供單點配置的功能。	為特定的應用程式提供縝密的控管，以及覆寫預設 SDK 設定檔的功能。
配置	<b>群組 &amp; 設定 &gt; 所有設定 &gt; APP &gt; 設定和原則 &gt; 安全性原則</b>	<b>群組 &amp; 設定 &gt; 所有設定 &gt; APP &gt; 設定和原則 &gt; 設定檔</b>
閱讀更多資訊	繼續讀取此章節，以便瞭解哪個預設的 SDK 設定檔可以套用到已部署 APP。	在《 <b>VMware Workspace ONE UEM 行動應用程式管理指南</b> 》中進一步瞭解自訂 SDK 設定檔設定。

## 配置預設 SDK 安全性設定

預設的 SDK 設定廣泛地套用在所有 Workspace ONE UEM 和包裝應用程式上，所以能夠在裝置上提供統一的使用者體驗。由於配置的 SDK 設定會依預設套用到所有 Workspace ONE UEM 和包裝應用程式，因此您能以整個 Workspace ONE UEM 和包裝應用程式套件為考量來配置預設 SDK 設定檔。

提供的建議可以應用在以下這些 APP 套件：

- VMware Workspace ONE Web
- 已註冊的裝置
- VMware Workspace ONE Content
- Workspace ONE UEM 或已包裝 APP
- SDK 設定

並非所有平台或 Workspace ONE UEM 應用程式均支援所有可用的預設 SDK 設定檔設定。若是平台和 App 皆支援，則配置的設定值僅適用於裝置。此外，還意味著已啟用的設定在多平台的部署或應用程式之間的運作可能會有不一致的情況發生。「SDK 設定」矩陣涵蓋了適用 SDK 設定檔的設定，以及這些設定檔所套用的 APP 和平台。

- 1 導覽至**群組 & 設定 > 所有設定 > 應用程式 > 設定和原則 > 安全性原則**。
- 2 配置**安全性原則**，然後選取**儲存**。

動作	描述	
驗證類型		
密碼	在初次啟動 APP 以及 APP 工作階段逾時後，提示終端使用者透過使用者所建立的密碼來驗證。啟用或停用 SSO，決定了所建立之 APP 工作階段的數目。 如果執行抹除，即使用者已達到嘗試輸入密碼的允許次數上限，則應用程式就不會切換到 Hub，而會啟動獨立式登入流程。	-
使用者名稱和密碼	在初次啟動 APP 以及 APP 工作階段逾時，提示終端使用者透過使用者所建立的密碼來驗證。啟用或停用 SSO，決定了所建立之 APP 工作階段的數目。	-
已停用	允許終端使用者不需輸入認證，即可開啟 APP。	✓
SSO		
啟用	建立適用於所有 Workspace ONE UEM 和 Workspace ONE UEM 包裝 APP 的單一 APP 工作階段。	✓
已停用	按照個別的 APP 來建立 APP 工作階段。	-
離線存取		
啟用	允許終端使用者在不與 Wi-Fi 連線的狀態下，也能開啟並使用 Workspace ONE UEM 和包裝 APP。離線的 Workspace ONE UEM APP 無法執行下載工作，因此終端使用者必須重新上線才能成功下載。配置允許離線的最長時間以設定離線存取的限制。	✓
已停用	在離線的裝置上，移除 Workspace ONE UEM 和包裝 APP 的存取權。	-
破解防護		
啟用	覆寫 MDM 防護 APP 層級的破解防護會封鎖破解裝置，禁止其註冊；並且封鎖曾回報為破解狀態、遭到企業抹除的註冊裝置。	✓



動作	描述
已停用	已破解的裝置防護將僅能仰賴 MDM 合規引擎。 -
資料遺失防護	
啟用	<p>旨在減少資料遺失的存取和配置設定。 ✓</p> <hr/> <p>啟用複製和貼到 設定為<b>是</b>時，允許複製外部應用程式的內容並貼到 Workspace ONE UEM 應用程式中。</p> <hr/> <p>啟用複製和貼上 設定為<b>是</b>時，允許複製 Workspace ONE UEM 應用程式的內容並貼到外部應用程式中。</p> <p>使用 Workspace ONE Swift SDK 時，會在產生連結和複製不受剪貼簿限制影響的記錄時強制執行限制。</p> <p>複製和貼上動作與其他 DLP 限制無關，且不遵循應用程式允許清單。</p> <p>舉例而言，如果允許，複製和貼上動作可在任何外部應用程式上進行，且不限於允許清單應用程式。</p> <hr/> <p>啟用列印 設為「<b>是</b>」時，便可允許應用程式在裝置上列印。</p> <hr/> <p>啟用相機 設為<b>是</b>時可允許應用程式存取裝置上的相機。</p> <hr/> <p>啟用撰寫 Email 設為「<b>是</b>」時，便可允許應用程式使用本機的 Email 用戶端來傳送 Email。</p> <hr/> <p>啟用資料備份 設為「<b>是</b>」時，便可允許包裝的應用程式與存放服務 (比如 iCloud) 同步資料。</p> <hr/> <p>啟用位置服務 設為「<b>是</b>」時，便可允許包裝的應用程式接收有關裝置之經緯度的資訊。</p> <hr/> <p>啟用藍牙 設為「<b>是</b>」時，便可允許應用程式存取裝置上的藍牙功能。</p> <hr/> <p>啟用螢幕擷取畫面 設為「<b>是</b>」時，便可允許應用程式存取裝置上「螢幕擷取畫面」的功能。</p>

動作	描述
	<p>啟用浮水印</p> <p>選項設為是時，便可在 VMware Workspace ONE Content 的文件中以浮水印顯示文字。在「重疊文字」欄位中輸入文字，或使用查閱值。您無法在 UEM 主控台中變更浮水印的設計。</p> <hr/> <p>限制文件只能在被允許的 APP 中開啟輸入選項以控制用來開啟裝置資源的應用程式。(僅限 iOS) 您可以使用 Workspace ONE UEM 組態值來限制使用者將來自第三方應用程式的檔案匯入 Workspace ONE Content。如需詳細資訊，請參閱〈在 Workspace ONE Content 中設定匯入限制〉一節。</p> <hr/> <p>允許的應用程式清單</p> <p>輸入您允許用來開啟文件的應用程式。</p>
已停用	允許終端使用者存取所有的裝置功能。 -

3 導覽至群組與設定 > 所有設定 > 應用程式 > 設定和原則 > 設定。

4 配置設定，然後選取儲存。

動作	描述
品牌	
已啟用	在能夠使用適用的設定時，將特定的企業標誌和色彩套用到 APP 套件。 -
已停用	維持整個 APP 套件中的 Workspace ONE UEM 品牌形象。 ✓
正在記錄中	
已啟用	存取和配置有關收集記錄的設定。
	<p><b>記錄層級</b> ✓</p> <p>從記錄頻率範圍的選項中選擇：</p> <ul style="list-style-type: none"> <li>■ <b>錯誤</b> - 僅記錄「錯誤」事件。「錯誤」表示處理過程出錯了，例如：無法查詢 UID 或 URL 不受支援。</li> <li>■ <b>警告</b> - 記錄「錯誤」和「警告」。「警告」表示處理過程中有可能發生的問題，例如：回覆碼錯誤和 Token 驗證無效。</li> <li>■ <b>資訊</b> - 記錄大量數據以供參考。資訊記錄層級顯示一般的流程、警告和錯誤訊息。</li> <li>■ <b>偵錯</b> - 記錄所有數據以幫助疑難排解。此選項並不適用於所有的功能。</li> </ul>

動作	描述	
	僅透過 Wi-Fi 傳送記錄	
	選取此項，可禁止在漫遊時傳送資料，並限制資料的使用費用。	
已停用	不收集任何記錄。	-
分析		
已啟用	收集並檢視 SDK 套件中有用的 APP 統計資料。	✓
已停用	不收集有用的統計資料。	-
自訂設定		
已啟用	將自訂的 XML 代碼套用在 APP 套件。	-
已停用	不將自訂的 XML 代碼套用在 APP 套件。	✓

您可以透過在預設或自訂的 SDK 設定檔中新增特定的組態金鑰，來啟用或停用 Workspace ONE Content 和 Workspace ONE Smartfolio 應用程式的特定功能。如需使用組態金鑰配置 SDK 設定檔的詳細資訊，請參閱 [第 5 章 VMware Workspace ONE Content](#) 和 [第 6 章 Workspace ONE Smartfolio](#)

## SDK 驗證的預期性行為

透過啟用或停用 SSO 來決定所建立之 APP 工作階段的數目，這會直接影響到終端使用者所接收之驗證提示的數目。

驗證	SSO	工作階段	認證	可預期的行為
已停用	已啟用	單一	註冊認證	開啟應用程式而不提示終端使用者輸入認證。
密碼	已啟用	單一	密碼	在第一個 APP 首次啟動時出現提示來建立單一 APP 工作階段。該工作階段逾期後，即會出現下一個驗證提示。
使用者名稱和密碼	已啟用	單一	註冊認證	在第一個 APP 首次啟動時出現提示來建立單一 APP 工作階段。該工作階段逾期後，即會出現下一個驗證提示。

驗證	SSO	工作階段	認證	可預期的行為
密碼	已停用	個別 APP	密碼	依個別的 APP 來提示，建立個別的 APP 工作階段。請注意，每個 APP 可能都會有專屬的密碼。當啟動一個新的 APP，或是某個別的 APP 工作階段逾期時，下一個驗證提示便會出現。
使用者名稱和密碼	已停用	個別 APP	註冊認證	依個別的 APP 來提示，建立個別的 APP 工作階段。當啟動一個新的 APP，或是某個別的 APP 工作階段逾期時，下一個驗證提示便會出現。

# VMware Workspace ONE Content

# 5

內容管理解決方案提供您 VMware Workspace ONE Content 應用程式，讓終端使用者能夠存取受管理內容。Workspace ONE Content 應用程式可部署至終端使用者裝置，而受管理內容可在應用程式中於設定參數內存取。

## 功能

- 內容設定即可設定專屬的 APP 行為。
- 在配置為 Workspace ONE UEM 應用程式套件時，中使用預設的 SDK 設定。
- 內容管理儀表板和清單檢視可從 UEM 主控台管理內容部署。

## 安全

- SSL 加密，可保護資料傳輸。
- AES 256 位元加密，可保護部署的內容。
- iOS 版 VMware Workspace ONE Content v2.2 和更新版本使用 NSFileProtectionComplete 類別來儲存內容。

## VMware Workspace ONE Content 各平台上的功能

下表適用於在應用程式商店中所提供的 VMware Workspace ONE Content 平台版本。

**備註** VMware Workspace ONE 已宣告從 2020 年 7 月 31 日開始終止適用於 Windows 的 Workspace ONE Content 的一般支援 (EOGS) 期間，並於 2021 年 7 月 31 日正式終止。如需 EOGS 的相關詳細資訊，請參閱知識庫文章：[終止適用於 Windows 的 AirWatch Content Locker 一般支援。](#)

功能	iOS	Android	Win 10
<b>安全性</b>			
<b>驗證</b>			
基本功能	✓	✓	✓
AD/LDAP	✓	✓	✓
Token	✓	✓	✓
第二要素密碼	✓	✓	✓
<b>加密</b>			
SSL 加密傳輸中的資料	✓	✓	✓
AES 256 位元加密靜態資料	✓	✓	✓
在記憶體中加密	✓	✓	
FIPS 140-2	✓	✓	✓
固定憑證	✓		
<b>IT 原則</b>			
破解偵測	✓	✓	✓
裝置被破解時自動離線撤銷	✓	✓	
需要註冊	✓	✓	✓
文件逾期時自動離線撤銷	✓	✓	✓
離線登入次數上限	✓	✓	✓
達到嘗試登入失敗次數之上限時即抹除內容	✓	✓	✓
禁止刪除必要的內容	✓	✓	✓
<b>DLP</b>			
禁止複製/貼上	✓	✓	✓
啟用/停用「列印」	✓		
啟用/停用「在第三方應用程式中開啟」	✓	✓	✓
啟用/停用「透過 Email 共享」	✓	✓	
啟用/停用「文件級加密」	✓	✓	✓
啟用/停用「文件浮水印」	✓*	✓*	

\*浮水印功能只能用於管理員存放庫、使用者存放庫和 Workspace ONE UEM 所管理內容。這不可用於在

## 各平台所支援的檔案類型表格

此表格列出不同平台上的 Workspace ONE Content 應用程式支援的檔案類型。

此表格適用於應用程式商店提供的 VMware Workspace ONE Content 版本。

支援的檔案類型	iOS		Android		Windows 10		備註
	編輯	檢視	編輯	檢視	編輯	檢視	
AD/Azure RMS	✓	✓	✓ Content 應 用程式 v3.5+	✓ Content 應 用程式 v3.5+			
AAC (音訊檔/aac)		✓		✓			您無法編輯音訊和影片檔案。您只能從 Content iOS 和 Android 應用程式新增檔案。 在音訊檔案中，您只能新增 .m4a 檔案。
ALAC (音訊檔/m4a)		✓		✓			
WAV (音訊檔/wav)		✓		✓			
MP3 (音訊檔/mpeg)		✓		✓			
MOV (視訊檔/quicktime)		✓		✓			Android 裝置預設不支援 MOV 檔案；但是，有極少部份 OEM 會提供支援。 Samsung 裝置不支援 MOV 檔案。
MP4 (視訊檔/mp4)		✓		✓			
M4B、M4R		✓					
M4V		✓		✓			
CSV (.csv)		✓		✓		✓	
ePub (.epub)		✓					
iBooks							



支援的檔案類型	iOS	Android	Windows 10	備註	
iWorks - Keynote (.key) 應用程式/ vnd.apple.keynote		✓			
iWorks - Numbers (.numbers) 應用程式/ vnd.apple.numbers		✓			
iWorks - Pages (.pages) 應用程式/ vnd.apple.pages		✓			
MS Office - Excel (.xls) 應用程式/ vnd.ms-excel	✓	✓	✓	✓	
XLSM		✓	✓		
MS Office - PowerPoint (.ppt/.pptx) 應用程式/ vnd.ms-powerpoint	✓	✓	✓	✓	
PPTM		✓	✓		
MS Office - Word (.docx) 應用程式/ msword	✓	✓	✓	✓	不支援對 .doc 檔案進行編輯
DOCM		✓	✓		
MS Office - 受密碼保護 (.docx、.pptx、.xlsx、.xltx) MS Office 2007 或更新版本)	✓	✓	✓	✓	不支援對 .doc 檔案進行編輯

支援的檔案類型	iOS	Android	Windows 10	備註
MS Office - 含有樞紐分析表的文件	✓	✓	✓	
HTML (.html) 文字檔/html	✓	✓	✓	HTML 瀏覽器不支援 JavaScript
PDF (.pdf) 應用程式/pdf	✓	✓	✓	
Rich Text Format (.rtf) 應用程式/rtf	✓	✓		
Rich Text Format Dictionary (.rtfd) 應用程式/octet-stream	✓	✓		
XML (.xml) 應用程式/xml	✓	✓	✓	
PNG (.png) 圖像檔/png	✓	✓	✓	您可以新增圖像，但無法編輯檔案。
JPG (.jpg) 圖像檔/jpeg	✓	✓	✓	
TIF (.tif, .tiff) 圖像檔/tif	✓	✓	✓	
Bitmap (.bmp) 圖像檔/bmp	✓	✓	✓	
GIF (.gif) 圖像檔/gif	✓	✓	✓	
Zip (.zip) 應用程式/zip	✓	✓	✓	✓
密碼保護的 Zip 檔	✓	✓	✓	✓
RAR (.rar) 應用程式/rar	✓	✓		
密碼保護的 RAR				
GZIP (.gzip) 應用程式/zip				
BZIP (.bzip) 應用程式/zip				

支援的檔案類型	iOS	Android	Windows 10	備註
BZIP2 (.bzip2) 應用程式/zip				
TAR (.tar) 應用程式/zip				
TXT	✓	✓	✓	✓
MSG		✓		

## 設定 VMware Workspace ONE Content

使用 Workspace ONE Content 應用程式，為終端使用者提供從裝置端存取公司內容的權限。於 UEM 主控台中設定的組態將決定終端使用者從其裝置存取企業內容時的自由度。

- 1 導覽至**群組與設定 > 所有設定 > 內容 > 應用程式 > Workspace ONE Content 應用程式**。
- 2 配置**設定和原則**的設定：

設定	描述
應用程式設定檔	設定此項，以定義此應用程式所用的安全性原則和設定。 保留 <b>預設值</b> 不變，並配置推薦的預設 SDK 設定，以便使用 Workspace ONE UEM 的建議來定義 APP 的行為。 另外也可以選取 <b>自訂</b> 應用程式設定來覆寫預設的 SDK 設定，並為 APP 配置一組獨特的行為。
iOS 設定檔	從下拉式清單中選取自訂建立的 SDK 設定檔。
Android 設定檔	從下拉式清單中選取自訂建立的 SDK 設定檔。

- 3 配置**一般**設定。

設定	描述
顯示為新內容的天數	選取近期新增的文件將在 Workspace ONE Content 中標示為新內容的天數。
封鎖經由 Content、Boxer 和 Web 進行註冊	啟用後，會禁止透過 Workspace ONE Content、VMware Workspace ONE Boxer 和 VMware Workspace ONE Web 註冊。 如果 Workspace ONE Content 在 Objective-C 中使用 iOS 適用的 VMware Workspace ONE SDK，則單一登入 SDK 設定需要 MDM 註冊才能正常運作。
變更受管理內容的存放庫名稱	啟用此項，以便在出現的 <b>根存放庫名稱</b> 欄位中，變更存放庫名稱。
根存放庫名稱	輸入您要使用的新存放庫名稱。
允許超連結	啟用此項，以允許終端使用者開啟位於文件中，所出現的 <b>開啟網路連結的方式</b> 欄位中的超連結。
開啟網路連結的方式	選擇要開啟「連結」的應用程式。
本機儲存區	啟用此項，為使用者內容提供替代的儲存空間。
僅限使用 Wi-Fi 上傳	啟用後，會限制 Workspace ONE Content 僅能透過 Wi-Fi 連線來上傳。

- 4 實作應用程式的**使用條款**協議。

## 5 將通知指派給特定平台的 Workspace ONE Content 應用程式。

設定	描述
應用程式類型	表示類型為 <b>系統</b> 或 <b>內部</b> 。
應用程式名稱	指派給應用程式。
配套 ID	指派給應用程式。
徽章數量	<p>設為<b>必要</b>、<b>僅限更新</b>或<b>無</b>。</p> <p><b>必要</b>：徽章數量代表使用者未透過 Workspace ONE Content 開啟的必要文件數量。(僅限 Windows) 徽章數量可在多個裝置上追蹤每位使用者的必要文件「讀取」狀態。當擁有多個裝置的使用者讀取必要文件時，所有其他裝置會將該文件反映為已讀取。</p> <p><b>僅限更新</b> (用於下載的內容)：徽章數量代表具有可用更新內容或新版本的下載文件數量。</p> <p><b>無</b>：徽章數量在 Workspace ONE Content 為停用狀態。</p>

## 6 選取儲存。

# 入門培訓 VMware Workspace ONE Content 概覽

入門培訓要求終端使用者必須先檢閱並瞭解培訓的資料和影片，才能在其裝置上取得完整的 VMware Workspace ONE Content 存取權限。

若要將入門培訓的功能最大化，需先設定必要的內容，並將單一應用程式模式設定檔推送至終端使用者的裝置上。一旦入門培訓完成，請移除設定檔，終端使用者才能存取完整的裝置功能。

此外，設定入門培訓也可以選擇不使用單一 APP 模式，以便為終端使用者提供更具彈性的經驗。在這樣的設定下，終端使用者雖能使用裝置，但在檢閱過必要內容之前，都將無法存取 Workspace ONE Content。

	使用單一 APP 模式	不使用單一 APP 模式
VMware Workspace ONE Content	鎖定在必要的「內容檢視」。	鎖定在必要的「內容檢視」。
其他的裝置 APP	無法存取。無法存取：裝置在「必要內容檢視」中保持鎖定狀態。	可存取。終端使用者仍能使用其裝置。

強制執行內容檢閱前，請先考量到這些選擇將如何影響終端使用者的體驗。例如，將必要內容推播至裝置可能會讓使用者感到困惑，結果導致其提交服務台票證。一般而言，在入門培訓或其他引導式的案例中，根據有限的裝置行為來提供程度適中的上下文，可以避免終端使用者到困惑。

另外，使用單一應用程式模式來部署 Workspace ONE Content 時，也請考量到即將造成的影響，因為這麼做會使裝置的功能受限於單一應用程式，以此處的例子來說，正是 Workspace ONE Content。如果計畫在設定時移除單一 APP 模式限制，請確保終端使用者未存取其他應用程式。此外，請確保終端使用者在其裝置受限制時，在其裝置上執行與工作相關的任務。

# 啟用 VMware Workspace ONE Content 入門培訓

入門培訓可為 Workspace ONE Content 提供一種部署選項，這種選項會鎖定應用程式，使其只顯示必要的內容，直到使用者檢視該內容為止。

## 1 滿足作業系統與應用程式的最低需求。

- 2 決定並設定註冊流程。
- 3 導覽至 **內容 > 設定 > 進階 > 入門培訓**。
- 4 將**入門培訓**設定為**啟用**，並且在出現的欄位上進行配置。

設定	描述
管理解鎖碼	以管理員身分設定此解鎖碼，並覆寫監督模式。
入口訊息	向終端使用者提供訊息，說明使用者必須先檢閱必要內容才能開始使用裝置。
出口訊息	向終端使用者提供訊息，說明使用者已檢視所有必要的內容，從此便可隨心所欲地使用該裝置。

## 配置文件副檔名

文件副檔名可讓終端使用者從第三方應用程式與 iOS 裝置上的 VMware Workspace ONE Content 檔案互動。此功能需在 UEM 主控台內的特定配置，也需另外考量企業檔案伺服器的特定類型。

藉由在 UEM 主控台中完成所需的配置，確保文件副檔名功能出現在具有 Workspace ONE Content v3.1 及更新版本的裝置上。

### ■ 停用驗證類型

啟用驗證類型的應用程式會限制使用者使用文件副檔名從 Workspace ONE Content 應用程式上傳檔案。若要允許使用者將檔案上傳到第三方應用程式，必須停用驗證類型。

- a 導覽至**群組 & 設定 > 所有設定 > 應用程式 > 設定和原則 > 安全性原則**。
- b 在 [驗證類型] 下拉式功能表中，選取**停用**，然後選取**儲存**。

### ■ 停用應用程式允許清單

必須停用列入允許清單的應用程式，以允許使用者將文件從第三方應用程式開啟至 Workspace ONE Content。

- a 導覽至**群組 & 設定 > 所有設定 > 應用程式 > 設定和原則 > 安全性原則**。
- b 將**限制檔案僅能在核准的 APP 中開啟**設為否。
- c 選取**儲存**。

### ■ 啟用允許於第三方應用程式中開啟

必須啟用允許於第三方應用程式中開啟的選項，終端使用者才能在第三方應用程式中的使用匯出功能。

- a 導覽至**內容 > 存放庫 > 管理員存放庫**。
- b 選取同步至終端使用者裝置之企業檔案伺服器旁的**編輯**圖示。
- c 在**安全性**頁籤中，選取**允許於第三方應用程式中開啟**，然後選取**儲存**。

## 啟用儲存區存取權

僅在 Android 裝置上的 Workspace ONE Content 檔案和儲存區存取權啟用時，終端使用者才可以從第三方應用程式存取檔案和儲存區。

若要啟用儲存區存取，請在主控台上完成必要的組態。

- 使用 Android SDK 預設設定來啟用第三方應用程式的儲存體存取

在預設 SDK 設定檔中新增組態金鑰，以啟用第三方應用程式的內容檔案與儲存體存取。

- 導覽至 **應用程式 > 設定與原則 > 設定 > 自訂設定**。
- 選取 **啟用自訂設定**，並貼上 `{"PolicyEnableFileProvider": "true"}`。
- 選取 **儲存**。

- 使用 Android SDK 自訂設定檔啟用第三方應用程式的儲存體存取

在 Workspace ONE Content 的自訂 SDK 設定檔中新增組態金鑰，以啟用第三方應用程式的內容檔案與儲存區存取。

- 如果您有現有的自訂設定檔，請導覽至 **應用程式 > 設定 > 設定檔 > 自定設定檔 > 自訂設定裝載**。
- 如果您要新增自訂設定檔，請導覽至 **應用程式 > 設定 > 設定檔 > 新增設定檔 > SDK 設定檔 > Android > 自訂設定 > 自訂設定裝載**。
- 貼上 `{"PolicyEnableFileProvider": "true"}`，然後選取 **儲存**。

如果您有多個自訂設定，請在 `{ }` 中將 `PolicyEnableFileProvider` 金鑰附加於現有自訂金鑰之後。  
例如：`{"CustomSetting Default": "true", "PolicyEnableFileProvider": "true" }`。

- 您也必須啟用 [允許於第三方應用程式中開啟] 設定，以允許終端使用者存取第三方應用程式的檔案。請參閱 [List item](#)。

## 第三方應用程式的儲存體存取限制 (僅適用於 Android)

下列清單說明了第三方應用程式儲存區存取的限制。

- 「允許在第三方 APP 中開啟」旗標可用來允許或拒絕存取第三方 APP。「允許 Email」權限旗標不適用於檔案，因為無法決定 (按照應用程式 ID) 第三方 APP 是否為 Email APP。
- 根據預設，已停用從第三方 APP 進行內容檔案和儲存空間存取的 Android 架構支援，以便管理 APP 容器以及這些容器之間共用的資料。
- 無法存取本機儲存空間檔案，因為在第三方 APP 中開啟的功能預設為停用。
- Workspace ONE Content 驗證啟用時，您必須將 Workspace ONE Content 解鎖，才能透過第三方應用程式加以存取 (顯示訊息)。
- 如果您的管理員已設定應用程式允許清單，而且第三方應用程式未列入允許清單，則您無法透過 Workspace ONE Content 開啟或建立檔案。
- 對於管理內容，透過第三方 APP 瀏覽時，可使用所有內容。對於其他存放庫，只有在 Workspace ONE Content 中同步的資料夾可使用內容 (一個層級)。

## 掃描 QR 代碼以存取自訂 URL (僅 Android)

使用自訂 URL，可讓終端使用者直接存取 Workspace ONE Content 應用程式中的檔案。掃描時，若檔案已下載，內含自訂 URL 的 QR 碼會允許終端使用者搜尋或檢視該檔案。

您必須使用搜尋查詢或特定的內容 ID 做為自訂 URL。系統會針對您上傳至 Workspace ONE UEM Console 的每個檔案自動產生內容 ID。當您指向檔案名稱時，檔案路徑會顯示內容 ID。

自訂 URL 為：

- awsc://search/?query=text
- awsc://search?query=text
- awsc://search/?query="text"
- awsc://search?query="text"
- awsc://contentid={內容 ID}
- awsc://contentid="{內容 ID}"

搜尋查詢會搜尋指定的文字字串和特定的內容 ID，並且直接開啟指定文件。

## 使用 Swift SDK 對 iOS 上的 Content 進行行為變更

iOS 版 Workspace ONE Content 5.0 是第一個使用 Workspace ONE Swift SDK 的 Content 版本。先前版本的 Content 採用 Objective C 版本的 Workspace ONE SDK。隨著此架構變更，只有少數變更可能會影響到終端使用者習慣的 Content 應用程式行為。

下列清單說明了行為的變更：

- Workspace ONE SDK 不支援獨立模式下的登出功能。

---

**備註** 使用者必須在其裝置上使用登錄模式下的 Intelligent Hub。對於未受 MDM 管理或沒有 Workspace ONE Intelligent Hub 的裝置，使用者不得以獨立模式嘗試登入 Content 應用程式。

---

- 不再支援使用者名稱/密碼畫面上的離線工作選項。使用者可透過導覽至「應用程式設定」及啟用「離線工作」，來進行離線工作。您仍可以進行網路呼叫，並僅透過 Content 特定互動來接受離線工作。
- 更新後的 SDK 驗證畫面，成為使用者的全新體驗。
- 如果 SDK 在啟動後無法擷取 Content 設定，則會向使用者顯示失敗訊息。
- 在忘記密碼的情況下，無需簽入/簽出 (CICO) 即可體驗使用者變更的更新。

如需 Content 應用程式行為變更的相關資訊，請參閱知識庫文章 [Workspace ONE Content 5.0 中的行為變更](#)。

## Workspace ONE Content 中的文件確認

Content 應用程式使用者現在可確認您指派給他們的文件為必要內容。使用者可以在您的檔案中檢視需要確認的檔案，以在應用程式的 [通知] 畫面中檢閱區段。

在 Workspace ONE UEM Console 上，您可以在 [內容清單檢視] 和 [裝置詳細資料] 頁面中檢視這些確認。

在 [內容清單檢視] 頁面的 [安裝狀態] 欄位下選取 [檢視] 時，會出現一個快顯方塊，顯示已檢視並確認內容的確切使用者數目。

下列清單說明支援的文件確認功能：

- 若要啟用對必要內容進行確認，請在 UEM console 上套用自訂設定 `EnableDocumentAcknowledgment: true`。
- 當使用者開啟文件時，[已確認] 按鈕會顯示為停用狀態，並且在預設延遲五秒後啟用。可透過在 UEM console 上套用值 `AcknowledgementTimeInterval` 做為自訂的 SDK 設定，來將預設值變更為 0-600 秒的範圍。
- 系統不會提示使用者確認已確認的文件。
- 若已經確認的文件發佈新版本，則系統會提示使用者再次進行確認。
- [裝置詳細資料] 頁面會顯示已確認的狀態和文件確認的日期。
- 「依裝置顯示內容詳細資料」報告包含個別裝置的已確認狀態。

## Workspace ONE Content 中的匯入限制 (僅適用於 iOS)

您可以使用 UEM console 中的某些組態金鑰，限制或允許匯入第三方應用程式的內容至 Workspace ONE Content。這些組態金鑰僅允許從經過核准的原生應用程式清單匯入內容。

使用下列組態金鑰來限制或允許將內容從第三方應用程式匯入 Workspace ONE Content。

設定金鑰	值類型	支援的值	描述
<code>{"ContentImportRestriction"}</code>	布林值	<code>true</code> = 已啟用的限制 <code>false</code> = 已停用的限制 例如， <code>{"ContentImportRestriction": true}</code>	啟用時，裝置使用者無法將來自任何非允許清單所列之第三方應用程式 (包括原生 iOS 應用程式) 的內容匯入 Workspace ONE Content。
<code>{"ContentImportAllowNative Apps"}</code>	布林值	<code>true</code> = 允許從原生應用程式匯入 <code>false</code> = 不允許從原生應用程式匯入 例如， <code>{"ContentImportAllowNative Apps": true}</code>	啟用時，裝置使用者可以在啟用匯入限制的情況下，匯入來自原生應用程式的內容。

`ContentImportRestriction` 和 `ContentImportAllowNativeApps` 設定值可搭配使用以依照您的需求配置匯入限制。如果您想要允許匯入來自所有的原生 App 的內容，請啟用 `ContentImportAllowNativeApps` 金鑰。`ContentImportAllowNativeApps` 金鑰為預設啟用項目，並允許匯入所有的原生 App，例如 iOS 原生的 Email、Files、Safari、AirDrop 等 App。啟用時，裝置使用者可以透過 Safari 使用非允許清單所列應用程式的網頁版，從非允許清單應用程式開啟內容並匯入 Workspace ONE Content。

如果您只想允許特定的應用程式，請停用 `ContentImportAllowNativeApps` 金鑰並在允許清單中將其新增為允許的應用程式。



如果想要限制匯入來自特定原生應用程式的內容，請停用 `ContentImportAllowNativeApps` 金鑰並在允許清單中將其新增為允許的原生應用程式。

---

**備註** 在啟用組態金鑰值之前，必須先啟用「資料外洩防護」設定中的「限制文件僅於核准的 App 中開啟」選項。Safari 和 AirDrop 不可列入允許清單，因為它們沒有任何相關聯的服務包識別碼。

---

### 使用預設的 SDK 設定檔配置匯入限制

在預設的 SDK 設定檔中新增組態金鑰，來限制將內容從第三方應用程式匯入至 Workspace ONE Content。

- 1 請導覽至**群組 & 設定 > 所有設定**。
- 2 從所有設定，導覽至 **App > 設定 & 原則 > 設定**。
- 3 選取**啟用自訂設定**，然後依據您的需求，貼上設定金鑰。
  - 若只允許從原生應用程式匯入，`{ "ContentImportRestriction": true, "ContentImportAllowNativeApps": true}`。
- 4 允許從特定應用程式清單匯入 (允許清單)。
  - a 導覽至**設定 & 原則 > 安全性原則**。
  - b 選取**允許應用程式清單**文字方塊，並列出您想要允許使用者將內容匯入至 Workspace ONE Content 的應用程式。
- 5 選取**儲存**。

### 使用自訂 SDK 設定檔配置匯入限制

在自訂 SDK 設定檔中新增組態金鑰，來限制將內容從第三方應用程式匯入至 Workspace ONE Content。

- 1 請導覽至**群組 & 設定 > 所有設定**。
- 2 如果您具有現有的自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 自訂設定檔 > 自訂設定**。
- 3 如果要新增自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 新增設定檔 > SDK 設定檔 > iOS > 自訂設定**。
- 4 依據您的需求，從 [自訂設定] 中選取**配置**並貼上組態金鑰。若要允許僅從原生應用程式匯入，`{ "ContentImportRestriction": true, "ContentImportAllowNativeApps": true}`。
- 5 從 [限制] 區段中，選取**限制文件**，以在下列應用程式中開啟，然後新增您想要依需求允許的應用程式清單 (允許清單)。
- 6 選取**儲存**。

## Workspace ONE Content 中的 PDF 自動儲存功能 (僅適用於 iOS)

Workspace ONE Content v4.13.2 從裝置使用者可以啟用或停用 PDF 自動儲存功能使用 Workspace ONE Content 應用程式中啟用 PDF 自動儲存設定。

PDF 自動儲存設定預設為停用。可使用 Workspace ONE Content 中自動儲存時間的秒數設定，將 PDF 自動儲存功能設定為 30 秒、60 秒以及 120 秒。管理員可以使用 Workspace ONE UEM Console 中的 Workspace ONE UEM 提供的設定金鑰，強制啟用 Workspace ONE Content 中的 PDF 自動儲存功能。使用設定金鑰啟用功能時，裝置使用者無法停用 PDF 自動儲存功能，且無法使用 Workspace ONE Content 中的啟用 PDF 自動儲存設定。PDF 自動儲存功能啟用時，無法儲存於自動儲存功能進行時對 PDF 檔案所做的變更。每次進行自動儲存後，系統將重新載入 PDF 文件。

使用下列設定金鑰啟用 Workspace ONE Content 中的 PDF 自動儲存功能：

設定金鑰	值類型	支援的值	描述
{ "ContentPDFAutoSaveEnabled" }	布林值	true = 啟用 false = 可由裝置使用者啟用或停用	設為 True 時，PDF 自動儲存功能已啟用，裝置使用者無法停用此設定。裝置使用者無法使用 Workspace ONE Content 中的啟用 PDF 自動儲存設定。

### 使用預設的 SDK 設定檔配置 PDF 自動儲存

在預設的 SDK 設定檔中新增組態金鑰，以允許或限制使用者停用 PDF 自動儲存功能。

- 1 請導覽至**群組 & 設定 > 所有設定**。
- 2 從 [所有設定]，導覽至**應用程式 > 設定與原則 > 設定**。
- 3 選取**啟用自訂設定**，然後依據您的需求，貼上設定金鑰。若要啟用 PDF 自動儲存功能，  
{ "ContentPDFAutoSaveEnabled": true }。
- 4 選取**儲存**。

### 使用自訂的 SDK 設定檔配置 PDF 自動儲存

在自訂的 SDK 設定檔中新增組態金鑰，以允許或限制使用者在 Workspace ONE Content 應用程式中停用 PDF 自動儲存功能。

- 1 請導覽至**群組 & 設定 > 所有設定**。
- 2 如果您有現有的自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 自訂設定檔 > 自訂設定**。
- 3 如果要新增自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 新增設定檔 > SDK 設定檔 > iOS > 自訂設定**。
- 4 依據您的需求，從 [自訂設定] 中選取**配置**並貼上組態金鑰。若要啟用 PDF 自動儲存功能，  
{ "ContentPDFAutoSaveEnabled": true }。
- 5 選取**儲存**。

## Workspace ONE Content 的隱私設定 (僅適用於 iOS 與 Android)

使用 UEM console 中的特定組態金鑰，即可執行額外的隱私權披露和資料收集作業。

升級或開始使用最新版本之 Workspace ONE Content 的使用者，會在啟動應用程式時，看到新的隱私權對話畫面。

隱私權對話畫面可讓使用者瞭解下列資訊：

- 應用程式收集的資料 – 提供應用程式收集和處理之資料的摘要。Workspace ONE UEM 管理主控台的管理員可看到此資料的部分內容。
- 裝置權限 – 提供應用程式要求之裝置權限的摘要，以啟用產品特色和功能，例如推送通知至裝置。
- 公司隱私權政策 – 訊息依預設會向使用者顯示，以便使用者與其雇主聯絡瞭解詳細資訊。您可以在 UEM 主控台中配置隱私權政策 URL。配置完成後，使用者可從應用程式存取雇主的隱私權政策。

使用下列組態金鑰，可在 Workspace ONE Content 中啟用隱私全通知和資料共用設定。

設定金鑰	值類型	支援的值	描述
{ "DisplayPrivacyDialog" }	整數	0 = 停用 1 = 啟用 (預設值)	設定為「1」(啟用) 時，Workspace ONE Content 會向使用者顯示收集之資料和裝置需要之權限 (用於提升應用程式運作效能) 相關的隱私權通知。
{ "PolicyAllowFeatureAnalytics" }	整數	0 = 停用 1 = 啟用 (預設值)	設定為「1」(啟用) 時，Workspace ONE Content 會向使用者顯示參與匿名功能使用量分析 (可協助 VMware 改善產品功能與創造新產品功能) 之選項的相關通知。設定為「0」時，資料共用通知不會顯示，且不會從裝置收集任何資料來最佳化應用程式使用體驗。
{ "PolicyAllowCrashReporting" }	布林值	True = 啟用 False = 停用	設為 True 時，會將應用程式當機回報至 VMware。
{ "PrivacyPolicyLink" }	字串	[ "https://www.url.com" ]	當貴公司的隱私權政策在隱私權通知中受到選取，請提供您要求使用者造訪的政策 URL。

### 使用預設的 SDK 設定檔配置隱私權設定

在預設的 SDK 設定檔中新增組態金鑰，以啟用或停用顯示隱私及資料收集公告。

- 1 請導覽至 **群組 & 設定 > 所有設定**。
- 2 從所有設定，導覽至 **應用程式 > 設定與原則 > 設定**。
- 3 選取 **啟用自訂設定**，然後依據您的需求，貼上設定金鑰。若要啟用當機報告功能，  
{ "PolicyAllowCrashReporting": true }。
- 4 選取 **儲存**。

### 使用自訂 SDK 設定檔來設定隱私權設定

在自訂的 SDK 設定檔中新增組態金鑰，以啟用或停用顯示隱私權及資料收集公告。

- 1 導覽至**群組與設定 >> 所有設定**。
- 2 如果您有現有的自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 自訂設定檔 > 自訂設定**。
- 3 如果要新增自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 新增設定檔 > SDK 設定檔 > iOS > 自訂設定**。
- 4 依據您的需求，從 [自訂設定] 中選取**配置**並貼上組態金鑰。
- 5 選取**儲存**。

## Workspace ONE Content 的畫面逾時限制 (僅適用於 iOS)

您可以使用 Workspace ONE UEM Console 中的特定組態金鑰，限制裝置使用者無法在 Workspace ONE Content 應用程式中停用畫面逾時。

組態金鑰	值類型	支援的值	描述
{ "PolicyAllowScreenTimeoutToggle" }	布林值	True (預設值) = 啟用 False = 停用	透過設定「True」或「False」來控制 Content 應用程式的逾時設定。若未設定值，系統會套用預設設定，並讓使用者能切換逾時設定。設定為「false」時，使用者將無法切換逾時設定。

### 使用預設的 SDK 設定檔停用畫面逾時

在預設的 SDK 設定檔中新增組態金鑰來限制裝置使用者，使其無法在 Workspace ONE Content 應用程式中停用畫面逾時。

- 1 請導覽至**群組與設定 >>> 所有設定**。
- 2 從所有設定，導覽至 **App > 設定 & 原則 > 設定**。
- 3 選取**啟用自訂設定**，然後依據您的需求，貼上設定金鑰。停用畫面逾時，  
{ "PolicyAllowScreenTimeoutToggle": false }。
- 4 選取**儲存**。

### 使用自訂的 SDK 設定檔停用畫面逾時

在自訂的 SDK 設定檔中新增組態金鑰來限制裝置使用者，使其無法在 Workspace ONE Content 應用程式中停用畫面逾時。

- 1 請導覽至**群組與設定 > 所有設定**。
- 2 如果您有現有的自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 自訂設定檔 > 自訂設定**。
- 3 如果要新增自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 新增設定檔 > SDK 設定檔 > iOS > 自訂設定**。
- 4 依據您的需求，從 [自訂設定] 中選取**配置**並貼上組態金鑰。停用畫面逾時，  
{ "PolicyAllowScreenTimeoutToggle": false }。

## 5 選取儲存。

## 存放庫的自動同步控制項 (僅限 Android)

對於含有不受管理內容的存放庫類型，在預設或自訂的 SDK 設定檔中加入組態金鑰以便控制其自動同步與驗證檢查。

設定金鑰	值類型	支援的值	描述
{"AutoSyncEnabled"}	布林值	TRUE (預設值) = 啟用 FALSE = 停用	設為 False 時，唯有使用者導覽至存放庫時，存放庫才會執行自動同步和驗證檢查。套用預設值時，在執行自動或手動同步時便會執行同步和驗證檢查。

### 使用預設的 SDK 設定檔停用存放庫自動同步

針對含有不受管理內容的存放庫或個人內容存放庫類型，在預設的 SDK 設定檔中新增組態金鑰，以便控制自動同步與驗證檢查。

- 1 導覽至**群組與設定 > 所有設定**。
- 2 從所有設定，導覽至 **App > 設定 & 原則 > 設定**。
- 3 選取**啟用自訂設定**，然後依據您的需求，貼上設定金鑰。停用自動同步功能，{ "AutoSyncEnabled": false }
- 4 選取**儲存**。

### 使用自訂的 SDK 設定檔停用存放庫自動同步

針對含有不受管理內容的存放庫或個人內容存放庫類型，在自訂的 SDK 設定檔中新增組態金鑰，以便控制自動同步與驗證檢查。

- 1 導覽至**群組與設定 > 所有設定**。
  2. 如果您有現有的自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 自訂設定檔 > 自訂設定**。
  3. 如果要新增自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 新增設定檔 > SDK 設定檔 > Android > 自訂設定**。
  4. 依據您的需求，從 [自訂設定] 中選取**配置**並貼上組態金鑰。停用畫面逾時，{ "AutoSyncEnabled": false }。
  5. 選取**儲存**。

## 適用於 Content 的 Workspace ONE Send

藉由整合 Workspace ONE Send 與 Workspace ONE Content，您可以限制在 Workspace ONE Content 的檔案僅能透過 Workspace ONE Send 開啟。若要透過 Send 應用程式強制開啟檔案，請在 UEM Console 中新增組態金鑰。

使用下列組態金鑰來限制檔案須透過 Workspace ONE Send 開啟。

設定金鑰	值類型	支援的值	描述
{ "PolicyAllowAIPFilesToOpenInOffice" }	布林值	True = 啟用 False = 停用	設為 True 時，檔案將會透過 Workspace ONE Send 開啟。

### 使用預設的 SDK 設定檔在 Send 開啟檔案

在預設 SDK 設定檔新增組態金鑰，讓檔案僅能透過 Workspace ONE Send 開啟。

1. 導覽至 **群組與設定 > 所有設定**。
2. 從所有設定，導覽至 **應用程式 > 設定與原則 > 設定**。
3. 選取**啟用自訂設定**，然後依據您的需求，貼上組態金鑰。啟用限制，以便透過 Send 開啟檔案，{ "PolicyAllowAIPFilesToOpenInOffice": true }。
4. 選取**儲存**。

### 使用自訂的 SDK 設定檔在 Send 開啟檔案

在自訂 SDK 設定檔中新增組態金鑰，讓檔案僅能透過 Workspace ONE Send 開啟。

- 1 導覽至 **群組與設定 > 所有設定**。
- 2 如果您有現有的自訂設定檔，請導覽至 **應用程式 > 設定與原則 > 設定檔 > 自訂設定檔 > 自訂設定**。
- 3 如果要新增自訂設定檔，請導覽至 **應用程式 > 設定與原則 > 設定檔 > 新增設定檔 > SDK 設定檔 > iOS > 自訂設定**。
- 4 依據您的需求，從 [自訂設定] 中選取**配置**並貼上組態金鑰。啟用限制，以便透過 Send 開啟檔案，{ "PolicyAllowAIPFilesToOpenInOffice": true }
- 5 選取**儲存**。

# Workspace ONE Smartfolio

# 6

Smartfolio 是一種強大又安全的應用程式，可協助您的組織輕鬆地管理和共用公司內容。它為一般業務線使用案例提供了量身制定的內容發佈和合規性經驗。

Smartfolio 目前僅支援 iOS 裝置。

## 功能

- 遠端管理並整理檔案，然後將重要檔案傳遞給終端使用者。
- 提供終端使用者離線存取文件的權限。
- 根據相關程度排列文件的優先順序。
- 管理每個文件層級的安全性，以符合文件導向的法規需求。
- 將文件設定為自動或手動下載，並收集讀取回條，作為企業合規原則的一部分。
- 在配置為 Workspace ONE UEM 應用程式套件時，中使用預設的 SDK 設定。

**備註** Workspace ONE Smartfolio 應用程式會收集各種分析目的所需的資料，例如當機報告、記錄資料和其他資訊。此資料可協助 VMware 改善產品功能。如需 VMware 如何處理所收集資料的相關資訊，請參閱 <https://www.vmware.com/help/privacy.html>。

## Smartfolio 和內容比較表

表中所列出的內容是比較 Smartfolio 所支援的功能與 Workspace ONE Content 所支援的功能。使用此表可協助判斷哪個應用程式更適合您的使用案例。

	Workspace ONE Content	Workspace ONE Smartfolio
應用程式平台支援	支援 iOS、Android 和 Windows 10。	僅支援 iOS
存放庫支援	支援所有存放庫類型 (OneDrive、SharePoint、NFS)	僅支援 UEM 管理的內容存放庫
檔案管理	允許建立、查看和編輯文件	僅允許查看文件 僅在 PDF 上支援註釋
APP 的大小	安裝大小約 200 MB	安裝大小低於 100 MB 的輕裝應用程式

	Workspace ONE Content	Workspace ONE Smartfolio
應用程式用途	強化內容彙總和員工生產力工作流程	提升管理員的內容發佈體驗
使用者體驗	輕鬆方便的理解具進階功能的 UI。 允許使用者在文件上建立、查看、編輯和執行更多動作。	輕鬆方便的理解具基本功能的 UI。限制使用者只能查看和標註 (僅限 PDF) 文件。

## Workspace ONE Smartfolio 部署

使用 Workspace UEM 行動應用程式管理功能，輕鬆地將 Smartfolio 部署為受管理的應用程式。將 Smartfolio 應用程式部署至終端使用者裝置時，需要在 Workspace ONE UEM console 上完成數個步驟。部署完成後，終端使用者即可在其已註冊的裝置上下載應用程式。

透過 VMware Workspace ONE Intelligent Hub 所註冊的終端使用者裝置，依預設會由 MDM 管理。在不使用 MDM 管理的情況下，您也可以透過啟用智慧群組的未受管理模式來註冊這些裝置。可以在受管理模式或未受管理模式註冊的裝置上，存取 Smartfolio 應用程式。

如需有關部署公用應用程式的詳細資訊，請參閱 Workspace ONE UEM 行動應用程式管理說明文件。

如需為裝置啟用未受管理模式的相關資訊，請參閱 Workspace ONE Hub 服務說明文件中的啟用 iOS 裝置的未受管理註冊。

## 將 Smartfolio 新增至 Workspace ONE UEM Console

若要將 SDK 設定檔套用到 Smartfolio 應用程式，您必須先將其在 Workspace ONE UEM console 新增為公共應用程式。套用的 SDK 設定檔會為該應用程式提供其他功能。

- 1 導覽至 **資源 > 應用程式 > 原生 > 清單檢視**。
- 2 選取 **公用**，然後選取 **新增應用程式**。
- 3 配置顯示的文字方塊，並選取 **下一步**。

設定	描述
管理者	選取應用程式所上傳的企業群組。
平台	選取適當的平台。目前僅支援 iOS 裝置。
來源	使用應用程式名稱或 URL 在 App Store 中搜尋此應用程式。
名稱	輸入 Workspace ONE Smartfolio。

- 4 從 **搜尋** 結果頁面找到並選取 Smartfolio 應用程式。
- 5 審查在 **詳細資料** 標籤中自動填入的資訊。
- 6 指派使用者第一次從應用程式目錄存取應用程式時顯示的 **使用條款**。
- 7 選取 **SDK** 索引標籤，然後將 SDK 設定檔指派到 Smartfolio 應用程式。
- 8 選取 **儲存並指派**。



## 新增指派到 Smartfolio

若要將 Smartfolio 應用程式部署給您的終端使用者，您可以新增單一指派群組或多個指派群組。

您必須將 Smartfolio 上傳至 Workspace ONE UEM console 作為公共應用程式。

- 1 導覽至 **資源 > 應用程式 > 原生 > 清單檢視**。
- 2 在 Smartfolio 應用程式的 [安裝狀態] 欄位下，選取**指派**連結。或者，您也可以選取 [編輯] 圖示，然後選取**儲存 & 指派**。
- 3 在 [指派] 頁面上，選取**新增指派**並完成選項。
  - a 在**散發**索引標籤中，輸入下列資訊。

設定	描述
名稱	輸入指派名稱。
描述	輸入指派的說明。
指派群組	輸入您要為其指派應用程式的智慧群組名稱。 當您輸入智慧群組名稱時會顯示選項，您可以從清單中選取適當的智慧群組。 如有必要，您可以新增更多指派群組。
APP 交付方式	<ul style="list-style-type: none"> <li>■ <b>隨選</b> - 將內容部署至目錄或其他部署 Agent (代理程式)。裝置使用者可以決定是否要安裝該內容以及何時安裝。 對企業不太重要的內容來說，這是最佳的選擇。當使用者想要節省頻寬和限制非必要的流量時，即可透過此方式來下載這些內容。</li> <li>■ <b>自動</b> - 註冊時將內容部署至目錄或裝置上的其他部署 Hub。裝置註冊後，系統即會提示使用者將內容安裝在裝置上。 對於您企業及其行動使用者相當重要的內容，此選項為最佳的選擇。</li> </ul>

- b 在**限制索引標籤**中，輸入下列資訊。

設定	描述
取消註冊時移除	設定當裝置向 Workspace ONE UEM 取消註冊時，便將該應用程式從裝置上移除。Workspace ONE UEM 預設為啟用此設定。 如果啟用此設定，受監管的裝置會受無訊息應用程式安裝的限制。這是因為裝置已遭鎖定，而且佈建的設定檔安裝在需要解鎖裝置才能完成安裝的命令佇列中。 如果您停用此設定，則佈建設定檔不會隨已安裝的應用程式一起推播。亦即，更新佈建設定檔時，新的佈建設定檔不會自動部署到裝置。在這種情況下，需要具有新佈建設定檔的新版應用程式。
禁止應用程式備份	不允許將應用程式資料備份到 iCloud。但是應用程式本身仍可備份到 iCloud。
由 MDM 來管理使用者安裝的 APP	承擔使用者先前在其裝置上所安裝之應用程式 (不管是受監管或未受監管的應用程式) 的管理工作。 啟用此功能，使用者便不需要刪除裝置上所安裝的應用程式版本。使用者不需要在裝置上安裝 AirWatch Catalog 版本，Workspace ONE UEM 就能管理應用程式。

- c 在 **Tunnel 和其他屬性索引標籤**中，輸入下列資訊。

設定	描述
個別應用程式 VPN 設定檔	選取要用於應用程式的 VPN 設定檔。使用者可透過 VPN 存取應用程式，有助於確保應用程式的存取和使用都是可信賴且安全的。
其他屬性	應用程式屬性提供特定裝置詳細資料給應用程式使用。例如，當您想要設定與不同組織相關聯的網域清單時。

- d 在**應用程式組態索引標籤**中，輸入下列資訊。

設定	描述
上傳 XML	您可以上傳一個 XML 檔案，其中包含應用程式為了應用程式組態而支援的金鑰值配對。

- 4 選取**建立**。
- 5 選取**新增指派**，為您的出版新增更多指派。
- 6 透過設定應用程式指派的優先順序來設定彈性部署設定。

設定	描述
優先順序	從下拉式功能表中選取值，以設定指派的優先順序。 裝置會根據指派群組的優先順序設定，從指派群組接收應用程式。調整單一指派的優先順序將會自動重新排列其他指派的優先順序。
複製	從更多選項功能表中，選取 [複製] 以複製選取的指派。
刪除	從更多選項功能表中，選取 [刪除] 以移除選取的指派。

如需深入瞭解如何新增指派，請參閱 [Workspace ONE UEM 行動應用程式管理說明文件](#) 中的新增指派和排除項目至應用程式。

## 將內容指派到 Smartfolio

UEM 所管理存放庫是您可以儲存檔案的位置，讓您能將檔案指派到終端使用者裝置上的 Smartfolio 應用程式。

若要儲存檔案，您必須先在 [Workspace ONE UEM console](#) 上針對 UEM 所管理內容設定類別結構。根據設定的結構，這些檔案會以有條理的方式顯示在 Smartfolio 應用程式中。

---

**備註** 單一類別可指派子類別或檔案。具有子類別的類別無法指派給已發佈的內容。

---

您也可以根據內容的重要性來排列檔案的優先順序，這些檔案會依關聯性順序顯示在 Smartfolio 應用程式中。

關於設定 UEM 所管理類別結構和新增內容的資訊，請參閱 [為 UEM 所管理內容設定類別結構](#) 和 [將內容上傳至 UEM 所管理存放庫](#)。

## Smartfolio 的確認

Smartfolio 使用者現在可確認您指派給他們的文件為必要內容。在 [Workspace ONE UEM Console](#) 上，您可以在 [內容清單檢視] 和 [裝置詳細資料] 頁面中檢視這些確認。

在 [內容清單檢視] 頁面的 [安裝狀態] 欄位下選取 [檢視] 時，會出現一個快顯方塊，顯示已檢視並確認內容的確切使用者數目。

下列清單說明支援的文件確認功能：

- 當使用者開啟文件時，[已確認] 按鈕會顯示為停用狀態，並且在預設延遲五秒後啟用。可透過在 UEM console 上套用值 `AcknowledgementTimeInterval` 做為自訂的 SDK 設定，來將預設值變更為 0-600 秒的範圍。
- 系統不會提示使用者確認已確認的文件。
- 如果您將新版本標記為「必要」，則系統會提示使用者確認新版本的已確認文件。
- [裝置詳細資料] 頁面會顯示已確認的狀態和文件確認的日期。
- 「依裝置顯示內容詳細資料」報告包含個別裝置的已確認狀態。

## Smartfolio 的暫存內容支援

當終端使用者簽出裝置時，系統會清除多使用者裝置上暫存的內容。在這種案例下，在下次登入時，使用者必須重新下載內容。若要在終端使用者的裝置上取得任何受管理的內容，您必須為該內容啟用註冊預備模式。啟用註冊預備模式後，即使終端使用者簽入或簽出裝置後，暫存的內容仍會保留在終端使用者的裝置上。

只有在使用者被指派了內容時，該內容才可供簽出裝置的新使用者使用。如果未將內容指派給新使用者，則系統會清除內容。

若要啟用內容的註冊預備模式，請在 Workspace ONE UEM Console 上新增下列組態金鑰。

設定金鑰	值類型	支援的類型	描述
{ "RetainContentBetweenCheckoutSessions": true }	布林值	True = 啟用 False (預設值) = 停用	設定為 true 時，下載的內容會在裝置簽入和簽出工作階段期間保留，且不會遭到清除。 設定為 false 時，下載的內容會在裝置簽入和簽出工作階段期間遭到清除，且不會保留。

### 使用預設的 SDK 設定檔啟用暫存內容支援

在預設的 SDK 設定檔中新增組態金鑰，以針對在 Smartfolio 應用程式上下載的受管理內容啟用暫存模式。

- 1 導覽至 **群組 & 設定 > 所有設定 > 應用程式 > 設定和原則 > 設定**。
- 2 選取**啟用自訂設定**，然後依據您的需求，輸入組態金鑰。

```
{
  "CustomAppSettings": {
    "com_vmware_folio": {
      "SharedDeviceSettings": {
        "RetainContentBetweenCheckoutSessions": true
      },
    }
  }
}
```

- 3 選取**儲存**。

### 使用自訂 SDK 設定檔啟用暫存內容支援

在自訂 SDK 設定檔中新增組態金鑰，以便在 Smartfolio 應用程式上啟用受管理內容的暫存模式。

- 1 導覽至**群組與設定 > 所有設定**。
- 2 如果您具有現有的自訂設定檔，請導覽至**應用程式 > 設定與原則 > 設定檔 > 自訂設定檔 > 自訂設定**。
- 3 如果要新增自訂設定檔，請導覽至 **APP > 設定和原則 > 設定檔 > 新增設定檔 > SDK 設定檔 > iOS > 自訂設定**。
- 4 依據您的需求，從 [自訂設定] 中選取**設定**並輸入組態金鑰。

```
{
  "CustomAppSettings": {
    "com_vmware_folio": {
      "SharedDeviceSettings": {
        "RetainContentBetweenCheckoutSessions": true
      },
    }
  }
}
```

- 5 選取**儲存**。

## Smartfolio 的預設索引標籤變更設定

登入 Smartfolio 應用程式時，終端使用者會先登陸預設首頁索引標籤。若要協助使用者輕鬆存取必要的內容，且在應用程式中進行最少的導覽，您可以將使用者最常存取的索引標籤設定為預設登陸索引標籤。您可以使用 Workspace ONE UEM Console 上的自訂設定，將預設首頁索引標籤變更為其他可用的索引標籤。

若要將預設的索引標籤從首頁變更為其他可用的索引標籤，請在 UEM console 中新增下列組態金鑰。

設定金鑰	值類型	支援的類型	描述
{DefaultBottomBarTab: 0}	整數	首頁 - 0 所有檔案 - 1 最近 - 2 我的最愛 - 3 下載 - 4	Smartfolio 應用程式的預設索引標籤會根據所選支援的值來設定。

### 使用預設 SDK 設定檔變更預設索引標籤

您可以在預設的 SDK 設定檔中新增組態金鑰，以變更 Smartfolio 應用程式的預設登陸索引標籤。

- 1 導覽至 **群組與設定 > 所有設定 > APP > 設定和原則 > 設定**。
- 2 選取 **啟用自訂設定**，然後依據您的需求，輸入組態金鑰。

```
{
  "CustomAppSettings": {
    "com_vmware_folio": {
      "DefaultBottomBarTab": 1
    }
  }
}
```

- 3 選取 **儲存**。

### 使用自訂 SDK 設定檔變更預設索引標籤

您可以在自訂 SDK 設定檔中新增組態金鑰，以變更 Smartfolio 應用程式的預設登陸索引標籤。

- 1 請導覽至 **群組 & 設定 > 所有設定**。
- 2 如果您有現有的自訂設定檔，請導覽至 **應用程式 > 設定與原則 > 設定檔 > 自訂設定檔 > 自訂設定**。
- 3 如果要新增自訂設定檔，請導覽至 **APP > 設定和原則 > 設定檔 > 新增設定檔 > SDK 設定檔 > iOS > 自訂設定**。
- 4 依據您的需求，從 [自訂設定] 中選取 **設定** 並輸入組態金鑰。

```
{
  "CustomAppSettings": {
    "com_vmware_folio": {
      "DefaultBottomBarTab": 1
    }
  }
}
```

5 選取儲存。

# 使用 Workspace ONE 主控台管理內容

# 7

內容管理解決方案提供您多個選項來管理從 Workspace ONE UEM 主控台儲存、同步或部署的內容。

## 功能

內容管理解決方案提供下列管理內容的功能：

- 內容管理儀表板可用於快速概覽使用者和受管理的內容。
- 清單檢視可用於檢視並管理內容。
- 內容設定功能表可為不同類型的內容配置存放庫、儲存空間、部署和管理選項。

## 內容管理功能表選項

除了這個在主控台內的預設視圖外，還有幾個其他的畫面可以簡化內容管理。這些都顯示在 UEM 主控台之內容儀表板左側的次要導覽功能表中。

檢閱內容管理可用的功能表選項。

設定	描述
清單檢視	清單檢視可在 [UEM 所管理伺服器] 與 [企業檔案伺服器] 間切換。
存放庫	選取存放庫以存取存放庫配置選項。存放庫有兩種：管理員新增的存放庫和使用者新增的存放庫。使用者可以使用您在主控台內所配置的範本來新增存放庫。
類別	新增類別與子類別。已新增的類別會以清單檢視的方式顯示在畫面中，並且帶有動作功能表。
精選內容	此畫面可管理您從清單檢視或類別清單檢視中所加入的精選內容。將精選內容放在 VMware Workspace ONE Content 中最醒目的位置，讓終端使用者能夠輕易地存取高使用量的內容。使用拖放功能或刪除不相關的內容，利用此畫面控制精選內容在 Workspace ONE Content 中的顯示順序。
批次狀態	執行批次匯入，並在此畫面上審視批次上傳之檔案的詳細資料。
設定	選取此項，以存取特定內容的設定。

## 行動內容管理儀表板

內容管理儀表板是預設的內容檢視，可在此檢視並管理裝置團隊的一般內容狀態。使用主控台的集中式頁面，可立即獲得使用者的相關資訊，以分析制定商務決策的內容，並根據警告採取行動。

下列是顯示在儀表板上的不同檢視畫面和參數。

設定	描述
儲存歷程記錄	利用 6 個長條方格的摘要圖來概述儲存空間的配額。
使用者/內容狀態	利用狀態圖示，快速歸納各種內容的合規性。(當把游標懸浮在這些圖示時) 每個圖示上所出現的百分比，代表有問題的裝置或檔案的百分比。選擇這些圖示來檢視違規的裝置並對這些裝置採取適當的管理動作。
內容的參與狀況	瞭解哪些文件最實用和最受您的終端使用者歡迎，以及哪些文件是您應該考慮棄用的。點選所顯示的訊息，直接導覽至可讓您編輯內容的畫面。
使用者明細	關於終端使用者今日、本週或本月活動的資訊。這些圖示即代表您的終端使用者，而把游標懸浮在這些圖示時，也會顯示有多少百分比的終端使用者目前正處於使用中狀態。

## 內容管理清單檢視

在 Workspace ONE UEM console 內容清單檢視中，對上傳的 UEM 所管理內容或同步的 [企業檔案伺服器] 內容採取動作。「內容清單檢視」自動填入您在上傳內容或存放庫時所輸入的資訊，以此提供您所有內容概覽。

導覽至 [內容 > 清單檢視](#) 來存取此清單。

設定	描述
已納管的 UEM	檢視並管理您已在此預設清單檢視中直接新增到 UEM 主控台的內容。
UEM 所管理功能表	使用可用的清單檢視選項，對 UEM 所管理內容採取動作。 <ul style="list-style-type: none"> <li>■ <b>新增內容</b> – 選取此項目以將 UEM 所管理內容新增至 UEM console。</li> <li>■ <b>已使用的儲存空間</b> – 檢視狀態列，瞭解終端使用者已使用了多少百分比的已分配儲存空間。</li> </ul>
企業檔案伺服器	檢視並管理在此清單檢視中已同步的存放庫，或者使用個別存放庫的內容清單檢視。
企業檔案伺服器功能表	若要在清單檢視中顯示配置的存放庫，請選取 <b>顯示存放庫</b>
篩選條件	使用適當的篩選條件來尋找所要的文件。 <ul style="list-style-type: none"> <li>■ <b>類別</b> – 使用 UEM 主控台指派的類別來篩選內容。</li> <li>■ <b>類型</b> – 按照檔案類型來篩選內容。</li> <li>■ <b>到期狀態</b> – 篩選內容以僅顯示將在 14 天內到期的內容。</li> </ul>
啟用/停用	關於終端使用者內容可用性的資訊。 <ul style="list-style-type: none"> <li>■ 綠色圓圈顯示在「使用中」的內容旁邊。</li> <li>■ 紅色圓圈顯示在「停用」的內容旁邊。您無法搜尋、檢視或將停用的內容自動傳送到裝置。</li> </ul>
名稱	在新增內容時，選取此項來編輯您要配置的一般 <b>資訊</b> 、 <b>詳細資料</b> 、 <b>先前版本</b> 、 <b>安全性</b> 、 <b>指派</b> 和 <b>部署</b> 等資訊。您還可以下載或刪除先前內容的版本。
動作功能表	使用適用的功能表選項來管理您的內容。兩個「內容清單檢視」動作功能表稍有差異。針對 UEM 所管理內容，選取單一檔案時會顯示 [檢視裝置]、[新增版本]、[下載] 以及 [更多動作]。選取多個檔案時，僅會顯示 [更多動作] 功能表。在 [更多動作] 功能表中，選取 [刪除] 可同時移除多個檔案。



## 內容管理選項

使用這些選項來管理「清單檢視」中已上傳或同步的內容和中繼資料，以及 Workspace ONE UEM 主控台上的其他功能表。

動作	UEM 代管	企業 檔案伺服器	自動 範本	手動 範本	使用者新增 存放庫	類別
<b>編輯</b>						
管理個別檔案的設定。已編輯的設定只會影響個別檔案，而不會影響整個存放庫的設定。	✓	✓	✓	✓	✓	
下載先前檔案版本的本機複本。	✓					
從主控台中刪除先前檔案版本。	✓					
將現有的檔案更新為新版本，並封存原檔。	✓					
<b>刪除</b>						
在 UEM 主控台中移除檔案。	✓					
在 UEM 主控台中移除檔案中繼資料。		✓	✓	✓	✓	
開始在網路內容與 Workspace ONE UEM 之間進行手動同步。		✓	✓	✓	✓	
在 UEM 主控台中移除空的子類別或空的類別。						✓
<b>新增</b>						
將現有的檔案更新為新版本，並封存原檔。	✓					
將子類別新增至類別。						✓
<b>同步</b>						

動作						
開始在 Workspace ONE UEM 與已整合的企業檔案伺服器之間進行同步。		✓	✓	✓	✓	
檢視裝置						
開啟裝置清單，檢視已獲指派個別檔案的裝置。	✓	✓	✓	✓	✓	
將個別檔案推播至所選裝置。	✓	✓	✓	✓	✓	
從所選裝置刪除個別檔案。	✓	✓	✓	✓	✓	
其他選項						
新增至精選內容的檔案會顯示在 VMware Workspace ONE Content 中最醒目的位置。	✓	✓	✓	✓	✓	✓
下載所選的內容的複本。	✓	✓	✓	✓	✓	
在 UEM 主控台中移除檔案。	✓					
在 UEM 主控台中移除檔案中繼資料。		✓	✓	✓	✓	

## 內容管理設定

內容管理設定包含各種與內容管理有關的配置。

若要存取可用配置的功能表，請選取**設定**。

設定	描述
應用程式	存取 VMware Workspace ONE Content 和 VMware Content Locker Sync 的配置畫面。
Content Gateway	<p>配置 Content Gateway 並下載安裝程式。</p> <p>從 Workspace ONE UEM console 版本 9.6 開始，設定 Content Gateway 節點時，建議的安裝類型為 Unified Access Gateway (UAG)。您可以使用此選項在 Unified Access Gateway 上設定新的 Content Gateway，或將您現有的 Content Gateway 轉移至 Unified Access Gateway。</p> <p>如需在 Unified Access Gateway 上設定 Content Gateway 的詳細資訊，請參閱 UAG 說明文件中的〈Unified Access Gateway 上的 Workspace ONE UEM 元件〉。如需移轉的詳細資訊，請參閱「將 Content Gateway 移轉至 Unified Access Gateway」說明文件。</p>
使用者儲存空間	為個別使用者配置使用者儲存空間的例外狀況。這些例外狀況能將儲存空間指派至最細微的層級，並覆寫個人內容中組織或使用者群組的配置集。
進階	配置檔案類型限制、入門培訓和要求入門培訓的內容，以及與第三方電子簽名提供者整合。