行動電子郵件管理

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 行動電子郵件管理解決方案是什麼？ 1

能在裝置上查看公司資料可提供方便性，並提高生產力，但同時也帶來了安全性和部署方面的挑戰。為克服此類挑戰，Workspace ONE UEM powered by AirWatch 行動電子郵件管理 (MEM) 解決方案，可為貴公司的電子郵件基礎架構提供全面的安全保障。使用 Workspace ONE UEM powered by AirWatch 來管理您的行動 Email 部署。

能在裝置上查看公司資料可提供方便性，並提高生產力，但同時也帶來了安全性和部署方面的挑戰。為克服此類挑戰，Workspace ONE UEM powered by AirWatch 行動電子郵件管理 (MEM) 解決方案，可為貴公司的電子郵件基礎架構提供全面的安全保障。

各種挑戰

行動 Email 雖然提供了很多優點，但也帶來了下列各種更大的挑戰：

- 跨裝置類型、作業系統和 Email 用戶端佈建 Email。
- 在非安全的網路中保全 Email 之存取。
- 保護來自第三方應用程式的機密資訊。
- 限制未授權、遺失或遭竊的裝置存取 Email 之權限。
- 在透過第三方的閱讀程式應用程式讀取 Email 附件時，防止遺失或隨意散發該附件。

行動 Email 管理 (MEM) 的優點

Workspace ONE UEM powered by AirWatch MEM 提供所需的各種要素以建立成功又安全的行動 Email 部署。以下是使用 MEM 的部分優點：

- 強制 SSL 安全性
- 隔空配置 Email
- 偵測現有的未受管裝置
- 防止 Email 資料遺失
- 封鎖未受管裝置存取 Email 的權限
- 限制只有公司核准的裝置才能存取 Email
- 使用憑證的整合和撤銷功能。

MEM 需求

在您繼續使用 VMware AirWatch® Mobile Email Management® (MEM) 解決方案前，請先驗證本節提到的瀏覽器需求。

免責聲明

不保證與第三方產品的整合，且取決於第三方的解決方案是否正常運作。

支援的瀏覽器

Workspace ONE UEM 主控台支援下列網頁瀏覽器最新的穩定版本：

- Chrome
- Firefox
- Safari
- Internet Explorer 11
- Microsoft Edge

備註 如果您正在使用 IE 來存取 UEM 主控台，請導覽至**控制面板 > 設定 > 網際網路選項 > 安全性**，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。

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 Workspace ONE 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，可能會有些許問題。

Email 基礎結構管理的部署模式

2

為了保護和管理您的電子郵件基礎架構，Workspace ONE UEM 提供了兩種類型的部署模式：Proxy 模式和直接模式。

您可使用下列 Email 部署模式之一，與您在 UEM console 中定義的 Email 原則，來有效管理您的行動裝置。

- 在 Proxy 部署模式中，會在 Workspace ONE 伺服器與公司 Email 伺服器之間放置個別的伺服器，稱為 Secure Email Gateway (SEG) Proxy 伺服器。所有由裝置送往 Email 伺服器的要求，都會經過這部代理伺服器的篩選，且只會為經核准的裝置轉送流量。公司的 Email 伺服器無需直接與行動裝置通訊，便能藉此獲得保護。
- 在直接部署模式中，不再有 Proxy 伺服器的參與，且 Workspace ONE UEM 會直接與 Email 伺服器通訊。由於這種模式沒有代理伺服器，因此安裝與配置的步驟都會簡化。

備註 Proxy 部署模式有兩個變體，即 [傳統] 和 [SEG v2] 平台。不再支援傳統的 SEG 平台，因為 SEG V2 平台可確保提供高於傳統平台的效能。SEG V2 平台可安裝在現有 SEG 伺服器上，只需要最少的停機時間，並可在升級期間執行，不必變更設定檔，也不需要與終端使用者互動。

部署模式	配置模式	郵件基礎結構
Proxy 部署模式	Microsoft Exchange 2010/2013/2016 Exchange Office 365	Microsoft Exchange 2010/2013/2016/2019 Exchange Office 365 HCL Domino w/ HCL Gmail
直接部署模式 - PowerShell	PowerShell 模式	Microsoft Exchange 2010/2013/2016/2019 Microsoft Office 365
直接部署模式 - Gmail	Gmail	

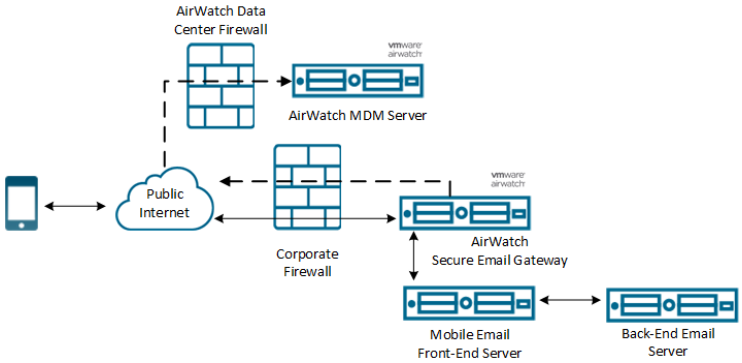
備註 Workspace ONE UEM 僅支援 Email 伺服器提供者目前支援的第三方 Email 伺服器版本。提供者取代伺服器版本時，Workspace ONE UEM 將不再支援與已淘汰版本整合。

安全 Email 閘道 Proxy 模式

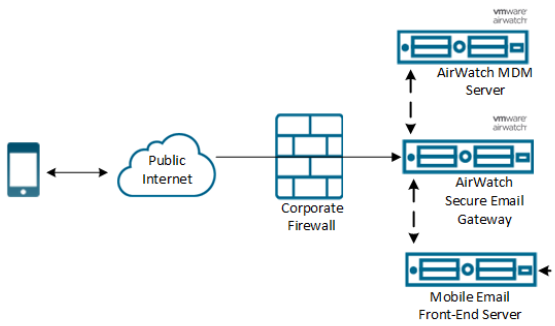
安全 Email 閘道 (SEG) 代理伺服器是一個單獨的伺服器，與您現有的 Email 伺服器一併安裝以代理所有通到行動裝置上的 Email 流量。根據您在 UEM 主控台中所定義的設定，SEG Proxy 伺服器會允許或封鎖其所管理的每台行動裝置。

所有由裝置送往 Email 伺服器的要求，都會經過 SEG 代理伺服器的篩選，且只會為經核准的裝置轉送流量。此轉送功能不允許任何裝置與公司的 Email 伺服器通訊，以保護該伺服器。

將 SEG 伺服器安裝在您的網路上，使其與企業的 Email 流量一致。您也可以將該伺服器安裝在 DMZ 區中，或是安裝在反向代理伺服器後方。無論您的 Workspace ONE MDM 伺服器是在雲端或是在內部部署，您都必須在資料中心內裝載 SEG 伺服器。



Cloud Architecture

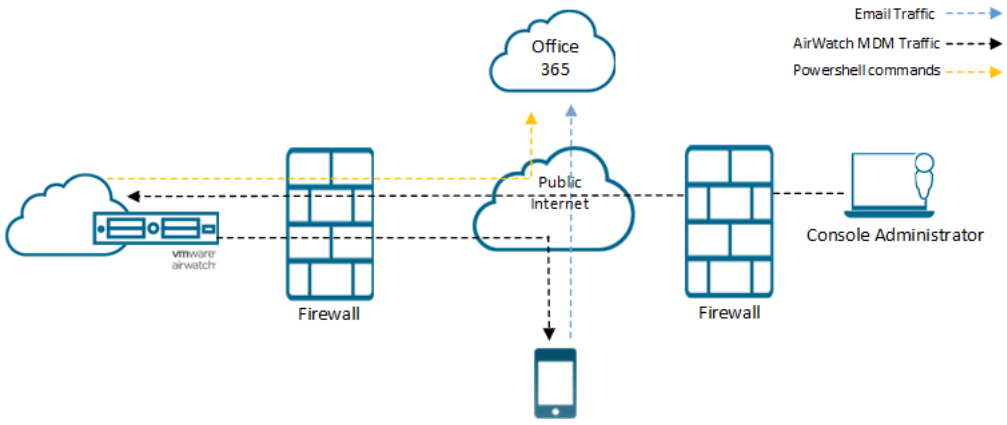


On-premise Architecture

直接部署 PowerShell 模式

在 PowerShell 模式中，Workspace ONE UEM 採用 PowerShell 管理員身份，將指令發送到 Exchange ActiveSync (EAS) 基礎結構，再依照 UEM console 定義的原則來允許或拒絕存取 Email。PowerShell 部署不需要使用單獨的 Email 代理伺服器，而且其安裝過程也較爲容易。

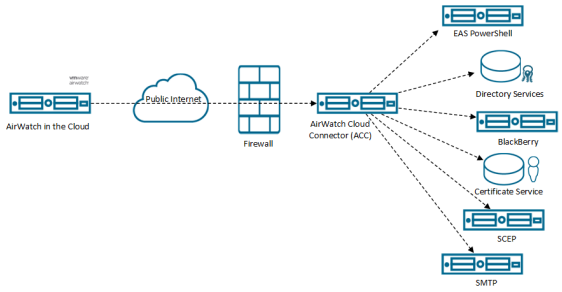
PowerShell 部署適用於使用 Microsoft Exchange 2010、2013、2016、2019 或 Office 365 的組織。



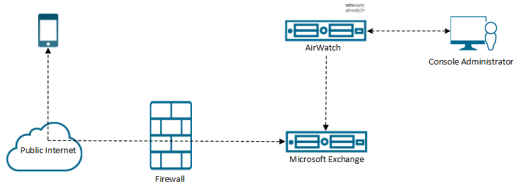
Microsoft Office 365

根據 Workspace ONE UEM 伺服器與 Exchange 伺服器的所在位置，而有兩種發送 PowerShell 指令的方式：

- 當 Workspace ONE 伺服器部署於雲端而 Exchange 伺服器部署於內部時 - Workspace ONE UEM 伺服器會發送 PowerShell 指令。VMware 企業系統 Connector 會使用 Email 伺服器來設定 PowerShell 工作階段。
- Workspace ONE UEM 伺服器與 Email 伺服器在內部部署 - Workspace ONE UEM 伺服器會直接與 Email 伺服器設定 PowerShell 工作階段。此情形便不需要使用 VMware Enterprise Systems Connector 伺服器，除非 Workspace ONE UEM 伺服器無法直接與 Email 伺服器通訊。



Microsoft Exchange 2010 with AirWatch Cloud



Microsoft Exchange 2010 with AirWatch On-Prem

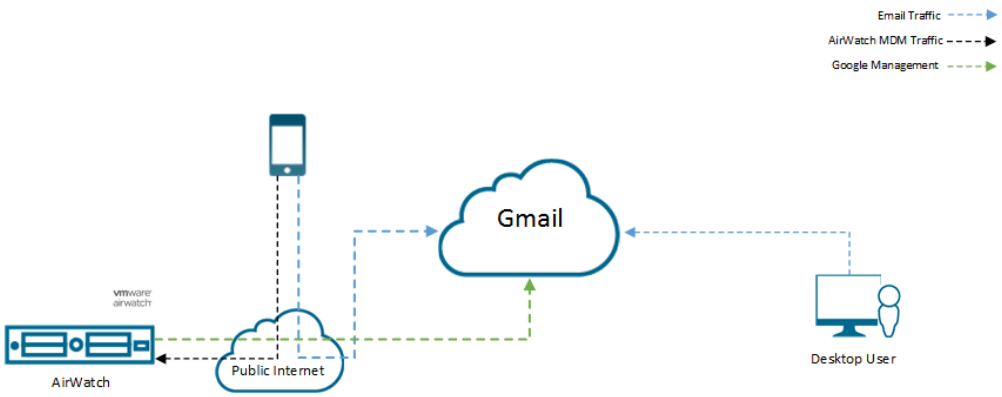
若需要在 Secure Email Gateway 與 PowerShell 部署模式之間作抉擇，請參閱〈Workspace ONE UEM 建議〉一節，以取得相關的協助。

Gmail 直接模式

整合 Workspace ONE UEM 伺服器與 Google。

使用 Gmail 基礎結構的企業，或許已相當瞭解保護 Gmail 的 Email 端點和防止郵件繞過安全端點所面臨的挑戰。Workspace ONE UEM 提供您安全又有彈性的方法來整合並保護您的 Email 基礎結構，以應付這些挑戰。

在直接 Gmail 部署模式中，Workspace ONE UEM 伺服器能與 Google 直接通訊。根據安全性需求，Workspace ONE 可以管理使用者的 Google 密碼，並控制使用者信箱的存取權。



API 呼叫 Google 套件 - 您可以藉由指定備用屬性而非使用者電子郵件地址，自訂用於 Google 套件的 API 呼叫。依預設，會採用使用者的電子郵件地址。如需如何設定 Gmail 直接模式的詳細資訊，請參閱使用密碼管理的直接整合模式。

MEM 部署模式矩陣

使用以下功能對照表比較不同 MEM 部署模式中可用的功能。

Office 365 對於 SEG Proxy 模式需要其他額外的配置。Workspace ONE UEM 建議針對雲端式 Email 伺服器使用直接整合模式。如需詳細資訊，請參閱〈Workspace ONE UEM 建議〉一節。

✓	支援	□	不受 Workspace ONE UEM 支援
X	不提供該功能	N/A	不適用

表 2-1. 部署對照表

	SEG 代理伺服器模式			直接模式		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365 (PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Email 安全性工具						
加強的安全性設定						
透過 S/MIME 功能來使用數位簽名	✓	□	□	✓	✓	N/A
強制加密來保護機密資料	✓	✓	✓	✓	✓	✓
強制執行 SSL 的安全性	✓	✓	✓	✓	✓	✓
Email 附件和超連結的安全性						
強制附件和超連結只能在 VMware AirWatch Content Locker 或 Workspace ONE Web 中開啟	✓	✓	✓	x	x	x
自動的 Email 配置						
隔空配置裝置上的 Email	✓	✓	✓	✓	✓	✓
Email 存取權的控管						
封鎖未受管裝置存取 Email 的權限	✓	✓	✓	✓	✓	✓

表 2-1. 部署對照表 (續)

	SEG 代理伺服器模式			直接模式		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365 (PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
偵測現有的未受管裝置	✓	✓	✓	✓	✓	N/A
透過自訂的合規原則來存取 Email	✓	✓	✓	✓	✓	✓
需要加密裝置以存取 Email	✓	✓	✓	✓	✓	✓
禁止遭破解的裝置存取 Email	✓	✓	✓	✓	✓	✓
允許/封鎖 Email - 郵件用戶端	✓	✓	✓	✓	✓	x
Email 存取權的控管						
允許/封鎖 Email - 使用者	✓	✓	✓	✓	✓	x
允許/封鎖 Email - 裝置型號	✓	✓	✓	✓	✓	✓
允許/封鎖 Email - 裝置作業系統	✓	✓	✓	✓	✓	✓
允許/封鎖 Email - EAS 裝置類型	✓	✓	✓	✓	✓	x
管理可見度						
Email 流量統計資料	✓	✓	✓	x	x	x
Email 用戶端統計資料	✓	✓	✓	x	x	x
憑證管理						
CA 整合/撤銷	✓	□	□	✓	✓	N/A
架構						
內嵌閘道 (代理伺服器)	✓	✓	✓	N/A	N/A	✓
Exchange PowerShell	N/A	N/A	N/A	✓	✓	N/A
Gmail 密碼管理	N/A	N/A	✓	N/A	N/A	✓
Gmail 目錄 API 整合	N/A	N/A	N/A	N/A	N/A	✓
支援						

表 2-1. 部署對照表 (續)

	SEG 代理伺服器模式			直接模式		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365 (PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Workspace ONE Boxer iOS 版和 Android 版 [^]	✓	✓	✓	✓	✓	✓
iOS 本機 Email 用戶端	✓	✓	✓	✓	✓	✓
Android 原生 Email 用戶端 (Gmail)	✓	✓	✓	✓	✓	✓
Android HCL Notes 用戶端*	N/A	✓	N/A	N/A	N/A	N/A

*Android HCL Notes 用戶端並不支援電子郵件附件和超連結的安全性。

+ 不支援 Exchange 2003

^ Workspace ONE Boxer 不支援 Exchange 2003、必要的 ActiveSync 設定檔及多重 MEM。

Workspace ONE UEM 建議事項

本節將列出 Workspace ONE UEM 所支援的功能與適合的部署大小。用決策矩陣來選擇最符合您需求之部署方式。

附件加密

透過在行動裝置上強制執行附件的加密，Workspace ONE UEM 可幫助您保持 Email 附件的安全性，而不會妨礙使用者的操作體驗。

	本機	Traveler	Workspace ONE Boxer
iOS	✓		
Android	✓		
只有已經在 UEM 主控台上對於 Boxer 應用程式組態啟用附件加密和超連結轉換的情況下，SEG 才支援 Workspace ONE Boxer 的這些功能。 SEG 支援 Exchange 2010/2013/2016/2019 和 Office 365 的附件加密。			

備註 SEG 不會加密 Workspace ONE Boxer 的附件，但可以在應用程式層級強制執行 DLP。

Email 管理

該清單列出能夠為您提供最輕鬆的部署和管理方法，以及最高層次的安全性。

電子郵件基礎結構	Gmail	PowerShell	安全 Email 閘道 (SEG)
雲端郵件基礎結構			
Office 365		✓	✓
Gmail	✓		✓
內部部署 Email 基礎結構			
Exchange 2010		✓	✓
Exchange 2013		✓	✓
Exchange 2016		✓	✓
Exchange 2019		✓	✓
HCL Notes			✓

所有部署超過十萬台裝置的內部部署 Email 基礎架構，^請使用 Secure Email GatewaySecure Email Gateway (SEG)。少於十萬台裝置的部署，亦可選擇使用 PowerShell 來管理 Email。詳情請參閱安全 Email 閘道與 PowerShell 決策矩陣的比較。

**PowerShell 實行閾值是根據最新且完整的效能測試組而取得的，此值可能會在每次新版本發行時有所變動。當部署規模不超過五萬台裝置時，預期同步和執行合規性的時間會相當快速 (不到 3 小時)。部署將近十萬台裝置時，管理員所預期同步和執行合規程序的時間會隨之增加到 3 – 7 小時。

安全 Email 閘道與 PowerShell 決策矩陣的比較

下方對照表說明 SEG 和 PowerShell 的部署功能，協助您選擇符合您需求的部署模式。

	優點	缺點
SEG	■ 即時合規性 ■ 附件加密 ■ 超連結轉換	■ 需要其他伺服器
PowerShell	■ Email 管理不需要其他的內部部署伺服器 ■ 郵件流量在經路由傳送到 Office 365 之前，不會經路由傳送到內部部署伺服器，所以不需要 ADFS	■ 不需要即時合規同步 ■ 不適合用於大型部署 (十萬台以上的裝置)
Microsoft 建議您使用 Active Directory Federated Services (ADFS) 來禁止直接存取 Office 365 的 Email 帳戶。		

將電子郵件基礎架構移轉至 Workspace ONE UEM

3

您可以使用 Workspace ONE UEM 將您的 Email 移轉至 Mobile Email Management (MEM) 模式。移轉至下列其中一個 MEM 模式，您就能強制執行 Email 存取控制原則，從而確保 Email 的存取權只會提供給已核准的使用者與裝置。

- Secure Email Gateway (SEG)
- PowerShell
- Gmail

移轉至安全 Email 閘道

Email 移轉至 Secure Email Gateway (SEG) 可讓使用者僅透過 SEG Proxy 存取 Email。

使用 SEG 強制執行 Email 的存取控制原則，僅將存取權給予核准的使用者和裝置。附件加密原則可確保資料的安全性。

1 在 Workspace ONE UEM Console，請在 [全域] 下方針對您需要的組織群組配置 SEG。。

2 下載並安裝 SEG。。

3 使用 Email 合規原則來測試 SEG 的功能。

   a 暫時停用所有合規性原則。

   b 要求所有使用者向 Workspace ONE UEM 註冊其裝置。

   c 在所有註冊裝置上，佈建新的 Email 設定檔 (以 SEG 伺服器的 URL 作為主機名稱)。

   d 定期提醒擁有未受管裝置的使用者，請他們向 註冊。Workspace ONE UEM

   e 若要在特定的日期封鎖 EAS 存取郵件伺服器，請修改防火牆 (或是威脅管理閘道) 規則。這樣便可確定行動裝置直接存取郵件伺服器的權限已遭封鎖。

   f 啟用所有合規性原則。

備註 現有的網頁郵件、Outlook Web Access (OWA) 和其他的 Email 用戶端可以繼續存取郵件伺服器。

移轉至 PowerShell

移轉至 PowerShell 能保護您的裝置，並讓裝置的 Email 與 Exchange 或 Office 365 同步。

PowerShell 能探索受管理與未受管理的裝置，並透過 Email 存取權控制原則的協助，只將存取權授與核准的使用者與裝置。

1 在 Workspace ONE UEM console，請在 [全域] 下方針對您需要的組織群組設定 PowerShell 整合。

2 配置與使用者群組的整合 (自訂或事先定義的)。

3 透過使用者子集來測試 PowerShell 的功能 (例如：測試使用者) 來確保下列功能都能正常運作：

   a 同步處理 Email 伺服器以偵測裝置。

   b 即時存取控管。

4 暫時停用所有合規性原則。

5 以 Email 伺服器的主機名稱，為已經在 Workspace ONE UEM 中註冊的所有裝置，佈建一個新的 Email 設定檔。

6 與 Email 伺服器同步，來尋找所有同步 Email 的裝置 (受管與未受管的)。

7 定期提醒擁有未受管理裝置的使用者，請他們向 Workspace ONE UEM 註冊。

8 若要在特定日期封鎖所有不合規裝置 (包含未受管理裝置) 的 Email 存取權，請啟用並強制執行合規性規則。

9 設定 Email 伺服器，依預設來封鎖所有的裝置。

備註 電子郵件儀表板會將未受管理的裝置清單顯示為已封鎖，以及顯示允許存取電子郵件的受管理裝置。

整合 Gmail 與 Workspace ONE UEM

移轉至 Gmail 便能將您的裝置與 Gmail 伺服器同步。您可以選擇是否使用 Secure Email Gateway (SEG) 來整合 Gmail，也可以直接使用目錄 API 來整合。

1 啟用 Gmail 的單一登入 (SSO) 選項，或是建立服務帳戶憑證。

2 利用 MEM 組態精靈，在 Workspace ONE UEM Console 上設定 Gmail 整合。

3 利用新的隨機密碼，提供使用者佈建的 EAS 設定檔。未收到此設定檔的裝置即會自動被封鎖而無法存取 Gmail。

移轉裝置

您可以使用 Workspace ONE UEM 跨組織群組和 MEM 部署來移轉裝置。

1 在 Workspace ONE UEM Console，導覽至 **Email 儀表板**。

2 篩選目前在 MEM 部署下的受管理裝置。

3 在**清單檢視**頁面中，選取全部的裝置，並從下拉式選單中，點選**系統管理 > 移轉裝置**。

4 在**移轉裝置確認**頁面中，輸入您所取得的金鑰代碼來確認移轉，並選擇您要部署在裝置上的配置。

5 按一下**繼續**。

結果

在執行這些步驟之後，Workspace ONE UEM 便會自動移除先前所使用的 Exchange ActiveSync (EAS) 設定檔，並藉由目標部署群組來推送新的 EAS 設定檔。然後，裝置便會與其新的部署群組建立連線。Email 儀表板上會顯示該裝置已更新的 MEM 組態名稱。

設定行動電子郵件管理部署

4

只要幾個簡單的步驟，即可利用 Mobile Email Management (MEM) 配置精靈來整合您的 Email 基礎結構。MEM 只能在父組織群組中設定，無法在子組織群組中覆寫。

單一 MEM 配置可以與一或多個 Exchange ActiveSync (EAS) 設定檔建立關聯性。

1 導覽至 **Email** > **設定**，然後點選**配置**。

2 選擇部署模式，再選擇 Email 類型。選擇**下一步**。

a 如果部署模式是「Proxy」，請選擇 Email 類型。

從下列項目中選擇：

- Exchange
- Google
- HCL Notes

b 如果部署模式是「直接」，請選擇 Email 類型。

從下列項目中選擇：

- Exchange
- 具有 Direct API 的 Google 應用程式
- 使用密碼佈建的 Google 應用程式 - 並為 Gmail 部署類型選擇保留密碼或不保留密碼。

如需部署方法的詳細資訊，請參閱〈Email 部署類型〉一節。

3 輸入所選部署類型的詳細資料。

從下列項目中選擇：

- 若為 SEG 部署：
  1. 輸入此部署的暱稱。
  2. 輸入 SEG Proxy 伺服器詳細資訊。
- 對於 PowerShell 部署：
  1. 輸入此部署的暱稱。
  2. 輸入 PowerShell 伺服器、驗證和同步設定的詳細資料。

- 對於 Gmail：
  1. 輸入此部署的暱稱。
  2. 輸入 Gmail 設定、驗證、Gmail 目錄 API 整合與 SEG Proxy 設定的詳細資料。

4. 建立範本 EAS 設定檔與 MEM 部署的關聯，再選取**下一步**。
   a. 建立用於此部署的 EAS 範本設定檔。

      新的設定檔並不會自動發佈到裝置上。您可以從「設定檔」的頁面，將裝置發佈到您的裝置上。

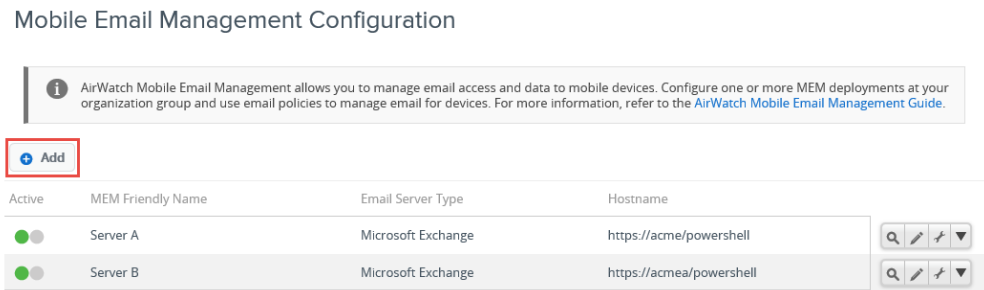
   b. (可選) 若要在單一企業群組中設定多個 MEM 部署，請將現有的設定檔與此部署相關聯。

   MEM 配置摘要頁面會顯示該配置的詳細資料。
5. **儲存**設定。
6. 一旦儲存完畢後，您即可在此部署中新增進階設定。
   a. 選取與您部署對應的**進階**圖示  。
   b. 依照**行動 Email 管理進階配置**頁面中的每項要求，來配置可用於使用者郵箱的各種設定。
   c. 選取**儲存**。

下一步

若要設定多個 MEM 部署，請選取**新增** (位於 **Mobile Email Management 進階配置**的首頁)，然後執行步驟 2 到 7。

在 SEG 部署中，您可藉由使用  下方的**設為預設值**選項，來將某個配置指派為預設值。



備註

- 在將多重的 PowerShell 環境連結到同一個 Exchange 伺服器時，您必須手動建立各自專用的使用者群組。
- 連結多重的 Gmail 環境時，請在配置中使用不同的網域。
- 只有在使用適當設定移轉 MEM 部署的過程中，才能考慮將 SEG 和 PowerShell 整合連接到相同的 Email 環境。Workspace ONE 支援團隊可協助您實行此作業。

啟用憑證式 Email

為標準使用者名稱和密碼認證使用憑證有各種好處，因為憑證能針對未經授權的存取進行更嚴謹的驗證。此外，也可省去終端使用者必須輸入密碼或每月更新密碼的麻煩。收件者間的敏感性的 Email 可透過 S/MIME 加密，或由您的訊息簽名加以核准。

1 導覽至**裝置 > 設定檔與資源 > 設定檔**。

2 選取**新增 > 新增設定檔**，然後選取所需的平台。

3 選擇**認證**設定檔的設定，然後進行配置。

a 在**認證來源**中，從可用的清單中選取任一項目。

從下列項目中選擇：

- **上傳** – 上傳憑證並輸入憑證的名稱。
- **定義的憑證授權單位** – 從您的企業群組下拉式功能表中，選擇 CA 和憑證範本。

使用**裝置 > 憑證 > 憑證授權機構**，新增企業群組的憑證授權機構和範本。

4 **儲存並發佈**設定。

設定 MEM 呼叫 Google 套件的使用者屬性

依預設，Gmail 部署會使用 Google API 來管理 Gmail 存取。傳送命令至 Google 時您可以透過使用者的電子郵件地址識別已註冊的使用者。或者，管理員也可以選取 Active Directory 的自訂屬性，而不是使用者的電子郵件地址來識別 Google 的使用者。

當 Google 電子郵件地址位於客戶的 Active Directory 的自訂屬性欄位時即可使用此自訂屬性。自訂屬性設定適用於使用密碼佈建的 Google 應用程式、具有 Direct API 的 Goolge 應用程式，以及具有自動密碼佈建部署方法的 SEG V2。

1 導覽至**帳戶 > 管理員 > 管理員設定 > 目錄服務 > 使用者**。Workspace ONE UEM 管理員可以對應自訂屬性值，並使用客戶 Active Directory 中的對應值。

2 在**目錄服務**頁面中啟用自訂屬性，輸入對應值，並同步 Active Directory 使用者以更新註冊使用者自訂屬性。如需啟用自訂屬性的詳細資訊，請參閱《在目錄服務整合中對應目錄服務使用者資訊》指南。

3 導覽至 **Email > Email 設定**，然後選取**配置**。設定平台閘道，然後選取**下一步**。

4 在**新增 Email 組態**頁面中，部署模式請選取**直接**，Email 類型請選取**具有 Direct API 的 Google 應用程式**，然後選取**下一步**。

5 在 [部署] 頁面中，輸入此部署的暱稱。輸入 Gmail 設定、驗證、Gmail 目錄 API 整合與 SEG Proxy 設定的詳細資料。

6 輸入 **Google 使用者電子郵件地址**。Google 使用者電子郵件地址的預設值為電子郵件地址。管理員可以選取自訂屬性，而不是預設的 Email 地址。

7 設定 Email 設定檔。參閱 第 6 章 設定 Email 設定檔 。

結果：

當 Google 電子郵件地址位於客戶的 Active Directory 的自訂屬性欄位時，您即可使用此自訂屬性。

將裝置指派至行動電子郵件管理

5

裝置註冊、將 Email 設定檔指派到裝置，以及裝置合規性狀態的變更，都會有所影響。MEM 配置會根據裝置上顯示的 EAS 設定檔指派給裝置。受管和「需要 ActiveSync 設定檔」合規原則可確保維持不允許未受管和手動配置的狀態。

具有 Exchange Active Sync (EAS) 設定檔的裝置

具有 EAS 設定檔的裝置與特定 MEM 配置建立關聯時，Workspace ONE UEM 會將原則更新傳送到該 MEM 配置。此功能會加速移轉和多個 MEM 配置，其中會有一或多個 Email 環境為受管理。

不論 Email 用戶端為何，所有的 Google MEM 模式都需要有 EAS 設定檔。若為新安裝，必須將 EAS 設定檔與 MEM 配置建立關聯。若為升級，管理員必須在升級程序完成時，建立 EAS 設定檔與 MEM 配置的關聯。

整合 SEG Proxy

Workspace ONE UEM 會針對已註冊裝置的組織群組，傳送廣播訊息給該組織群組的所有 MEM 配置。此訊息呈現裝置的合規狀態。合規變更時，將傳送更新的訊息。一旦裝置與特定的 SEG 伺服器連線後，SEG 便會根據先前所傳送的廣播訊息辨識裝置。然後 SEG Proxy 便會向 VMware AirWatch 報告已偵測到該裝置。Workspace ONE UEM 接著會使該裝置與 SEG 的 MEM 配置建立關聯，並在 Email 儀表板上顯示該裝置。

如果多部 SEG 伺服器負載平衡，則單一原則的廣播訊息僅會套用在一個 SEG。這包括在註冊、違規或修正時 Workspace ONE UEM Console 傳送到 SEG 的訊息。使用重新整理的間隔時間設為 10 分鐘的 Delta Sync，來協助處理剛註冊或合規的裝置。這些裝置等候 Email 開始同步的時間最長為 10 分鐘。

優點：

- 所有 SEG 伺服器更新的原則均來自相同的 API 來源。
- 對 API 伺服器的性能影響較小。
- 相較於 SEG 叢集化模式，減低了實作或維護的複雜度。
- 因為每個 SEG 各自負責自己的原則集，因此減少了故障點。
- 改善的使用者體驗。

整合 PowerShell

在原則更新方面，PowerShell MEM 配置與 SEG 的運作方式相同。若是移轉到 PowerShell，重要的是讓新的設定檔與 PowerShell MEM 配置建立關聯。與新設定檔建立關聯可減少與之前 MEM 配置的不必要通訊。

整合 Gmail

除了與 Google 目錄 API 整合之外，此部署類型必須要有設定檔。除非裝置已透過設定檔來佈建，否則您配置的 Gmail 部署無法辨識或管理該裝置。

同步裝置

使用 MEM 同步與組織群組相關聯的裝置。

一旦設定 Mobile Email Management (MEM) 部署，相關組織群組的裝置便會透過 MEM 同步。您可以從 Workspace ONE UEM Console 的 **Email 儀表板**頁面檢視裝置狀態和其他詳細資訊。

裝置在儀表板上出現的時機取決於裝置所指派的部署模式為何。

- SEG Proxy - 當 SEG Proxy 報告裝置已連線並接受管理後，由 SEG Proxy 所管理的裝置便會出現在儀表板上。
- PowerShell - 當 Workspace ONE UEM 傳送 PowerShell Cmdlet 以允許裝置與 Email 連線時，由 PowerShell 所管理的裝置便會出現在儀表板上。
- Gmail - 當 Workspace ONE UEM EAS 設定檔排入裝置佇列後，由 Gmail 所管理的裝置便會出現在儀表板上。

Email 儀表板會顯示下列其中一種狀態：

- **受管理且已指派** - 具有已識別之 *memconfigID* 的註冊裝置。
- **受管理但未指派** - 未能透過指派設定檔或自動探索來識別其 *memConfigID* 的註冊裝置。
- **未受管理但已偵測到** - 這些裝置尚未向 Workspace ONE UEM 註冊，但組織群組中特定的 MEM 配置已偵測到這些裝置。

設定 Email 設定檔

6

若要使用 Gmail 用戶端 (Android) 部署 EAS 郵件，請建立 Gmail 用戶端的組態設定檔。

1 導覽至**裝置 > 設定檔與資源 > 設定檔 > 新增 > 新增設定檔 > Android**。

2 點選**裝置**，將您的設定檔部署在裝置上。

3 配置設定檔的**一般**設定。這些設定會決定如何部署設定檔，以及誰可接收此設定檔。

4 選擇 **Exchange ActiveSync** 裝載。

5 配置 **Exchange ActiveSync** 設定。

設定	描述
郵件用戶端	選取 **Gmail** 作為郵件用戶端類型。
帳號名稱	輸入對郵件帳戶的描述。
Exchange ActiveSync 主機	輸入貴公司 ActiveSync 伺服器的外部 URL。 ActiveSync 伺服器可以為執行 ActiveSync 通訊協定的任何郵件伺服器，例如：HCL Notes Traveler、Novell Data Synchronizer 和 Microsoft Exchange 等。在執行「安全 Email 閘道」(SEG) 部署時，請使用 SEG 的 URL，而不使用 Email 伺服器的 URL。
略過 SSL 錯誤	啟用後，會允許裝置在 Workspace ONE Intelligent Hub 程序中略過 SSL 錯誤。
網域	輸入終端使用者的網域。 使用「查閱值」，而不必再爲每位終端使用者建立個別的設定檔。
使用者	輸入終端使用者的使用者名稱。 使用「查閱值」，而不必再爲每位終端使用者建立個別的設定檔。
Email 地址	輸入終端使用者的 Email 地址。 您可以使用查閱值，而不必再爲每位終端使用者建立個別的設定檔。 **備註** 如果您要將自訂屬性用於 GSuite，您必須在 Exchange ActiveSync Email 設定檔的 **Email 地址**欄位中使用自訂屬性查閱值。請參閱「設定 MEM 呼叫 Google 套件的使用者屬性」。

設定	描述
密碼	輸入終端使用者密碼。 使用「查閱值」，而不必再爲每位終端使用者建立個別的設定檔。
身份識別憑證	如果您要求終端使用者必須通過憑證才能與 Exchange ActiveSync 連結，您可以依需求從下拉式功能表中選擇「識別憑證」，否則請選取**無** (預設)。 如需為此裝載選取憑證的必要詳細資訊，請參閱「部署認證設定檔」。
要同步過去多少天的郵件	選擇要同步處理裝置過去多少天的郵件。
要同步過去多少天的行事曆	選擇要同步處理裝置過去多少天的行事曆。
同步行事曆	啟用此項，允許行事曆與裝置同步。
同步聯絡人	啟用此項，允許聯絡人與裝置同步。
允許同步工作	啟用此項，允許工作與裝置同步。
Email 截斷大小上限	指明在將 Email 訊息同步到裝置時，在多大的額度後 Email 即會被截斷。
Email 簽名	輸入 Email 的簽名，此簽名將顯示在傳出的 Email 上。
允許附件	啟用此項，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	啟用此項，允許轉寄 Email。
允許 HTML 格式	指定與裝置同步的 Email 是否可為 HTML 格式。 如果將此設定設為 False，所有 Email 會被轉換成純文字。
停用螢幕擷取畫面	啟用此項，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	■ 排定每週同步的尖峰日期，以及在指定日期進行同步時的**開始時間**和**結束時間**。 ■ 設定**同步排程尖峰日期**和**同步排程離峰日期**的頻率。 ■ 選擇**自動**，在每次更新時便自動同步 Email。 ■ 選擇**手動**，只有在點選此項時才會同步 Email。 ■ 選擇一個時間值，在設定的時間點上同步 Email。 ■ 如有需要，您可以啟用**使用 SSL**、**使用 TLS** 和**預設帳戶**。
S/MIME 設定	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**。 ■ **S/MIME 憑證** – 選擇要使用的憑證。 ■ **需要加密的 S/MIME 訊息** – 啟用此項以要求加密。 ■ **要求簽署的 S/MIME 訊息** – 啟用此項以要求 S/MIME 簽署的訊息。 如果您使用 S/MIME 憑證來加密，請提供**移轉主機**。 選擇**儲存**來儲存設定；或選擇**儲存並發佈**來儲存並將設定檔的設定推播到必要的裝置上。

6 選擇**儲存**來儲存設定；或選擇**儲存並發佈**來儲存並將設定檔的設定推播到必要的裝置上。

設定原生郵件用戶端的 EAS 郵件設定檔

在 iOS 裝置上建立原生郵件用戶端的 Email 配置設定檔。

1 導覽至**裝置 > 設定檔與資源 > 設定檔 > 新增**。選取 **Apple iOS**。

2 配置設定檔的**一般**設定。

3 選擇 **Exchange ActiveSync** 裝載。

4 在**郵件用戶端**選擇**本機郵件用戶端**。在**帳戶名稱**文字方塊填入此郵件帳戶的描述。在 **Exchange ActiveSync 主機**欄位中，填入貴公司 ActiveSync 伺服器的外部 URL。

備註 ActiveSync 伺服器可以為執行 ActiveSync 通訊協定的任何郵件伺服器，例如：HCL Notes Traveler、Novell Data Synchronizer 和 Microsoft Exchange 等。在部署安全 Email 閘道 (SEG) 的情況下，請使用 SEG URL (而不使用 Email 伺服器 URL)。

5 勾選**使用 SSL** 方格，來爲傳入的 Email 流量啟用「安全通訊端層」。

6 勾選 **S/MIME** 方格來使用更多加密憑證。在啟用此項目之前，請確認您已將必要的憑證上傳到**認證**設定檔的設定中。

   a 選取 **S/MIME 憑證**來簽署 Email 訊息。

   b 選取 **S/MIME 加密憑證**來簽署並加密 Email 訊息。

   c 勾選**每個訊息切換**方格，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)。

7 利用查詢值來填寫**登入資訊**，包括**網域名稱、使用者名稱和 Email 地址**等。使用直接從使用者帳戶記錄所擷取的查詢值。在使用 {EmailDomain}、{EmailUserName} {EmailAddress} 查閱值之前，請先確定您的 Workspace ONE UEM 使用者帳戶有已定義的 Email 地址和 Email 使用者名稱。

8 將**密碼**欄位留白，來提示使用者輸入密碼。

9 將憑證加入**認證**裝載後，請選擇**裝載憑證**來爲憑證式的驗證定義所需的憑證。

10 視需要來配置下列可選的**設定和安全性設定**：

   a **要同步處理過去多少天的郵件** – 下載已定義的郵件數量。注意：下載郵件的時間越長，數據消耗量就越大。

   b **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。

   c **禁止在第三方 APP 中使用** – 不允許其他 APP 使用 Exchange 信箱來傳送訊息。

   d **禁止同步近期地址** – 在 Exchange 中傳送郵件時，停用建議聯絡人功能。

   e **禁止「郵包投送」** - 停用 Apple 的「郵包投送」功能。

   f (iOS 13) **啟用郵件** – 啟用 Exchange 帳戶之個別郵件應用程式的組態。

   g (iOS 13) **允許切換郵件** – 若停用，使用者就無法將郵件切換為開啟或關閉。

   h (iOS 13) **啟用聯絡人** – 啟用 Exchange 帳戶之個別聯絡人應用程式的組態。

i (iOS 13) **允許切換聯絡人** – 若停用，使用者就無法將聯絡人切換為開啟或關閉。

j (iOS 13) **啟用行事曆** – 啟用 Exchange 帳戶之個別行事曆應用程式的組態。

k (iOS 13) **允許切換行事曆** – 若停用，使用者就無法將行事曆切換為開啟或關閉。

l **啟用備註** – 啟用 Exchange 帳戶之個別備註應用程式的組態。

m (iOS 13) **允許切換備註** – 若停用，使用者就無法將備註切換為開啟或關閉。

n (iOS 13) **啟用提醒事項** – 啟用 Exchange 帳戶之個別提醒事項應用程式的組態。

o (iOS 13) **允許切換提醒事項** – 若停用，使用者就無法將提醒事項切換為開啟或關閉。

11 為您的本機 EAS 帳戶指派要使用的**預設的語音通話應用程式**，當您在 Email 訊息選取電話號碼時，即可使用該應用程式加以撥打。

12 點選**儲存並發佈**，將此設定檔推播到適用的裝置上。

Exchange ActiveSync 設定檔 (Windows 桌面)

Exchange ActiveSync 設定檔可讓您配置 Windows 桌面型裝置，以存取 Exchange ActiveSync 伺服器供 Email 和行事曆之用。

使用由信任的第三方憑證授權單位 (CA) 所簽署的憑證。憑證中的錯誤可促使您的安全連線遭到攔截式攻擊。這種攻擊會降低產品組件之間傳輸資料的機密性和整合性，並且會讓駭客有機會在傳輸途中攔截或變更資料。

Exchange ActiveSync 設定檔支援 Windows Desktop 版的原生郵件用戶端。配置變更會依您使用的郵件用戶端而不同。

移除設定檔或企業抹除

如果設定檔是透過移除設定檔指令、合規原則，或透過企業抹除來移除，所有的 Email 資料均會被刪除，包括：

- 使用者帳戶/登入資訊。
- Email 訊息資料。
- 聯絡人和行事曆資訊。
- 已儲存在內部用應用程式儲存空間中的附件。

使用者名稱和密碼

如果您的 Email 使用者名稱和使用者 Email 地址不相同，您可以使用 **{EmailUserName}** 文字方塊，與此方塊對應的是目錄服務整合時所匯入的 Email 使用者名稱。即使您使用者的使用者名稱與其 Email 地址相同，仍請使用 **{EmailUserName}** 文字方塊，因為它所使用的 Email 地址將直接從目錄整合服務匯入。

配置 Exchange ActiveSync 設定檔 (Windows 桌面)

建立 Exchange ActiveSync 設定檔，讓 Windows Desktop 裝置可以存取您的 Exchange ActiveSync 伺服器以供 Email 和行事曆使用。

備註 對於 Exchange ActiveSync 設定檔，Workspace ONE UEM 不支援 Outlook 2016。Microsoft Exchange 2016 版本不再支援 Windows Desktop 裝置上透過 Workspace ONE UEM 管理的 Outlook 應用程式 Exchange Web 服務 (EWS) 設定檔組態。

1 導覽至**裝置 > 設定檔 > 清單檢視 > 新增**，然後選取**新增設定檔**。

2 點選 **Windows**，然後選擇 **Windows Desktop** 平台。

3 選擇**使用者設定檔**。

4 配置設定檔的**一般**設定。

5 選擇 **Exchange ActiveSync** 裝載。

6 配置 Exchange ActiveSync 設定：

設定	描述
郵件用戶端	選取 EAS 設定檔配置的郵件用戶端。 Workspace ONE UEM 支援原生郵件用戶端。
帳號名稱	輸入 Exchange ActiveSync 的帳戶名稱。
Exchange ActiveSync 主機	輸入託管 EAS 伺服器的伺服器 URL 或 IP 位址。
使用 SSL	啟用此項，透過安全通訊端層來傳送所有通訊。
網域	輸入電子郵件網域。 該設定檔支援用來插入註冊使用者資訊和登入資訊的查詢值欄位。如需詳細資訊，請參閱頁面底部的〈使用者名稱和密碼〉一節。
使用者名稱	輸入 Email 使用者名稱。
Email 地址	輸入 Email 地址。此文字方塊是必要設定。
密碼	輸入 Email 密碼。
身份識別憑證	選擇 EAS 裝載的憑證。如需詳細資訊，請參閱「設定認證裝載」。
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)。
要同步過去多少天的郵件	選擇要將多少天前的 Email 同步至裝置。
診斷性記錄	啟用此項目以記錄資訊，供進行疑難排解時使用。
需要「鎖定下的資料保護」	啟用此項目，要求在裝置鎖定時資料必須受到保護。
允許 Email 同步	啟用此項目以允許同步 Email 訊息。
允許聯絡人資訊同步	啟用此項目以允許同步聯絡人。
允許行事曆同步	啟用此項目以允許同步行事曆活動。

7 選取**儲存**，將設定檔保留在 Workspace ONE UEM 主控台上；或選取**儲存並 發佈**，將設定檔推送到裝置上。

Email 存取權的強制控管

7

設定存取控制，以提供安全存取 Email 基礎結構的方式。

Email 合規原則

完成 Email 的部署之後，您可加入存取權的控管更進一步地保護您的行動 Email。存取權的控管功能，僅允許安全及合規的裝置來存取您郵件的基礎結構。系統會根據 Email 合規原則的說明而強制執行存取控制。

Email 合規原則能針對不合規、未加密、非使用中或未受管的裝置限制其 Email 存取權，從而增強安全性。這些原則讓您能夠把 Email 的存取權只提供給必要而且已核准的裝置。Email 原則也能根據裝置的型號與作業系統來限制 Email 的存取權。

這些原則可分類為一般 Email 原則、受管裝置原則和 Email 安全性原則。下表列出不同原則的分類方式及其適用的部署類型：

下表列出支援的 Email 合規性原則。

表 7-1. 支援的 Email 合規性原則

	SEG (Exchange、HCL Traveler、G Suite)	PowerShell (Exchange)	密碼管理 (Gmail)	直接整合 (Gmail)
一般 Email 原則				
同步設定	是	否		
受管裝置	是	是		
郵件用戶端	是	是		
使用者	是	是		
EAS 裝置類型	是	是		
受管裝置原則				
非使用狀態	是	是		
遭破解的裝置	是	是		
加密	是	是		

表 7-1. 支援的 Email 合規性原則 (續)

	SEG (Exchange、HCL Traveler、G Suite)	PowerShell (Exchange)	密碼管理 (Gmail)	直接整合 (Gmail)
型號	是	是		
作業系統	是	是		
需要 ActiveSync 設定檔	是	是		
Email 安全性原則				
Email 安全性分級	是	否		
附件 (受管裝置)	是	否		
附件 (未受管裝置)	是	否		
超連結	是	否		

啟用 Email 合規原則

可在 Workspace ONE UEM Console 上取得的 Email 合規性原則包括一般 Email 原則、受管理裝置原則和 Email 安全性原則。您可以個別啟用上述 Email 合規原則，也可以編輯其規則以允許或封鎖裝置。

1 導覽至 **Email > 合規性原則**。

2 使用**動作**欄位下的編輯原則圖示，來編輯某項原則之規定。

備註 **一般 Email 原則**會在所有存取 Email 的裝置上，強制執行原則。當您選擇一個使用者群組時，此原則會套用在該群組的所有使用者上。

Email 原則	描述
同步設定	禁止裝置與特定的 EAS 資料夾同步。 ■ 無論其他合規性原則為何，Workspace ONE UEM 禁止裝置與所選資料夾同步。 ■ 為了要讓原則生效，必須重新將 EAS 設定檔發佈到裝置上。(這會強制裝置重新與 Email 伺服器同步)。
受管裝置	將 Email 存取侷限於受管裝置。
郵件用戶端	將 Email 存取權限制在一組郵件用戶端。 ■ 您可以根據用戶端類型 (例如**自訂**和**已偵測到的**) 來允許或封鎖郵件用戶端 ■ 您也可以替郵件用戶端和最新偵測到但並未顯示在「郵件用戶端」下拉式功能表中的郵件用戶，設定預設動作。對自訂用戶端類型，支援萬用字元 (*) 和自動完成的功能。

Email 原則	描述
使用者	將 Email 存取權限定在某組使用者。您可以允許或封鎖的使用者類型包含自訂、已偵測到、Workspace ONE UEM 使用者帳戶，以及使用者群組。還可以替「使用者名稱」或「群組」下拉式功能表中未顯示的 Email 使用者名稱，設定預設動作。對自訂使用者類型，支援萬用字元 (*) 和自動完成的功能。
EAS 裝置類型	根據終端使用者裝置所呈報的 EAS 裝置類型屬性，將裝置列入允許清單或封鎖清單。您可以依用戶端類型 (包含自訂及已偵測到的郵件用戶端)，來允許或封鎖裝置。還可以替「裝置類型」下拉式欄位中未顯示的 EAS 裝置類型，設定預設動作。對自訂用戶端類型，支援萬用字元 (*) 和自動完成的功能。

受管裝置原則會在存取電子郵件的受管裝置上，強制執行原則。

Email 原則	描述
非使用狀態	禁止非使用中的受管裝置存取 Email。您可指定裝置顯示「非使用中」(也就是未簽入 VMware AirWatch) 而 Workspace ONE UEM 不會禁止存取 Email 的天數。系統所能接受的最小值為 1，而最大值為 32767。
遭破解的裝置	禁止遭破解的裝置存取 Email。若是裝置尚未向 AirWatch 呈報已遭破解的狀態，此原則便不會封鎖該裝置存取 Email 的權限。
加密	禁止未加密的裝置存取 Email。此原則僅適用於那些已向 VMware AirWatch 呈報資料防護狀態的裝置。
型號	根據裝置的平台和型號來限制 Email 的存取權。
作業系統	限制某特定平台僅能使用一組作業系統來存取 Email。
需要 ActiveSync 設定檔	限制只有非使用 Exchange ActiveSync 設定檔來管理的裝置，才可存取 Email。對於透過應用程式組態而非 ActiveSync 設定檔進行設定的電子郵件用戶端，將應用程式組態傳送至受管理的電子郵件用戶端，可確保電子郵件用戶端符合合規性原則。

Email 安全性原則會在附件和超連結上強制執行原則。此原則僅適用於 SEG 部署。如需詳細資訊，請參閱 Email 存取權的強制控管一節。

Email 原則	描述
Email 安全性分級	定義 SEG 對有標記和無標記的 Email 所採取的原則。您可以使用預先定義的標籤，或者使用自訂選項來建立新標籤。您可以根據分類方式，選擇允許或封鎖 Email 用戶端的 Email。
附件 (受管裝置)	將所選檔案類型的 Email 附件加密。裝置上的這些附件都已受到保護，而且僅能在 VMware AirWatch Content Locker 中檢視這些附件。 目前此功能僅適用於已安裝 VMware AirWatch Content Locker 應用程式的受管理 iOS 裝置與 Android 裝置。至於其他的受管裝置，您可選擇允許已加密的附件、封鎖附件，或是允許未加密的附件。
附件 (未受管裝置)	加密和封鎖附件，或允許使用未受管裝置上之未加密的附件。 您無法在未受管的裝置上查看加密的 Email 附件。此功能是為了保持 Email 的完整性。如果未受管的裝置轉寄了一封含有加密附件的 Email，收件者還是可以從 PC 或其他行動裝置上檢視此附件。
超連結	允許裝置使用者透過裝置上的 VMware Browser 來直接開啟 Email 中的超連結。Secure Email Gateway 會動態修改超連結，以便在 VMware Browser 中開啟。您可以選擇下列其中一種修改類型： ■ 全部 - 選擇透過 VMware Browser 開啟所有的超連結。 ■ 排除 - 如果您不想要裝置使用者透過 VMware Browser 開啟特定網域之連結，請選擇此項目。在**修改除了這些網域之外的所有超連結**的欄位中，提及所要排除的網域。您也可以從 `.csv` 檔案，大量上傳網域名稱。 ■ 包含 - 如果您希望裝置使用者透過 VMware Browser 開啟特定網域之連結，請選擇此項目。在**僅修改這些網域的超連結**欄位中提及包含的網域。您也可以從 `.csv` 檔案，大量上傳網域名稱。

3 建立您的合規原則，然後再**儲存**。

4 選擇**使用中**欄位下的合規原則灰色圓圈來啟用該合規原則。出現一個含有金鑰代碼的頁面。

5 在對應的欄位中輸入金鑰代碼，並選擇**繼續**。

結果：**使用中**欄位下的圓圈如顯示為綠色，則表示該原則已啟用。

Email 內容、附件與超連結防護

使用 Workspace ONE UEM Web 和 Workspace ONE UEM Content 確保 Email 安全。

Workspace ONE UEM 協助您保護與控制行動 Email 的附件，防止受管理與未受管理的裝置發生資料遺失的狀況。Workspace ONE UEM 允許裝置使用者透過裝置上的 Workspace ONE Web 來直接開啟 Email 中的超連結。Secure Email Gateway 會動態地修改超連結，以便在 Workspace ONE Web 中開啟。

在您開始保護 Email 附件之前，必須先安裝下列應用程式：

- Secure Email Gateway (SEG)
- VMware Content Locker (iOS 與 Android)
- 支援 Microsoft Exchange 2010/2013/2016/2019、HCL Notes、Novell GroupWise 和 Gmail

啟用 Email 安全性分類

您可以在 UEM 主控台 Workspace ONE UEM Console 上選取特定的安全性分類，使 Secure Email Gateway 針對這些分類採取動作。

下表提供了預先定義的安全性分類讓您選擇，以及供您用來建立自訂分類的的選項。

1 導覽至 **Email > 合規性原則 > Email 安全性原則**。

2 選擇**使用中**欄位下 **Email 安全性分類**合規原則的灰色圓圈。出現一個含有金鑰代碼的頁面。

3 在對應的欄位中輸入金鑰代碼，並選擇**繼續**。已啟用的原則會在**使用中**欄位下以綠色圓圈表示。

4 選擇**動作**欄位下方的**編輯**選項。

5 選擇**新增**，再從**類型**下拉式功能表中選擇標籤類型。

   預先定義及自訂為可用的選項。從下列項目中選擇：

   - 選取「事先定義」的標籤類型，從**安全分類**的下拉式功能表中，取得適用的標籤之清單。
   - 選取「自訂」的標籤類型，並在**安全分類**欄位中輸入您自訂的標籤。

6 輸入標籤的**描述**，然後選擇**下一步**。

7 配置 SEG 對有標記或無標記的 Email 所該採取的動作。點選**下一步**。

   您可以選擇允許或封鎖 Email 用戶端的 Email。

8 檢視**摘要**並按一下**儲存**。

啟用 Email 附件保護功能

使用 Workspace ONE UEM 保護 Email 附件。

Email 附件可能包括各類型的檔案。您可以在 UEM 主控台選取特定的檔案類型，使該類型的檔案須先經過 Secure Email Gateway 加密才能做為 Email 附件。這些已加密的附件能在行動裝置上獲得保護，且只能使用 VMware AirWatch Content Locker 應用程式檢視。

有細微的設定可供受管理 iOS 與 Android 裝置使用。至於其它的受管裝置和所有未受管裝置，您可以禁止在第三方應用程式中開啟 (大量) 其附件。

1 導覽至 **Email > 合規性原則 > Email 安全性原則**。

2 選擇**使用中**欄位下之**附件 (受管裝置)** 或**附件 (未受管裝置)** 合規原則的灰色圓圈。

結果：出現一個含有金鑰代碼的頁面。

3 在對應的欄位中輸入金鑰代碼，並選擇**繼續**。

結果：**使用中**欄位下的綠色圓圈表示已啟用並使用該原則。

4 選擇**動作**欄位下方的**編輯**選項。

5 在每個檔案類別中 (僅限受管理 iOS 與 Android 裝置)，選取是否要加密並允許附件、封鎖附件，或者允許不加密的附件 。

6 勾選**允許在 Content Locker 中儲存附件**的方格，以便在 Content Locker 中儲存附件。

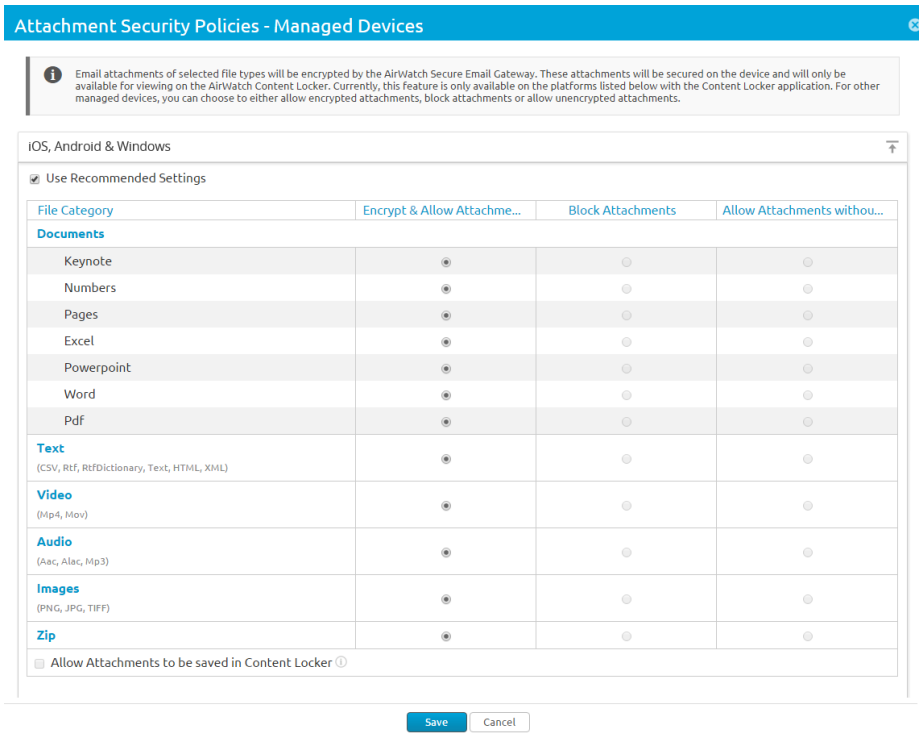
結果：附件保持加密狀態，並會套用 Content Locker 的原則。

7 您也可以為尚未在此處提及的**其他檔案**選擇適用的原則。

8 在**排除清單**中，輸入仍需被排除在**其他**檔案所配置的動作之外的副檔名。

9 輸入**封鎖附件的自訂訊息**，以便通知收件者某附件已被封鎖。

10 **儲存**設定。



啟用超連結防護

您可以使用超連結 Email 安全性原則來控制並修改 Email 中的超連結，使其能夠直接在 Workspace ONE Web 中開啟。

1 導覽至 **Email > 合規性原則 > Email 安全性原則**。

2 選擇**使用中**欄位下之**超連結**合規原則的灰色圓圈。

結果：出現一個含有金鑰代碼的頁面。

3 在對應的欄位中輸入金鑰代碼，並選擇**繼續**。

結果：**使用中**欄位下的綠色圓圈表示已啟用並使用原則。

4 選擇**動作**欄位下方的**編輯**選項。

5 選取您要略過超連結轉換的平台。

6 選擇下列其中一種**修改類型**

從下列項目中選擇：

- **全部** - 選擇透過 Workspace ONE Web 開啟所有超連結。
- **包含** - 如果您要讓裝置使用者透過 Workspace ONE Web 開啟指定網域的超連結，請選擇此項目。在**僅修改這些網域的超連結**欄位中提及包含的網域。您也可以從 CSV 檔案，大量上傳網域名稱。
- **不包含** - 如果您不想讓裝置使用者透過 Workspace ONE Web 開啟指定網域，請選擇此項目。在**修改除了這些網域之外的所有超連結**的文字方塊中，提及所要排除的網域。您也可以從 CSV 檔案，大量上傳網域名稱。

7 **儲存**設定。

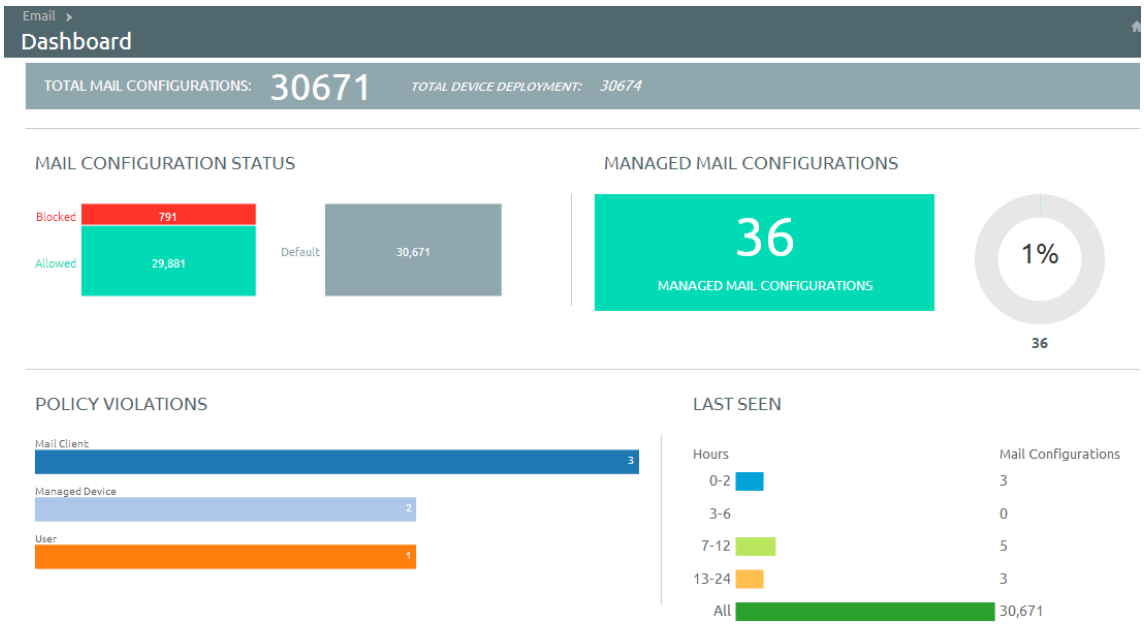
監控 Email 流量

8

透過 **Email 儀表板**來監控使用者群組的 Email 流量和裝置。

此 **Email > 儀表板**提供您連線到 Email 伺服器的裝置狀態摘要。

您還可以使用提供的圖表來篩選搜尋。例如：若要檢視某企業群組中所有受管裝置，請選取「受管裝置」的圖表，圖表就會顯示在「清單檢視」的畫面中。



檢視詳細的裝置資訊與特定的使用者資訊。

您可以從 **Email > 清單檢視**頁面，針對您透過 Mobile Email Management (MEM) 管理的終端使用者裝置檢視其所有即時更新資訊。

在**裝置**與**使用者**索引標籤間切換，以檢視使用者和裝置資訊。為了能夠檢視資訊摘要或自訂清單，如有需要請變更版面配置。

- 檢視受管、未受管、合規、不合規、遭封鎖或是已允許的裝置。

- 檢視裝置的 IP 位址。

  備註 Workspace ONE UEM 2107 版及更新版本的**清單檢視**頁面中不會顯示「作業系統」、「型號」、「平台」、「電話號碼」、「IMEI」等裝置詳細資料。

裝置與特定使用者的資訊均可透過摘要清單或者按需求重新整理成的自訂清單來檢視。

清單檢視頁面可提供下列詳細資訊：

設定	描述
上次請求	上次裝置狀態的變更來自 Workspace ONE UEM 或是來自 PowerShell 整合中的 Exchange。在 SEG 的整合中，此欄位顯示上次裝置同步郵件的時間。
使用者	使用者帳戶名稱。
暱稱	裝置的暱稱。
MEM 配置	此設定的 MEM 部署是用於管理該裝置。
Email 地址	使用者帳戶的 Email 地址。
識別碼	與裝置有關聯的特殊英數字元識別碼。
郵件用戶端	在裝置上同步 Email 的 Email 用戶端。
上次指令	裝置上次的狀態變更，並自動填入**上次請求**的欄位。
上次的閘道伺服器	與裝置連線的伺服器。
狀態	裝置的即時狀態，以及根據個別定義原則來決定是否要封鎖或允許裝置上的 Email。
原因	允許或封鎖裝置上的 Email 之原因代碼。 ■ 當您依照預設之企業的「允許」、「封鎖」或「隔離」原則來定義存取狀態時，其原因代碼即為「全域」。當 Exchange 管理員或 Workspace ONE UEM 明確地為指定的郵箱設定裝置 ID 時，其原因代碼即為「個別」。如果 EAS 原則封鎖了裝置，則原因代碼為「原則」。 ■ Workspace ONE UEM 提供您在不合規裝置 (例如：具有封鎖清單應用程式的裝置) 上封鎖電子郵件的選項。一旦裝置合規後，Email 便能立即啟用。您可在 **Email 儀表板**上檢視原因標籤為「MDM 合規性」之不合規裝置的清單。

- **IP 位址** - 裝置的 IP 位址。

  備註 Workspace ONE UEM 2107 版及更新版本的**清單檢視**頁面中不會顯示「作業系統」、「型號」、「平台」、「電話號碼」、「IMEI」等裝置詳細資料。

- **信箱識別** - Active Directory 中使用者信箱的位置。

篩選條件

使用「清單檢視」頁面中的**篩選條件**選項來縮小裝置搜尋範圍。

設定	描述
最後上線時間	全部、在 24 小時內、12 小時內、6 小時內、2 小時內。
受管的	全部、受管的、未受管的。
允許的	全部、允許的、封鎖的。
原則覆寫	全部、已列入封鎖清單、已列入允許清單、預設。
原則違犯	已遭破解的、非使用中的裝置、資料未被保護/已註冊/MDM 合規的、未被核准的 EAS 裝置類型/Email 帳戶/郵件用戶端/型號/作業系統
MEM 配置	根據已配置的 MEM 部署來篩選裝置。
EAS 裝置類型	根據裝置類型來篩選。
Email 地址	根據 Email 地址來篩選。
上次的閘道伺服器	根據可用的安全 Email 閘道來篩選。

Email 動作

覆寫、**動作**和**管理**下拉式功能表提供您單一的位置來執行各種動作。

重要 這些動作無法復原。

覆寫

勾選與某裝置對應的方格，並在該裝置上執行動作。忽視合規性原則，將裝置列入允許清單或封鎖清單，並在必要時還原原則。

- **允許清單** - 允許裝置接收電子郵件。
- **封鎖清單** - 封鎖裝置使其無法接收電子郵件。
- **預設** - 根據裝置是否合規來允許或封鎖裝置。

動作

- **同步郵箱** - 查詢 Exchange 伺服器來取得更新的裝置清單，而這些裝置已嘗試同步 Email (PowerShell 直接模式)。如果您不選擇此選項，除非其中一個未受管裝置註冊至 Workspace ONE UEM，或是您手動將裝置列入允許清單或封鎖清單，因而觸發狀態變更的命令，否則未受管的裝置清單將不會有任何更動。

  Workspace ONE UEM 在自助入口網站 (SSP) 中提供 [Email 同步] 選項，讓終端使用者可以透過郵件伺服器來同步其裝置，同時也能執行所有的裝置上預先配置的合規原則。此程序通常要比在所有裝置上大量執行同步作業要快很多。
- **執行合規原則** - 觸發合規引擎來執行所選的 MEM 設定。使用 PowerShell 模式和 SEG 模式時，此指令的運作方式會有所不同。
  - 如果已配置 SEG，此指令會以最新的合規原則來更新 SEG。

- 如果已配置 PowerShell 模式，此指令會在所有裝置上手動執行合規性檢查，並且封鎖或允許裝置讀取 Email 的權限。

  PowerShell 直接模式配置完畢後，Workspace ONE UEM 會透過由主控台伺服器或 VMware 企業系統 Connector (視部署結構而定) 所建立的遠端簽署 PowerShell 工作階段，直接與 CAS 矩陣通訊。使用遠端簽署工作階段時，系統會根據裝置在 Workspace ONE UEM 中的合規性狀態傳送 PowerShell 命令，將 Exchange 2010/2013 中指定使用者 CAS 郵箱上的裝置 ID 列入封鎖清單或允許清單。

- **啟用測試模式** - 不需將 Email 原則套用在已透過 SEG 整合的部署裝置上，就直接測試這些原則。

管理

勾選與某裝置對應的方格，並在該裝置上執行動作。

設定	描述
註冊 Email	將含有註冊所需之各種詳細資料的 Email 傳送給使用者。 當偵測到未受管的裝置時，便傳送一封註冊 Email 要求使用者註冊其裝置 (僅適用於 PowerShell)。
開啟 Dx 模式	執行所選之使用者郵箱的診斷工作，可以提供您裝置的活動記錄。此功能僅適用於 SEG。
關閉 Dx 模式	關閉所選之使用者郵箱的診斷工作。
更新加密金鑰	重設加密，然後重新同步所選裝置的 Email。
遠端抹除	將裝置重設為原廠設定。 當含有公司機密資訊的裝置遺失或遭竊時，執行「企業重設」(重設為原廠設定，此功能僅適用於 PowerShell)。
刪除未受管裝置	從儀表板中刪除所選之未受管裝置的記錄。
移轉裝置	跨企業群組和 MEM 部署來移轉裝置。
同步已選的郵箱	同步已選裝置的郵箱。每次僅可同步一個裝置郵箱。

備註 此記錄可能會在下次同步時，再次出現。

檢查是否有未受管的裝置

為了確保所有裝置都能夠受到妥善的管理和監控，請瀏覽至清單檢視頁面。在「清單檢視」頁面篩選未受管裝置，然後從「管理」下拉式功能表中傳送註冊郵件。