

VMware Identity Manager 管理

VMware Identity Manager 2.8

vmware®

您可以在 VMware 網站上找到最新的技術說明文件，網址為：

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

VMware 網站還提供了最新的產品更新。

如果您對此文件有何想法，請將您的回應意見提交至：

docfeedback@vmware.com

Copyright © 2013–2016 VMware, Inc. 版權所有。 [版權和商標資訊](#)。

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

內容

- 關於 VMware Identity Manager 管理 7
- 1 在 VMware Identity Manager 管理主控台中工作 9
 - 在管理主控台中瀏覽 9
 - 身分識別與存取管理設定概觀 10
- 2 與您的企業目錄整合 13
 - 目錄整合的相關重要概念 13
- 3 與 Active Directory 整合 15
 - Active Directory 環境 15
 - 關於網域控制站選項 (domain_krb.properties 檔案) 17
 - 管理從 Active Directory 同步的使用者屬性 20
 - 加入網域所需的權限 21
 - 設定服務的 Active Directory 連線 22
 - 讓使用者能夠變更 Active Directory 密碼 26
 - 設定目錄同步保護 27
- 4 與 LDAP 目錄整合 29
 - LDAP 目錄整合的限制 29
 - 整合 LDAP 目錄與服務 30
- 5 使用本機目錄 33
 - 建立本機目錄 34
 - 變更本機目錄設定 38
 - 刪除本機目錄 39
 - 設定系統管理員使用者的驗證方法 39
- 6 Just-in-Time 使用者佈建 41
 - 關於 Just-in-Time 使用者佈建 41
 - 準備 Just-in-Time 佈建 42
 - 設定 Just-in-Time 使用者佈建 43
 - SAML 宣告的需求 44
 - 停用 Just-in-Time 使用者佈建 45
 - 刪除 Just-in-Time 目錄 45
 - 錯誤訊息 46
- 7 在 VMware Identity Manager 中設定使用者驗證 47
 - 為 VMware Identity Manager 設定 Kerberos 48

- 為 VMware Identity Manager 設定 SecurID 52
- 針對 VMware Identity Manager 設定 RADIUS 54
- 在 VMware Identity Manager 中設定 RSA 調適性驗證 56
- 設定憑證或智慧卡介面卡以搭配 VMware Identity Manager 使用 58
- 設定雙重要素驗證適用的 VMware Verify 60
- 設定內建身分識別提供者 62
- 設定其他 Workspace 身分識別提供者 64
- 將第三方身分識別提供者執行個體設定為驗證使用者 64
- 管理要套用至使用者的驗證方法 66

- 8 管理存取原則 69**
 - 設定存取原則設定 69
 - 管理 Web 和桌面平台應用程式特定的原則 71
 - 新增 Web 或桌面平台應用程式特定原則 73
 - 設定自訂存取遭拒錯誤訊息 74
 - 編輯存取原則 74
 - 在行動裝置上啟用持續性 Cookie 75

- 9 管理使用者和群組 77**
 - 使用者和群組類型 77
 - 關於使用者名稱和群組名稱 78
 - 管理使用者 79
 - 建立群組和設定群組規則 80
 - 編輯群組規則 81
 - 將資源新增至群組 82
 - 建立本機使用者 82
 - 管理密碼 84

- 10 管理目錄 87**
 - 管理目錄中的資源 87
 - 將資源分組為類別 90
 - 管理目錄設定 92

- 11 操作管理主控台儀表板 97**
 - 從儀表板監控使用者和資源使用 97
 - 監控系統資訊與健全狀況 98
 - 檢視報告 98

- 12 自訂品牌 VMware Identity Manager 服務 101**
 - 在 VMware Identity Manager 中自訂品牌 101
 - 自訂使用者入口網站的品牌 102
 - 為 VMware Verify 應用程式自訂品牌 103

- 13 整合 AirWatch 與 VMware Identity Manager 105**
 - 設定 AirWatch 以便與 VMware Identity Manager 整合 105

- 在 VMware Identity Manager 中設定 AirWatch 執行個體 108
- 為 AirWatch 啟用整合目錄 109
- 使用 AirWatch Cloud Connector 實作驗證 110
- 為 AirWatch 管理的 iOS 裝置實作 Mobile Single Sign-in 驗證 112
- 實作 Android 裝置的行動單一登入驗證 118
- 為 AirWatch 管理的裝置啟用符合性檢查 124

索引 127

關於 VMware Identity Manager 管理

VMware Identity Manager 管理提供關於使用和維護 VMware Identity Manager 服務的資訊和指示。利用 VMware Identity Manager™，您可以設定及管理驗證方法和存取原則、為組織的應用程式自訂資源的目錄，並且讓受到管理的使用者能夠在多個裝置上安全地存取這些資源。這類資源包括 Web 應用程式、擷取為 ThinApp 套件的 Windows 應用程式、Citrix 式應用程式，以及 View 桌面平台和應用程式集區。

主要對象

這些資訊適用於想要設定和管理 VMware Identity Manager 的任何人。此資訊是針對熟悉虛擬機器技術、身分識別管理、Kerberos 和目錄服務且富有經驗的 Windows 或 Linux 系統管理員而撰寫。其他技術，例如 VMware ThinApp®、View、Citrix 應用程式虛擬化和驗證方法 (如 RSA SecurID) 的知識，若您計劃實作這些功能則也有所幫助。

在 VMware Identity Manager 管理主控台中工作

1

VMware Identity Manager™ 管理主控台為您提供了集中的管理主控台，讓您可其中管理使用者和群組、將資源新增至目錄、管理目錄中各項資源的權利、設定 AirWatch 整合，以及設定和管理驗證與存取原則。

您在管理主控台中執行的主要工作，是管理使用者驗證和存取原則，以及將資源的權利賦予使用者。其他工作則可讓您深入控制哪些使用者或群組在哪些情況下有權使用哪些資源，而支援上述主要工作。

使用者可從桌面平台或行動裝置登入其 VMware Workspace™ ONE™ 入口網站以存取工作資源，包括桌面平台、瀏覽器、共用公司文件，以及各種您有權使用的應用程式類型。

本章節討論下列主題：

- “在管理主控台中瀏覽,” 第 9 頁
- “身分識別與存取管理設定概觀,” 第 10 頁

在管理主控台中瀏覽

管理主控台的工作會依索引標籤進行整理。

索引標籤	說明
儀表板	[使用者參與] 儀表板可用來監控使用者和資源使用。此儀表板會顯示已登入的使用者、正在使用的應用程式，以及應用程式的存取頻率等相關資訊。 [系統診斷儀表板] 會顯示您環境中服務健全狀況的詳細概觀，以及服務的其他相關資訊。 您可以建立報告，以追蹤使用者和群組的活動、資源和裝置使用，以及依使用者的稽核事件。
使用者 和群組	在 [使用者和群組] 索引標籤中，您可以管理與監控從您的 Active Directory 或 LDAP 目錄匯入的使用者和群組、建立本機使用者和群組，以及將資源授權給使用者和群組。您可以設定本機使用者的密碼原則。
目錄	目錄是您可授權給使用者之所有資源的存放庫。在 [目錄] 索引標籤中，您可以新增 Web 應用程式、ThinApp 套件、View 集區和應用程式、Horizon Air 桌面平台，以及 Citrix 型應用程式。您可以建立新的應用程式、將應用程式分組到類別中，以及存取每個資源的相關資訊。在 [目錄設定] 頁面上，您可以下載 SAML 憑證、管理資源組態，以及自訂使用者入口網站的外觀。
身分識別 與存取 管理	在 [身分識別與存取管理] 索引標籤中，您可以設定連接器服務、設定 AirWatch 整合、設定驗證方法，以及將自訂品牌套用至登入頁面和管理主控台。您可以管理目錄設定、身分識別提供者和存取原則。您也可以設定第三方身分識別提供者。
應用裝置 設定	在 [應用裝置設定] 索引標籤中，您可以管理應用裝置的組態，包括設定應用裝置的 SSL 憑證、變更服務管理員和系統密碼，以及管理其他基礎結構功能。您也可以更新授權設定以及進行 SMTP 設定。

支援存取管理主控台的 Web 瀏覽器

VMware Identity Manager 管理主控台是可讓您用來管理承租人的 Web 型應用程式。您可以從下列瀏覽器存取管理主控台。

- Internet Explorer 11 (適用於 Windows 系統)
- Google Chrome 42.0 或更新版本 (適用於 Windows 和 Mac 系統)
- Mozilla Firefox 40 或更新版本 (適用於 Windows 和 Mac 系統)
- Safari 6.2.8 和更新版本 (適用於 Mac 系統)

備註 在 Internet Explorer 11 中必須啟用 JavaScript，並且允許 Cookie 以透過 VMware Identity Manager 進行驗證。

VMware Identity Manager 使用者元件

使用者可從其 Workspace ONE 入口網站存取獲授權的資源。

使用者可以從 Identity Manager 桌面平台存取擷取做為 ThinApp 套件的虛擬化 Windows 應用程式。

表格 1-1. 使用者用戶端元件

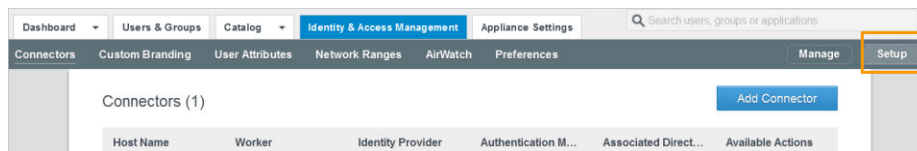
使用者元件	說明	可用的端點
Workspace ONE 使用者應用程式入口網站	應用程式入口網站是無代理程式的 Web 型應用程式。它是使用者透過瀏覽器存取及使用其授權資源時所使用的預設介面。 如果使用者具有授權的 ThinApp 應用程式，且位於 Identity Manager 桌面平台應用程式安裝及運作所在的 Windows 電腦上，則可以由此應用程式入口網站檢視及啟動其授權的 ThinApp 套件。	Web 型應用程式入口網站可在所有支援的系統端點上使用，例如 Windows 電腦、Mac 電腦、iOS 裝置、Android 裝置等。
Identity Manager 桌面平台	當此程式安裝在使用者的 Windows 電腦上時，使用者將可使用其以 ThinApp 套件的形式擷取的虛擬化 Windows 應用程式。	Windows 電腦

身分識別與存取管理設定概觀

在管理主控台的 [身分識別與存取管理] 索引標籤中，您可以設定及管理驗證方法、存取原則、目錄服務，以及自訂使用者入口網站和管理主控台的外觀與操作方式。

以下將說明 [身分識別與存取管理] 索引標籤中的設定。

圖 1-1 身分識別與存取管理設定頁面

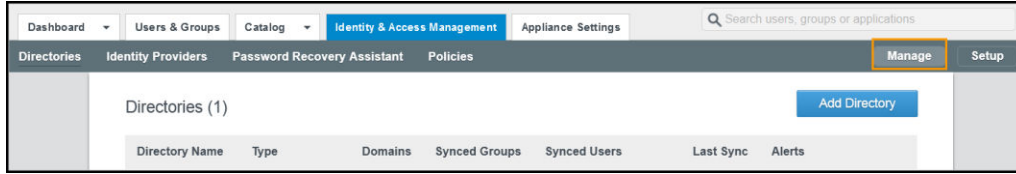


表格 1-2. 身分識別與存取管理設定

設定	說明
設定 > 連接器	<p>[連接器] 頁面會列出您的企業網路內所部署的連接器。連接器會用來同步企業目錄與服務之間的使用者和群組資料，並在作為身分識別提供者時，用來向服務驗證使用者身分。</p> <p>當您將某個目錄與連接器執行個體建立關聯時，連接器會為名為 Worker 的相關聯目錄建立一個磁碟分割。一個連接器執行個體可以有許多個相關聯的 Worker。每個 Worker 都充當一個身分識別提供者。您可針對每個 Worker 定義並設定驗證方法。</p> <p>連接器會透過一或多個 Worker 同步企業目錄和服務之間的使用者和群組資料。</p> <ul style="list-style-type: none"> ■ 在 Worker 資料行中，選取某個 Worker 以檢視連接器的詳細資料，並導覽至 [驗證配接器] 頁面，以查看可用驗證方法的狀態。如需驗證的相關資訊，請參閱第 7 章, “在 VMware Identity Manager 中設定使用者驗證,” 第 47 頁。 ■ 在 [身分識別提供者] 資料行中，選取要檢視、編輯或停用的 IdP。請參閱“新增和設定身分識別提供者執行個體,” 第 64 頁。 ■ 在 [關聯的目錄] 資料行中，存取與此 Worker 相關聯的目錄。 <p>您必須先按一下 [新增連接器]，產生要在設定精靈中貼上以便與連接器建立通訊的啟動碼，才能新增連接器。</p> <p>加入網域連結</p> <ul style="list-style-type: none"> ■ 您可以按一下 [加入網域]，將連接器加入特定的 Active Directory 網域。例如，在設定 Kerberos 驗證時，您必須加入包含使用者的 Active Directory 網域，或加入與包含使用者的網域之間有信任關係的網域。 ■ 使用整合式 Windows 驗證 Active Directory 設定目錄時，連接器會根據組態詳細資料加入網域。
設定 > 自訂品牌	<p>在 [自訂品牌] 頁面中，您可以自訂管理主控台標頭和登入畫面的外觀。請參閱“在 VMware Identity Manager 中自訂品牌,” 第 101 頁。</p> <p>若要自訂使用者 Web 入口網站、行動裝置和平板電腦等檢視，請移至 [目錄] > [設定] > [使用者入口網站品牌]。請參閱“自訂使用者入口網站的品牌,” 第 102 頁。</p>
設定 > 使用者屬性	<p>[使用者屬性] 頁面會顯示目錄中同步的預設使用者屬性，而您可以新增與 Active Directory 屬性對應的其他屬性。請參閱“選取要與目錄同步的屬性,” 第 21 頁。</p>
設定 > 網路範圍	<p>此頁面會列出您所新增的網路範圍。您可以設定網路範圍，讓使用者可透過這些 IP 位址進行存取。您可以新增其他網路範圍，也可以編輯現有的範圍。請參閱“新增或編輯網路範圍,” 第 66 頁。</p>
設定 > 自動探索	<p>當 VMware Identity Manager 與 AirWatch 整合時，您可以整合您在 AirWatch 組態中部署的 Windows 自動探索服務與 VMware Identity Manager 服務。如需關於在 AirWatch 中設定自動探索的詳細資訊，請參閱 AirWatch 網站中提供的 AirWatch 說明文件《VMware AirWatch Windows 探動探索服務安裝指南》，網址是 http://air-watch.com</p> <p>登錄您的電子郵件網域以使用自動探索服務，讓使用者能更輕鬆地使用 Workspace ONE 存取其應用程式入口網站。使用者在透過 Workspace ONE 存取其應用程式入口網站時，將可輸入其電子郵件地址，而不是組織的 URL。</p> <p>如需自動探索的詳細資訊，請參閱《在裝置上設定 VMware Workspace ONE 應用程式》指南。</p>
設定 > AirWatch	<p>在此頁面上，您可以設定與 AirWatch 的整合，且在整合設定並儲存後，您可以啟用整合目錄，將設定於 AirWatch 目錄中的應用程式合併到整合目錄；啟用符合性檢查，以確認受管理的裝置符合 AirWatch 符合性原則，以及啟用透過 AirWatch Cloud Connector (ACC) 的使用者密碼驗證。請參閱第 13 章, “整合 AirWatch 與 VMware Identity Manager,” 第 105 頁。</p>
設定 > 喜好設定	<p>[喜好設定] 頁面會顯示管理員可啟用的功能。其中包括</p> <ul style="list-style-type: none"> ■ 持續性 Cookie 可從這個頁面啟用。請參閱“啟用持續性 Cookie,” 第 75 頁。 ■ 在您的服務中設定本機使用者時，若要將本機使用者顯示為登入頁面上的網域選項，請啟用在登入頁面顯示本機使用者。

以下說明用來在 [身分識別與存取管理] 索引標籤中管理服務的設定。

圖 1-2 身分識別與存取管理的管理頁面



表格 1-3. 身分識別與存取管理的管理設定

設定	說明
管理 > 目錄	<p>[目錄] 頁面會列出您所建立的目錄。建立一或多個目錄，然後將這些目錄與企業目錄部署同步。在此頁面上，您可以檢視已同步至目錄的群組數目和使用者數目，以及上次同步時間。您可以按一下 [立即同步] 以啟動目錄同步。</p> <p>請參閱第 2 章, “與您的企業目錄整合,” 第 13 頁。</p> <p>按一下目錄名稱時，您將可編輯同步設定、導覽 [身分識別提供者] 頁面，以及檢視同步記錄。</p> <p>從目錄同步設定頁面，您可以排程同步頻率、查看與此目錄相關聯的網域清單、變更對應的屬性清單、更新同步的使用者及群組清單，並設定保護目標。</p>
管理 > 身分識別提供者	<p>[身分識別提供者] 頁面會列出您所設定的身分識別提供者。連接器是初始身分識別提供者。也可以新增協力廠商身分識別提供者執行個體，或同時使用兩者。</p> <p>VMware Identity Manager 內建身分識別提供者可設定為用於驗證。</p> <p>請參閱“新增和設定身分識別提供者執行個體,” 第 64 頁。</p>
管理 > 密碼恢復助理	<p>在 [密碼恢復助理] 頁面上，您可以變更使用者在登入畫面上按一下「忘記密碼」時的預設行為。</p>
管理 > 原則	<p>[原則] 頁面會列示預設存取原則，以及您建立的任何其他 Web 應用程式存取原則。原則是一組規則集，用於指定使用者存取其 [我的應用程式] 入口網站或啟動為其啟用的 Web 應用程式時所須遵循的準則。您可以編輯預設原則，且若 Web 應用程式新增至目錄，您也可以新增原則以管理對這些 Web 應用程式的存取。請參閱第 8 章, “管理存取原則,” 第 69 頁。</p>

與您的企業目錄整合

您可以整合 VMware Identity Manager 與您的企業目錄，以將使用者和群組從企業目錄同步至 VMware Identity Manager 服務。

支援的目錄類型如下。

- Active Directory over LDAP
- Active Directory, 整合式 Windows 驗證
- LDAP 目錄

若要整合企業目錄，您必須執行下列工作。

- 指定您要讓使用者在 VMware Identity Manager 服務中具備的屬性。
- 在 VMware Identity Manager 服務中建立與您的企業目錄相同類型的目錄，並指定連線詳細資料。
- 將 VMware Identity Manager 屬性對應至您 Active Directory 或 LDAP 目錄中使用的屬性。
- 指定要同步的使用者和群組。
- 同步使用者和群組。

在您整合企業目錄並執行初始同步後，您可以更新組態、設定會定期執行同步的同步排程，或隨時啟動同步。

目錄整合的相關重要概念

若要瞭解 VMware Identity Manager 服務如何與您的 Active Directory 或 LDAP 目錄環境整合，則必須具備幾項整體概念。

連接器

服務元件連接器將執行下列功能。

- 將使用者和群組資料從您的 Active Directory 或 LDAP 目錄同步至服務。
- 做為身分識別提供者時，驗證服務的使用者。

連接器是預設身分識別提供者。您也可以使用支援 SAML 2.0 通訊協定的第三方身分識別提供者。如果根據您的企業安全性原則，第三方身分識別提供者更為適用，請針對連接器不支援的驗證類型使用第三方身分識別提供者。

備註 如果您使用第三方身分識別提供者，您可以將連接器設定為同步使用者和群組資料，也可以設定 Just-in-Time 使用者佈建。如需詳細資訊，請參閱《VMware Identity Manager 管理》中的〈Just-in-Time 使用者佈建〉一節。

目錄

VMware Identity Manager 服務有其本身的目錄概念，對應於您環境中的 Active Directory 或 LDAP 目錄。此目錄會使用屬性來定義使用者和群組。您可以在服務中建立一或多個目錄，然後將這些目錄與 Active Directory 或 LDAP 目錄同步。您也可以在此服務中建立下列目錄類型。

- Active Directory
 - Active Directory over LDAP。如果您計劃連線至單一 Active Directory 網域環境，請建立此目錄類型。對於 Active Directory over LDAP 目錄類型，連接器使用簡單繫結驗證繫結至 Active Directory。
 - Active Directory (整合式 Windows 驗證)。如果您計劃連線至多網域或多樹系 Active Directory 環境，請建立此目錄類型。連接器使用整合式 Windows 驗證繫結至 Active Directory。

視您的 Active Directory 環境 (例如單一網域或多網域) 以及網域之間使用的信任類型而定，您所建立的目錄類型和數目會有所不同。在大多數環境中，建立一個目錄。

- LDAP 目錄

服務無法直接存取您的 Active Directory 或 LDAP 目錄。只有連接器可以直接存取。因此，您可將服務中建立的每一個目錄與連接器執行個體相關聯。

Worker

將目錄與連接器執行個體相關聯時，連接器會為名稱為 Worker 的相關聯目錄建立一個磁碟分割。連接器執行個體可將多個 Worker 與其關聯。每個 Worker 都充當一個身分識別提供者。您可針對每個 Worker 定義並設定驗證方法。

連接器可透過一或多個 Worker，同步您的 Active Directory 或 LDAP 目錄與服務之間的使用者和群組資料。

重要事項 您無法在同一連接器執行個體上擁有類型為整合式 Windows 驗證的兩個 Active Directory Worker。

安全考量事項

針對與 VMware Identity Manager 服務整合的企業目錄，必須直接在企業目錄中設定使用者密碼複雜性規則和帳戶鎖定原則之類的安全設定。VMware Identity Manager 不會覆寫這些設定。

與 Active Directory 整合

您可以整合 VMware Identity Manager 與 Active Directory 部署，以將使用者和群組從 Active Directory 同步至 VMware Identity Manager。

另請參閱“目錄整合的相關重要概念,” 第 13 頁。

本章節討論下列主題:

- “Active Directory 環境,” 第 15 頁
- “關於網域控制站選項 (domain_krb.properties 檔案),” 第 17 頁
- “管理從 Active Directory 同步的使用者屬性,” 第 20 頁
- “加入網域所需的權限,” 第 21 頁
- “設定服務的 Active Directory 連線,” 第 22 頁
- “讓使用者能夠變更 Active Directory 密碼,” 第 26 頁
- “設定目錄同步保護,” 第 27 頁

Active Directory 環境

您可以將服務與 Active Directory 環境整合，該環境可由單一 Active Directory 網域、單一 Active Directory 樹系中的多個網域，或多個 Active Directory 樹系中的多個網域組成。

單一 Active Directory 網域環境

單一 Active Directory 部署可讓您同步單一 Active Directory 網域中的使用者和群組。

針對此環境，將目錄新增至服務時，請選取 Active Directory over LDAP 選項。

如需詳細資訊，請參閱：

- “關於網域控制站選項 (domain_krb.properties 檔案),” 第 17 頁
- “管理從 Active Directory 同步的使用者屬性,” 第 20 頁
- “加入網域所需的權限,” 第 21 頁
- “設定服務的 Active Directory 連線,” 第 22 頁

擁有多網域的單一樹系 Active Directory 環境

擁有多網域的單一樹系 Active Directory 部署可讓您同步單一樹系內多個 Active Directory 網域中的使用者和群組。

您可針對此 Active Directory 環境，將服務設定為單一 Active Directory (整合式 Windows 驗證) 目錄類型；或者，將服務設定為設定有全域目錄選項的 Active Directory over LDAP 目錄類型。

- 建議的選項是建立單一 Active Directory (整合式 Windows 驗證) 目錄類型。

為此環境新增目錄時，請選取 Active Directory (整合式 Windows 驗證) 選項。

如需詳細資訊，請參閱：

- “關於網域控制站選項 (domain_krb.properties 檔案),” 第 17 頁
- “管理從 Active Directory 同步的使用者屬性,” 第 20 頁
- “加入網域所需的權限,” 第 21 頁
- “設定服務的 Active Directory 連線,” 第 22 頁
- 如果整合式 Windows 驗證無法在您的 Active Directory 環境中運作，請建立 Active Directory over LDAP 目錄類型，然後選取全域目錄選項。

選取全域目錄選項的部分限制包括：

- 複寫至全域目錄的 Active Directory 物件屬性，在 Active Directory 結構描述中會被識別為部分屬性組 (PAS)。只有這些屬性可供服務用於屬性對應。如有需要，請編輯結構描述，以新增或移除儲存在全域目錄中的屬性。
- 全域目錄只會儲存萬用群組的群組成員資格 (成員屬性)。只有萬用群組會同步至服務。如有需要，請將群組的範圍從本機網域或全域變更為萬用。
- 您在服務中設定目錄時所定義的繫結 DN 帳戶，必須具有讀取 Token-Groups-Global-And-Universal (TGGAU) 屬性的權限。

Active Directory 會使用連接埠 389 和 636 進行標準 LDAP 查詢。對於全域目錄查詢，則會使用連接埠 3268 和 3269。

當您為全域目錄環境新增目錄時，請在設定期間指定下列項目。

- 選取 Active Directory over LDAP 選項。
- 取消選取此目錄支援 DNS 服務位置選項的核取方塊。
- 選取此目錄具有全域目錄選項。當您選取此選項時，伺服器連接埠號碼會自動變更為 3268。此外，由於在設定全域目錄選項時並不需要基準 DN，因此 [基準 DN] 文字方塊不會顯示。
- 新增 Active Directory 伺服器主機名稱。
- 如果您的 Active Directory 需要透過 SSL 進行存取，請選取此目錄要求所有連線使用 SSL 選項，然後將憑證貼到提供的文字方塊中。當您選取此選項時，伺服器連接埠號碼會自動變更為 3269。

具備信任關係的多樹系 Active Directory 環境

具備信任關係的多樹系 Active Directory 部署，可讓您在網域之間存在雙向信任的所有樹系中，同步多個 Active Directory 網域中的使用者和群組。

為此環境新增目錄時，請選取 Active Directory (整合式 Windows 驗證) 選項。

如需詳細資訊，請參閱：

- “關於網域控制站選項 (domain_krb.properties 檔案),” 第 17 頁
- “管理從 Active Directory 同步的使用者屬性,” 第 20 頁
- “加入網域所需的權限,” 第 21 頁
- “設定服務的 Active Directory 連線,” 第 22 頁

不具備信任關係的多樹系 Active Directory 環境

不具備信任關係的多樹系 Active Directory 部署，可讓您在網域之間不存在信任關係的所有樹系之間，同步多個 Active Directory 網域中的使用者和群組。在此環境中，您在服務中建立多個目錄，為每一個樹系建立一個目錄。

在服務中建立的目錄類型視樹系而定。針對具備多個網域的樹系，請選取 Active Directory (整合式 Windows 驗證) 選項。針對具備單一網域的樹系，請選取 Active Directory over LDAP 選項。

如需詳細資訊，請參閱：

- “關於網域控制站選項 (domain_krb.properties 檔案),” 第 17 頁
- “管理從 Active Directory 同步的使用者屬性,” 第 20 頁
- “加入網域所需的權限,” 第 21 頁
- “設定服務的 Active Directory 連線,” 第 22 頁

關於網域控制站選項 (domain_krb.properties 檔案)

domain_krb.properties 檔案會決定要針對已啟用 DNS 服務位置 (SRV 記錄) 查閱之目錄所使用的網域控制站。它包含每個網域的網域控制站清單。一開始連接器會建立檔案，但您後續必須加以維護。此檔案會覆寫 DNS 服務位置 (SRV) 查閱。

下列類型的目錄已啟用 DNS 服務位置查閱：

- 已選取此目錄支援 DNS 服務位置選項的 Active Directory over LDAP。
- Active Directory (整合式 Windows 驗證)，其一律會啟用 DNS 服務位置查閱

當您先建立已啟用 DNS 服務位置查閱的目錄時，系統會自動在虛擬機器的 /usr/local/horizon/conf 目錄中建立 domain_krb.properties 檔案，並對每個網域自動填入網域控制站。為了填入檔案，連接器會嘗試尋找與連接器相同站台的網域控制站，並選取兩個可連接與回應最快的連接器。

建立已啟用 DNS 服務位置的其他目錄，或新增網域至整合式 Windows 驗證目錄時，系統會將新網域和其網域控制站的清單新增至檔案。

您可以隨時透過編輯 domain_krb.properties 檔案來覆寫預設選項。最佳做法是在您建立目錄後檢視 domain_krb.properties 檔案，並確認所列出的網域控制站是您組態的理想選擇。針對具有跨不同地理位置之多個網域控制站的全域 Active Directory 部署，使用與連接器鄰近的網域控制站可確保與 Active Directory 的通訊更快速。

您也必須手動更新檔案以進行任何其他變更。適用下列規則。

- domain_krb.properties 檔案會在包含連接器的虛擬機器中建立。在沒有部署其他連接器的一般部署中，則會在 VMware Identity Manager 服務虛擬機器中建立檔案。如果您針對目錄使用其他連接器，則會在連接器虛擬機器中建立檔案。一部虛擬機器只能有一個 domain_krb.properties 檔案。
- 隨即建立檔案，並且當您先建立已啟用 DNS 服務位置查閱的目錄時，系統會為每個網域自動填入網域控制站。
- 每個網域的網域控制站將以優先順序列出。為了連接至 Active Directory，連接器會嘗試清單中的第一個網域控制站。如果無法連線，它會嘗試清單中的第二個，以此類推。
- 只有在您建立已啟用 DNS 服務位置查閱的新目錄，或是新增網域至整合式 Windows 驗證目錄時，該檔案才會更新。新網域和其網域控制站的清單會新增至檔案。

請注意，如果檔案中已存在某網域的項目，則不會更新檔案。例如，如果您建立目錄，然後將它刪除，則原始網域項目會保留在檔案中，並且不會加以更新。

- 在任何其他案例中均不會自動更新檔案。例如，如果您刪除目錄，則不會從檔案刪除網域項目。

- 如果檔案中所列出的某個網域控制站無法連接，請編輯該檔案並加以移除。
- 如果手動新增或編輯網域項目，則不會覆寫您的變更。

如需編輯 `domain_krb.properties` 檔案的相關資訊，請參閱“[編輯 domain_krb.properties 檔案](#),” 第 19 頁。

重要事項 `/etc/krb5.conf` 檔案必須與 `domain_krb.properties` 檔案一致。每當您更新 `domain_krb.properties` 檔案時，請同時更新 `krb5.conf` 檔案。如需詳細資訊，請參閱“[編輯 domain_krb.properties 檔案](#),” 第 19 頁和[知識庫文章 2091744](#)。

如何選取網域控制站以自動填入 `domain_krb.properties` 檔案

為了自動填入 `domain_krb.properties` 檔案，系統會先判斷連接器所在的子網路 (根據 IP 位址和網路遮罩) 來選取網域控制站，然後使用 Active Directory 組態來識別該子網路的站台、取得該站台的網域控制站清單、篩選清單以取得適當網域，並選取回應最快的兩個網域控制站。

若要偵測最鄰近的網域控制站，VMware Identity Manager 有下列需求：

- Active Directory 組態中必須出現連接器的子網路，或必須在 `runtime-config.properties` 檔案中指定子網路。請參閱“[覆寫預設子網路選擇](#),” 第 18 頁。

子網路是用來判斷站台。

- Active Directory 組態必須是站台感知。

如果無法判斷子網路，或如果您的 Active Directory 組態不是站台感知，則會使用 DNS 服務位置查閱來尋找網域控制站，並且以一些可連接的網域控制站來填入檔案。請注意，這些網域控制站不能與連接器位在相同的地理位置，因為如此可能在與 Active Directory 通訊時造成延遲或逾時。在此情況下，請手動編輯 `domain_krb.properties` 檔案，並指定要用於每個網域的正確網域控制站。請參閱“[編輯 domain_krb.properties 檔案](#),” 第 19 頁。

範例 `domain_krb.properties` 檔案

```
example.com=host1.example.com:389,host2.example.com:389
```

覆寫預設子網路選擇

為了自動填入 `domain_krb.properties` 檔案，連接器會嘗試尋找位在相同站台上的網域控制站，以便將連接器和 Active Directory 之間的延遲降至最低。

為了尋找網站，連接器會根據其 IP 位址和網路遮罩來判斷其所位在的子網路，接著使用 Active Directory 組態來識別該子網路的網站。如果虛擬機器的子網路不在 Active Directory 中，或是您想覆寫自動子網路選擇，則可在 `runtime-config.properties` 檔案中指定子網路。

程序

- 1 以根使用者身分登入 VMware Identity Manager 虛擬機器。

備註 如果您針對目錄使用其他連接器，請登入連接器虛擬機器。

- 2 編輯 `/usr/local/horizon/conf/runtime-config.properties` 檔案，新增下列屬性。

```
siteaware.subnet.override=subnet
```

其中 `subnet` 是您想使用其網域控制站之網站的子網路。例如：

```
siteaware.subnet.override=10.100.0.0/20
```

- 3 儲存並關閉該檔案。

- 4 重新啟動服務。

```
service horizon-workspace restart
```

編輯 domain_krb.properties 檔案

`/usr/local/horizon/conf/domain_krb.properties` 檔案會決定已啟用 DNS 服務位置查閱的目錄將使用哪個網域控制站。您隨時可以編輯此檔案，以便修改網域的網域控制站清單，或是新增或刪除網域項目。您的變更不會被覆寫。

此檔案一開始由連接器建立並自動填入。遇到如下情形時，您必須手動更新此檔案。

- 如果依預設選取的網域控制站對您的組態而言不是最佳選擇，請編輯檔案並指定要使用的網域控制站。
- 如果您刪除目錄，請從檔案中刪除對應的網域項目。
- 如果檔案中有任何網域控制站無法連線，請從檔案中將其移除。

另請參閱“關於網域控制站選項 (`domain_krb.properties` 檔案),” 第 17 頁。

程序

- 1 以根使用者身分登入 VMware Identity Manager 虛擬機器。

備註 如果您針對目錄使用其他連接器，請登入連接器虛擬機器。

- 2 將目錄變更至 `/usr/local/horizon/conf`。
- 3 編輯 `domain_krb.properties` 檔案，以新增或編輯網域對主機值清單。

使用以下格式：

```
domain=host:port,host2:port,host3:port
```

例如：

```
example.com=examplehost1.example.com:389,examplehost2.example.com:389
```

請依優先順序列出網域控制站。為了連接至 Active Directory，連接器會嘗試清單中的第一個網域控制站。如果無法連線，它會嘗試清單中的第二個，以此類推。

重要事項 網域名稱必須是小寫字母。

- 4 使用下列命令，將 `domain_krb.properties` 檔案的擁有者變更為 `horizon`，以及將群組變更為 `www`。

```
chown horizon:www /usr/local/horizon/conf/domain_krb.properties
```

- 5 重新啟動服務。

```
service horizon-workspace restart
```

下一個

在編輯 `domain_krb.properties` 檔案後，接著編輯 `/etc/krb5.conf` 檔案。`krb5.conf` 檔案必須與 `domain_krb.properties` 檔案一致。

- 1 編輯 `/etc/krb5.conf` 檔案並更新領域區段，以指定在 `/usr/local/horizon/conf/domain_krb.properties` 檔案中使用的相同「網域-主機」值。您不需要指定連接埠號碼。例如，如果您的 `domain_krb.properties` 檔案具有網域項目 `example.com=examplehost.example.com:389`，則您應將 `krb5.conf` 檔案更新為下列內容。

```
[realms]
GAUTO-QA.COM = {
auth_to_local = RULE:[1:$0\1](^GAUTO-QA\.COM\.*s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\1](^GAUTO-QA\.COM\.*s/^GAUTO-QA\.COM/GAUTO-QA/
```

```

auth_to_local = RULE:[1:$0\$1](^GAUTO2QA\.GAUTO-QA\.COM\\.*s/^GAUTO2QA\.GAUTO-
QA\.COM/GAUTO2QA/
auth_to_local = RULE:[1:$0\$1](^GLOBEQUE\.NET\\.*s/^GLOBEQUE\.NET/GLOBEQUE/
auth_to_local = DEFAULT
kdc = examplehost.example.com
}

```

備註 可以有多个 kdc 項目。不過不一定要如此，因為 kdc 值通常只有一個。如果您選擇定義其他 kdc 值，則每一行會各有一個 kdc 項目，分別定義一個網域控制站。

2 重新啟動工作區服務。

```
service horizon-workspace restart
```

另請參閱[知識庫文章 2091744](#)。

疑難排解 domain_krb.properties

使用下列資訊以疑難排解 domain_krb.properties 檔案。

「解析網域發生錯誤」錯誤

如果 domain_krb.properties 檔案已包含網域項目，而您嘗試建立相同網域之不同類型的新目錄，就會發生「解析網域發生錯誤」。您必須在建立新目錄前，先編輯 domain_krb.properties 檔案並手動移除網域項目。

網域控制站無法存取

網域項目新增至 domain_krb.properties 檔案後，並不會自動更新。如果檔案中列出的任何網域控制站變成無法存取，請手動編輯檔案並將其移除。

管理從 Active Directory 同步的使用者屬性

在 VMware Identity Manager 服務目錄設定期間，請選取 Active Directory 使用者屬性和篩選器，以選取要在 VMware Identity Manager 目錄中同步的使用者。您可以從管理主控台上 [身分識別和存取管理] 索引標籤的 [設定] > [使用者屬性] 變更同步的使用者屬性。

已做出且儲存在 [使用者屬性] 頁面中的變更，將新增至 VMware Identity Manager 目錄中的 [對應屬性] 頁面。在下次與 Active Directory 同步時，將屬性變更更新至目錄中。

[使用者屬性] 頁面會列出可對應至 Active Directory 屬性的預設目錄屬性。您可選取所需屬性，並新增其他要同步到目錄的 Active Directory 屬性。新增屬性時，您輸入的屬性名稱會區分大小寫。例如 address、Address 和 ADDRESS 是不同的屬性。

表格 3-1. 要同步到目錄的預設 Active Directory 屬性

VMware Identity Manager 目錄屬性名稱	Active Directory 屬性的預設對應
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
網域	canonicalName。新增物件的完整網域名稱。
已停用 (已停用外部使用者)	userAccountControl。標記為 UF_Account_Disable 停用帳戶時，使用者無法登入以存取其應用程式和資源。系統不會從帳戶中移除使用者授權的資源，以便從帳戶中移除旗標後，使用者仍可登入並存取其已獲授權的資源
手機	telephoneNumber
lastName	sn

表格 3-1. 要同步到目錄的預設 Active Directory 屬性 (繼續)

VMware Identity Manager 目錄屬性名稱	Active Directory 屬性的預設對應
firstName	givenName
電子郵件	mail
userName	sAMAccountName。

選取要與目錄同步的屬性

當您設定 VMware Identity Manager 目錄以與 Active Directory 同步時，請指定要同步至目錄的使用者屬性。設定目錄前，您可以在 [使用者屬性] 頁面上指定所需的預設屬性，並新增要對應至 Active Directory 屬性的其他屬性。

在建立目錄前設定 [使用者屬性] 頁面時，您可以將預設屬性從需要變更為不需要、按需要標示屬性以及新增自訂屬性。

目錄建立後，您可以將需要屬性變更為不需要，並可以刪除自訂屬性。無法將屬性變更為需要屬性。

在目錄建立後，若要新增其他要同步至目錄的屬性，請移至目錄的 [已對應屬性] 頁面，將這些屬性與 Active Directory 屬性對應。

重要事項 如果計劃將 XenApp 資源與 VMware Identity Manager 同步，您必須將 **distinguishedName** 設為需要屬性。必須在建立 VMware Identity Manager 目錄前指定此項目。

程序

- 1 在管理主控台的 [身分識別和存取管理] 索引標籤中，按一下 **設定 > 使用者屬性**。
- 2 在 [預設屬性] 區段中，檢閱需要屬性清單並做出適當變更，以反映需要的屬性。
- 3 在 [屬性] 區段中，將 VMware Identity Manager 目錄屬性名稱新增至清單。
- 4 按一下 **儲存**。
預設屬性狀態已更新，您新增的屬性已新增至目錄的 [已對應屬性] 清單。
- 5 目錄建立後，移至 **管理 > 目錄** 頁面並選取目錄。
- 6 按一下 **同步設定 > 對應的屬性**。
- 7 在已新增屬性的下拉式功能表中，選取要對應的 Active Directory 屬性。
- 8 按一下 **儲存**。

目錄會在下次同步至 Active Directory 時更新。

加入網域所需的權限

有時候您可能需要將 VMware Identity Manager 連接器加入網域。對於 Active Directory over LDAP 目錄，您可先建立目錄然後再加入網域。對於 Active Directory 類型的目錄 (整合式 Windows 驗證)，連接器會在您建立目錄時自動加入網域。在這兩種案例中，系統都會提示您輸入認證。

若要加入網域，您需要具備「將電腦加入 AD 網域」權限的 Active Directory 認證。這是在 Active Directory 中使用下列權限設定的：

- 建立電腦物件
- 刪除電腦物件

當您加入網域時，除非您指定了自訂 OU，否則系統會在 Active Directory 的預設位置中建立電腦物件。

如果您沒有加入網域的權限，請遵循下列步驟來加入網域。

- 1 請您的 Active Directory 管理員在公司原則決定的位置建立 Active Directory 中的電腦物件。提供連接器的主機名稱。請務必提供完整網域名稱，例如 `server.example.com`。



Tip 您可在管理主控台 [連接器] 頁面的**主機名稱**資料行中查看主機名稱。按一下**身分識別與存取管理 > 設定 > 連接器**，檢視 [連接器] 頁面。

- 2 電腦物件建立以後，使用 VMware Identity Manager 管理主控台中的任意網域使用者帳戶來加入網域。**連接器**頁面上提供**加入網域**命令，您可透過按一下**身分識別與存取管理 > 設定 > 連接器**來進行存取。

選項	說明
網域	選取或輸入要加入的 Active Directory 網域。請確定您輸入的是完整網域名稱。例如 <code>server.example.com</code> 。
網域使用者	有權將系統加入 Active Directory 網域之 Active Directory 使用者的使用者名稱。
網域密碼	使用者的密碼。
組織單位 (OU)	(選擇性) 電腦物件的組織單位 (OU)。此選項會在指定的 OU 中建立電腦物件，而非在預設電腦 OU 中建立。 例如， <code>ou=testou,dc=test,dc=example,dc=com</code> 。

設定服務的 Active Directory 連線

在管理主控台中，指定連線至您的 Active Directory 所需的資訊，並選取要與 VMware Identity Manager 目錄同步的使用者和群組。

Active Directory 連線選項是 Active Directory over LDAP 或 Active Directory 整合式 Windows 驗證。Active Directory over LDAP 連線支援 DNS 服務位置查閱。透過 Active Directory 整合式 Windows 驗證，您可以設定要加入的網域。

先決條件

- 在 [使用者屬性] 頁面上選取必要的屬性，並視需要新增其他屬性。請參閱“[選取要與目錄同步的屬性](#),” 第 21 頁。

重要事項 如果計劃將 XenApp 資源與 VMware Identity Manager 同步，您必須將 **distinguishedName** 設為必要屬性。您必須先進行此選擇，之後才能建立目錄，因為建立目錄之後，即無法將屬性變更為必要屬性。

- 要從 Active Directory 進行同步的 Active Directory 群組和使用者清單。
- 對於 Active Directory over LDAP，所需的資訊包括基準 DN、繫結 DN 及繫結 DN 密碼。

備註 建議您使用繫結 DN 使用者帳戶與不會到期的密碼。

- 對於 Active Directory 整合式 Windows 驗證，所需的資訊包括網域的繫結使用者 UPN 位址和密碼。

備註 建議您使用繫結 DN 使用者帳戶與不會到期的密碼。

- 如果 Active Directory 需要透過 SSL 或 STARTTLS 存取，則需要 Active Directory 網域控制站的根 CA 憑證。
- 對於 Active Directory 整合式 Windows 驗證，如果您已設定多樹系 Active Directory 並且網域本機群組包含來自不同樹系中網域的成員，請確保已將繫結使用者新增至網域本機群組所在網域的管理員群組。如果未這麼做，網域本機群組中會遺失這些成員。

程序

- 1 在管理主控台，按一下**身分識別與存取管理**索引標籤。
- 2 在 [目錄] 頁面上，按一下**新增目錄**。
- 3 輸入此 VMware Identity Manager 目錄的名稱。

4 選取在您環境中的 Active Directory 類型，並設定連線資訊。

選項	說明
Active Directory over LDAP	<p>a 在同步 Connector 欄位中，選取 連接器 以用來與 Active Directory 同步。</p> <p>b 在驗證欄位中，如果是使用此 Active Directory 來驗證使用者，請按一下是。</p> <p>如果是使用第三方身分識別提供者來驗證使用者，請按一下否。設定 Active Directory 連線來同步使用者和群組之後，前往 [身分識別與存取管理] > [管理] > [身分識別提供者] 頁面來新增用於驗證的第三方身分識別提供者。</p> <p>c 在目錄搜尋屬性欄位中，選取包含使用者名稱的帳戶屬性。</p> <p>d 如果 Active Directory 使用 DNS 服務位置查閱，請選取以下項目。</p> <ul style="list-style-type: none"> ■ 在伺服器位置區段中，選取此目錄支援 DNS 服務位置核取方塊。 當您建立目錄時，系統會建立自動填入網域控制站清單的 <code>domain_krb.properties</code> 檔案。請參閱“關於網域控制站選項 (domain_krb.properties 檔案),” 第 17 頁。 ■ 如果 Active Directory 要求 STARTTLS 加密，請在憑證區段中選取此目錄要求所有連線使用 SSL核取方塊，然後將 Active Directory 根 CA 憑證複製貼到 SSL 憑證欄位。 確認憑證為 PEM 格式且包含 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 文字行。 備註 如果 Active Directory 要求 STARTTLS 但您未提供憑證，將無法建立目錄。 <p>e 如果 Active Directory 不使用 DNS 服務位置查閱，請選取以下項目。</p> <ul style="list-style-type: none"> ■ 在伺服器位置區段中，確認此目錄支援 DNS 服務位置核取方塊未選取，然後輸入 Active Directory 伺服器主機名稱和連接埠號碼。 若要將目錄設定為全域目錄，請參閱“Active Directory 環境” 第 15 頁中的〈擁有多網域的單一樹系 Active Directory 環境〉一節。 ■ 如果 Active Directory 要求透過 SSL 存取，請在憑證區段中選取此目錄要求所有連線使用 SSL核取方塊，並將 Active Directory 根 CA 憑證複製和貼到 SSL 憑證欄位。 確認憑證為 PEM 格式且包含 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 文字行。 備註 如果 Active Directory 要求 SSL 但您未提供憑證，將無法建立目錄。 <p>f 在基準 DN 欄位中，輸入要從中開始帳戶搜尋的 DN。例如，<code>OU=myUnit,DC=myCorp,DC=com</code>。</p> <p>g 在繫結 DN 欄位中，輸入可搜尋使用者的帳戶。例如，<code>CN=binduser,OU=myUnit,DC=myCorp,DC=com</code>。 備註 建議您使用繫結 DN 使用者帳戶與不會到期的密碼。</p> <p>h 輸入繫結密碼之後，按一下測試連線以確認該目錄可以連線至您的 Active Directory。</p>
Active Directory (整合式 Windows 驗證)	<p>a 在同步連接器 欄位中，選取 連接器 以用來與 Active Directory 同步。</p> <p>b 在驗證欄位中，如果是使用此 Active Directory 來驗證使用者，請按一下是。</p> <p>如果是使用第三方身分識別提供者來驗證使用者，請按一下否。設定 Active Directory 連線來同步使用者和群組之後，前往 [身分識別與存取管理] > [管理] > [身分識別提供者] 頁面來新增用於驗證的第三方身分識別提供者。</p> <p>c 在目錄搜尋屬性欄位中，選取包含使用者名稱的帳戶屬性。</p> <p>d 如果 Active Directory 要求 STARTTLS 加密，請在憑證區段中選取此目錄要求所有連線使用 STARTTLS核取方塊，然後將 Active Directory 根 CA 憑證複製貼到 SSL 憑證欄位。</p>

選項	說明
	<p>確認憑證為 PEM 格式且包含 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 文字行。</p> <p>如果目錄有多個網域，請為所有網域新增根 CA 憑證，一次新增一個。</p> <p>備註 如果 Active Directory 要求 STARTTLS 但您未提供憑證，將無法建立目錄。</p> <p>e 輸入要加入之 Active Directory 網域的名稱。輸入擁有加入網域權限的使用者名稱和密碼。如需詳細資訊，請參閱“加入網域所需的權限,” 第 21 頁。</p> <p>f 在 [繫結使用者 UPN] 欄位中，輸入可透過網域進行驗證之使用者的使用者主體名稱。例如，username@example.com。</p> <p>備註 建議您使用繫結 DN 使用者帳戶與不會到期的密碼。</p> <p>g 輸入繫結使用者密碼。</p>

- 5 按一下**儲存 & 下一步**。

顯示網域清單的頁面隨即會顯示。

- 6 對於 Active Directory over LDAP，網域將與核取記號一併列出。

對於 Active Directory (整合式 Windows 驗證)，選取應與此 Active Directory 連線相關聯的網域。

備註 如果您在建立目錄後新增信任網域，則服務不會自動偵測到新的信任網域。若要讓服務能夠偵測到網域，連接器必須離開後再重新加入該網域。當連接器重新加入網域時，信任網域會顯示在清單中。

按**下一步**。

- 7 驗證 VMware Identity Manager 目錄屬性名稱對應至正確的 Active Directory 屬性，並視需要進行變更，然後按**下一步**。
- 8 選取要從 Active Directory 同步到 VMware Identity Manager 目錄的群組。

選項	說明
指定群組 DN	<p>若要選取群組，您必須指定一或多個群組 DN，並選取其下的群組。</p> <p>a 按一下 +，然後指定群組 DN。例如 CN=users,DC=example,DC=company,DC=com。</p> <p>重要事項 指定您在基準 DN 下所輸入的群組 DN。如果某個群組 DN 在基準 DN 的外部，則來自該 DN 的使用者仍會進行同步，但將無法登入。</p> <p>b 按一下尋找群組。</p> <p>要同步的群組資料行會列出在 DN 中找到的群組數目。</p> <p>c 若要選取 DN 中的所有群組，請按一下全選，否則請按一下選取，並選取要同步的特定群組。</p> <p>備註 同步群組時，在 Active Directory 中未使用網域使用者做為其主要群組的任何使用者，皆不會進行同步。</p>
同步巢狀群組成員	<p>依預設會啟用同步巢狀群組成員選項。啟用此選項時，系統會同步直接屬於您選取群組的所有使用者，以及屬於其下巢狀群組的所有使用者。請注意，系統不會對巢狀群組進行同步；只會對屬於巢狀群組的使用者進行同步。在 VMware Identity Manager 目錄中，這些使用者將會是您選取要同步之父系群組的成員。</p> <p>如果停用同步巢狀群組成員選項，當您指定要同步的群組時，將會對直接屬於該群組的所有使用者進行同步。系統不會對屬於其下方巢狀群組的使用者進行同步。停用此選項對於大型 Active Directory 組態有幫助，其中，周遊群組樹狀目錄為耗用大量資源和時間的作業。如果您停用此選項，請確保您選取您要同步其使用者的所有群組。</p>

- 9 按**下一步**。

- 10 如有必要，請指定其他要同步的使用者。
 - a 按一下 **+**，然後輸入使用者 DN。例如
CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com。

重要事項 指定您在基準 DN 下所輸入的使用者 DN。如果某個使用者 DN 在基準 DN 的外部，則來自該 DN 的使用者仍會進行同步，但將無法登入。

- b (選用) 若要排除使用者，請建立篩選器以排除某些使用者類型。
選取要做為篩選依據的使用者屬性、查詢規則及值。
- 11 按**下一步**。
- 12 檢閱頁面，以查看將同步至目錄的使用者和群組數目，以及檢視同步排程。
若要對使用者和群組或同步頻率進行變更，請按一下**編輯**連結。
- 13 按一下**同步目錄**來開始同步至目錄。

Active Directory 的連線隨即建立，且使用者和群組會從 Active Directory 同步至 VMware Identity Manager 目錄。依預設，繫結 DN 使用者會具有 VMware Identity Manager 中的管理員角色。

下一個

- 如果您建立支援 DNS 服務位置的目錄，系統會建立 `domain_krb.properties` 檔案，並自動填入網域控制站的清單。檢視檔案來確認或編輯網域控制站的清單。請參閱“[關於網域控制站選項 \(domain_krb.properties 檔案\)](#),” 第 17 頁。
- 設定驗證方法。當使用者和群組同步到目錄後，如果連接器同樣用於驗證，則可在連接器上設定其他驗證方法。如果驗證身分識別提供者為第三方，請在連接器中設定該身分識別提供者。
- 檢閱預設的存取原則。已將預設存取原則設定為允許所有網路範圍中的所有應用裝置存取網頁瀏覽器 (工作階段逾時設為八小時) 或存取用戶端應用程式 (工作階段逾時為 2160 小時，即 90 天)。您可以變更預設存取原則，並且當您新增 Web 應用程式至目錄時可建立新原則。
- 將自訂商標套用至管理主控台、使用者入口網站頁面和登入螢幕。

讓使用者能夠變更 Active Directory 密碼

您可以讓使用者能夠在需要時，從 Workspace ONE 入口網站或應用程式變更其 Active Directory 密碼。若密碼到期，或 Active Directory 管理員重設密碼而強制在下次登入時變更密碼，使用者也可以從 VMware Identity Manager 登入頁面變更其 Active Directory 密碼。

您可以在 [目錄設定] 頁面中選取**允許變更密碼**，以就個別的目錄啟用此選項。

使用者可以在登入 Workspace ONE 入口網站時變更其密碼，方法是在右上角按一下其名稱，接著從下拉式功能表中選取**帳戶**，然後按一下**變更密碼**連結。在 Workspace ONE 應用程式中，使用者可以透過按一下三列式功能表圖示，再選取**密碼**來變更其密碼。

到期的密碼或 Active Directory 中管理員所重設的密碼，皆可從登入頁面變更。當使用者嘗試以到期的密碼登入時，使用者將會看見重設密碼的提示。使用者必須輸入舊密碼和新密碼。

新密碼的需求由 Active Directory 密碼原則決定。允許的嘗試次數同樣也取決於 Active Directory 密碼原則。

適用下列限制。

- 如果您使用其他外部連接器虛擬應用裝置，則請注意**允許變更密碼**選項僅適用於連接器 2016.11.1 版和更新版本。
- 當目錄新增至 VMware Identity Manager 作為全域目錄時，**允許變更密碼**選項將無法使用。目錄可使用連接埠 389 或 636 新增為 Active Directory over LDAP 或整合式 Windows 驗證。

- 即使密碼已到期或 Active Directory 管理員重設了密碼，繫結 DN 使用者的密碼仍無法從 VMware Identity Manager 進行重設。

備註 建議您使用繫結 DN 使用者帳戶與不會到期的密碼。

- 使用者的登入名稱若包含多位元組字元 (非 ASCII 字元)，則無法從 VMware Identity Manager 重設該使用者的密碼。

先決條件

- 若要啟用**允許變更密碼**選項，您必須使用繫結 DN 使用者帳戶，且必須具有 Active Directory 的寫入權限。
- 必須在網域控制站上開啟連接埠 464。

程序

- 1 在管理主控台，按一下**身分識別與存取管理**索引標籤。
- 2 在**目錄**索引標籤中，按一下**目錄**。
- 3 在**允許變更密碼**區段中，選取**啟用變更密碼**核取方塊。
- 4 在**繫結使用者詳細資料**區段中輸入繫結 DN 密碼，然後按一下**儲存**。

設定目錄同步保護

您可以在目錄中設定同步保護臨界值限制，以避免從 Active Directory 同步到目錄的使用者和群組受到意外的組態變更。

設定的同步保護臨界值可限制目錄同步時針對使用者和群組所做的變更數目。在達到目錄保護臨界值時，目錄同步化隨即停止，且目錄的 [同步記錄] 頁面上會顯示一則訊息。在 VMware Identity Manager 管理主控台中設定 SMTP 時，如果同步化因保護違規而失敗，您將會收到一則電子郵件訊息。

同步化失敗時，您可以移至目錄的 [同步設定] > [同步記錄] 頁面，以檢視保護違規類型的說明。

若要順利完成同步化，您可以在 [同步保護] 設定頁面上增加保護的百分比臨界值，或排程同步的試執行並勾選 [忽略保護]。當您選擇忽略保護臨界值時，將只有這個同步工作階段不會強制執行保護值。

第一次執行目錄同步時，並不會強制執行同步保護值。

備註 如果您不想使用同步保護功能，請從下拉式功能表中刪除其值。當同步保護臨界值文字方塊為空白時，將不會啟用同步保護。

設定目錄同步保護

設定同步保護措施臨界值設定，可限制在目錄同步時對使用者和群組所做的變更數目。

備註 如果您不想使用同步保護功能，請從下拉式功能表中刪除其值。當同步保護臨界值文字方塊為空白時，將不會啟用同步保護。

程序

- 1 若要變更保護設定，請在 [身分識別與存取管理] 索引標籤中選取**管理 > 目錄**。
- 2 選取要設定保護的目錄，然後按一下**同步設定**。
- 3 按一下**保護**。
- 4 設定要觸發同步作業失敗的變更百分比。
- 5 按一下**儲存**。

忽略保護設定以完成對目錄的同步

當您因保護違規而收到未完成同步的通知時，若要覆寫保護設定並完成同步，您可以排程同步的試執行，並勾選 [忽略保護]。

程序

- 1 在 [身分識別與存取管理] 索引標籤中，選取**管理 > 目錄**。
- 2 選取未完成同步的目錄，然後移至**同步記錄**頁面。
- 3 若要檢視保護違規的類型，請在 [同步詳細資料] 資料行中按一下**無法完成同步。請檢查保護設定**。
- 4 按一下**確定**。
- 5 若要繼續同步而不變更保護設定，請按一下**立即同步**。
- 6 在 [檢閱] 頁面上，選取**忽略保護**核取方塊。
- 7 按一下**同步目錄**。

目錄同步隨即執行，且系統會針對此同步工作階段忽略其保護臨界值設定。

與 LDAP 目錄整合

您可以將企業 LDAP 目錄與 VMware Identity Manager 整合，以將使用者和群組從 LDAP 目錄同步至 VMware Identity Manager 服務。

另請參閱“[目錄整合的相關重要概念](#),” 第 13 頁。

本章節討論下列主題:

- “[LDAP 目錄整合的限制](#),” 第 29 頁
- “[整合 LDAP 目錄與服務](#),” 第 30 頁

LDAP 目錄整合的限制

LDAP 目錄整合功能目前受到下列限制。

- 您只能整合單一網域 LDAP 目錄環境。

若要整合 LDAP 目錄中的多個網域，您必須為每個網域建立一個額外的 VMware Identity Manager 目錄。
- 屬於 LDAP 目錄類型的 VMware Identity Manager 目錄不支援下列驗證方法。
 - Kerberos 驗證
 - RSA 調適性驗證
 - 作為第三方身分識別提供者的 ADFS
 - SecurID
 - 使用 Vasco 和 SMS 通行碼伺服器的 Radius 驗證
- 您無法加入 LDAP 網域。
- 屬於 LDAP 目錄類型的 VMware Identity Manager 目錄不支援與 View 或 Citrix 發行的資源進行整合。
- 使用者名稱不可包含空格。如果使用者名稱包含空格，則系統仍會同步使用者，但使用者將不具有權利。
- 如果您預計要同時新增 Active Directory 和 LDAP 目錄，請確保您未在 [使用者屬性] 頁面中將使用者名稱 (可標示為必要) 以外的任何屬性標示為必要。[使用者屬性] 頁面中的設定會套用至服務中的所有目錄。如果屬性標示為必要，不具該屬性的使用者將不會同步至 VMware Identity Manager 服務。
- 如果您的 LDAP 目錄中有多個具有相同名稱的群組，則必須在 VMware Identity Manager 服務中為其指定唯一名稱。您可以在選取要同步的群組時指定這些名稱。
- 允許使用者重設過期密碼的選項無法使用。
- 不支援 domain_krb.properties 檔案。

整合 LDAP 目錄與服務

您可以將企業 LDAP 目錄與 VMware Identity Manager 整合，以將使用者和群組從 LDAP 目錄同步至 VMware Identity Manager 服務。

若要整合您的 LDAP 目錄，您必須建立對應的 VMware Identity Manager 目錄，並將使用者和群組從 LDAP 目錄同步至 VMware Identity Manager 目錄。您可以設定定期的同步排程以進行後續更新。

您也可以選取要為使用者同步的 LDAP 屬性，並將其對應至 VMware Identity Manager 屬性。

您的 LDAP 目錄組態可能是以預設結構描述為基礎，或您可能已建立自訂結構描述。您可能也定義了自訂屬性。若要讓 VMware Identity Manager 能夠查詢您的 LDAP 目錄以取得使用者或群組物件，您必須提供適用於 LDAP 目錄的 LDAP 搜尋篩選器和屬性名稱。

特別是，您必須提供下列資訊。

- 用以取得群組、使用者和繫結使用者的 LDAP 搜尋篩選器
- 群組成員資格的 LDAP 屬性名稱、UUID 和辨別名稱

LDAP 目錄整合功能有其特定限制。請參閱“[LDAP 目錄整合的限制](#),” 第 29 頁。

先決條件

- 如果您使用其他外部連接器虛擬應用裝置，則請注意，整合 LDAP 目錄的功能僅適用於連接器 2016.6.1 版和更新版本。
- 檢閱 **身分識別與存取管理 > 設定 > 使用者屬性** 頁面中的屬性，然後新增您要同步的其他屬性。後續在建立目錄時，您會將這些 VMware Identity Manager 屬性對應至 LDAP 目錄屬性。這些屬性會針對目錄中的使用者進行同步。

備註 當您對使用者屬性進行變更時，請考量這對服務中的其他目錄有何影響。如果您預計要同時新增 Active Directory 和 LDAP 目錄，請確保您未將**使用者名稱**(可標示為必要)以外的任何屬性標示為必要。[使用者屬性] 頁面中的設定會套用至服務中的所有目錄。如果屬性標示為必要，不具該屬性的使用者將不會同步至 VMware Identity Manager 服務。

- 繫結 DN 使用者帳戶。建議您使用繫結 DN 使用者帳戶與不會到期的密碼。
- 在您的 LDAP 目錄中，使用者和群組的 UUID 必須採用純文字格式。
- 在您的 LDAP 目錄中，所有的使用者和群組都必須要有網域屬性。
在建立 VMware Identity Manager 目錄時，您會將此屬性對應至 VMware Identity Manager **網域** 屬性。
- 使用者名稱不可包含空格。如果使用者名稱包含空格，則系統仍會同步使用者，但使用者將不具有權利。
- 如果您使用憑證驗證，則使用者必須要有 userPrincipalName 的值，以及電子郵件地址屬性。

程序

- 1 在管理主控台，按一下 **身分識別與存取管理** 索引標籤。
- 2 在 [目錄] 頁面中按一下 **新增目錄**，然後選取 **新增 LDAP 目錄**。

- 3 在 [新增 LDAP 目錄] 頁面中輸入必要資訊。

選項	說明
目錄名稱	VMware Identity Manager 目錄的名稱。
目錄同步和驗證	<p>a 在同步連接器欄位中，選取要用來將使用者和群組從 LDAP 目錄同步至 VMware Identity Manager 目錄的連接器。</p> <p>依預設，VMware Identity Manager 服務隨時附有可用的連接器元件。此連接器會顯示在下拉式清單中。如果您為了實現高可用性而安裝多個 VMware Identity Manager 應用裝置，每個連接器元件均會顯示在清單中。</p> <p>您不需要為單一 LDAP 目錄使用個別的連接器。無論這些目錄是 Active Directory 或 LDAP 目錄，一個連接器可支援多個目錄。</p> <p>若想瞭解需要其他連接器的案例，請參閱《VMware Identity Manager 安裝指南》中的〈安裝其他連接器應用裝置〉。</p> <p>b 在驗證欄位中，如果您想要使用此 LDAP 目錄來驗證使用者，請選取是。</p> <p>如果您想要使用第三方身分識別提供者來驗證使用者，請選取否。在新增要用來同步使用者和群組的目錄連線後，請移至身分識別與存取管理 > 管理 > 身分識別提供者頁面，新增用於驗證的第三方身分識別提供者。</p> <p>c 在目錄搜尋屬性欄位中，指定要用於使用者名稱的 LDAP 目錄屬性。如果屬性未列出，請選取自訂，並輸入屬性名稱。例如 cn。</p>
伺服器位置	<p>輸入 LDAP Directory 伺服器主機和連接埠號碼。對於伺服器主機，您可以指定完整網域名稱或 IP 位址。例如 myLDAPserver.example.com 或 100.00.00.0。</p> <p>如果在負載平衡器後方有伺服器叢集，請改為輸入負載平衡器資訊。</p>
LDAP 組態	<p>指定可讓 VMware Identity Manager 用來查詢您的 LDAP 目錄的 LDAP 搜尋篩選器和屬性。系統會根據核心 LDAP 結構描述提供預設值。</p> <p>LDAP 查詢</p> <ul style="list-style-type: none"> ■ 取得群組：用來取得群組物件的搜尋篩選器。 <p>例如：(objectClass=group)</p> <ul style="list-style-type: none"> ■ 取得繫結使用者：用來取得繫結使用者物件 (繫結至目錄的使用者) 的搜尋篩選器。 <p>例如：(objectClass=person)</p> <ul style="list-style-type: none"> ■ 取得使用者：用來取得所要同步之使用者的搜尋篩選器。 <p>例如：(&(objectClass=user)(objectCategory=person))</p> <p>屬性</p> <ul style="list-style-type: none"> ■ 成員資格：在您的 LDAP 目錄中用來定義群組成員的屬性。 <p>例如：member</p> <ul style="list-style-type: none"> ■ 物件 UUID：在您的 LDAP 目錄中用來定義使用者或群組之 UUID 的屬性。 <p>例如：entryUUID</p> <ul style="list-style-type: none"> ■ 辨別名稱：在您的 LDAP 目錄中用於使用者或群組之辨別名稱的屬性。 <p>例如：entryDN</p>

選項	說明
憑證	如果您的 LDAP 目錄需要透過 SSL 進行存取，請選取 此目錄要求所有連線使用 SSL ，然後複製並貼上 LDAP 目錄伺服器的根 CA SSL 憑證。確認憑證為 PEM 格式且包含 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 文字行。
繫結使用者詳細資料	基準 DN ：輸入要從中開始搜尋的 DN。例如 <code>cn=users,dc=example,dc=com</code> 繫結 DN ：輸入要用來繫結至 LDAP 目錄的使用者名稱。 備註 建議您使用繫結 DN 使用者帳戶與不會到期的密碼。 繫結 DN 密碼 ：輸入繫結 DN 使用者的密碼。

- 若要測試 LDAP 目錄伺服器的連線，請按一下**測試連線**。
如果連線失敗，請檢查您所輸入的資訊，並進行適當的變更。
- 按一下**儲存 & 下一步**。
- 在 [網域] 頁面中，確認正確的網域已列出，然後按**下一步**。
- 在 [對應屬性] 頁面中，確認 VMware Identity Manager 屬性已對應至正確的 LDAP 屬性。

重要事項 您必須指定**網域**屬性的對應。

您可以在 [使用者屬性] 頁面中，將屬性新增至清單。

- 按**下一步**。
- 在群組頁面中按一下 **+**，以選取要從 LDAP 目錄同步至 VMware Identity Manager 目錄的群組。

如果您的 LDAP 目錄中有多個具有相同名稱的群組，您必須在群組頁面中為其指定唯一名稱。

依預設，**同步巢狀群組使用者**選項已啟用。啟用此選項時，系統會同步直接屬於您選取群組的所有使用者，以及屬於其下巢狀群組的所有使用者。請注意，系統不會對巢狀群組進行同步；只會對屬於巢狀群組的使用者進行同步。在 VMware Identity Manager 目錄中，這些使用者會顯示為選為同步之群組的最上層群組成員。實際上，所選群組下的階層將會扁平化，而所有層級中的使用者都會在 VMware Identity Manager 中顯示為所選群組的成員。

如果停用此選項，則指定要同步的群組時，會對直接屬於該群組的所有使用者進行同步。系統不會對屬於其下方巢狀群組的使用者進行同步。停用此選項，對於周遊群組樹狀目錄會耗用大量資源和時間的大型目錄組態，將有所幫助。如果您停用此選項，請確保您選取您要同步其使用者的所有群組。

- 按**下一步**。
- 按一下 **+** 以新增其他使用者。例如，輸入 `CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com`。
若要排除使用者，請建立篩選器以排除某些使用者類型。選取要做為篩選依據的使用者屬性、查詢規則及值。
按**下一步**。
- 檢閱頁面以查看將同步至目錄的使用者和群組數目，以及檢視預設同步排程。
若要對使用者和群組或同步頻率進行變更，請按一下**編輯**連結。
- 按一下**同步目錄**以啟動目錄同步。

LDAP 目錄的連線隨即建立，且使用者和群組會從 LDAP 目錄同步至 VMware Identity Manager 目錄。依預設，繫結 DN 使用者會具有 VMware Identity Manager 中的管理員角色。

使用本機目錄

本機目錄是您可在 VMware Identity Manager 服務中建立的目錄類型之一。本機目錄可讓您將本機使用者佈建在服務中，並為他們提供特定應用程式的存取權，而不需將其新增至您的企業目錄。本機目錄不會連線至企業目錄，且不會從企業目錄中同步使用者和群組。您必須直接在本機目錄中建立本機使用者。

服務中所提供的預設本機目錄稱為「系統目錄」。您也可以建立多個新的本機目錄。

系統目錄

系統目錄是服務在第一次設定時自動建立的本機目錄。此目錄具有系統網域的網域。您無法變更系統目錄的名稱或網域，或是為其新增網域。您也無法刪除系統目錄或系統網域。

您在第一次設定 VMware Identity Manager 應用裝置時建立的本機管理員使用者，會建立在系統目錄的系統網域中。

您可以將其他使用者新增至系統目錄。系統目錄通常用來設定數個負責管理服務的本機管理員使用者。若要佈建使用者和其他管理員，並將應用程式授權給他們，建議您建立新的本機目錄。

本機目錄

您可以建立多個本機目錄。每個本機目錄可以有一或多個網域。當您建立本機使用者時，您可以指定使用者的目錄和網域。

您也可以為本機目錄中的所有使用者選取屬性。userName、lastName 和 firstName 等使用者屬性會指定於 VMware Identity Manager 服務的全域層級上。有預設屬性清單可供使用，且您可以新增自訂屬性。全域使用者屬性會套用至服務中的所有目錄，包括本機目錄。在本機目錄層級上，您可以選取目錄所需的屬性。這可讓您為不同的本機目錄建立自訂屬性集。請注意，本機目錄一律須有 userName、lastName、firstName 和電子郵件屬性。

備註 在目錄層級上自訂使用者屬性的功能僅適用於本機目錄，不適用於 Active Directory 或 LDAP 目錄。

在下列情況下，建立本機目錄將有所幫助。

- 您可以為不屬於您企業目錄的特定使用者類型，建立本機目錄。例如，您可以為通常不屬於您企業目錄的合作夥伴建立本機目錄，並使其僅能存取其所需的特定應用程式。
- 如果您想讓不同組的使用者有不同的使用者屬性或驗證方法，您可以建立多個本機目錄。例如，您可以為經銷商建立一個具有區域和市場大小等使用者屬性的本機目錄，並且為供應商建立另一個具有產品類別和供應商類型等使用者屬性的本機目錄。

系統目錄和本機目錄的身分識別提供者

依預設，系統目錄會與稱為「系統身分識別提供者」的身分識別提供者相關聯。此身分識別提供者依預設會啟用「密碼(雲端目錄)」方法，且此方法會套用至 [所有範圍] 網路範圍的 `default_access_policy_set` 原則，以及 Web 瀏覽器裝置類型。您可以設定其他驗證方法，以及設定驗證原則。

當您建立新的本機目錄時，該目錄並不會與任何身分識別提供者相關聯。在建立目錄之後，請建立類型為「內嵌」的新身分識別提供者，並將目錄與它產生關聯。對身分識別提供者啟用「密碼(雲端目錄)」驗證方法。同一個身分識別提供者可以有許多與其相關聯的本機目錄。

系統目錄或您所建立的本機目錄皆不需要 VMware Identity Manager Connector。

如需詳細資訊，請參閱《VMware Identity Manager 管理》中的〈在 VMware Identity Manager 中設定使用者驗證〉。

本機目錄使用者的密碼管理

依預設，本機目錄的所有使用者皆能在 Workspace ONE 入口網站或應用程式中變更其密碼。您可以設定本機使用者的密碼原則。您也可以視需要重設本機使用者密碼。

使用者可以在登入 Workspace ONE 入口網站時變更其密碼，方法是在右上角按一下其名稱，接著從下拉式功能表中選取**帳戶**，然後按一下**變更密碼**連結。在 Workspace ONE 應用程式中，使用者可以透過按一下三列式功能表圖示，再選取**密碼**來變更其密碼。

如需設定密碼原則及重設本機使用者密碼的相關資訊，請參閱《VMware Identity Manager 管理》中的〈管理使用者和群組〉。

本章節討論下列主題：

- “[建立本機目錄](#),” 第 34 頁
- “[變更本機目錄設定](#),” 第 38 頁
- “[刪除本機目錄](#),” 第 39 頁
- “[設定系統管理員使用者的驗證方法](#),” 第 39 頁

建立本機目錄

若要建立本機目錄，您可以指定目錄的使用者屬性、建立目錄，並使用身分識別提供者加以識別。

在全域層級設定使用者屬性

在建立本機目錄之前，請檢閱 [使用者屬性] 頁面上的全域使用者屬性，並視需要新增自訂屬性。

使用者屬性 (例如 `firstName`、`lastName`、電子郵件和網域) 是使用者設定檔的一部分。在 VMware Identity Manager 服務中，使用者屬性會定義於全域層級上，並且套用至服務中的所有目錄，包括本機目錄。在本機目錄層級上，您可以就某個屬性對於該本機目錄中的使用者而言屬於必要或選用進行覆寫，但您無法新增自訂屬性。如果屬性是必要的，您在建立使用者時就必須提供該屬性的值。

當您建立自訂屬性時無法使用下列文字。

表格 5-1. 無法用作自訂屬性名稱的文字

<code>active</code>	<code>addresses</code>	<code>costCenter</code>
<code>department</code>	<code>displayName</code>	<code>division</code>
<code>emails</code>	<code>employeeNumber</code>	<code>entitlements</code>
<code>externalId</code>	<code>groups</code>	<code>id</code>

表格 5-1. 無法用作自訂屬性名稱的文字 (繼續)

ims	locale	manager
meta	name	nickName
organization	password	phoneNumber
photos	preferredLanguage	profileUrl
roles	timezone	title
userName	userType	x509Certificate

備註 在目錄層級上覆寫使用者屬性的功能僅適用於本機目錄，而不適用於 Active Directory 或 LDAP 目錄。

程序

- 1 在管理主控台，按一下**身分識別與存取管理**索引標籤。
- 2 按一下**設定**，然後按一下**使用者屬性**索引標籤。
- 3 檢閱使用者屬性清單，並視需要新增其他屬性。

備註 雖然此頁面可讓您選取哪些是必要屬性，但仍建議您在本機目錄層級上選取本機目錄。在此頁面上標示為必要屬性，將會套用至服務中的所有目錄，包括 Active Directory 或 LDAP 目錄。

- 4 按一下**儲存**。

下一個

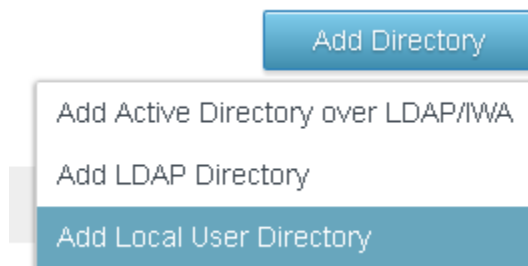
建立本機目錄。

建立本機目錄

在您檢閱及設定全域使用者屬性後，請建立本機目錄。

程序

- 1 在管理主控台中，按一下**身分識別與存取管理**索引標籤，然後按一下**目錄**索引標籤。
- 2 按一下**新增目錄**，然後從下拉式功能表中選取**新增本機使用者目錄**。



- 3 在 [新增目錄] 頁面中輸入目錄名稱，然後指定至少一個網域名稱。
網域名稱在服務中的所有目錄間必須是唯一的。
例如：

Add Directory

Directory Name*

Partners

Domains*

Domains



Partner



- 4 按一下**儲存**。
- 5 在 [目錄] 頁面中，按一下新目錄。
- 6 按一下**使用者屬性**索引標籤。

對於本機目錄，系統會列出 [身分識別與存取管理] > [設定] > [使用者屬性] 頁面中的所有屬性。在該頁面上標示為必要的屬性，在本機目錄頁面中也會列為必要屬性。

- 7 自訂本機目錄的屬性。

您可以指定哪些屬性是必要的，而哪些屬性是選用的。您也可以變更屬性的顯示順序。

重要事項 本機目錄一律須有 `userName`、`firstName`、`lastName` 和電子郵件屬性。


- 若要讓某個屬性成為必要屬性，請選取屬性名稱旁的核取方塊。
- 若要讓某個屬性成為選用屬性，請取消選取屬性名稱旁的核取方塊。
- 若要變更屬性的順序，請按住屬性並拖曳到新位置。

對於必要屬性，當您建立使用者時，您必須指定該屬性的值。

例如：

[← Back to Directories](#)

Settings Identity Providers **User Attributes**



Partners
Domain(s): Partner
Type: Local Directory

Delete Directory

Attributes

Select the attributes that are required for local users. To arrange the attributes in a specific order, drag and drop the attribute name.

- userName
- firstName
- email
- phone
- lastName
- domain
- userPrincipalName

8 按一下**儲存**。

下一個

建立本機目錄與您要用來驗證目錄中使用者之身分識別提供者之間的關聯。

建立本機目錄與身分識別提供者的關聯

請將本機目錄與身分識別提供者產生關聯，以便該目錄中的使用者可以通過驗證。建立類型為「內嵌」的新身分識別提供者，並對它啟用「密碼 (本機目錄)」驗證方法。


備註 請勿使用內建的身分識別提供者。不建議對內建的身分識別提供者啟用「密碼 (本機目錄)」驗證方法。

程序

- 1 在**身分識別與存取管理**索引標籤中，按一下**身分識別提供者**索引標籤。
- 2 按一下**新增身分識別提供者**，然後選取**建立內建 IDP**。
- 3 輸入下列資訊。

選項	說明
身分識別提供者名稱	輸入身分識別提供者的名稱。
使用者	選取您建立的本機目錄。
網路	選取可從中存取此身分識別提供者的網路。
驗證方法	選取 [密碼 (本機目錄)]。
KDC 憑證匯出	除非是為 AirWatch 管理的 iOS 裝置設定 Mobile SSO，否則不需要下載憑證。

[← Back to IDP List](#)



PartnerIDP
Type: EMBEDDED
Status: Unknown

Identity Provider Name:

Users: Select which users can authenticate using this IDP. Choose from the available Directories from the list below.

Corporate Directory
 Partners

Network: Select which networks this IDP can be accessed from. Choose from the available network ranges from the list below.

ALL RANGES

Authentication Methods: Select which authentication methods the IDP will use to authenticate users.

Authentication Methods	Enable Auth Method	
Device Compliance (with AirWatch)	<input type="checkbox"/>	
Password (AirWatch Connector)	<input type="checkbox"/>	
VMware Verify	<input type="checkbox"/>	
Mobile SSO (for iOS)	<input type="checkbox"/>	
Password (Local Directory)	<input checked="" type="checkbox"/>	
Mobile SSO (for Android)	<input type="checkbox"/>	

KDC Certificate Export: Download Certificate
Export the KDC server root certificate for use in a Mobile Device Management profile.

4 按一下新增。

身分識別提供者隨即會建立，並與本機目錄產生關聯。之後您可以對身分識別提供者設定其他驗證方法。如需關於驗證的詳細資訊，請參閱《VMware Identity Manager 管理》中的〈在 VMware Identity Manager 中設定使用者驗證〉。

您可以對多個本機目錄使用相同的身分識別提供者。

下一個

建立本機使用者和群組。您可以在管理主控台的**使用者和群組**索引標籤中建立本機使用者和群組。如需詳細資訊，請參閱《VMware Identity Manager 管理》中的〈管理使用者和群組〉一節。

變更本機目錄設定

建立本機目錄後，您可以隨時修改其設定。

您可以變更下列設定。

- 變更目錄名稱。
- 新增、刪除或重新命名網域。
 - 網域名稱在服務中的所有目錄間必須是唯一的。
 - 當您變更網域名稱時，與舊網域相關聯的使用者將會與新網域建立關聯。
 - 目錄至少要有一個網域。
 - 您無法將網域新增至系統目錄，或刪除系統網域。
- 新增使用者屬性，或使現有屬性成為必要或選用屬性。
 - 如果本機目錄還沒有任何使用者，您可以新增選用或必要的新屬性，以及將現有屬性變更為必要或選用屬性。
 - 如果您已在本機目錄中建立使用者，則您只能新增選用的新屬性，以及將現有的必要屬性變更為選用屬性。您無法在建立使用者之後將選用屬性變更為必要屬性。
 - 本機目錄一律須有 `userName`、`firstName`、`lastName` 和電子郵件屬性。
 - 由於使用者屬性定義於 VMware Identity Manager 服務中的全域層級上，因此您所新增的任何新屬性都會顯示在服務的所有目錄中。

- 變更屬性的顯示順序。

程序

- 1 按一下**身分識別與存取管理**索引標籤。
- 2 在 [目錄] 頁面中，按一下您要編輯的目錄。
- 3 編輯本機目錄設定。

選項	動作
變更目錄名稱	<ol style="list-style-type: none"> a 在設定索引標籤中，編輯目錄名稱。 b 按一下儲存。
新增、刪除或重新命名網域	<ol style="list-style-type: none"> a 在設定索引標籤中，編輯網域清單。 b 若要新增網域，請按一下綠色加號圖示。 c 若要刪除網域，請按一下紅色刪除圖示。 d 若要將網域重新命名，請在文字方塊中編輯網域名稱。
將使用者屬性新增至目錄	<ol style="list-style-type: none"> a 按一下身分識別與存取管理索引標籤，然後按一下設定。 b 按一下使用者屬性索引標籤。 c 新增新增其他要使用的屬性清單中的屬性，然後按一下儲存。
使屬性成為目錄的必要或選用屬性	<ol style="list-style-type: none"> a 在身分識別與存取管理索引標籤中，按一下目錄索引標籤。 b 按一下本機目錄名稱，然後按一下使用者屬性索引標籤。 c 選取屬性旁的核取方塊使其成為必要屬性，或取消選取該核取方塊使其成為選用屬性。 d 按一下儲存。
變更屬性的順序	<ol style="list-style-type: none"> a 在身分識別與存取管理索引標籤中，按一下目錄索引標籤。 b 按一下本機目錄名稱，然後按一下使用者屬性索引標籤。 c 按住屬性並拖曳至新位置。 d 按一下儲存。

刪除本機目錄

您可以刪除您在 VMware Identity Manager 服務中建立的本機目錄。您無法刪除第一次設定服務時依預設建立的系統目錄。



警告 在刪除目錄時，該目錄中的所有使用者也都會從服務中刪除。

程序

- 1 按一下**身分識別與存取管理**索引標籤，然後按一下**目錄**索引標籤。
- 2 按一下您要刪除的目錄。
- 3 在 [目錄] 頁面中，按一下**刪除目錄**。

設定系統管理員使用者的驗證方法

管理員使用者從系統目錄登入時使用的預設驗證方法為「密碼 (本機目錄)」。預設存取原則將「密碼 (本機目錄)」設定為後援方法，讓管理員可登入 VMware Identity Manager 管理主控台和 Workspace ONE 入口網站

如果您針對系統管理員有權使用的特定 Web 和桌面平台應用程式建立存取原則，則您必須將這些原則設定為包含其「密碼 (本機目錄)」作為後援驗證方法。否則，管理員無法登入應用程式。

Edit Policy Rule

If a user's Network Range is...

and the user is trying to access content from...

then the user may authenticate using the following method...

+

If preceding Authentication Method fails or is not applicable, then:

+

Just-in-Time 使用者佈建

Just-in-Time 使用者佈建可讓您在登入時，使用第三方身分識別提供者傳送的 SAML 宣告，於 VMware Identity Manager 服務中動態建立使用者。Just-in-Time 使用者佈建僅適用於第三方身分識別提供者。不適用於 VMware Identity Manager 連接器。

本章節討論下列主題：

- “關於 Just-in-Time 使用者佈建,” 第 41 頁
- “準備 Just-in-Time 佈建,” 第 42 頁
- “設定 Just-in-Time 使用者佈建,” 第 43 頁
- “SAML 宣告的需求,” 第 44 頁
- “停用 Just-in-Time 使用者佈建,” 第 45 頁
- “刪除 Just-in-Time 目錄,” 第 45 頁
- “錯誤訊息,” 第 46 頁

關於 Just-in-Time 使用者佈建

Just-in-Time 佈建提供在 VMware Identity Manager 服務中佈建使用者的另一個方式。不需要從 Active Directory 執行個體同步使用者，利用 Just-in-Time 佈建，在使用者登入時會根據身分識別提供者傳送的 SAML 宣告來動態建立和更新使用者。

在此案例中，VMware Identity Manager 可做為 SAML 服務提供者 (SP)。

只能針對第三方身分識別提供者設定 Just-in-Time 組態。連接器無法使用。

利用 Just-in-Time 組態，您不需在內部部署安裝連接器，因為所有使用者的建立和管理是透過 SAML 宣告處理，而驗證則是由第三方身分識別提供者處理。

使用者建立和管理

如果已啟用 Just-in-Time 使用者佈建，當使用者前往 VMware Identity Manager 服務登入頁面並選取網域時，頁面會將使用者重新導向至正確的身分識別提供者。隨即驗證使用者的登入，並由身分識別提供者重新導向回具有 SAML 宣告的 VMware Identity Manager 服務。SAML 宣告中的屬性可用來在服務中建立使用者。只會使用符合服務中定義之使用者屬性的那些屬性；並忽略其他屬性。系統也會根據屬性將使用者新增至群組，並且使用者可獲得針對這些群組設定的權利。

在後續登入時，如果 SAML 宣告中有任何變更，則會在服務中更新使用者。

無法刪除 Just-in-Time 佈建的使用者。若要刪除使用者，您必須刪除 Just-in-Time 目錄。

請注意，所有使用者管理均透過 SAML 宣告來處理。您無法直接透過服務來建立或更新這些使用者。無法從 Active Directory 同步 Just-in-Time 使用者。

如需 SAML 宣告中所需之屬性的相關資訊，請參閱 [“SAML 宣告的需求”](#) 第 44 頁。

Just-in-Time 目錄

第三方身分識別提供者在服務中必須具有與其關聯的 Just-in-Time 目錄。

當您先為身分識別提供者啟用 Just-in-Time 佈建時，即會建立新的 Just-in-Time 目錄，並為其指定一或多個網域。系統會將屬於這些網域的使用者佈建至目錄。如果對目錄設定了多個網域，則 SAML 宣告必須包含網域屬性。如果對目錄設定了單一網域，則 SAML 宣告中不需要網域屬性，但如果已指定，其值必須符合網域名稱。

只有一個類型為 Just-in-Time 的目錄，可以與已啟用 Just-in-Time 佈建的身分識別提供者相關聯。

準備 Just-in-Time 佈建

在您設定 Just-in-Time 使用者佈建前，請先檢閱群組、群組權利以及使用者屬性設定，並視需要進行變更。此外，請識別您要用於 Just-in-Time 目錄的網域。

建立本機群組

對於透過 Just-in-Time 佈建功能佈建的使用者，系統會根據他們的使用者屬性將他們新增至群組，再從他們隸屬的群組衍生資源權利。在設定 Just-in-Time 佈建之前，請確認服務中具有本機群組。請根據需求建立一或多個本機群組。對於每個群組，請設定群組成員資格的規則並新增權利。

程序

- 1 在管理主控台內按一下 **使用者和群組** 索引標籤。
- 2 按一下 **建立群組**、提供群組的名稱和說明，然後按一下 **新增**。
- 3 在 [群組] 頁面中按一下新群組。
- 4 設定群組的使用者。
 - a 在左窗格中，選取 **此群組中的使用者**。
 - b 按一下 **修改此群組中的使用者**，接著設定群組成員資格的規則。
- 5 新增群組的權利。
 - a 在左窗格中選取 **權利**。
 - b 按一下 **新增權利**，然後選取應用程式和每個應用程式的部署方法。
 - c 按一下 **儲存**。

檢閱使用者屬性

在 [使用者屬性] 頁面中檢閱針對所有 VMware Identity Manager 目錄設定的使用者屬性，並在必要時修改它們。透過 Just-in-Time 佈建來佈建使用者時，SAML 宣告會用來建立使用者。系統僅會使用 SAML 宣告中符合 [使用者屬性] 頁面中所列屬性的那些屬性。

重要事項 如果屬性在 [使用者屬性] 頁面上標示為必要，SAML 宣告必須包含該屬性，否則登入會失敗。

對使用者屬性進行變更時，請考慮對您的承租人中其他目錄和組態的影響。[使用者屬性] 頁面會套用到您的承租人中的所有目錄。

備註 您不需將 `domain` 屬性標示為必要。

程序

- 1 在管理主控台，按一下**身分識別與存取管理**索引標籤。
- 2 按一下**設定**，然後按一下**使用者屬性**。
- 3 如有必要，請檢閱屬性並進行變更。

The screenshot shows the 'User Attributes' configuration page in the VMware Identity Manager console. The page is titled 'User Attributes' and has a sub-header 'Default Attributes'. Below this, there is a list of attributes with a 'Required' column. The attributes and their 'Required' status are as follows:

Attribute	Required
domain	<input type="checkbox"/>
userPrincipalName	<input type="checkbox"/>
distinguishedName	<input type="checkbox"/>
employeeID	<input type="checkbox"/>
disabled	<input type="checkbox"/>
phone	<input type="checkbox"/>
lastName	<input checked="" type="checkbox"/>
firstName	<input checked="" type="checkbox"/>
email	<input checked="" type="checkbox"/>
userName	<input checked="" type="checkbox"/>

Below the list, there is an 'Attributes' section with a text input field and a '+' button. A 'Save' button is located at the bottom of the page.

設定 Just-in-Time 使用者佈建

您可以針對第三方身分識別提供者設定 Just-in-Time 使用者佈建，同時在 VMware Identity Manager 服務中建立或更新身分識別提供者。

當您啟用 Just-in-Time 佈建時，您會建立新的 Just-in-Time 目錄，並為其指定一或多個網域。系統會將隸屬於這些網域的使用者新增至目錄中。

您必須指定至少一個網域。網域名稱在 VMware Identity Manager 服務中的所有目錄之間必須是唯一的。如果您指定多個網域，SAML 宣告必須包含網域屬性。如果您指定一個網域，系統會將它當做無網域屬性之 SAML 宣告的網域。如果您指定網域屬性，屬性值必須與任一個網域相符，否則登入會失敗。

程序

- 1 登入 VMware Identity Manager 服務管理主控台。

- 2 依序按一下 **身分識別與存取管理** 索引標籤和 **身分識別提供者**。
- 3 按一下 **新增身分識別提供者** 或選取身分識別提供者。
- 4 在 **Just-in-Time 使用者佈建** 區段中按一下 **啟用**。
- 5 指定下列資訊。
 - 新 Just-in-Time 目錄的名稱。
 - 一或多個網域。

重要事項 網域名稱在承租人中所有目錄間必須是唯一的。

例如：

Just-in-Time User Provisioning Configure Just-in-Time provisioning to create users in the Identity Manager service dynamically when they first log in, based on SAML assertions.

Enable

Create Just-in-Time Directory

Directory Name

Domains

Domains	
<input type="text" value="myco.com"/>	✖ +

Enter one or more domains. Users belonging to these domains are added to the directory. If only one domain is specified, it is used as the domain for SAML assertions without a domain attribute.

- 6 完成頁面的其他內容，然後按一下 **新增** 或 **儲存**。如需相關資訊，請參閱 [“將第三方身分識別提供者執行個體設定為驗證使用者”](#) 第 64 頁。

SAML 宣告的需求

啟用第三方身分識別提供者的 Just-in-Time 使用者佈建時，登入期間會根據 SAML 宣告而在 VMware Identity Manager 服務中建立或更新使用者。該身分識別提供者傳送的 SAML 宣告必須包含特定屬性。

- SAML 宣告必須包含 `userName` 屬性。
- SAML 宣告必須包含 VMware Identity Manager 服務中標示為必要的所有使用者屬性。

若要在管理主控台中檢視或編輯使用者屬性，請在 **身分識別與存取管理** 索引標籤中，依序按一下 **設定** 和 **使用者屬性**。

重要事項 確定 SAML 宣告中的金鑰完全符合屬性名稱，包括大小寫。

- 如果您為 Just-in-Time 目錄設定多個網域，則 SAML 宣告必須包含 `domain` 屬性。屬性的值必須符合為目錄設定的其中一個網域。如果此值不符合或未指定網域，則登入會失敗。
- 如果您為 Just-in-Time 目錄設定單一網域，則在 SAML 宣告中指定 `domain` 屬性為選用。

如果指定 `domain` 屬性，請確定其值符合為目錄設定的網域。如果 SAML 宣告不含網域屬性，則使用者會關聯至為目錄設定的網域。
- 如果想允許使用者名稱更新，請在 SAML 宣告中加入 `ExternalId` 屬性。使用者將由 `ExternalId` 識別。如果在後續登入中 SAML 宣告包含不同的使用者名稱，則仍可正確識別使用者而登入成功，接著會更新 Identity Manager 服務中的使用者名稱。

SAML 宣告中的屬性將用來建立或更新使用者，方法如下所示。

- 系統會使用 Identity Manager 服務中的必要或選用屬性 (如 [使用者屬性] 頁面中所列)。
- 系統會忽略不符合 [使用者屬性] 頁面中任何屬性的屬性。
- 系統會忽略沒有值的屬性。

停用 Just-in-Time 使用者佈建

您可以停用 Just-in-Time 使用者佈建。當此選項停用時，在登入期間將不會建立新的使用者，且不會更新現有使用者。現有使用者會繼續由身分識別提供者驗證。

程序

- 1 在管理主控台中，按一下 **身分識別與存取管理** 索引標籤，然後按一下 **身分識別提供者**。
- 2 按一下您要編輯的身分識別提供者。
- 3 在 **Just-in-Time 使用者佈建** 區段中，取消選取 **啟用** 核取方塊。



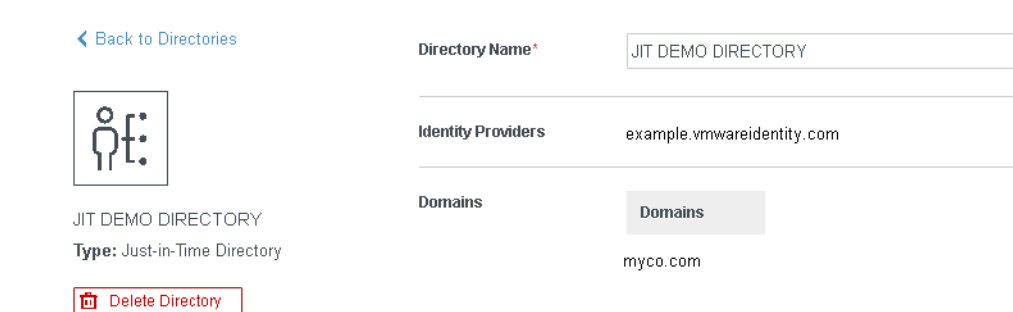
刪除 Just-in-Time 目錄

Just-in-Time 目錄是與啟用 Just-in-Time 使用者佈建之第三方身分識別提供者相關聯的目錄。當您刪除目錄時，目錄中的所有使用者均會遭到刪除，而 Just-in-Time 組態也會停用。由於每個 Just-in-Time 身分識別提供者只能擁有單一目錄，因此當您刪除目錄時，將無法再使用該身分識別提供者。

若要再次啟用身分識別提供者的 Just-in-Time 組態，您需要建立新目錄。

程序

- 1 在管理主控台，按一下 **身分識別與存取管理** 索引標籤。
- 2 在 [目錄] 頁面中，找出要刪除的目錄。
您可以透過查找 **類型** 資料行中的目錄類型來識別 Just-in-Time 目錄。
- 3 按一下目錄名稱。
- 4 按一下 **刪除目錄**。



錯誤訊息

管理員或使用者可能會看見有關於 **Just-in-Time** 佈建的錯誤。例如，如果 SAML 判斷提示中遺漏了某個必要屬性，即會發生錯誤，且使用者將無法登入。

以下是可能出現在管理主控台中的錯誤：

錯誤訊息	解決方案
如果啟用 JIT 使用者佈建，則至少必須要有一個目錄與身分識別提供者相關聯。	<p>沒有與身分識別提供者相關聯的目錄。已啟用 Just-in-Time 佈建選項的身分識別提供者，至少要有一個相關聯的 Just-in-Time 目錄。</p> <ol style="list-style-type: none"> 1 在管理主控台的身分識別與存取管理索引標籤中，按一下身分識別提供者，然後按一下身分識別提供者。 2 在 Just-in-Time 使用者佈建區段中，指定一個目錄名稱和一或多個網域。 3 按一下儲存。 <p>Just-in-Time 目錄隨即建立。</p>

以下是可能出現在登入頁面中的錯誤：

錯誤訊息	解決方案
遺漏使用者屬性： <i>name</i> 。	<p>第三方身分識別提供者所傳送的 SAML 判斷提示中遺漏必要的使用者屬性。[使用者屬性] 頁面中所有標示為必要的屬性，都必須納入 SAML 判斷提示中。請修改第三方身分識別提供者設定，以傳送正確的 SAML 判斷提示。</p>
網域遺漏且無法推斷。	<p>SAML 判斷提示中未包含網域屬性，而無法判斷網域。在下列情況下，網域屬性是必要的：</p> <ul style="list-style-type: none"> ■ 為 Just-in-Time 目錄設定了多個網域時。 ■ 網域在 [使用者屬性] 頁面中標示為必要屬性時。 <p>如果指定了網域屬性，則其值必須符合為目錄指定的其中一個網域。</p> <p>請修改第三方身分識別提供者設定，以傳送正確的 SAML 判斷提示。</p>
屬性名稱： <i>name</i> 、值： <i>value</i> 。	<p>SAML 判斷提示中的屬性不符合承租人的 [使用者屬性] 頁面中的任何屬性，而將被忽略。</p>
無法建立或更新 JIT 使用者。	<p>使用者無法建立於服務中。可能的原因包括：</p> <ul style="list-style-type: none"> ■ SAML 判斷提示中遺漏必要屬性。 <p>請檢閱 [使用者屬性] 頁面中的屬性，並確定 SAML 判斷提示中包含所有標示為必要的屬性。</p> <ul style="list-style-type: none"> ■ 無法判斷使用者的網域。 <p>請在 SAML 判斷提示中指定網域屬性，並確定其值符合為 Just-in-Time 目錄設定的其中一個網域。</p>

在 VMware Identity Manager 中設定使用者驗證

7

VMware Identity Manager 支援多個驗證方法。您可以設定單一驗證方法，也可以設定鏈結的雙重要素驗證。您也可以使用 RADIUS 和 SAML 通訊協定外部的驗證方法。

與 VMware Identity Manager 服務搭配使用的身份識別提供者執行個體，會建立使用 SAML 2.0 判斷提示與服務通訊的網路內部聯盟授權機構。

在您初次部署 VMware Identity Manager 服務時，連接器將是服務的初始身份識別提供者。您現有的 Active Directory 基礎結構會用於使用者驗證和管理。

支援的驗證方法如下。您可以從管理主控台設定這些驗證方法。

驗證方法	說明
密碼 (內部部署)	設定 Active Directory 後無需進行任何設定，VMware Identity Manager 即可支援 Active Directory 密碼驗證。此方法可直接針對 Active Directory 驗證使用者。
桌面平台的 Kerberos	Kerberos 驗證可為網域使用者提供其應用程式入口網站的單一登入存取。使用者在登入網路後，將不需要再次登入其應用程式入口網站。您可以設定兩個 Kerberos 驗證方法：適用於採用整合式 Windows 驗證之桌面平台的 Kerberos 驗證，以及當 Active Directory 和 AirWatch 之間的信任關係已建立時，適用於 iOS 9 行動裝置的內建 Kerberos 驗證。
憑證 (內部部署)	憑證式驗證可設定為允許用戶端在其桌面或行動裝置上使用憑證進行驗證，或使用智慧卡介面卡進行驗證。 憑證式驗證以使用者所有和人員所知為基礎。X.509 憑證使用公開金鑰基礎結構標準，確認憑證中所包含的公開金鑰屬於使用者。
RSA SecurID (內部部署)	設定 RSA SecurID 驗證時，會在 RSA SecurID 伺服器中將 VMware Identity Manager 設定為驗證代理程式。RSA SecurID 驗證需要使用者使用 Token 式驗證系統。RSA SecurID 驗證方法適用於從企業網路外部存取 VMware Identity Manager 的使用者。
RADIUS (內部部署)	RADIUS 驗證提供雙因素驗證選項。您可以設定 VMware Identity Manager 服務可以存取的 RADIUS 伺服器。使用者使用其使用者名稱與密碼登入時，會提交存取申請至 RADIUS 伺服器，以進行驗證。
RSA 調適性驗證 (內部部署)	與針對 Active Directory 僅進行使用者名稱及密碼驗證相比，RSA 驗證提供更強大的多因素驗證。當 RSA 調適性驗證啟用時，指定於風險原則中的風險指標將會在 RSA 原則管理應用程式中進行設定。調適性驗證的 VMware Identity Manager 服務組態會用來決定必要的驗證提示。
Mobile SSO (iOS 版)	iOS 版 Mobile SSO 驗證可用於 AirWatch 管理的 iOS 裝置的單一登入驗證。Mobile SSO (iOS 版) 驗證會使用 Identity Manager 服務中的金鑰發佈中心 (KDC)。您必須先在 VMware Identity Manager 服務中啟動 KDC 服務，才能啟用此驗證方法。
Mobile SSO (Android 版)	Android 版 Mobile SSO 驗證可用於 AirWatch 管理的 Android 裝置的單一登入驗證。在 VMware Identity Manager 服務與 AirWatch 之間會設定一個 Proxy 服務，以從 AirWatch 擷取驗證所需的憑證。
密碼 (AirWatch Connector)	AirWatch Cloud Connector 可與 VMware Identity Manager 服務整合，用於使用者密碼驗證。您可以設定 VMware Identity Manager 服務，以從 AirWatch 目錄同步使用者。

驗證方法	說明
VMware Verify	在必須使用雙重要素驗證時，VMware Verify 可作為第二個驗證方法。第一個驗證方法是使用者名稱和密碼，第二個驗證方法則是 VMware Verify 要求核准或代碼。 VMware Verify 會使用第三方雲端服務，將此功能提供給使用者裝置。為了執行此作業，名稱、電子郵件和電話號碼等使用者資訊將會儲存在服務中，但不會用於提供該功能以外的任何用途。
密碼 (本機目錄)	針對搭配系統目錄使用的「系統 IDP」身分識別提供者，依預設會啟用「密碼 (本機目錄)」方法。此方法會套用至預設存取原則。

設定驗證方法之後，您可以建立存取原則規則，以指定裝置類型所要使用的驗證方法。系統會根據您所設定的驗證方法、預設存取原則規則、網路範圍和身分識別提供者執行個體來驗證使用者。請參閱“[管理要套用於使用者的驗證方法](#),” 第 66 頁。

本章節討論下列主題:

- “[為 VMware Identity Manager 設定 Kerberos](#),” 第 48 頁
- “[為 VMware Identity Manager 設定 SecurID](#),” 第 52 頁
- “[針對 VMware Identity Manager 設定 RADIUS](#),” 第 54 頁
- “[在 VMware Identity Manager 中設定 RSA 調適性驗證](#),” 第 56 頁
- “[設定憑證或智慧卡介面卡以搭配 VMware Identity Manager 使用](#),” 第 58 頁
- “[設定雙重要素驗證適用的 VMware Verify](#),” 第 60 頁
- “[設定內建身分識別提供者](#),” 第 62 頁
- “[設定其他 Workspace 身分識別提供者](#),” 第 64 頁
- “[將第三方身分識別提供者執行個體設定為驗證使用者](#),” 第 64 頁
- “[管理要套用於使用者的驗證方法](#),” 第 66 頁

為 VMware Identity Manager 設定 Kerberos

Kerberos 驗證可讓已成功登入其網域的使用者存取其應用程式入口網站，無需其他認證提示。

您可以在 Identity Manager 服務中針對採用整合式 Windows 驗證的桌面平台設定 Kerberos 驗證通訊協定，進而保護使用者瀏覽器和 Identity Manager 服務之間的互動，以及實現輕觸一下即可單一登入至 AirWatch 中受管理的 iOS 9 行動裝置。如需 iOS 9 裝置上 Kerberos 驗證的相關資訊，請參閱“[為 AirWatch 管理的 iOS 裝置實作 Mobile Single Sign-in 驗證](#),” 第 112 頁。

使用整合式 Windows 驗證實作桌面平台的 Kerberos

若要為桌面平台設定 Kerberos 驗證，您必須啟用 [整合式 Windows 驗證]，使 Kerberos 通訊協定能夠保護使用者的瀏覽器與 Identity Manager 服務之間的互動。

為桌面平台啟用 Kerberos 驗證時，Identity Manager 服務會使用在 Active Directory 中實作為網域服務的金鑰發佈中心 (KDC) 所發佈的 Kerberos 票證來驗證使用者的桌面平台認證。您不需要直接將 Active Directory 設定為使 Kerberos 與您的部署一起運作。

您必須設定使用者 Web 瀏覽器，使其在使用者登入時將您的 Kerberos 認證傳送至服務。請參閱“[針對 Kerberos 設定瀏覽器](#),” 第 49 頁。

針對採用整合式 Windows 驗證的桌面平台設定 Kerberos 驗證

若要設定 VMware Identity Manager 服務以提供適用於桌面平台的 Kerberos 驗證，您必須加入網域並在 VMware Identity Manager 連接器上啟用 Kerberos 驗證。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**設定**。
- 2 在 [連接器] 頁面上，針對設定用於 Kerberos 驗證的連接器，按一下**加入網域**。
- 3 在 [加入網域] 頁面上，輸入 Active Directory 網域的資訊。

選項	說明
網域	輸入 Active Directory 的完整網域名稱。您輸入的網域名稱必須與連接器伺服器的相同，即 Windows 網域。
網域使用者	輸入 Active Directory 中有權將系統加入至該 Active Directory 網域之帳戶的使用者名稱。
網域密碼	輸入與 AD 使用者名稱相關聯的密碼。VMware Identity Manager 不會儲存此密碼。

按一下**儲存**。

[加入網域] 頁面隨即重新整理並顯示您目前已加入網域的訊息。

- 4 在連接器的 Worker 資料行中，按一下**驗證介面卡**。
- 5 按一下 **KerberosIdpAdapter**
系統會將您重新導向到 [Identity Manager 登入] 頁面。
- 6 在 KerberosIdpAdapter 資料列中按一下**編輯**，並設定 [Kerberos 驗證] 頁面。

選項	說明
名稱	名稱為必填。預設名稱為 KerberosIdpAdapter。您可以變更此名稱。
目錄 UID 屬性	輸入包含使用者名稱的帳戶屬性。
啟用 Windows 驗證	選取此選項以延伸使用者瀏覽器與 VMware Identity Manager 之間的驗證互動。
啟用 NTLM	僅在 Active Directory 基礎結構依賴於 NTLM 驗證時，選取此選項以啟用 NT LAN Manager (NTLM) 通訊協定式驗證。
啟用重新導向	如果循環配置資源 DNS 和負載平衡器沒有 Kerberos 支援，則選取此選項。驗證申請會重新導向至 [重新導向主機名稱]。如果選取此選項，請在 重新導向主機名稱 文字方塊中輸入重新導向主機名稱。此名稱通常為服務的主機名稱。

- 7 按一下**儲存**。

下一個

將驗證方法新增至預設存取原則。移至 [身分識別與存取管理] > [管理] > [原則] 頁面，並編輯預設原則規則，以將 Kerberos 驗證方法按正確的驗證順序新增至規則。

針對 Kerberos 設定瀏覽器

啟用 Kerberos 時，您需要設定 Web 瀏覽器，以在使用者登入時將 Kerberos 認證傳送給服務。

以下瀏覽器在經過設定後，可將 Kerberos 認證傳送到執行 Windows 之電腦上的 Identity Manager 服務：Firefox、Internet Explorer 及 Chrome。所有瀏覽器都需要進行額外設定。

設定 Internet Explorer 以存取 Web 介面

如果已針對部署設定 Kerberos 並且您想要透過 Internet Explorer 授與使用者對於 Web 介面的存取權，則必須對 Internet Explorer 瀏覽器進行設定。

在 Windows 作業系統上，Kerberos 驗證可與 VMware Identity Manager 搭配使用。

備註 請不要在其他作業系統上實作這些 Kerberos 相關的步驟。

先決條件

設定 Kerberos 之後，為每個使用者設定 Internet Explorer 瀏覽器或向使用者提供相關指示。

程序

- 1 確認以網域使用者的身分登入 Windows。
- 2 在 Internet Explorer 中，啟用自動登入。
 - a 選取工具 > 網際網路選項 > 安全性。
 - b 按一下自訂等級。
 - c 選取只在近端內部網路區域自動登入。
 - d 按一下確定。
- 3 確認此連接器虛擬應用裝置的執行個體屬於近端內部網路區域。
 - a 使用 Internet Explorer 存取 VMware Identity Manager 登入 URL，網址為 *https://myconnectorhost.domain/authenticate/*。
 - b 在瀏覽器視窗右下角的狀態列中找到該區域。
如果區域是近端內部網路，則 Internet Explorer 組態完成。
- 4 如果區域不是近端內部網路，則將 VMware Identity Manager 登入 URL 新增至內部網路區域。
 - a 選取工具 > 網際網路選項 > 安全性 > 近端內部網路 > 站台。
 - b 選取自動偵測內部網路。
如果未選取此選項，選取它即可將新增至內部網路區域。
 - c (選擇性) 如果選取了自動偵測內部網路，按一下確定直到所有對話方塊均關閉。
 - d 在 [近端內部網路] 對話方塊中，按一下進階。
隨即顯示第二個名為 [近端內部網路] 的對話方塊。
 - e 在將此網站加到該區域文字方塊中輸入 VMware Identity Manager URL。
https://myconnectorhost.domain/authenticate/
 - f 按一下新增 > 關閉 > 確定。
- 5 確認 Internet Explorer 能夠將 Windows 驗證傳遞到受信任的站台。
 - a 在 [網際網路選項] 對話方塊中，按一下進階索引標籤。
 - b 選取啟用整合的 Windows 驗證。
此選項將在您重新啟動 Internet Explorer 後生效。
 - c 按一下確定。

- 登入 Web 介面以確認存取。

如果 Kerberos 驗證成功，測試 URL 將移至 Web 介面。

Kerberos 通訊協定會確保此 Internet Explorer 瀏覽器執行個體與 VMware Identity Manager 之間所有互動的安全。現在，使用者可使用單一登入存取其 Workspace ONE 入口網站。

設定 Firefox 以存取 Web 介面

如果已針對部署設定 Kerberos 並且您想要使用 Firefox 授與使用者對於 Web 介面的存取權，則必須對 Firefox 瀏覽器進行設定。

在 Windows 作業系統上，Kerberos 驗證可與 VMware Identity Manager 搭配使用。

先決條件

設定 Kerberos 之後，為每個使用者設定 Firefox 瀏覽器或向使用者提供相關指示。

程序

- 在 Firefox 瀏覽器的 URL 文字方塊中，輸入 `about:config` 以存取進階設定。
- 按一下**我保證會小心**。
- 在 [喜好設定名稱] 資料行中按兩下 **network.negotiate-auth.trusted-uris**。
- 在文字方塊中輸入 VMware Identity Manager URL。
https://myconnectorhost.domain.com
- 按一下**確定**。
- 在 [喜好設定名稱] 資料行中按兩下 **network.negotiate-auth.delegation-uris**。
- 在文字方塊中輸入 VMware Identity Manager URL。
https://myconnectorhost.domain.com/authenticate/
- 按一下**確定**。
- 使用 Firefox 瀏覽器登入登入 URL 來測試 Kerberos 功能。例如
https://myconnectorhost.domain.com/authenticate/。
如果 Kerberos 驗證成功，測試 URL 將移至 Web 介面。

Kerberos 通訊協定會確保此 Firefox 瀏覽器執行個體與 VMware Identity Manager 之間所有互動的安全。現在，使用者可使用單一登入存取其 Workspace ONE 入口網站。

設定 Chrome 瀏覽器以存取 Web 介面

如果已針對部署設定 Kerberos 並且您想要使用 Chrome 瀏覽器授與使用者對於 Web 介面的存取權，則必須對 Chrome 瀏覽器進行設定。

在 Windows 作業系統上，Kerberos 驗證可與 VMware Identity Manager 搭配使用。

備註 請勿在其他作業系統上實作這些 Kerberos 相關步驟。

先決條件

- 設定 Kerberos。
- 由於 Chrome 使用 Internet Explorer 組態啟用 Kerberos 驗證，因此必須將 Internet Explorer 設定為允許 Chrome 使用 Internet Explorer 組態。如需如何設定 Chrome 進行 Kerberos 驗證的相關資訊，請參閱 Google 說明文件。

程序

- 1 使用 Chrome 瀏覽器來測試 Kerberos 功能。
- 2 於 `https://myconnectorhost.domain.com/authenticate/` 登入 VMware Identity Manager。

如果 Kerberos 驗證成功，測試 URL 將連線至 Web 介面。

如果所有相關的 Kerberos 組態均正確，則相關通訊協定 (Kerberos) 會確保此 Chrome 瀏覽器執行個體與 VMware Identity Manager 之間所有互動的安全性。使用者可使用單一登入存取其 Workspace ONE 入口網站。

為 VMware Identity Manager 設定 SecurID

設定 RSA SecurID 伺服器時，您必須在 RSA SecurID 伺服器上將 VMware Identity Manager 服務資訊新增為驗證代理程式，並在 VMware Identity Manager 服務上設定 RSA SecurID 伺服器資訊。

設定 SecurID 以提供額外安全性時，必須確保已針對 VMware Identity Manager 部署正確設定您的網路。特別對於 SecurID，您必須確保適當的連接埠已開啟，才能啟用 SecurID 來驗證網路外的使用者。

執行 [VMware Identity Manager 設定] 精靈並設定 Active Directory 連線後，您擁有準備 RSA SecurID 伺服器的必要資訊。針對 VMware Identity Manager 準備 RSA SecurID 伺服器後，您可在管理主控台中啟用 SecurID。

- [準備 RSA SecurID 伺服器](#) 第 52 頁

必須藉由 VMware Identity Manager 應用裝置的相關資訊，將 RSA SecurID 伺服器設定為驗證代理程式。所需的資訊是網路介面的主機名稱和 IP 位址。

- [設定 RSA SecurID 驗證](#) 第 53 頁

在 RSA SecurID 伺服器中將 VMware Identity Manager 應用裝置設定為驗證代理程式後，您必須將 RSA SecurID 組態資訊新增至連接器。

準備 RSA SecurID 伺服器

必須藉由 VMware Identity Manager 應用裝置的相關資訊，將 RSA SecurID 伺服器設定為驗證代理程式。所需的資訊是網路介面的主機名稱和 IP 位址。

先決條件

- 確認安裝下列其中一種 RSA 驗證管理員版本並在企業網路上正常運作：RSA AM 6.1.2、7.1 SP2 及更新版本，以及 8.0 及更新版本。VMware Identity Manager 伺服器使用 AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1)，其僅支援 RSA 驗證管理員 (RSA SecurID 伺服器) 的上述版本。如需安裝和設定 RSA 驗證管理員 (RSA SecurID 伺服器) 的相關資訊，請參閱 RSA 說明文件。

程序

- 1 在受支援版本的 RSA SecurID 伺服器上，將 VMware Identity Manager 連接器新增為驗證代理程式。輸入下列資訊。

選項	說明
主機名稱	VMware Identity Manager 的主機名稱。
IP 位址	VMware Identity Manager 的 IP 位址。
備用 IP 位址	如果連接器的流量通過網路位址轉譯 (NAT) 裝置連線到 RSA SecurID 伺服器，則請輸入應用裝置的私人 IP 位址。

- 2 下載已壓縮組態檔並解壓縮 `sdconf.rec` 檔案。

準備好在稍後於 VMware Identity Manager 中設定 RSA SecurID 時上傳此檔案。

下一個

移至管理主控台並在 [設定] 頁面的 [身分識別和存取管理] 索引標籤中，選取連接器並在 AuthAdapters 頁面中設定 SecurID。

設定 RSA SecurID 驗證

在 RSA SecurID 伺服器中將 VMware Identity Manager 應用裝置設定為驗證代理程式後，您必須將 RSA SecurID 組態資訊新增至連接器。

先決條件

- 確認 RSA 驗證管理員 (RSA SecurID 伺服器) 已安裝並正確設定。
- 從 RSA SecurID 伺服器下載壓縮檔並擷取伺服器組態檔。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**設定**。
- 2 在 [連接器] 頁面中，選取將要設定 RSA SecurID 之連接器的 Worker 連結。
- 3 按一下**驗證介面卡**，然後按一下 **SecurIDIdpAdapter**。

系統會將您重新導向到 [Identity Manager 登入] 頁面。

- 4 在 [驗證介面卡] 頁面的 [SecurIDIdpAdapter] 資料列中，按一下**編輯**。
- 5 設定 [SecurID 驗證介面卡] 頁面。

設定 SecurID 頁面時，需要 RSA SecurID 伺服器上所用的資訊和產生的檔案。

選項	動作
名稱	名稱為必填。預設名稱為 SecurIDIdpAdapter。您可以變更此名稱。
啟用 SecurID	選取此方塊可啟用 SecurID 驗證。
允許嘗試的驗證次數	使用 RSA SecurID Token 時，輸入登入嘗試失敗次數上限。預設為五次嘗試。 備註 當您設定多個目錄且利用額外的目錄實作 RSA SecurID 驗證時，請將 允許的驗證嘗試次數 設定為與每個 RSA SecurID 組態相同的值。如果值不同，SecurID 驗證將會失敗。
連接器位址	輸入連接器執行個體的 IP 位址。輸入的值必須與將連接器應用裝置做為驗證代理程式新增至 RSA SecurID 伺服器時所用的值相符。如果 RSA SecurID 伺服器為備用 IP 位址提示指派了一個值，請將該值做為連接器 IP 位址輸入。如果未指派備用 IP 位址，請輸入指派給 IP 位址提示的值。
代理程式 IP 位址	在 RSA SecurID 伺服器中輸入指派給 IP 位址 提示的值。
伺服器組態	上傳 RSA SecurID 伺服器組態檔。首先，您必須從 RSA SecurID 伺服器下載壓縮檔，並解壓縮伺服器組態檔 (預設名稱為 <code>sdconf.rec</code>)。
節點密碼	保留節點密碼欄位空白可自動產生節點密碼。建議您清除 RSA SecurID 伺服器上的節點密碼檔案，並且注意不要上傳節點密碼檔案。確保 RSA SecurID 伺服器與伺服器連接器執行個體上的節點密碼檔案永遠相符。如果變更一個位置上的節點密碼，在另一位置上也要進行變更。

- 6 按一下**儲存**。

下一個

將驗證方法新增至預設存取原則。移至 [身分識別與存取管理] > [管理] > [原則] 頁面，然後編輯預設原則規則，以將 SecurID 驗證方法新增至規則。請參閱“[管理要套用至使用者的驗證方法](#),” 第 66 頁。

針對 VMware Identity Manager 設定 RADIUS

您可以對 VMware Identity Manager 進行設定，以讓使用者必須使用 RADIUS (遠端驗證撥入使用者服務) 驗證。您可以在 VMware Identity Manager 服務上設定 RADIUS 伺服器資訊。

RADIUS 支援提供範圍廣泛的替代式雙因素 Token 型驗證選項。由於雙因素驗證解決方案 (例如，RADIUS) 與安裝在個別伺服器上的驗證管理員搭配使用，您必須設定 RADIUS 伺服器並使其可供 Identity Manager Service 存取。

使用者登入其 Workspace ONE 入口網站，且 RADIUS 驗證啟用時，瀏覽器中會顯示一個特殊的登入對話方塊。使用者在登入對話方塊中輸入其 RADIUS 驗證使用者名稱和密碼。如果 RADIUS 伺服器發出存取挑戰，Identity Manager Service 會顯示提示您再次輸入密碼的對話方塊。目前的 RADIUS 挑戰支援限制為提示文字輸入。

使用者在對話方塊中輸入認證之後，RADIUS 伺服器可將 SMS 簡訊或電子郵件，或使用一些其他額外機制的文字，連同程式碼傳送到使用者手機。使用者可在登入對話方塊中輸入此文字和程式碼，以完成驗證。

如果 RADIUS 伺服器允許從 Active Directory 匯入使用者，則系統可能會先提示使用者提供 Active Directory 認證，再提示其輸入 RADIUS 驗證使用者名稱和密碼。

準備 RADIUS 伺服器

設定 RADIUS 伺服器，然後將 RADIUS 伺服器設定為接受來自 VMware Identity Manager 服務的 RADIUS 要求。

如需設定 RADIUS 伺服器的相關資訊，請參閱 RADIUS 廠商的設定指南。記下您的 RADIUS 組態資訊，在服務中設定 RADIUS 時會用到此資訊。若想查看設定 VMware Identity Manager 所需的 RADIUS 資訊類型，請前往“[在 VMware Identity Manager 中設定 RADIUS 驗證](#),” 第 54 頁。

您可以設定用於高可用性的次要 RADIUS 驗證伺服器。如果主要 RADIUS 伺服器在為 RADIUS 驗證設定的伺服器逾時內沒有回應，此申請將路由至次要伺服器。當主要伺服器沒有回應時，次要伺服器會收到所有未來驗證申請。

在 VMware Identity Manager 中設定 RADIUS 驗證

在 VMware Identity Manager 管理主控台中啟用 RADIUS 驗證並設定 RADIUS 設定。

先決條件

在驗證管理員伺服器上安裝與設定 RADIUS 軟體。對於 RADIUS 驗證，請依照供應商的組態文件進行。

您需要瞭解下列 RADIUS 伺服器資訊，才能在服務上設定 RADIUS。

- RADIUS 伺服器的 IP 位址或 DNS 名稱。
- 驗證連接埠號碼。驗證連接埠通常為 1812。
- 驗證類型。驗證類型包括 PAP (密碼驗證通訊協定)、CHAP (Challenge Handshake 驗證通訊協定)、MSCHAP1、MSCHAP2 (Microsoft Challenge Handshake 驗證通訊協定版本 1 和版本 2)。
- 用於在 RADIUS 通訊協定訊息中加密和解密的 RADIUS 共用密碼。
- RADIUS 驗證所需的特定逾時和重試值

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**設定**。
- 2 在 [連接器] 頁面上，針對設定用於 RADIUS 驗證的連接器，選取 Worker 連結。
- 3 按一下**驗證介面卡**，然後按一下 **RadiusAuthAdapter**。
系統會將您重新導向到 [Identity Manager 登入] 頁面。
- 4 按一下**編輯**在 [驗證介面卡] 頁面上設定這些欄位。

選項	動作
名稱	名稱為必填。預設名稱為 RadiusAuthAdapter。您可以變更此名稱。
啟用 Radius 介面卡	選取此核取方塊以啟用 RADIUS 驗證。
允許嘗試的驗證次數	輸入使用 RADIUS 登入時，登入嘗試失敗次數的上限。預設為五次嘗試。
Radius 伺服器的嘗試次數	指定重試嘗試次數的總數。如果主要伺服器沒有回應，則服務會先等待已設定的時長後再次嘗試。
Radius 伺服器的主機名稱/位址	輸入 Radius 伺服器的主機名稱或 IP 位址。
驗證連接埠	輸入 Radius 驗證連接埠號碼。連接埠號碼通常為 1812。
帳戶處理連接埠	輸入 0 做為連接埠號碼。此時不會使用帳戶處理連接埠。
驗證類型	輸入 RADIUS 伺服器支援的驗證通訊協定。可以是 PAP、CHAP、MSCHAP1 或 MSCHAP2。
共用密碼	輸入在 RADIUS 伺服器和 VMware Identity Manager Service 之間使用的共用密碼。
以秒為單位的伺服器逾時值	輸入 RADIUS 伺服器逾時值 (以秒為單位)，如果 RADIUS 伺服器無回應，則將在該時長後重試。
領域首碼	(選擇性) 使用者帳戶位置稱為領域。 如果您指定領域首碼字串，則將名稱傳送至 RADIUS 伺服器時，將在使用者名稱的開頭放置該字串。例如，如果輸入 jdoe 做為使用者名稱，且指定領域首碼 DOMAIN-A\，則會向 RADIUS 伺服器傳送使用者名稱 DOMAIN-A\jdoe。如果您沒有設定這些欄位，則僅傳送輸入的使用者名稱。
領域尾碼	(選擇性) 如果您指定領域尾碼，則會在使用者名稱的結尾放置該字串。例如，如果尾碼為 @myco.com，則會向 RADIUS 伺服器傳送使用者名稱 jdoe@myco.com。
登入頁面複雜密碼提示	輸入要在使用者登入頁面上的訊息中顯示的文字字串，以引導使用者輸入正確的 Radius 密碼。例如，如果此欄位設定 先 AD 密碼，然後 SMS 密碼 ，則登入頁面訊息會顯示 先輸入您的 AD 密碼，然後再輸入 SMS 密碼 。預設文字字串為 RADIUS 密碼 。

- 5 您可以啟用次要 RADIUS 伺服器以獲得高可用性。
如步驟 4 所述設定次要伺服器。
- 6 按一下**儲存**。

下一個

將 RADIUS 驗證方法新增至預設存取原則。移至 [身分識別與存取管理] > [管理] > [原則] 頁面，然後編輯預設原則規則，以將 RADIUS 驗證方法新增至規則。請參閱“[管理要套用至使用者的驗證方法](#),” 第 66 頁。

在 VMware Identity Manager 中設定 RSA 調適性驗證

與針對 Active Directory 僅進行使用者名稱及密碼驗證相比，RSA 調適性驗證的實作能提供更強大的多重要素驗證。調適性驗證能根據風險程度和原則來監控及驗證使用者登入嘗試。

啟用調適性驗證時，系統會使用在 RSA Policy Management 應用程式中設定之風險原則內的風險指標，以及 VMware Identity Manager 的調適性驗證服務組態來判斷是否使用者名稱和密碼來驗證使用者，抑或是需要其他資訊來驗證使用者。

驗證支援的 RSA 調適性驗證方法

VMware Identity Manager 服務中支援的 RSA 調適性驗證強式驗證方法，即透過電話、電子郵件或 SMS 文字訊息和挑戰問題進行額外驗證。您可以在服務上啟用可提供的 RSA 調適型驗證方法。RSA 調適型驗證原則會判斷該使用哪個次要驗證方法。

額外驗證是要求在使用者名稱和密碼之外傳送額外驗證的程序。當使用者在 RSA 調適性驗證伺服器中註冊時，他們需要根據伺服器組態提供電子郵件地址、電話號碼或兩者。若需要額外驗證，RSA 調適性驗證伺服器會透過提供的通道傳送一次性通行碼。除了使用者名稱和通行碼之外，使用者還需要輸入該密碼。

當使用者在 RSA 調適性驗證伺服器中註冊時，挑戰問題會要求使用者回答一系列的問題。您可以設定要回答的註冊問題數目，以及登入頁面上出現的挑戰問題數目。

向 RSA 調適性驗證伺服器註冊使用者

您必須先在 RSA 調適性驗證資料庫中佈建使用者，才能使用調適型驗證來進行驗證。當使用者首次以他們的使用者名稱和密碼登入時，系統會將他們新增至 RSA 調適性驗證資料庫。根據您在服務中設定 RSA 調適性驗證的方式，當使用者登入時，系統會要求他們提供電子郵件地址、電話號碼、文字訊息服務號碼 (SMS)，或是要求他們設定挑戰問題的回應。

備註 RSA 調適性驗證不允許在使用者名稱中使用國際字元。如果您想要允許在使用者名稱中使用多字元組字元，請聯絡 RSA 支援以設定 RSA 調適性驗證和 RSA 驗證管理員。

在 Identity Manager 中設定 RSA 調適性驗證

若要為服務設定 RSA 調適性驗證，您需要啟用 RSA 調適性驗證；選取要套用的調適性驗證方法，以及新增 Active Directory 連線資訊和憑證。

先決條件

- 次要驗證使用之驗證方法已正確設定的 RSA 調適性驗證。
- 有關 SOAP 端點位址和 SOAP 使用者名稱的詳細資料。
- 可供使用的 Active Directory 組態資訊和 Active Directory SSL 憑證。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**設定**。
- 2 在 [連接器] 頁面的 [Workers] 資料行中，針對正在設定的連接器選取連結。
- 3 按一下**驗證配接器**，然後按一下 **RSAAldpAdapter**。
系統會將您重新導向到 Identity Manager 驗證配接器頁面。
- 4 按一下 RSAAldpAdapter 旁的**編輯**連結。

5 選取適合環境的設定。

備註 星號表示必填欄位。其他欄位為選填。

選項	說明
*名稱	名稱為必填。預設名稱為 RSAAALdpAdapter。您可變更此名稱。
啟用 RSA AA 配接器	選取此核取方塊可啟用 RSA 調適性驗證。
*SOAP 端點	輸入 RSA 調適性驗證配接器和服務整合所需的 SOAP 端點位址。
*SOAP 使用者名稱	輸入用來簽署 SOAP 訊息的使用者名稱和密碼。
RSA 網域	輸入調適性驗證伺服器的網域位址。
啟用 OOB 電子郵件	若要啟用透過電子郵件訊息將一次性通行碼傳送給使用者的頻外驗證，請選取此核取方塊。
啟用 OOB SMS	若要啟用透過 SMS 文字訊息將一次性通行碼傳送給使用者的頻外驗證，請選取此核取方塊。
啟用 SecurID	選取此核取方塊可啟用 SecurID。系統會要求使用者輸入其 RSA 權杖和通行碼。
啟用密碼問題	如果您要使用註冊和挑戰問題來進行驗證，請選取此核取方塊。
*註冊問題數	輸入使用者註冊驗證配接器伺服器時需要設定的問題數目。
*挑戰問題數	輸入使用者必須正確回答才能登入的挑戰問題數目。
*允許嘗試的驗證次數	輸入在認定驗證失敗之前，要向嘗試登入之使用者顯示挑戰問題的次數。
目錄類型	Active Directory 是唯一支援的目錄。
伺服器連接埠	輸入 Active Directory 連接埠號碼。
伺服器主機	輸入 Active Directory 主機名稱。
使用 SSL	如果您的目錄連線要使用 SSL，請選取此核取方塊。您可以在 [目錄憑證] 欄位中新增 Active Directory SSL 憑證。
使用 DNS 服務位置	如果目錄連線使用 DNS 服務位置，請選取此核取方塊。
基準 DN	輸入要開始搜尋帳戶的 DN。例如，OU=myUnit,DC=myCorp,DC=com。
繫結 DN	輸入可搜尋使用者的帳戶。例如，CN=binduser,OU=myUnit,DC=myCorp,DC=com
繫結密碼	輸入繫結 DN 帳戶的密碼。
搜尋屬性	輸入包含使用者名稱的帳戶屬性。
目錄憑證	若要建立安全的 SSL 連線，請將目錄伺服器憑證新增至文字方塊。若為多重伺服器案例，請新增憑證授權機構的根憑證。

6 按一下儲存。

下一個

在 [身分識別與存取管理] > [管理] 索引標籤的 [內建身分識別提供者] 中，啟用 [RSA 調適性驗證] 驗證方法。請參閱“設定內建身分識別提供者,” 第 62 頁。

將 RSA 調適性驗證驗證方法新增至預設存取原則。前往 [身分識別與存取管理] > [管理] > [原則] 頁面，接著編輯預設原則規則以新增調適性驗證。請參閱“管理要套用至使用者的驗證方法,” 第 66 頁。

設定憑證或智慧卡介面卡以搭配 VMware Identity Manager 使用

您可將 x509 憑證驗證設定為允許用戶端在其桌面和行動裝置上使用憑證進行驗證，或使用智慧卡介面卡進行驗證。憑證式驗證由使用者所擁有的是私密金鑰還是智慧卡，以及使用者所瞭解的內容是私密金鑰的密碼還是智慧卡 PIN 而定。X.509 憑證將使用公開金鑰基礎結構 (PKI) 標準來確認憑證中包含的公開金鑰屬於該使用者。使用者可藉由智慧卡驗證將智慧卡連線至電腦，然後輸入 PIN。

智慧卡憑證會複製到使用者電腦上的本機憑證存放區。本機憑證存放區中的憑證可供在此使用者電腦上執行的所有瀏覽器使用 (但存在一些例外狀況)，因此，這些憑證也可供瀏覽器中的 VMware Identity Manager 執行個體使用。

備註 設定了憑證驗證，且在負載平衡器後方設定服務應用裝置時，請確保在負載平衡器上的 VMware Identity Manager Connector 設定了 SSL 傳遞，且未將其設定為在負載平衡器上終止 SSL。此組態確保連接器與用戶端之間存在 SSL 信號交換，以便將憑證傳遞至連接器。將負載平衡器設定為在負載平衡器上終止 SSL 時，您可以在另一個負載平衡器後方部署第二個連接器，以支援憑證驗證。

如需新增第二個連接器的相關資訊，請參閱《VMware Identity Manager 安裝與組態指南》。

使用使用者主體名稱進行憑證驗證

您可以在 Active Directory 中使用憑證對應。憑證和智慧卡登入會使用 Active Directory 中的使用者主體名稱 (UPN) 來驗證使用者帳戶。嘗試在 VMware Identity Manager 服務中驗證的使用者 Active Directory 帳戶，必須包含與憑證中 UPN 相對應的有效 UPN。

如果憑證中不存在 UPN，您可以將 VMware Identity Manager 設定為使用電子郵件地址來驗證使用者帳戶。還可以啟用要使用的備用 UPN 類型。

驗證所需的憑證授權機構

若要啟用使用憑證驗證登入，必須將根憑證和中繼憑證上傳到 VMware Identity Manager。

憑證會複製到使用者電腦上的本機憑證存放區。本機憑證存放區中的憑證可供在此使用者電腦上執行的所有瀏覽器使用 (但存在一些例外狀況)，因此，這些憑證也可供瀏覽器中的 VMware Identity Manager 執行個體使用。

對於智慧卡驗證，當使用者起始 VMware Identity Manager 執行個體的連線時，VMware Identity Manager 服務會將受信任憑證授權機構 (CA) 的清單傳送至瀏覽器。瀏覽器會對照可用的使用者憑證檢查信任的 CA 清單，選取適當的憑證，再提示使用者輸入智慧卡 PIN。如果有多個有效的使用者憑證可供使用，瀏覽器會提示使用者選取其中一個憑證。

如果使用者無法驗證，則可能未正確設定根 CA 和中繼 CA，或是將根和中繼 CA 上傳到伺服器後未重新啟動服務。在這些情況下，瀏覽器無法顯示已安裝的憑證，使用者無法選取正確的憑證，且憑證驗證會失敗。

使用憑證撤銷檢查

您可以設定憑證撤銷檢查，以避免對使用者憑證已撤銷的使用者進行驗證。通常當使用者離開組織、遺失智慧卡，或調動部門時，就會撤銷憑證。

支援使用憑證撤銷清單 (CRL) 及線上憑證狀態通訊協定 (OCSP) 來進行憑證撤銷檢查。CRL 是核發憑證的 CA 所發佈的撤銷憑證清單。OCSP 是一種用於取得憑證撤銷狀態的憑證驗證通訊協定。

您可以在同一個憑證驗證介面卡組態中同時設定 CRL 和 OCSP。當您同時設定兩種類型的憑證撤銷檢查，且啟用了 [當 OCSP 失敗時使用 CRL] 核取方塊時，將會先檢查 OCSP，如果 OCSP 失敗，撤銷檢查會退而使用 CRL。如果 CRL 失敗，撤銷檢查不會退而使用 OCSP。

透過 CRL 檢查登入

當您啟用憑證撤銷時，VMware Identity Manager 伺服器會讀取 CRL 來判斷使用者憑證的撤銷狀態。

如果憑證已撤銷，則透過憑證進行驗證將會失敗。

登入時進行 OCSP 憑證檢查

當您設定憑證狀態通訊協定 (OCSP) 撤銷檢查時，VMware Identity Manager 會傳送一個請求給 OCSP 回應器，申請其判斷特定使用者憑證的撤銷狀態。VMware Identity Manager 伺服器會使用 OCSP 簽署憑證來確認從 OCSP 回應器收到的回應屬實。

如果憑證已撤銷，驗證將會失敗。

您可以將驗證設定為在未收到 OCSP 回應器的回應或回應無效時退而使用 CRL。

設定 VMware Identity Manager 的憑證驗證

您可從 VMware Identity Manager 管理主控台啟用並設定憑證驗證。

先決條件

- 從簽署由您的使用者提供之憑證的 CA 取得根憑證和中繼憑證。
- (選用) 適用於憑證驗證的有效憑證原則的物件識別碼 (OID) 清單。
- CRL 的檔案位置和 OCSP 伺服器的 URL，用於撤銷檢查。
- (選擇性) OCSP 回應簽署憑證檔案位置。
- 同意表單內容 (如果同意表單在驗證前顯示)。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**設定**。
- 2 在 [連接器] 頁面上，針對正在設定的連接器，選取 Worker 連結。
- 3 按一下**驗證介面卡**，然後按一下 **CertificateAuthAdapter**。
- 4 設定 [憑證驗證介面卡] 頁面。

備註 星號表示必填欄位。其他欄位為選填。

選項	說明
*名稱	名稱為必填。預設名稱為 CertificateAuthAdapter。您可變更此名稱。
啟用憑證配接器	選取此核取方塊可啟用憑證驗證。
*根和中繼 CA 憑證	選取要上傳的憑證檔案。您可選取多個編碼為 DER 或 PEM 的根 CA 和中繼 CA 憑證。
上傳的 CA 憑證	上傳的憑證檔案列於表單的 [上傳的 CA 憑證] 區段中。
如果憑證中沒有 UPN 便使用電子郵件	如果使用者主體名稱 (UPN) 不在憑證中，請選取此核取方塊將 emailAddress 屬性作為主體別名延伸，以驗證使用者的帳戶。
憑證原則已接受	建立憑證原則延伸中已接受之物件識別碼的清單。 輸入憑證核發原則的物件識別碼號碼 (OID)。按一下 新增另一個值 來新增其他 OID。
啟用憑證撤銷	選取此核取方塊可啟用憑證撤銷檢查。撤銷檢查會導致已撤銷使用者憑證的使用者無法驗證。
使用來自憑證的 CRL	選取此核取方塊，可使用由核發憑證的 CA 所發行的憑證撤銷清單 (CRL) 來驗證憑證的狀態 (已撤銷或未撤銷)。

選項	說明
CRL 位置	輸入要從中擷取 CRL 的伺服器檔案路徑或本機檔案路徑。
啟用 OCSP 撤銷	選取此核取方塊，以使用線上憑證狀態通訊協定 (OCSP) 憑證驗證通訊協定瞭解憑證的撤銷狀態。
OCSP 失敗時使用 CRL	如果您同時設定 CRL 和 OCSP，您可以勾選此方塊，以在 OCSP 檢查不可用時返回使用 CRL。
傳送 OCSP Nonce	如果您希望在回應中傳送 OCSP 申請的唯一識別碼，請選取此核取方塊。
OCSP URL	如果您已啟用 OCSP 撤銷，請輸入用於撤銷檢查的 OCSP 伺服器位址。
OCSP 回應程式的簽署憑證	針對回應程式輸入 OCSP 憑證的路徑 <code>/path/to/file.cer</code> 。
驗證前啟用同意表單	選取此核取方塊以包含同意表單頁面，使其在使用者使用憑證驗證登入其 Workspace ONE 入口網站前顯示。
同意表單內容	在此文字方塊中輸入要顯示在同意表單中的文字。

5 按一下**儲存**。

下一個

- 將憑證驗證方法新增至預設存取原則。移至 [身分識別與存取管理] > [管理] > [原則] 頁面，然後編輯預設原則規則以新增憑證。請參閱“[管理要套用至使用者的驗證方法](#),” 第 66 頁。
- 設定了憑證驗證，且在負載平衡器後方設定服務應用裝置時，請確保在負載平衡器上 VMware Identity Manager 連接器設定了 SSL 傳遞，且未將其設定為在負載平衡器上終止 SSL。此組態確保連接器與用戶端之間存在 SSL 信號交換，以便將憑證傳遞至連接器。

設定雙重要素驗證適用的 VMware Verify

在需要雙重要素驗證時，您可以在 VMware Identity Manager 管理主控台中啟用 VMware Verify 服務，作為第二個驗證方法。

您可以透過管理主控台，在內建身分識別提供者中啟用 VMware Verify，並新增從 VMware 支援收到的 VMware Verify 安全性權杖。

您可以在存取原則規則中設定雙重要素驗證，以要求使用者使用兩種驗證方法進行驗證。

使用者可將 VMware Verify 應用程式安裝在其裝置上，並提供電話號碼以向 VMware Verify 服務登錄其裝置。裝置和電話號碼也會登錄在管理主控台的 [使用者和群組] 使用者設定檔中。

使用者會在使用密碼驗證登入後先註冊其帳戶，然後輸入顯示在其裝置上的 VMware Verify 通行碼。在初始驗證後，使用者將可透過下列三種方法之一進行驗證。

- 使用 OneTouch 通知推送核准。使用者僅需按一下，即可核准或拒絕來自 VMware Identity Manager 的存取。使用者可在傳送的訊息上按一下 [核准] 或 [拒絕]。
- 以時間為基礎的一次性密碼 (TOTP) 通行碼。每 20 秒會產生一個一次性通行碼。使用者可在登入畫面上輸入此通行碼。
- 文字訊息。使用電話 SMS，以文字訊息的方式將一次性驗證碼傳送至已登錄的電話號碼。使用者可在登入畫面上輸入此驗證碼。

VMware Verify 會使用第三方雲端服務，將此功能提供給使用者裝置。為了執行此作業，名稱、電子郵件和電話號碼等使用者資訊將會儲存在服務中，但不會用於提供該功能以外的任何用途。

啟用 VMware Verify

若要啟用 VMware Verify 服務的雙重要素驗證，您必須將安全性權杖新增至 VMware Verify 頁面，然後在內建身分識別提供者中啟用 VMware Verify。

先決條件

透過 VMware 或 AirWatch 支援建立支援票證，以便接收可啟用 VMware Verify 的安全性權杖。支援團隊人員會處理您的要求，並更新含有指示和安全性權杖的支援票證。您可以將此安全性權杖新增至 VMware Verify 頁面。

(選用) 自訂裝置上 VMware Verify 應用程式中所顯示的標誌和圖示。請參閱“為 VMware Verify 應用程式自訂品牌,” 第 103 頁。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**管理 > 身分識別提供者**。
- 2 選取名為**內建**的身分識別提供者。
- 3 按一下 **VMware Verify** 齒輪圖示。
- 4 選取**啟用多重要素驗證**核取方塊。
- 5 將從 VMware 或 AirWatch 支援團隊收到的安全性權杖貼至 [安全性權杖] 文字方塊中。
- 6 按一下**儲存**。

下一個

在預設存取原則中建立存取原則規則，以將 VMware Verify 驗證方法新增為規則中的第二個驗證方法。請參閱“[管理要套用至使用者的驗證方法](#),” 第 66 頁。

將自訂品牌套用至 VMware Verify 登入頁面。請參閱“[為 VMware Verify 應用程式自訂品牌](#),” 第 103 頁。

向 VMware Verify 登錄使用者

需要透過 VMware Verify 驗證進行雙因素驗證時，使用者將必須安裝 VMware Verify 應用程式，並用它來登錄其裝置。

備註 VMware Verify 應用程式可從應用程式商店下載取得。

在 VMware Verify 雙因素驗證啟用的情況下，當使用者第一次登入 Workspace ONE 應用程式時，系統會要求使用者輸入其使用者名稱和密碼。驗證使用者名稱和密碼後，系統會提示使用者輸入其裝置電話號碼，以在 VMware Verify 中進行註冊。

當他們按一下 [註冊] 時，即會向 VMware Verify 登錄裝置電話號碼，且若他們尚未下載應用程式，則系統會要求他們下載 VMware Verify 應用程式。

應用程式安裝後，系統會要求使用者輸入先前輸入的相同電話號碼，並選取用來接收一次性登錄碼的通知方法。登錄碼可在登錄 PIN 碼頁面上輸入。

在登錄裝置電話號碼後，使用者可使用顯示於 VMware Verify 應用程式中以時間為基礎的一次性通行碼來登入 Workspace ONE。此通行碼是在裝置上產生，且會持續變更的唯一號碼。

使用者可登錄多個裝置。VMware Verify 通行碼會自動同步化至各個已登錄的裝置。

從使用者設定檔中移除已登錄的電話號碼

若要疑難排解登入 Workspace ONE 方面的問題，您可以在 VMware Identity Manager 管理主控台中，移除使用者設定檔中的使用者電話號碼。

程序

- 1 在管理主控台中，按一下**使用者和群組**。
- 2 在 [使用者] 頁面上，選取要重設的使用者名稱。

- 3 在 [VMware Verify] 索引標籤中，按一下 **重設 VMware Verify**。

電話號碼會從使用者設定檔中移除，且 [使用者] 清單中的 [VMware Verify 電話號碼] 資料行會顯示為 [N/A]。電話號碼會從 VMware Verify 服務中解除登錄。當使用者登入其 Workspace ONE 應用程式時，系統將會要求他們再次輸入要在 VMware Verify 服務中註冊的電話號碼。

設定內建身分識別提供者

管理主控台的 [身分識別與存取管理 > 身分識別提供者] 頁面中，提供了一個可用的內建身分識別提供者。您可以建立其他內建身分識別提供者。

您可以設定可用的內建身分識別提供者，以支援不需要連接器的驗證方法。以及在針對 VMware Identity Manager 服務的僅限輸出連線模式中，在部署於 DMZ 後方的連接器上進行設定的驗證方法。

您在此內建身分識別提供者中設定的驗證方法，可以在您新增的其他內建身分識別提供者中啟用。您不需要在您新增的內建身分識別提供者中設定驗證方法。

下列驗證方法不需連接器，並且可從預設的內建身分識別提供者進行設定。

- iOS 版 Mobile SSO
- 憑證 (雲端部署)
- 使用 AirWatch Connector 的密碼
- 雙重要素驗證適用的 VMware Verify
- Android 版 Mobile SSO
- 裝置與 AirWatch 的符合性
- 密碼 (本機目錄)

備註 在單向輸出連線模式下，不需要開啟任何防火牆連接埠。

在內建身分識別提供者中設定這些驗證方法時，如果使用者和群組位於企業目錄中，則在使用這些驗證方法之前，您必須將使用者和群組同步至 VMware Identity Manager 服務中。

啟用驗證方法後，接下來您可以建立套用至這些驗證方法的存取原則。

設定內建身分識別提供者

使用不需要連接器的驗證方法來設定預設內建身分識別提供者。您在此處設定的驗證方法，將可在新增至環境的其他內建身分識別提供者上啟用。

程序

- 1 在 [身分識別與存取管理] 索引標籤中，前往 **管理 > 身分識別提供者**。
- 2 選取標示為「內建」的身分識別提供者，並設定身分識別提供者詳細資料。

選項	說明
身分識別提供者名稱	輸入此內建身分識別提供者執行個體的名稱。
使用者	選取要驗證的使用者。系統會列出已設定的目錄。

選項	說明
網路	列出了服務中設定的現有網路範圍。根據要導向至此身分識別提供者執行個體以進行驗證的 IP 位址，選取使用者的網路範圍。
驗證方法	若要設定驗證方法，請按一下齒輪圖示，然後設定驗證方法。在整合 AirWatch 與 VMware Identity Manager 時，您可以選取所要使用的驗證方法。 針對 [裝置符合性 (與 AirWatch)] 和 [密碼 (AirWatch Connector)]，請確定選項已在 AirWatch 組態頁面中啟用。

- 3 在您建立驗證方法後，請選取要與此內建身分識別提供者搭配使用之驗證方法的核取方塊。
- 4 如果您使用內建的 Kerberos 驗證，請下載 KDC 簽發者憑證，以在 iOS 裝置管理設定檔的 AirWatch 組態中使用。
- 5 按一下**新增**。

您設定的驗證方法可在其他內建身分識別提供者中啟用，而不需進行額外設定。

在建立僅限輸出的連接器時，設定內建身分識別提供者

針對 VMware Identity Manager Cloud 服務的僅限輸出連線，在內建身分識別提供者中，啟用您在連接器中設定的驗證方法。

先決條件

- 位於企業目錄中的使用者和群組必須同步至 VMware Identity Manager 目錄。
- 您想要導向至內建身分識別提供者執行個體以進行驗證的網路範圍清單。
- 若要啟用內建身分識別提供者的驗證方法，請確定這些驗證方法已在連接器中設定。

程序

- 1 在 [身分識別與存取管理] 索引標籤中，前往**管理 > 身分識別提供者**。
- 2 選取標示為「內建」的身分識別提供者，並設定身分識別提供者詳細資料。

選項	說明
身分識別提供者名稱	輸入此內建身分識別提供者執行個體的名稱。
使用者	選取要驗證的使用者。系統會列出已設定的目錄。
網路	列出了服務中設定的現有網路範圍。根據要導向至此身分識別提供者執行個體以進行驗證的 IP 位址，選取使用者的網路範圍。
驗證方法	在整合 AirWatch 與 VMware Identity Manager 時，您可以選取所要使用的驗證方法。按一下要設定之驗證方法的齒輪圖示。 針對 [裝置符合性 (與 AirWatch)] 和 [密碼 (AirWatch Connector)]，請確定選項已在 AirWatch 組態頁面中啟用。
連接器	(選用) 選取在僅限輸出連線模式中設定的連接器。
連接器驗證方法	在連接器上設定的驗證方法會列在此區段中。選取此核取方塊可啟用驗證方法。

- 3 如果您使用內建的 Kerberos 驗證，請下載 KDC 簽發者憑證，以在 iOS 裝置管理設定檔的 AirWatch 組態中使用。
- 4 按一下**儲存**。

設定其他 Workspace 身分識別提供者

最初設定 VMware Identity Manager 連接器時，當您啟用連接器以驗證使用者，會將 Workspace IDP 建立為身分識別提供者，並且啟用密碼驗證。

您可以在不同負載平衡器之後設定其他連接器。當您的環境包括一個以上負載平衡器時，您可以在每個負載平衡的組態中設定不同的 Workspace 身分識別提供者，用於進行驗證。請參閱《安裝及設定 VMware Identity Manager 指南》中的〈安裝其他連接器應用裝置〉主題。

不同的 Workspace 身分識別提供者可以與相同的目錄產生關聯，或如果您已設定多個目錄，則可以選取要使用的目錄。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**管理 > 身分識別提供者**。
- 2 按一下**新增身分識別提供者**，然後選取**建立 Workspace IDP**。
- 3 編輯身分識別提供者執行個體設定。

選項	說明
身分識別提供者名稱	輸入此 Workspace 身分識別提供者執行個體的名稱。
使用者	選取可使用此 Workspace 身分識別提供者驗證之使用者的 VMware Identity Manager 目錄。
連接器	系統會列出未與您所選取目錄相關聯的連接器。選取要與目錄產生關聯的連接器。
網路	列出了服務中設定的現有網路範圍。 根據使用者的 IP 位址，為使用者選取想要導向至此身分識別提供者執行個體的網路範圍，以便進行驗證。

- 4 按一下**新增**。

將第三方身分識別提供者執行個體設定為驗證使用者

您可以設定用來對 VMware Identity Manager 服務中的使用者進行驗證的第三方身分識別提供者。

使用管理主控台新增第三方身分識別提供者執行個體之前，先完成下列工作。

- 確認第三方執行個體與 SAML 2.0 相容，且該服務可以連線到第三方執行個體。
- 在管理主控台中設定身分識別提供者時，取得要新增之適當的第三方中繼資料資訊。從第三方執行個體取得的中繼資料資訊可以是中繼資料的 URL，也可以是實際的中繼資料。
- 如果您已啟用該身分識別提供者的 Just-in-Time 佈建，請將 SAML 判斷提示的需求納入考量。該身分識別提供者傳送 SAML 判斷提示必須包含特定屬性。請參閱“[SAML 宣告的需求](#),” 第 44 頁。

新增和設定身分識別提供者執行個體

藉由新增和設定您 VMware Identity Manager 部署的身分識別提供者執行個體，您可以提供高可用性、支援其他使用者驗證方法，以及以您根據使用者 IP 位址範圍管理使用者驗證程序的方式增加彈性。

先決條件

- 設定您想要導向至此身分識別提供者執行個體的網路範圍，以便進行驗證。請參閱“[新增或編輯網路範圍](#),” 第 66 頁。
- 用於第三方中繼資料文件的存取權。這可以是中繼資料的 URL 或是實際中繼資料。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**管理 > 身分識別提供者**。
- 2 按一下**新增身分識別提供者**，然後選取**建立第三方 IDP**。編輯身分識別提供者執行個體設定。
- 3 編輯身分識別提供者執行個體設定。

表單項目	說明
身分識別提供者名稱	輸入此身分識別提供者執行個體的名稱。
SAML 中繼資料	新增第三方 IdP XML 式中繼資料文件，以建立與身分識別提供者的信任關係。 <ol style="list-style-type: none"> 1 在文字方塊中輸入 SAML 中繼資料 URL 或 xml 內容。 2 按一下處理 IdP 中繼資料。IdP 支援的 NameID 格式將從中繼資料擷取並新增至 [名稱識別碼格式] 資料表。 3 在 [名稱識別碼值] 資料行中，於服務中選取使用者屬性以與顯示的識別碼格式對應。您可以新增自訂第三方名稱識別碼格式，並將其對應至服務中的使用者屬性值。 4 (選擇性) 選取 NameIDPolicy 回應識別碼字串格式。
Just-in-Time 佈建	設定 Just-In-Time 佈建以在使用者登入時，動態地在 Identity Manager 服務中建立使用者。JIT 目錄隨即建立，且 SAML 判斷提示中的屬性可用來在服務中建立使用者。請參閱第 6 章, “Just-in-Time 使用者佈建,” 第 41 頁。
使用者	選取可使用此身分識別提供者進行驗證之使用者的目錄。
網路	列出了服務中設定的現有網路範圍。 根據使用者的 IP 位址，為使用者選取想要導向至此身分識別提供者執行個體的網路範圍，以便進行驗證。
驗證方法	新增第三方身分識別提供者支援的驗證方法。選取支援驗證方法的 SAML 驗證內容類別。
單一登出組態	啟用單一登出，可在使用者登出時將使用者登出其身分識別提供者工作階段。如果未啟用單一登出，當使用者登出時，其身分識別提供者工作階段仍會在作用中。 (選用) 如果身分識別提供者支援 SAML 單一登出設定檔，請啟用單一登出，並將 重新導向 URL 文字方塊保留為空白。如果身分識別提供者不支援 SAML 單一登出設定檔，請啟用單一登出，並輸入使用者從 VMware Identity Manager 登出時所將重新導向到的身分識別提供者的登出 URL。 如果您已設定重新導向 URL，並且想要讓使用者在重新導向至身分識別提供者登出 URL 之後返回 VMware Identity Manager 登入頁面，請輸入身分識別提供者重新導向 URL 所使用的參數名稱。
SAML 簽署憑證	按一下 服務提供者 (SP) 中繼資料 ，以查看 VMware Identity Manager SAML 服務提供者中繼資料 URL 的 URL。複製並儲存該 URL。在第三方身分識別提供者中編輯 SAML 判斷提示以對應 VMware Identity Manager 使用者時會設定此 URL。
IdP 主機名稱	如果顯示 [主機名稱] 文字方塊，請輸入身分識別提供者重新導向到的主機名稱，以進行驗證。如果使用的是 443 以外的非標準連接埠，您可以將主機名稱設定為「主機名稱:連接埠」。例如 myco.example.com:8443。

- 4 按一下**新增**。

下一個

- 將身分識別提供者的驗證方法新增至服務預設原則。請參閱“[將驗證方法套用至原則規則](#),” 第 67 頁。
- 編輯第三方身分識別提供者的組態，以新增您儲存的 SAML 簽署憑證 URL。

管理要套用至使用者的驗證方法

VMware Identity Manager 服務會嘗試根據驗證方法、預設的存取原則、網路範圍以及您設定的身分識別提供者執行個體，來驗證使用者。

使用者嘗試登入時，服務會評估預設的存取原則規則，以選取要套用原則中的哪項規則。驗證方法將按照在規則中列出的順序進行套用。系統會選取滿足規則的驗證方法和網路範圍需求的第一個身分識別提供者執行個體。使用者驗證要求會轉送至該身分識別提供者執行個體以進行驗證。如果驗證失敗，則會套用規則中設定的下一個驗證方法。

您可新增規則以指定依裝置類型而定，或依裝置類型且來自特定網路範圍而定的驗證方法。例如，您可以設定一項規則，要求使用 iOS 裝置從特定網路登入的使用者必須使用 RSA SecurID 進行驗證。接著，再設定另一項規則，要求使用任何類型裝置從內部網路 IP 位址登入的使用者必須使用其密碼進行驗證。

新增或編輯網路範圍

建立網路範圍，以定義使用者可以從中登入的 IP 位址。將建立的網路範圍新增至特定身分識別提供者執行個體及存取原則規則。

系統會建立一個名為 ALL RANGES 的網路範圍做為預設值。此網路範圍包括網際網路上可用的每個 IP 位址 (0.0.0.0 到 255.255.255.255)。如果部署中只有單一身分識別提供者執行個體，您可以變更 IP 位址範圍，並新增其他範圍，以在預設網路範圍中排除或包含特定 IP 位址。您可以建立包括適用於特定用途之特定 IP 位址的其他網路範圍。

備註 預設網路範圍 ALL RANGES 及其說明「所有範圍的網路」均可編輯。使用 [網路範圍] 頁面上的**編輯**功能，即可編輯名稱及說明，包括將文字變更為不同語言。

先決條件

- 根據網路拓撲定義 VMware Identity Manager 部署的網路範圍。
- 在服務中啟用 View 時，您可以根據網路範圍來指定 View URL。若要在啟用 View 模組時新增網路範圍，請記下 Horizon Client 存取 URL 和網路範圍的連接埠號碼。如需詳細資訊，請參閱 View 說明文件。
請參閱《在 VMware Identity Manager 中設定資源》的〈提供 View 桌面平台集區和應用程式的存取權〉章節。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**設定 > 網路範圍**。
- 2 編輯現有網路範圍或新增網路範圍。

選項	說明
編輯現有範圍	按一下網路範圍名稱以編輯。
新增範圍	按一下 新增網路範圍 以新增範圍。

- 3 編輯 [新增網路範圍] 頁面。

表單項目	說明
名稱	輸入網路範圍的名稱。
說明	輸入網路範圍的說明。
View 網繭	[View 網繭] 選項僅在 View 模組啟用時顯示。 用戶端存取 URL 主機。針對網路範圍輸入正確的 Horizon Client 存取 URL。 用戶端存取連接埠。針對網路範圍輸入正確的 Horizon Client 存取連接埠號碼。

表單項目	說明
IP 範圍	編輯或新增 IP 範圍，確保其中僅包含所有需要的 IP 位址。

下一個

- 將每個網路範圍與身分識別提供者執行個體相關聯。
- 視情況將網路範圍與存取原則規則相關聯。請參閱第 8 章, “管理存取原則,” 第 69 頁。

套用預設存取原則

VMware Identity Manager 服務包含一個預設存取原則，可控制使用者對其 Workspace ONE 入口網站和 Web 應用程式的存取。您可以在必要時編輯原則以變更原則規則。

當您啟用密碼驗證以外的驗證方法時，必須編輯預設原則以將啟用的驗證方法新增至原則規則。

預設存取原則中的每個規則需要滿足一組準則，才能允許使用者存取應用程式入口網站。您可以套用網路範圍、選取可存取內容的使用者類型，以及選取要使用的驗證方法。請參閱第 8 章, “管理存取原則,” 第 69 頁。

此服務嘗試使用指定驗證方法讓使用者登入的次數有所不同。在使用 Kerberos 驗證或憑證驗證的情況下，服務只會嘗試一次。如果這次嘗試無法成功讓使用者登入，將嘗試規則中的下一個驗證方法。Active Directory 密碼和 RSA SecurID 驗證的登入嘗試失敗次數上限預設為五次。當使用者嘗試登入失敗五次後，服務會嘗試使用清單上的下一個驗證方法讓使用者登入。當所有驗證方法已用盡時，服務會發出錯誤訊息。

將驗證方法套用至原則規則

預設原則規則中僅設定了密碼驗證方法。您必須編輯原則規則才能選取您所設定的其他驗證方法，並設定驗證方法用於驗證的順序。

您可以設定存取原則規則，要求使用者透過兩種驗證方法傳遞認證之後才能登入。請參閱“設定存取原則設定,” 第 69 頁。

先決條件

啟用並設定您組織支援的驗證方法。請參閱第 7 章, “在 VMware Identity Manager 中設定使用者驗證,” 第 47 頁。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**管理 > 原則**。
- 2 按一下要編輯的預設存取原則。
- 3 在 [原則規則] 區段中，按一下要編輯的驗證方法，或新增原則規則，然後按一下 **+** 圖示。
 - a 確認網路範圍正確。如果要新增新規則，請為此原則規則選取網路範圍。
 - b 從**且使用者正在嘗試存取來自下列裝置的內容**下拉式功能表中，選取此規則所管理的裝置。
 - c 設定驗證順序。在**則使用者必須使用下列方法進行驗證**下拉式功能表中，選取要先套用的驗證方法。若要要求使用者透過兩個驗證方法進行驗證，請按一下 **+**，然後在下拉式功能表中選取第二個驗證方法。
 - d (選用) 若要設定其他後援驗證方法，請在**如果前述驗證方法失敗，則:** 下拉式功能表中，選取其他已啟用的驗證方法。
您可以將多種後援驗證方法新增到規則中。
 - e 在**在以下時間之後重新驗證**下拉式功能表中選取工作階段長度，讓使用者必須在該時間長度經過後重新驗證。

- f (選用) 建立當使用者驗證失敗時要顯示的自訂存取遭拒訊息。您可以使用最多 4000 個字元，大約為 650 字。如果您要將使用者傳送至另一個頁面，請在**連結 URL** 文字方塊中輸入 URL 連結位址。在**連結文字**文字方塊中，輸入應顯示為連結的文字。如果您將此文字方塊保留空白，則會顯示字組繼續。
 - g 按一下**儲存**。
- 4 按一下**儲存**。

Edit Policy Rule

If a user's Network Range is...

and the user is trying to access content from...

then the user must authenticate using the following method...

+

If preceding Authentication Method fails, then:

+

+ fallback Method(s)

Re-authenticate after:

Custom Error Message Create an custom access denied error message that displays when user authentication fails.

Message Text

管理存取原則

若想提供安全存取使用者應用程式入口網站以及安全啟動 Web 桌面平台應用程式的方法，您可設定存取原則，其中包含指定必須符合準則才能登入其應用程式入口網站以及使用其資源的規則。

原則規則會將提出要求的 IP 位址對應至網路範圍並指定使用者可用來登入的裝置類型。規則可定義驗證方法以及驗證的有效時數。

VMware Identity Manager 服務包括控制整體服務存取權的預設原則。此原則設定為允許從所有裝置類型存取所有網路範圍，且工作階段逾時設為八小時，而驗證方法為密碼驗證。您可以編輯預設原則。

備註 原則不會控制應用程式工作階段持續的時間長度。它們會控制使用者必須啟動應用程式的時間長度。

本章節討論下列主題：

- [“設定存取原則設定,”](#) 第 69 頁
- [“管理 Web 和桌面平台應用程式特定的原則,”](#) 第 71 頁
- [“新增 Web 或桌面平台應用程式特定原則,”](#) 第 73 頁
- [“設定自訂存取遭拒錯誤訊息,”](#) 第 74 頁
- [“編輯存取原則,”](#) 第 74 頁
- [“在行動裝置上啟用持續性 Cookie,”](#) 第 75 頁

設定存取原則設定

原則包含一或多個存取規則。每個規則皆包含一些設定，可供您設定用來管理整個 Workspace ONE 入口網站或特定 Web 和桌面平台應用程式的使用者存取權。

原則規則可以設定為根據網路、裝置類型或 AirWatch 裝置註冊、相容狀態或正在存取應用程式之類的條件，執行封鎖、允許或逐步驗證使用者等動作。

網路範圍

對於每個規則，您均可透過指定網路範圍決定使用者基礎。網路範圍由一或多個 IP 範圍組成。您可以在設定存取原則集前，從 [身分識別與存取管理] 索引標籤的 [設定] > [網路範圍] 頁面建立網路範圍。

部署中的每個身分識別提供者執行個體連結網路範圍與驗證方法。設定原則規則時，請確定現有的身分識別提供者執行個體涵蓋了網路範圍。

您可以設定特定的網路範圍，藉以限制使用者可登入及存取應用程式。

裝置類型

選取規則管理的裝置類型。用戶端類型為 Web 瀏覽器、Workspace ONE 應用程式、iOS、Android、Windows 10、OS X 和所有裝置類型。

您可以透過設定規則來指定可存取內容的裝置類型，而來自該裝置類型的所有驗證要求都會使用原則規則。

驗證方法

在原則規則中，您可以設定驗證方法的套用順序。驗證方法會按照其列出的順序進行套用。系統會選取原則中第一個符合驗證方法和網路範圍組態的身分識別提供者執行個體。使用者驗證要求會轉送至身分識別提供者執行個體以進行驗證。如果驗證失敗，則會選取清單中的下一個驗證方法。

您可以設定存取原則規則，以要求使用者在登入前通過兩種驗證方法的認證。如果一或兩個驗證方法失敗，且後援方法已設定，系統將會提示使用者輸入其認證，以使用已設定的下一個驗證方法。下列兩個案例說明此驗證鏈結的運作方式。

- 在第一個案例中，存取原則規則設定為需要使用者使用其密碼及 Kerberos 認證進行驗證。後援驗證設定為需要密碼和 RADIUS 認證，以進行驗證。使用者可輸入正確的密碼，但無法輸入正確的 Kerberos 驗證認證。由於使用者輸入了正確的密碼，因此後援驗證要求僅針對 RADIUS 認證。使用者無需重新輸入密碼。
- 在第二個案例中，存取原則規則設定為需要使用者使用其密碼及其 Kerberos 認證進行驗證。後援驗證設定為需要 RSA SecurID 和 RADIUS 才能進行驗證。使用者可輸入正確的密碼，但無法輸入正確的 Kerberos 驗證認證。後援驗證要求同時包含對 RSA SecurID 認證和 RADIUS 認證的要求才能以進行驗證。

若要設定存取原則規則，則需要進行驗證和裝置符合性驗證，且必須在內建身分識別提供者頁面中啟用 [與 AirWatch 的裝置符合性]。請參閱“[設定符合性檢查的存取原則規則](#),” 第 124 頁。

驗證工作階段長度

對於每個規則，您可以設定此驗證有效的小時數。在以下時間之後重新驗證值會決定使用者從上次驗證事件到存取其入口網站，或啟動特定應用程式之間所擁有的時間上限。例如，若 Web 應用程式規則中的值為 4，則會給予使用者四小時啟動 Web 應用程式，除非他們起始了延長時間的其他驗證事件。

自訂存取遭拒錯誤訊息

當使用嘗試登入，但因為認證無效、組態錯誤或系統錯誤導致登入失敗時，會顯示存取遭拒訊息。預設訊息為由於找不到有效的驗證方法，因此存取遭拒。

您可以為每項存取原則規則建立自訂錯誤訊息，這些訊息能覆寫預設訊息。自訂訊息可包含文字和叫用動作訊息的連結。例如，在您要管理之行動裝置的原則規則中，如果使用者嘗試從未註冊的裝置登入，您可以建立下列自訂錯誤訊息。按一下此訊息結尾處的連結可註冊您的裝置以存取公司資源。如果您已註冊裝置，請聯絡支援服務以尋求協助。

預設原則範例

下列原則範例可說明如何設定預設原則以控制應用程式入口網站的存取權，以及尚未指派特定原則之 Web 應用程式的存取權。

預設原則

* 原則名稱: default_access_policy_set

說明: Default access policy set

套用到: 所有應用程式

原則規則

您可以建立這些 Web 應用程式的存取規則清單。針對每個規則，請選取 IP 網路範圍、可存取應用程式的裝置類型、方法和驗證順序，以及重新驗證之前使用者可以使用應用程式的時數上限。

網路範圍	裝置類型	驗證方法	重新驗證	
☒ 所有範圍	Web 瀏覽器	Password	8 小時	✖ +
☒ 所有範圍	Identity Manager 用戶端應用程式	Password	2160 小時	✖ +

系統會根據原則規則在原則中列出的順序來進行評估。您可以透過在 [原則規則] 區段中拖放規則來變更規則順序。

- 對於內部網路，針對規則設定了兩種驗證方法，**Kerberos** 為首個驗證方法，密碼驗證為後援方法。若要從內部網路存取應用程式入口網站，服務會先嘗試使用 **Kerberos** 驗證來驗證使用者，因為它是規則中列出的第一個驗證方法。如果失敗，系統會提示使用者輸入 **Active Directory** 密碼。使用者使用瀏覽器登入，現在可存取其使用者入口網站的八小時工作階段。
 - 對於來自外部網路 (所有範圍) 的存取，僅可設定 **RSA SecurID** 一種驗證方法。若要從外部網路存取應用程式入口網站，使用者必須使用 **SecurID** 登入。使用者使用瀏覽器登入，現在可存取其應用程式入口網站的四小時工作階段。
- 此預設原則會套用至並未具有應用程式特定原則的所有 Web 和桌面平台應用程式。


管理 Web 和桌面平台應用程式特定的原則

將 Web 和桌面平台應用程式新增至目錄時，您可建立應用程式特定的存取原則。例如，您可以建立含有多個適用於 Web 應用程式之規則的原則，此原則用於指定擁有應用程式存取權的 IP 位址、使用哪種驗證方法，以及需要重新驗證的時間間隔。

以下 Web 應用程式特定的原則提供了可建立用於控制指定 Web 應用程式存取權的原則範例。

範例 1 嚴格的 Web 應用程式特定的原則

在此範例中會建立一個新原則，並將該原則套用至敏感的 Web 應用程式。



Sensitive Web Applications
To be applied to Web applications that should have limited access.

Policy Name*

Description

Applies To Select the Web applications from your Catalog that this policy applies to.

AirWatch
Content Locker
Edit Apps

Policy Rules

Network Range	Device type	Authentication Method	Re-authenticate (Hours)	
Internal Network	Web Browser	First, try: Kerberos and 1 more...	8	✖ +
ALL RANGES	Web Browser	SecurId	4	✖ +

- 1 若要從企業網路外部存取服務，使用者必須使用 **RSA SecurID** 登入。使用者使用瀏覽器登入，且現在已獲得預設存取規則提供的應用程式入口網站四小時工作階段存取權。
- 2 四小時後，使用者嘗試啟動套用了「敏感 Web 應用程式」原則集的 Web 應用程式。
- 3 服務會檢查原則中的規則，並套用包含網路範圍為「所有範圍」的原則，因為使用者要求來自 Web 瀏覽器和「所有範圍」網路範圍。

使用者使用 **RSA SecurID** 驗證方法登入，但是工作階段剛剛已到期。系統會將使用者重新導向以進行重新驗證。重新驗證會為使用者再提供四小時的工作階段，以及啟動應用程式的能力。在接下來的四小時內，使用者可繼續執行應用程式，而不必重新驗證。

範例 2 更嚴格的 Web 應用程式特定的原則

若要將更嚴格的規則套用至更為敏感的 Web 應用程式，您可能需要於一小時後在任何裝置上使用 SecureId 重新驗證。以下是此類型原則存取規則的實作方式範例。

Restricted to One Hour
This policy is for highly restricted apps. Authentication is good for only 1 hours for these web apps.

Policy Name* Restricted to One Hour

Description This policy is for highly restricted apps. Authentication is good for only 1 hours for these web apps.

Applies To Select the Web applications from your Catalog that this policy applies to.
ADP Impl. Edit Apps

Policy Rules
You can create a list of rules to access these Web Applications. For each rule, select the IP network range, the type of devices that can access the applications, the methods and authentication order, and the maximum number of hours users can use the application before reauthenticating.

Network Range	Device type	Authentication Method	Re-authenticate	
ALL RANGES	All device types	SecureId	1 Hour(s)	✖ +

Save Cancel

- 1 使用者使用 Kerberos 驗證方法從企業網路內部登入。
現在，使用者可存取範例 1 中設定的應用程式入口網站八小時。
- 2 使用者立即嘗試啟動套用了範例 2 原則規則的 Web 應用程式，這需要 RSA SecurID 驗證。
- 3 系統會將使用者重新導向至 RSA SecurID 驗證登入頁面。
- 4 使用者成功登入後，服務會啟動應用程式並儲存驗證事件。
如原則規則所述，使用者可繼續執行此應用程式最多一小時，但在一小時後會被要求重新驗證。

新增 Web 或桌面平台應用程式特定原則

您可以建立應用程式特定原則，以管理使用者對於特定 Web 和桌面平台應用程式的存取。

先決條件

- 設定您部署的網路範圍。請參閱“[新增或編輯網路範圍](#),” 第 66 頁。
- 設定您部署的驗證方法。請參閱第 7 章, “[在 VMware Identity Manager 中設定使用者驗證](#),” 第 47 頁。
- 如果您計劃要編輯預設原則 (用以控制對整個服務的使用者存取), 請先對其進行設定, 然後建立應用程式特定的原則。
- 將 Web 和桌面平台應用程式新增至目錄。必須先將至少一個應用程式列在 [目錄] 頁面中, 才能新增應用程式特定原則。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中, 選取**管理 > 原則**。
- 2 按一下**新增原則**以新增原則。

- 3 在相應的文字方塊中新增原則名稱和說明。
- 4 在 [套用至] 區段中按一下 **選取**，然後在顯示的頁面中選取與此原則相關聯的應用程式。
- 5 在 [原則規則] 區段中，按一下 **+** 以新增規則。
系統將顯示 [新增原則規則] 頁面。
 - a 選取要套用到此規則的網路範圍。
 - b 針對此規則，選取可存取應用程式的裝置類型。
 - c 選取要按照應套用驗證方法的順序來使用的驗證方法。
 - d 指定可開啟應用程式工作階段的小時數。
 - e 按一下 **儲存**。
- 6 視情況設定其他規則。
- 7 按一下 **儲存**。

設定自訂存取遭拒錯誤訊息

您可以為每個原則規則建立自訂存取遭拒錯誤訊息，以在使用者嘗試登入但因為認證無效而失敗時顯示。

自訂訊息能包含文字，也能包含連往其他 URL 以協助使用者解決問題的連結。您可以使用最多 4000 個字元，大約為 650 字。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取 **管理 > 原則**。
- 2 按一下要編輯的存取原則。
- 3 若要開啟原則規則頁面，請針對要編輯的規則按一下 [驗證方法] 資料行中的驗證名稱。
- 4 在 **自訂錯誤訊息** 文字方塊中輸入錯誤訊息。
- 5 若要新增 URL 連結，請在 **連結文字** 方塊中輸入連結說明，在 **連結 URL** 中輸入 URL。

連結會出現在自訂訊息的結尾處。如果您新增了 URL 但未在 [連結文字] 方塊中新增文字，顯示的文字連結將會是

繼續。

- 6 按一下 **儲存**。

下一個

為其他原則規則建立自訂錯誤訊息。

編輯存取原則

您可以編輯預設存取原則以變更原則規則，您也可以編輯應用程式特定的原則，以新增或移除應用程式和變更原則規則。

您可以隨時移除應用程式特定的存取原則。預設存取原則是永久的。您無法移除預設原則。

先決條件

- 為您的部署設定適當的網路範圍。請參閱“[新增或編輯網路範圍](#),” 第 66 頁。
- 設定您部署的驗證方法。第 7 章, “[在 VMware Identity Manager 中設定使用者驗證](#),” 第 47 頁

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**管理 > 原則**。
- 2 按一下要編輯的原則。
- 3 如果此原則套用至 Web 或桌面平台應用程式，請按一下**編輯應用程式**，以在此原則中新增或刪除應用程式。
- 4 在 [原則規則] 區段的 [驗證方法] 資料行中，選取要編輯的規則。
[編輯原則規則] 頁面會以現有的組態顯示。
- 5 若要設定驗證順序，請在**然後使用者必須使用下列方法**下拉式功能表中選取要首先套用的驗證方法。
- 6 (選擇性) 若要設定第一種驗證失敗時要使用的後援驗證方法，請從下一個下拉式功能表選取另一個已啟用的驗證方法。
您可以將多種後援驗證方法新增到規則中。
- 7 按一下**儲存**，然後在 [原則] 頁面上再按一下**儲存**。

編輯的原則規則會立即生效。

下一個

如果原則是應用程式特定的存取原則，您也可以從 [目錄] 頁面中將原則套用至應用程式。請參閱“[新增 Web 或桌面平台應用程式特定原則](#),” 第 73 頁

在行動裝置上啟用持續性 Cookie

當應用程式使用 iOS 裝置上的 Safari 檢視控制器和 Android 裝置上的 Chrome 自訂索引標籤時，啟用持續性 Cookie 將可提供系統瀏覽器與原生應用程式間的單一登入，以及原生應用程式之間的單一登入。

持續性 Cookie 會儲存使用者的登入工作階段詳細資料，讓使用者在透過 VMware Identity Manager 存取其受管理的資源時，無須重新輸入其使用者認證。Cookie 逾時可設定在您為 iOS 和 Android 裝置設定的存取原則規則中。

備註 Cookie 很容易因為一般的瀏覽器 Cookie 竊取和跨網站指令碼攻擊而遭到破壞和影響。

啟用持續性 Cookie

持續性 Cookie 會儲存使用者的登入工作階段詳細資料，讓使用者在從 iOS 或 Android 行動裝置存取其受管理的資源時，無須重新輸入其使用者認證。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**設定 > 喜好設定**。
- 2 核取**啟用持續性 Cookie**。
- 3 按一下**儲存**。

下一個

若要設定持續性 Cookie 工作階段的逾時，請在 iOS 和 Android 裝置類型的存取原則規則中編輯重新驗證值。

管理使用者和群組

VMware Identity Manager 服務中的使用者和群組會從您的企業目錄中匯入，或是在 VMware Identity Manager 管理主控台中建立為本機使用者和群組。

在管理主控台中，[使用者和群組] 頁面可提供以使用者和群組為中心的服務檢視。您可以管理使用者和群組權利、群組關聯，以及 VMware Verify 電話號碼。對於本機使用者，您也可以管理密碼原則。

本章節討論下列主題：

- “使用者和群組類型,” 第 77 頁
- “關於使用者名稱和群組名稱,” 第 78 頁
- “管理使用者,” 第 79 頁
- “建立群組和設定群組規則,” 第 80 頁
- “編輯群組規則,” 第 81 頁
- “將資源新增至群組,” 第 82 頁
- “建立本機使用者,” 第 82 頁
- “管理密碼,” 第 84 頁

使用者和群組類型

VMware Identity Manager 服務中的使用者可以是從您企業目錄同步的使用者、您在管理主控台中佈建的本機使用者，或是透過 Just-in-Time 佈建而建立的使用者。

VMware Identity Manager 服務中的群組可以是從您企業目錄同步的群組，以及您在管理主控台中建立的本機群組。

從您的企業目錄匯入的使用者和群組，會根據您的伺服器同步化排程在 VMware Identity Manager 目錄中更新。您可以從 [使用者和群組] 頁面檢視使用者和群組帳戶。您無法編輯或刪除這些使用者和群組。

您可以建立本機使用者和群組。本機使用者會新增至本機目錄。您可以管理本機使用者的屬性對應和密碼原則。您可以建立本機群組以管理使用者的資源權利。

透過 Just-in-Time 佈建而建立的使用者會在使用者登入時，根據身分識別提供者所傳送的 SAML 宣告進行動態建立及更新。所有使用者管理均透過 SAML 宣告來處理。若要使用 Just-in-Time 佈建，請參閱第 6 章，[“Just-in-Time 使用者佈建,”](#) 第 41 頁。

關於使用者名稱和群組名稱

在 VMware Identity Manager 服務中，使用者和群組將同時依其唯一名稱和網域來識別。這可讓您在不同 Active Directory 網域中有多個使用者或群組使用相同的名稱。使用者名稱和群組名稱在網域內必須是唯一的。

使用者名稱

VMware Identity Manager 服務支援在不同 Active Directory 網域中有多個使用者使用相同的名稱。使用者名稱在網域內必須是唯一的。例如，您可以在網域 `eng.example.com` 中有使用者 `jane`，並在網域 `sales.example.com` 中有另一個使用者 `jane`。

系統將同時依使用者的唯一使用者名稱和網域來加以識別。VMware Identity Manager 中的 `userName` 屬性用於使用者名稱，且一般會與 Active Directory 中的 `sAMAccountName` 屬性對應。`domain` 屬性則用於網域，且一般會與 Active Directory 中的 `canonicalName` 屬性對應。

目錄同步期間，具有相同使用者名稱 (但不同網域) 的使用者可成功同步。如果網域內有使用者名稱衝突，則會同步第一個使用者，而具有相同使用者名稱的後續使用者會發生錯誤。

備註 如果您有現有的 VMware Identity Manager 目錄，其中的使用者網域不正確或遺漏時，請檢查網域設定並再次同步目錄。請參閱“[同步目錄以修正網域資訊](#)”第 79 頁。

在管理主控台中，您可以同時以使用者的唯一使用者名稱和網域加以識別。例如：

- 在 [儀表板] 索引標籤的 [使用者和群組] 資料行中，使用者會以 `user (domain)` 的形式列出。例如，`jane (sales.example.com)`。
- 在 [使用者和群組] 索引標籤的 [使用者] 頁面中，[網域] 資料行會指出使用者所屬的網域。
- 顯示使用者資訊 (例如「資源權利」報告) 的報告會包含 [網域] 資料行。

使用者登入使用者入口網站時，在登入頁面上，他們會選取其所屬的網域。如果多個使用者有相同的使用者名稱，則每個使用者可以使用適當的網域成功登入。

備註 此資訊適用於從 Active Directory 同步的使用者。如果您使用第三方身分識別提供者，並且已設定 Just-in-Time 使用者佈建，請參閱第 6 章, “[Just-in-Time 使用者佈建](#),” 第 41 頁以取得相關資訊。Just-in-Time 使用者佈建也支援在不同網域中有相同使用者名稱的多個使用者。

群組名稱

VMware Identity Manager 服務支援在不同 Active Directory 網域中有多個群組使用相同的名稱。群組名稱在網域內必須是唯一的。例如，您在網域 `eng.example.com` 中可以有名為 `allusers` 的群組，而在網域 `sales.example.com` 中有另一個名為 `allusers` 的群組。

系統將同時依群組的唯一名稱和網域來加以識別。

目錄同步期間，具有相同名稱 (但不同網域) 的群組將可成功同步。如果網域內有群組名稱衝突，則會同步第一個群組，而具有相同名稱的後續群組會發生錯誤。

在管理主控台 [使用者和群組] 索引標籤的 [群組] 頁面中，Active Directory 群組會依其群組名稱和網域列出。這可讓您區分具有相同名稱的群組。在 VMware Identity Manager 服務中建立的本機群組會依群組名稱列出。網域會列示為「本機使用者」。

同步目錄以修正網域資訊

如果您有現有的 VMware Identity Manager 目錄，且其中的使用者網域不正確或遺漏，您必須檢查網域設定，並再次同步目錄。您必須檢查網域設定才能將不同 Active Directory 網域中具有相同名稱的使用者或群組成功同步至 VMware Identity Manager 目錄，而讓使用者能夠登入。

程序

- 1 在管理主控台中，移至**身分識別與存取管理 > 目錄**頁面。
- 2 選取要同步的目錄，按一下**同步設定**，然後按一下**對應屬性**索引標籤。
- 3 在 [對應屬性] 頁面上，確認 VMware Identity Manager 屬性 **domain** 對應於 Active Directory 中的正確屬性名稱。

domain 屬性通常會與 Active Directory 中的 canonicalName 屬性對應。

domain 屬性未標示為 [必要]。

- 4 按一下**儲存並同步**以同步目錄。

管理使用者

管理主控台中的 [使用者] 頁面會顯示每個使用者的相關資訊，包括使用者識別碼、網域、使用者所屬的群組、VMware Verify 電話號碼，以及使用者是否已在 VMware Identity Manager 中啟用。

選取使用者名稱可檢視詳細的使用者資訊。可檢視的詳細資料包括使用者設定檔、群組關聯、已透過 VMware Verify 啟用的裝置，以及使用者權利。

使用者設定檔

使用者設定檔頁面會顯示與使用者和已指派角色 (使用者或管理員) 相關聯的個人資料。從外部目錄同步的使用者資訊也會包含主體名稱、辨別名稱和外部識別碼資料。本機使用者的設定檔頁面會顯示使用者在本機使用者目錄中的可用使用者屬性。

使用者之使用者設定檔頁面中的資料，若從外部目錄同步則無法進行編輯。您可以變更使用者的角色。

在本機使用者設定檔頁面上，您可以編輯屬性資訊、停用使用者而使其無法登入，以及刪除使用者。

群組關聯

使用者所屬群組的清單會顯示在 [群組] 頁面中。您可按一下群組名稱，顯示該群組的詳細資料頁面。

向 VMware Verify 登錄

VMware Verify 頁面會顯示使用者已向 VMware Verify 登錄的電話號碼，和已登錄的裝置。您也可以檢視上次使用帳戶的時間。

您可以移除使用者的電話號碼。當您重設 VMware Verify 時，使用者必須再次輸入其電話號碼，才能在 Verify 中重新註冊。請參閱“[從使用者設定檔中移除已登錄的電話號碼](#)”，第 61 頁。

應用程式權利

您可以按一下 [新增權利]，將目錄中的可用資源授權給使用者。接著，您可以設定如何將應用程式新增至其 Workspace ONE 入口網站。選取 [自動] 部署，可讓應用程式自動顯示在 Workspace ONE 入口網站中。選取 [使用者啟動]，可在應用程式從目錄集合新增至 Workspace ONE 入口網站之前，讓使用者啟動應用程式。

對於具有 X 按鈕的資源類型，您可以按一下 X 以移除使用者對資源的存取權。

建立群組和設定群組規則

您可以建立群組、將成員新增至群組，以及建立可讓您根據定義的規則填入群組的群組規則。

使用群組可以同時將相同資源授權給多位使用者，而不必個別授權每位使用者。使用者可以屬於多個群組。例如，如果您建立一個「銷售」群組和一個「管理」群組，銷售經理可以同時屬於這兩個群組。

您可以指定要套用於群組成員的原則設定。群組中的使用者會由您為使用者屬性設定的規則來定義。如果使用者的屬性值有所變更，而已不是定義的群組規則值，該使用者就會從群組中移除。

程序

- 1 在管理主控台的 [使用者和群組] 索引標籤中，按一下 **群組**。
- 2 按一下 **新增群組**。
- 3 輸入群組名稱和群組的說明。按**下一步**。
- 4 若要将使用者新增至群組，請輸入使用者名稱的字母。當您輸入文字時，系統會顯示相符的名稱清單。
- 5 選取使用者名稱，然後按一下 **+新增使用者**。
繼續將成員新增至群組。
- 6 在使用者新增至群組後，按**下一步**。
- 7 在 [群組規則] 頁面中，選取授與群組成員資格的方式。在下拉式功能表中，選取**任何**或**全部**。

選項	動作
任意	符合任一群組成員資格的條件時，授與群組成員資格。此動作的作用類似於 OR 條件。例如，如果您為 群組是銷售 和 群組是行銷 規則選取 任何 ，則銷售和行銷人員都會被授與此群組的成員資格。
全部	符合任一群組成員資格的條件時，即授與群組成員資格。使用「全部」的作用類似於 AND 條件。例如，如果您為 群組是銷售 和 電子郵件開頭為 'western_region' 規則選取 下列所有項目 ，則只有位在西部區域的銷售人員會被授與此群組的成員資格。其他區域的銷售人員不會被授與成員資格。

- 8 為您的群組設定一或多個規則。您可以巢狀規則。

選項	說明
屬性	從第一個資料行下拉式功能表中選取其中一個屬性。選取 [群組]，以將現有群組新增至您所建立的群組。您可以新增其他類型的屬性，以管理群組中那些使用者屬於您建立的群組的成員。
屬性規則	<p>下列規則是否可用，視您所選取的屬性而定。</p> <ul style="list-style-type: none"> ■ 選取是，可選取要與此群組相關聯的群組或目錄。請在文字方塊中輸入名稱。在您輸入時，將會顯示可用群組或目錄的清單。 ■ 選取不是，可選取要排除的群組或目錄。請在文字方塊中輸入名稱。在您輸入時，將會顯示可用群組或目錄的清單。 ■ 選取符合，可將群組成員資格授與完全符合您所輸入之準則的項目。例如，假設您的組織有一個共用中央電話號碼的商務旅行部門。如果您想將旅行預訂應用程式的存取權授與共用該電話號碼的所有員工，您可以建立一個類似「電話符合 (555) 555-1000」的規則。 ■ 選取不符合，可將群組成員資格授與不符合您所輸入之準則的所有目錄伺服器項目。例如，如果有一個部門共用一個中央電話號碼，您可以建立類似「電話不符合 (555) 555-2000」的規則，以排除該部門對某個社交網路應用程式的存取權。使用其他電話號碼的目錄伺服器項目都可以存取該應用程式。 ■ 選取開頭為，可將群組成員資格授與開頭為您所輸入之準則的目錄伺服器項目。例如，假設組織的電子郵件地址開頭為部門名稱，像是 <code>sales_username@example.com</code>。如果您想將某個應用程式的存取權授與每一位銷售人員，您可以建立一個類似「電子郵件開頭為 <code>sales_</code>」的規則。 ■ 選取開頭不是，可將群組成員資格授與開頭不是您所輸入之準則的所有目錄伺服器項目。例如，假設人力資源部門的電子郵件地址格式為 <code>hr_username@example.com</code>，那麼您可以設定類似「電子郵件開頭不是 <code>hr_</code>」的規則，以拒絕他們對某個應用程式的存取。使用其他電子郵件地址的目錄伺服器項目都可以存取該應用程式。
使用任何或全部屬性	<p>(選用) 若要将「任何」或「全部」屬性納入作為群組規則的一部分，請最後再新增此規則。</p> <ul style="list-style-type: none"> ■ 選取任何，可在任一群組成員資格條件符合此規則時，授與群組成員資格。使用「任何」是巢狀規則的方法。例如，您可建立內容為「下列所有項目：群組是銷售；群組是加州」的規則。針對「群組是加州」，「下列所有項目：電話開頭為 415；電話開頭為 510」。此群組成員必須屬於加州銷售人員，且電話號碼開頭為 415 或 510。 ■ 選取全部，可指定所有條件皆必須符合此規則。這是巢狀規則的方法。例如，您可建立規則，內容為「下列所有項目：群組是經理；群組是客户服務」。針對「群組是客户服務」，「下列所有項目：電子郵件開頭為 <code>cs_</code>；電話開頭為 555」。此群組成員可以是經理或客戶服務代表，但客戶服務代表的電子郵件開頭必須為 <code>cs</code>，且電話號碼開頭必須為 555。

- 9 (選用) 若要排除特定使用者，請在文字方塊中輸入使用者名稱，然後按一下**排除使用者**。

- 10 按**下一步**，然後檢閱群組資訊。按一下**建立群組**。

下一個

新增群組有權使用的資源。

編輯群組規則

您可以編輯群組規則，以變更群組名稱、新增和移除使用者，以及變更群組規則。

程序

- 1 在管理主控台中，按一下**使用者和群組 > 群組**。
- 2 按一下要編輯的群組名稱。

- 3 按一下**編輯群組**中的**使用者**。
- 4 依序按一下頁面以變更名稱、群組中的使用者和規則。
- 5 按一下**儲存**。

將資源新增至群組

要讓使用者有權使用資源，最有效的方式是將權利新增至群組。群組的所有成員皆可存取 該群組 有權使用的應用程式。

先決條件

應用程式 新增 至 [目錄] 頁面。

程序

- 1 在管理主控台中，按一下**使用者和群組 > 群組**。
頁面會顯示 群組的清單。
- 2 若要將資源新增至群組，請按一下群組名稱。
- 3 按一下**應用程式**索引標籤，然後按一下**新增權利**。
- 4 從下拉式功能表中選取要授權的應用程式類型。
顯示在下拉式清單中的應用程式類型，將以新增至目錄的應用程式類型為準。
- 5 選取要授權給群組的應用程式。您可以搜尋特定應用程式，或是選取**應用程式**旁的方塊以選取所有顯示的應用程式。
如果應用程式已授權給群組，則該應用程式不會列出。
- 6 按一下**儲存**。
應用程式會列示在 [應用程式] 頁面上，且群組中的使用者立即獲得使用這些資源的授權。

建立本機使用者

您可以在 VMware Identity Manager 服務中建立本機使用者，以新增及管理未在您的企業目錄中佈建的使用者。您可以建立不同的本機目錄，並且自訂每個目錄的屬性對應。

您可以建立目錄，並且為該本機目錄選取屬性及建立自訂屬性。必要的使用者屬性 `userName`、`lastName`、`firstName` 和電子郵件會指定在 [身分識別與存取管理] > [使用者屬性] 頁面中的全域層級上。在本機目錄使用者屬性清單中，您可以選取其他必要屬性，以及建立自訂屬性，讓不同的本機目錄有自訂的屬性集。請參閱《安裝和設定 VMware Identity Manager》指南中的〈使用本機目錄〉。

如果您想要讓使用者存取您的應用程式，但不想將其新增至您的企業目錄，請建立本機使用者。

- 您可以為不屬於您企業目錄的特定使用者類型，建立本機目錄。例如，您可以為通常不屬於您企業目錄的合作夥伴建立本機目錄，並使其僅能存取其所需的特定應用程式。
- 如果您想讓不同組的使用者有不同的使用者屬性或驗證方法，您可以建立多個本機目錄。例如，您可以為經銷商建立一個具有區域和市場大小等使用者屬性標籤的本機目錄。再為供應商建立另一個具有產品類別之使用者屬性標籤的本機目錄。

您可以設定讓本機使用者用來登入您企業網站的驗證方法。對於本機使用者密碼，系統會強制執行密碼原則。您可以定義密碼限制和密碼管理規則。

在您佈建使用者後，系統會傳送電子郵件訊息，其中包含如何登入以啟用其帳戶的相關資訊。使用者在登入後，將可建立密碼並啟用其帳戶。

新增本機使用者

您一次只能建立一個使用者。在新增使用者時，您必須選取以所要使用之本機使用者屬性進行設定的本機目錄，以及使用者登入的網域。

除了新增使用者資訊以外，您還必須選取使用者角色 (使用者或管理員)。管理員角色可讓使用者存取管理主控台，以管理 VMware Identity Manager 服務。

先決條件

- 已建立的本機目錄
- 為本機使用者識別的網域
- 必須在本機目錄 [使用者屬性] 頁面中選取的使用者屬性
- 已設定的密碼原則
- 在 [應用裝置設定] 索引標籤中設定的 SMTP 伺服器，用以將電子郵件通知傳送給新建立的本機使用者

程序

- 1 在管理主控台的 [使用者和群組] 索引標籤中，按一下**新增使用者**。
- 2 在**新增使用者**頁面中，選取此使用者的本機目錄。
頁面隨即展開，並顯示要設定的使用者屬性。
- 3 選取此使用者所指派到的網域，並完成必要的使用者資訊。
- 4 如果這個使用者的角色是管理員，請在 [使用者] 文字方塊中選取**管理員**。
- 5 按一下**新增**。

本機使用者隨即建立。系統會將電子郵件傳送給使用者，要求他們登入以啟用其帳戶並建立密碼。電子郵件中的連結會在 [密碼原則] 頁面中設定的值到期。預設值為七天。如果連結已到期，您可以按一下 [重設密碼] 以重新傳送電子郵件通知。

系統會根據已設定的群組屬性規則將使用者新增至現有群組。

下一個

前往本機使用者帳戶中檢閱設定檔、將使用者新增至群組，並將所要使用的資源授權給使用者。

如果您已在系統目錄中，建立對特定存取原則所管理資源具有權限的管理員使用者，請確定應用程式原則規則中包含作為後援驗證方法的「密碼 (本機目錄)」。若未設定「密碼 (本機目錄)」，則管理員便無法登入應用程式。

停用或啟用本機使用者

您可以停用本機使用者，讓使用者無法登入和存取其入口網站以及獲授權的資源，而非刪除使用者。

程序

- 1 在管理主控台中，按一下**使用者和群組**。
- 2 在 [使用者] 頁面中，選取使用者。
[使用者設定檔] 頁面隨即顯示。

- 3 根據本機使用者的狀態，執行下列其中一個動作。
 - a 若要停用帳戶，請取消選取 [啟用] 核取方塊
 - b 若要啟用帳戶，請選取 [啟用]。

停用的使用者將無法登入口網站或他們先前有權使用的資源。當本機使用者停用時，若他們正在使用獲授權的資源，則其在工作階段逾時之前仍可存取該資源。

刪除本機使用者

您可以刪除本機使用者。

程序

- 1 在管理主控台中，按一下**使用者和群組**。
- 2 選取要刪除的使用者。
[使用者設定檔] 頁面隨即顯示。
- 3 按一下**刪除使用者**。
- 4 在確認方塊中，按一下**確定**。
使用者會從 [使用者] 清單中移除。

刪除的使用者將無法登入口網站或他們先前有權使用的資源。

管理密碼

您可以建立用來管理本機使用者密碼的密碼原則。本機使用者可根據密碼原則規則變更其密碼。

本機使用者可透過 Workspace ONE 入口網站，從下拉式功能表中依其名稱進行「帳戶」選取以變更其密碼。

設定本機使用者的密碼原則

本機使用者密碼原則是關於本機使用者密碼的格式和到期時間的一組規則和限制。密碼原則只會套用至您從 VMware Identity Manager 管理主控台建立的本機使用者。

密碼原則可包含密碼限制、密碼存留期上限，以及適用於密碼重設的暫時密碼存留期上限。

預設密碼原則需要六個字元。密碼限制可包含大寫、小寫、數字和特殊字元的組合，以要求設定強式密碼。

程序

- 1 在管理主控台中，選取**使用者和群組 > 設定**。
- 2 按一下**密碼原則**，以編輯密碼限制參數。

選項	說明
密碼的最小長度	長度下限為六個字元，但您可以要求六個以上的字元。最小長度不得少於字母、數字和特殊字元需求的最小總和。
小寫字元	小寫字元數目下限。小寫 a-z
大寫字元	大寫字元數目下限。大寫字元 A-Z
數字字元 (0-9)	數字字元數目下限。十進位數字 (0-9)
特殊字元	非英數字元 (例如 & # % \$!) 的數目下限

選項	說明
連續的相同字元	相同相鄰字元的數目上限。例如，如果您輸入 1，則下列密碼是可使用的：p@s\$word，但下列密碼則不可使用：p@\$word。
密碼歷程記錄	無法選取之先前密碼的數目。例如，如果使用者不能重複使用最後六個密碼中的任何一個，則輸入 6。若要停用此功能，請將此值設定為 0。

- 3 在**密碼管理**區段中，編輯密碼存留期參數。

選項	說明
暫時密碼存留期	密碼重設或遺忘密碼連結有效的時數。預設值為 168 小時
密碼存留期	使用者必須變更密碼前，密碼可存在的天數上限。
密碼提醒	在密碼到期之前傳送密碼到期通知的天數。
密碼提醒通知頻率	在密碼到期通知首次傳送後，傳送提醒的頻率。

每個方塊都必須要有值，才能設定密碼存留期原則。若不想設定原則選項，請輸入 0。

- 4 按一下**儲存**。

管理目錄

目錄是您可授權給使用者之所有資源的存放庫。您可從 [目錄] 索引標籤直接新增應用程式至目錄。若要查看新增至目錄的應用程式，請在管理主控台中按一下 **目錄** 索引標籤。

在 [目錄] 頁面上，您可以執行下列工作：

- 新增新的資源至目錄。
- 檢視目前可授權給使用者的資源。
- 存取目錄中每個資源的相關資訊。

Web 應用程式可從 [目錄] 頁面直接新增至目錄。

其他資源類型則需在 管理主控台 外部執行動作。如需設定資源的相關資訊，請參閱《在 VMware Identity Manager 中設定資源》。

資源	如何在目錄中查看資源
Web 應用程式	在管理主控台 [目錄] 頁面上，選取 Web 應用程式 應用程式類型。
擷取做為 ThinApp 套件的虛擬化 Windows 應用程式	從管理主控台 [封裝應用程式 - ThinApp] 頁面將 ThinApp 套件同步至目錄。在管理主控台 [目錄] 頁面上，選取 ThinApp 套件 應用程式類型。
View 桌面平台集區	從管理主控台 [View 集區] 頁面將 View 集區同步至目錄。在管理主控台 [目錄] 頁面上，選取 View 桌面平台集區 應用程式類型。
View 主控應用程式	從管理主控台 [View 集區] 頁面將 View 主控應用程式同步至目錄。在管理主控台 [目錄] 頁面上，選取 View 主控應用程式 應用程式類型。
Citrix 型應用程式	從管理主控台 [已發佈的應用程式 - Citrix] 頁面將 Citrix 型應用程式同步至目錄。在管理主控台 [目錄] 頁面上，選取 Citrix 發佈的應用程式 應用程式類型。

本章節討論下列主題：

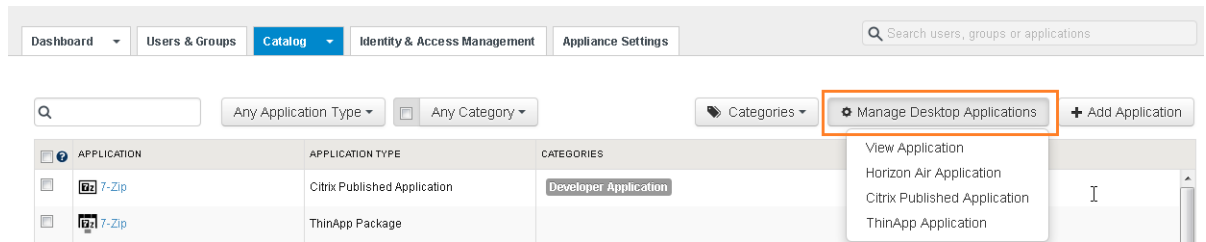
- [“管理目錄中的資源,”](#) 第 87 頁
- [“將資源分組為類別,”](#) 第 90 頁
- [“管理目錄設定,”](#) 第 92 頁

管理目錄中的資源

在您可以將特定資源授權給使用者之前，必須先將該資源填入目錄。用來將資源填入目錄的方法會因資源類型而異。

您可在目錄中定義權利並發佈給使用者的資源類型是 Web 應用程式、擷取做為 VMware ThinApp 套件的 Windows 應用程式、Horizon View 桌面平台集區和 View 主控應用程式或 Citrix 型應用程式。

若要整合並啟用 View 桌面平台和應用程式集區、Citrix 發行的資源或 ThinApp 封裝應用程式，可使用 [目錄] 索引標籤中的 [管理桌面平台應用程式] 功能表。



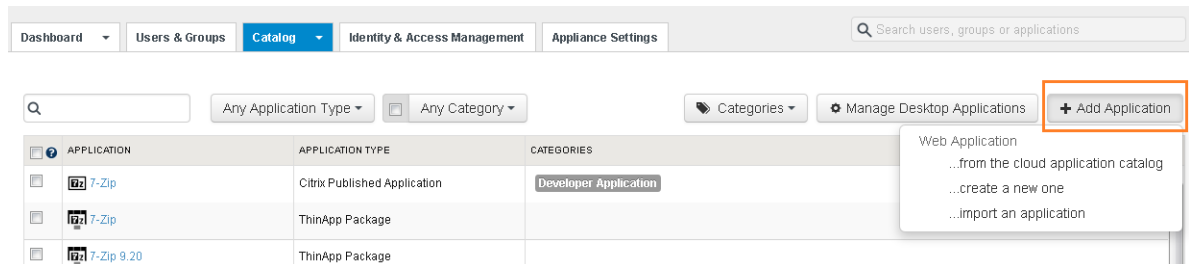
如需這些資源的相關資訊、需求、安裝與組態，請參閱《在 VMware Identity Manager 中設定資源》。

Web 應用程式

您可在管理主控台的 [目錄] 頁面上直接將 Web 應用程式填入目錄。按一下 [目錄] 頁面上顯示的 Web 應用程式時，就會顯示該應用程式的相關資訊。在顯示的頁面中，您可以設定 Web 應用程式，例如提供適當的 SAML 屬性以用來設定 VMware Identity Manager 和目標 Web 應用程式之間的單一登入。設定好 Web 應用程式後，接著可以將該 Web 應用程式授權給使用者和群組。請參閱“將 Web 應用程式新增至目錄,” 第 88 頁。

將 Web 應用程式新增至目錄

您可以直接使用管理主控台中的 [目錄] 頁面，將 Web 應用程式新增至您的目錄。



請參閱《在 VMware Identity Manager 中設定資源》的〈提供 Web 應用程式的存取權〉章節，以取得關於新增 Web 應用程式至您的目錄的詳細指示。

下列指示提供將這些類型的資源新增至您目錄所涉及步驟的概觀。

程序

- 1 在管理主控台中，按一下 **目錄** 索引標籤。
- 2 按一下 **+ 新增應用程式**。
- 3 根據應用程式的資源類型和位置，按一下選項。

連結名稱	資源類型	說明
Web 應用程式 ...從雲端應用程式目錄	Web 應用程式	VMware Identity Manager 包括可在雲端應用程式目錄中使用的預設 Web 應用程式存取權，您可以將該 Web 應用程式新增至您的目錄做為資源。
Web 應用程式 ... 建立新的	Web 應用程式	透過填寫適當的表單，您可以針對要新增至您目錄做為資源的 Web 應用程式建立應用程式記錄。
Web 應用程式 ... 匯入 ZIP 或 JAR 檔案	Web 應用程式	您可以將您先前設定的 Web 應用程式匯入。您可能想要使用此方法來展開從預備到生產環境的部署。在此情況下，您會從預備部署以 ZIP 檔案形式匯出 Web 應用程式。然後將 ZIP 檔案匯入到生產部署。

- 4 遵循提示來完成新增資源至目錄。

將 Web 應用程式新增至目錄

新增 Web 應用程式至目錄時，您會建立間接指向 Web 應用程式的項目。該項目是透過應用程式記錄來定義，該記錄為包括連至 Web 應用程式的 URL 的表單。

程序

- 1 在管理主控台中，按一下**目錄**索引標籤。
- 2 按一下**新增應用程式 > Web 應用程式 ...從雲端應用程式目錄**。
- 3 按一下您要新增的 Web 應用程式的圖示。
應用程式記錄會新增至您的目錄，隨即顯示 [詳細資料] 頁面，其中含有已指定的名稱和驗證設定檔。
- 4 (選擇性) 根據組織的需求，自訂 [詳細資料] 頁面上的資訊。

頁面上的項目隨即會填入 Web 應用程式的特定資訊。

視應用程式而定，您可以編輯部分項目。

表單項目	說明
名稱	應用程式的名稱。
說明	使用者可以讀取的應用程式的說明。
圖示	按一下 瀏覽 來上傳應用程式的圖示。支援 PNG、JPG 和 ICON 檔案格式的圖示，最大為 4 MB。 上傳的圖示大小會重新調整為 80px X 80px。 若要防止變形，請上傳高度和寬度相等，且盡可能接近 80px X 80px 調整大小維度的圖示。
類別	若要允許應用程式顯示在目錄資源的類別搜尋中，請從下拉式功能表選取類別。您必須先前已建立類別。

- 5 按一下**儲存**。
- 6 按一下**組態**，編輯應用程式記錄的組態詳細資料，然後按一下**儲存**。
表單上的部分項目隨即會預先填入 Web 應用程式的特定資訊。部分預先填入的項目可供編輯，但其他則無法編輯。要求的資訊因應用程式而有所不同。
對於部分應用程式，表單會具有「應用程式參數」區段。如果應用程式的該區段存在，並且區段中的參數沒有預設值，請提供值以允許應用程式啟動。如果已提供預設值，您可以編輯該值。
- 7 選取**權利**、**授權**和**佈建**索引標籤，並視情況來自訂資訊。

索引標籤	說明
權利	授權使用者和群組使用應用程式。最初設定應用程式時或日後隨時可以設定權利。
存取原則	套用存取原則來控制使用者對應用程式的存取權。
授權	設定核准追蹤。新增授權資訊，供應用程式在報告中追蹤授權使用。您必須在 [目錄] > [設定] 頁面中啟用並設定核准。您也必須登錄核准要求處理常式的回撥 URI。
佈建	佈建 Web 應用程式以從 VMware Identity Manager 服務擷取特定資訊。如果為 Web 應用程式設定佈建，則當您將應用程式授權給使用者時，該使用者就會佈建至該 Web 應用程式。目前提供適用於 Google Apps 和 Office 365 的佈建配接器。如需這些應用程式的設定指南，請移至 https://www.vmware.com/support/pubs/vidm_webapp_sso.html 中的「VMware Identity Manager 整合」。

新增 View 桌面平台和主控應用程式

您可將 View 桌面平台集區和 View 主控應用程式填入目錄，也可以將 VMware Identity Manager 部署與 Horizon View 整合。

當您按一下 [目錄] > [管理桌面平台應用程式] 功能表中的 [View 應用程式]，系統會將您重新導向至 [View 集區] 頁面。選取**啟用 View 集區**可新增 View 網繭、為 View 執行目錄同步，以及設定服務用來延伸 View 資源權利給使用者的部署類型。

執行這些工作後，您使用 Horizon View 授權給使用者的 View 桌面平台和主控應用程式就成為目錄中的可用資源。

您可隨時返回此頁面修改 View 組態或是新增或移除 View 網繭。

如需關於將 View 與 VMware Identity Manager 整合的詳細資訊，請參閱《設定資源指南》中的〈提供對 View 桌面平台的存取權〉。

新增 Citrix 發行的應用程式

您可使用 VMware Identity Manager 來與現有的 Citrix 部署整合，然後使用 Citrix 型應用程式填入目錄。

當您按一下 [目錄] > [管理桌面平台應用程式] 功能表中的 [Citrix 發行的應用程式]，系統會將您重新導向至 [已發佈的應用程式 - Citrix] 頁面。選取 [啟動 Citrix 型應用程式]，以在 VMware Identity Manager 和 Citrix 伺服器陣列之間建立通訊並排程同步化頻率。

如需將 Citrix 發行的應用程式與 VMware Identity Manager 整合的詳細資訊，請參閱《設定資源指南》中的〈提供對 Citrix 發行的應用程式的存取權〉。

新增 ThinApp 應用程式

使用 VMware Identity Manager，您可集中發佈與管理 ThinApp 套件。您必須啟用 VMware Identity Manager，才能找到儲存 ThinApp 套件的存放庫並將套件與 VMware Identity Manager 同步。

您可透過執行下列工作，將擷取做為 ThinApp 套件的 Windows 應用程式填入目錄。

- 1 如果您想提供給使用者存取的 ThinApp 套件尚不存在，請建立與 VMware Identity Manager 相容的 ThinApp 套件。請參閱 VMware ThinApp 說明文件。
- 2 建立網路共用並填入相容的 ThinApp 套件。
- 3 設定 VMware Identity Manager 以與網路共用上的套件整合。

當您按一下 [目錄] > [管理桌面平台應用程式] 功能表中的 [ThinApp 應用程式]，系統會將您重新導向至 [封裝應用程式 - ThinApp] 頁面。選取 [啟動封裝應用程式]。輸入 ThinApp 存放庫位置並設定同步頻率。

執行這些工作後，您新增至網路共用的 ThinApp 套件現在會成為目錄中的可用資源。

如需關於設定 VMware Identity Manager 來發佈與管理 ThinApp 套件的詳細資訊，請參閱《設定資源指南》中的〈提供對 VMware ThinApp 套件的存取權〉。

將資源分組為類別

您可將資源分組為邏輯類別，以便使用者在 Workspace ONE 入口網站工作區中找到他們需要的資源。

在建立類別時，請考量組織的結構、資源的工作功能，以及資源的類型。您可指派多個類別至資源。例如，您可以建立名為「文字編輯器」的類別，以及另一個名為「建議資源」的類別。將「文字編輯器」指派給類別中的所有文字編輯器資源，並將「建議資源」指派給您希望使用者優先使用的特定文字編輯器。

建立資源類別

您可以建立資源類別再留待日後套用，也可以建立類別並同時套用至資源。

程序

- 1 在管理主控台中，按一下**目錄**索引標籤。
- 2 若要同時建立及套用類別，請選取要套用新類別之應用程式的核取方塊。
- 3 按一下**類別**。
- 4 在文字方塊中輸入新類別名稱。
- 5 按一下**新增類別...**。

系統隨即會建立新類別，但不會套用至任何資源。

- 6 若要將類別套用至選定資源，請選取新類別名稱的核取方塊。
系統隨即會將類別新增至應用程式，並且會列示在 [類別] 資料行內。

下一個

將類別套用至其他應用程式。請參閱“[套用類別至資源](#)”第 91 頁。

套用類別至資源

建立類別之後，您可以將該類別套用至目錄中的任何資源。您可以套用多個類別至相同的資源。

先決條件

建立類別。

程序

- 1 在管理主控台中，按一下**目錄**索引標籤。
- 2 選取要套用類別之所有應用程式的核取方塊。
- 3 按一下**類別**，然後選取要套用的類別名稱。
類別隨即套用至所選取的應用程式。

從應用程式移除類別

您可從應用程式解除類別的關聯。

程序

- 1 在管理主控台中，按一下**目錄**索引標籤。
- 2 選取應用程式的核取方塊以移除類別。
- 3 按一下**類別**。
套用至應用程式的類別會成為已選取狀態。
- 4 取消選取您要從應用程式移除的類別，並關閉功能表方塊。
該類別就會從應用程式的 [類別] 清單中移除。

刪除類別

您可以從目錄永久移除類別。

程序

- 1 在管理主控台中，按一下**目錄**索引標籤。
- 2 按一下**類別**。
- 3 暫留至想要刪除的類別。即會顯示「x」。按一下**x**。
- 4 按一下**確定**以移除類別。

類別將不會在 [類別] 下拉式功能表出現，或在您先前套用的任何應用程式上顯示為標籤。

管理目錄設定

[目錄設定] 頁面可用來管理目錄中的資源、下載 SAML 憑證、自訂使用者入口網站，以及進行全域設定。

下載 SAML 憑證以設定信賴應用程式

當您設定 Web 應用程式時，您必須複製組織的 SAML 簽署憑證，並將其傳送至信賴應用程式，使其能夠接受來自服務的使用者登入。SAML 憑證會用來驗證從服務到信賴應用程式 (例如 WebEx 或 Google Apps) 的使用者登入。

您必須從服務中複製 SAML 簽署憑證和 SAML 服務提供者中繼資料，並在第三方身分識別提供者中編輯 SAML 判斷提示，以對應 VMware Identity Manager 使用者。

程序

- 1 登入管理主控台。
- 2 在 [目錄] 索引標籤中，選取**設定 > SAML 中繼資料**。
- 3 複製並儲存顯示的 SAML 簽署憑證。
 - a 複製 [簽署憑證] 區段中的憑證資訊。
 - b 將憑證資訊儲存至文字檔，以便您後續在設定第三方身分識別提供者執行個體時使用。
- 4 讓 SAML SP 中繼資料可供第三方身分識別提供者執行個體使用。
 - a 在 [下載 SAML 憑證] 頁面上，按一下**服務提供者 (SP) 中繼資料**。
 - b 使用最適合您的組織的方法複製並儲存顯示的資訊。
後續在您設定第三方身分識別提供者時，請使用這項複製的資訊。
- 5 決定從第三方身分識別提供者執行個體到 VMware Identity Manager 的使用者對應。

當您設定第三方身分識別提供者時，請在第三方身分識別提供者中編輯 SAML 判斷提示，以對應 VMware Identity Manager 使用者。

NameID 格式	使用者對應
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress	SAML 判斷提示中的 NameID 值會對應至 VMware Identity Manager 中的電子郵件地址屬性。
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	SAML 判斷提示中的 NameID 值會對應至 VMware Identity Manager 中的使用者名稱屬性。

下一個

套用您為此工作複製的資訊，以設定第三方身分識別提供者執行個體。

停用下載協助程式應用程式的提示

View 桌面平台、Citrix 發佈的應用程式和 ThinApp 資源需要將下列協助程式應用程式安裝在使用者的電腦或裝置上。

- View 桌面平台會使用 Horizon Client。
- Citrix 發佈的應用程式需要 Citrix Receiver。
- ThinApp 資源需要適用於桌面平台的 VMware Identity Manager。

使用者在第一次從這些資源類型啟動應用程式時，系統會要求他們將協助程式應用程式下載至其桌面平台或裝置。您可以從 [目錄] > [設定] > [全域設定] 頁面徹底停用此提示，使其不會在每次啟動資源時都顯示。

當電腦或裝置受到管理，且您知道協助程式應用程式位於使用者的本機映像時，停用提示而不加以顯示是適當的選項。

程序

- 1 在管理員主控台中，選取**目錄 > 設定**。
- 2 選取**全域設定**。
- 3 選取不應要求啟動協助程式應用程式的作業系統。
- 4 按一下**儲存**。

建立用戶端以啟用遠端應用程式的存取

您可以建立可讓單一應用程式對 VMware Identity Manager 進行登錄的單一用戶端，以允許使用者在管理主控台的 [目錄 > 設定] 頁面中存取特定應用程式。

SDK 會使用 OAuth 型驗證連線至 VMware Identity Manager。您必須在管理主控台中建立用戶端識別碼值和 clientSecret 值。

建立單一目錄資源的遠端存取

您可以建立可讓單一應用程式對 VMware Identity Manager 服務進行登錄的用戶端，以允許使用者存取特定應用程式。

程序

- 1 在管理主控台 [目錄] 索引標籤中，選取**設定 > 遠端應用程式存取**。
- 2 在 [用戶端] 頁面上，按一下**建立用戶端**。
- 3 在 [建立用戶端] 頁面上，輸入應用程式的下列相關資訊。

標籤	說明
存取類型	選項為 [使用者存取權杖] 或 [服務用戶端權杖]。
用戶端識別碼	輸入資源的唯一用戶端識別碼以便向 VMware Identity Manager 進行登錄。
應用程式	選取 [Identity Manager]。
範圍	選取適當範圍。選取 NAAPS 時也會一併選取 OpenID。
重新導向 URI	輸入登錄的重新導向 URI。
[進階] 區段	

標籤	說明
共用密碼	按一下 產生共用密碼 ，以產生在此服務與應用程式資源服務之間共用的密碼。 複製並儲存用戶端密碼，以在應用程式安裝中進行設定。 用戶端密碼應保密。如果部署的應用程式無法保密此密碼，則不會使用此密碼。共用密碼不會用於 Web 瀏覽器式的應用程式。
發出重新整理權杖	取消選取此核取方塊。
權杖類型	選取 [Bearer]
權杖長度	保留預設設定：32 個位元組。
發出重新整理權杖	選取 [重新整理權杖]。
存取權杖 TTL	(選用) 變更 存取權杖存留時間 設定。
重新整理權杖 TTL	(選用)
使用者授與	請勿選取 [提示使用者進行存取]。

4 按一下**新增**。

用戶端組態會連同已產生的共用密碼，顯示在 [OAuth2 用戶端] 頁面上。

下一個

在資源組態頁面中，輸入用戶端識別碼和共用密碼。請參閱應用程式說明文件。

建立遠端存取範本

您可以藉由建立範本來讓一組用戶端動態地向 VMware Identity Manager 服務登錄，進而允許使用者存取特定應用程式。

程序

- 1 在管理主控台 [目錄] 索引標籤中，選取**設定 > 遠端應用程式存取**。
- 2 按一下**範本**。
- 3 按一下**建立範本**。
- 4 在 [建立範本] 頁面中輸入以下應用程式的相關資訊。

標籤	說明
範本識別碼	輸入這項資源的唯一識別碼。
應用程式	選取 [Identity Manager]
範圍	選取適當範圍。選取 NAAPS 時也會一併選取 OpenID。
重新導向 URI	輸入登錄的重新導向 URI。
[進階] 區段	
權杖類型	選取 [Bearer]
權杖長度	保留預設設定：32 個位元組。
發出重新整理權杖	選取 [重新整理權杖]。
存取權杖 TTL	(選用)
重新整理權杖 TTL	(選用)
使用者授與	請勿選取 [提示使用者進行存取]。

5 按一下**新增**。

下一個

在資源應用程式中，將 VMware Identity Manager 服務 URL 設定為支援整合式驗證的站台。

在 Citrix 發佈的應用程式中編輯 ICA 內容

您可以在 VMware Identity Manager 部署中，從 [目錄] > [設定] > [Citrix 發佈的應用程式] 頁面為 Citrix 發佈的個別應用程式和桌面平台編輯設定。

系統會設定個別應用程式的 [ICA 組態] 頁面。在您手動新增內容之前，個別應用程式的 ICA 內容文字方塊會空的。當您編輯個別 Citrix 發佈資源的應用程式傳遞設定 (即 ICA 內容) 時，這些設定的優先順序會高於全域設定。

在 [NetScaler 組態] 頁面中，您可以為服務設定適當的設定，以便在使用者啟動 Citrix 型應用程式時，讓流量透過 NetScaler 路由至 XenApp 伺服器。

當您在 [Citrix 發佈的應用程式] > [Netscaler ICA 組態] 索引標籤中編輯 ICA 內容時，這些設定會套用至透過 NetScaler 路由的應用程式啟動流量。

如需設定 ICA 內容的相關資訊，請參閱文件中心裡的「設定 NetScaler」主題和「為單一 Citrix 發佈的資源編輯 VMware Identity Manager 應用程式傳遞設定」主題。

檢閱 ThinApp 警示

[設定] 功能表之 [目錄] 中的 [ThinApp 應用程式警示] 會將您重新導向至 [封裝應用程式警示] 頁面。

此頁面中會列出當 ThinApp 套件與 VMware Identity Manager 同步時所找到的錯誤。

針對資源使用量啟用應用程式核准

您可以要求必須在組織核准後才可使用應用程式，以管理對應用程式的存取。您可以從 [目錄設定] 頁面啟用 [核准]，並設定用來接收核准要求的 URL。

當您新增需要通過目錄核准的應用程式時，您會啟用**授權**選項。設定授權選項時，使用者會在其 Workspace ONE 目錄中檢視應用程式，並要求使用該應用程式。

VMware Identity Manager 會將核准要求訊息傳送至組織已設定的核准 URL。伺服器工作流程程序會檢閱要求，然後傳回核准或拒絕訊息。如需設定步驟，請參閱《VMware Identity Manager 指南》中的〈管理應用程式核准〉。

您可以檢視 VMware Identity Manager 資源使用量和資源權利報告，以查看正在使用的已核准應用程式數量。

設定核准工作流程並設定核准引擎

您可以從兩個類型的核准工作流程選項中選擇。您可以登錄標註 REST URI 以整合您的應用程式管理系統與 VMware Identity Manager，或者您可以透過 VMware Identity Manager Connector 進行整合。

先決條件

當您設定 REST API 時，您必須已設定應用程式管理系統，並且可透過從 VMware Identity Manager 接受要求的標註 REST API 來取得 URI。

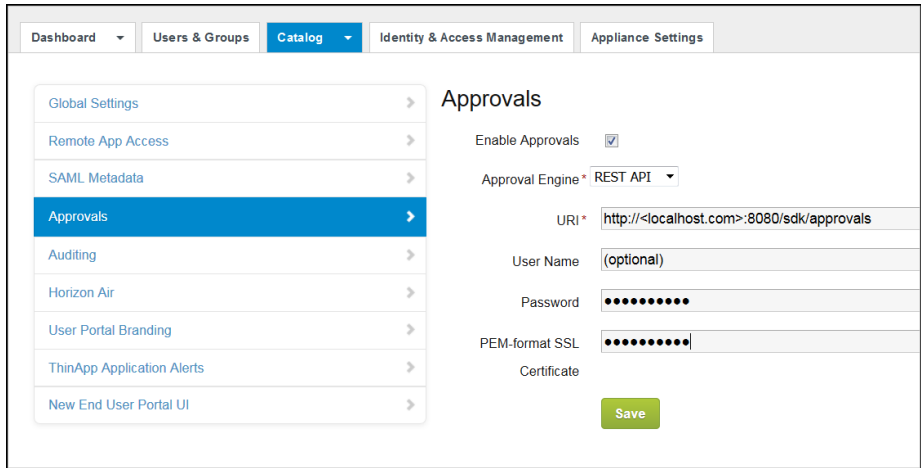
當核准工作流程系統位於內部部署資料中心時，請透過連接器設定 REST API。連接器可將核准要求訊息從 VMware Identity Manager Cloud 服務路由至內部部署核准應用程式，然後再傳回回應訊息。

程序

- 1 在管理主控台的 [目錄] 索引標籤中，選取**設定 > 核准**。
- 2 勾選**啟用核准**。

- 3 在 [核准引擎] 下拉式功能表中，選取要使用的 REST API 核准引擎，可以是透過 Web 伺服器的 REST API，或透過連接器的 REST API。
- 4 設定下列文字方塊。

選項	說明
URI	輸入接聽圖說文字要求之 REST API 的核准要求處理常式 URI。
使用者名稱	(選擇性) 如果 REST API 需要使用者名稱和密碼才能存取，請在此處輸入名稱。如果不需要驗證，則可將使用者名稱和密碼保留為空白。
密碼	(選用) 輸入使用者的密碼。
PEM 格式 SSL 憑證	(選擇性) 如果您選取了 REST API，且您的 REST API 使用 SSL，並且位於不具公用 SSL 憑證的伺服器上，請在此處貼上 PEM 格式的 REST API SSL 憑證。



下一個

移至 [目錄] 頁面，並為需要核准的應用程式設定授權功能，以便讓使用者使用應用程式。

操作管理主控台儀表板

管理主控台中有兩種儀表板可供使用。使用者參與儀表板可用來監控使用者和資源使用量。系統診斷儀表板可用來監控 VMware Identity Manager 服務的健全狀況。

本章節討論下列主題：

- “從儀表板監控使用者和資源使用,” 第 97 頁
- “監控系統資訊與健全狀況,” 第 98 頁
- “檢視報告,” 第 98 頁

從儀表板監控使用者和資源使用

[使用者參與儀表板] 會顯示使用者和資源的相關資訊。您可查看已登入的使用者、正在使用的應用程式，以及存取應用程式的頻率。您可以建立報告來追蹤使用者和群組活動以及資源使用。

[使用者參與儀表板] 上的顯示時間是以瀏覽器的設定時區為準。儀表板每一分鐘會更新一次。

程序

- 標頭會顯示當天已登入的唯一使用者數量，並顯示一個時間表來表示七天期間內的每日登入事件數量。[今天登入的使用者] 數量周圍有一個圓圈，用來顯示已登入的使用者百分比。[登入] 滑動圖會顯示一週內的登入事件。指向圖中某一點，即可查看當天的登入次數。
- [使用者和群組] 區段顯示 VMware Identity Manager 中設定的使用者帳戶和群組數量。最近登入的使用者會最先顯示出來。您可按一下 **查看完整報告** 建立稽核事件報告，以顯示特定天數範圍內登入的使用者。
- [應用程式受歡迎度] 區段顯示一個依應用程式類型分組的條狀圖，顯示七天內啟動應用程式的次數。指向特定某一天，可查看工具提示，當中會顯示使用的應用程式類型，以及當天的啟動次數。圖表下方的清單會顯示特定應用程式的啟動次數。展開右側箭頭可選取並檢視一天、一週、一個月或 12 週範圍的此項資訊。您可按一下 **查看完整報告** 建立 [資源使用] 報告，顯示特定時間範圍內的應用程式、資源類型和使用者活動數量。
- [應用程式採用] 區段會顯示一個條狀圖，當中顯示開啟獲授權應用程式的人數百分比。指向應用程式可查看工具提示，當中會顯示採用和權利的實際數量。
- [啟動的應用程式] 圓形圖會以佔整體百分比的形式，顯示已啟動的資源。指向圓形圖中的特定區段，可依資源類型查看實際數量。展開右側箭頭可選取並檢視一天、一週、一個月或 12 週範圍的此項資訊。
- [用戶端] 區段會顯示使用中的 Identity Manager 桌面平台數量。

監控系統資訊與健全狀況

VMware Identity Manager 系統診斷儀表板會顯示您環境中 VMware Identity Manager 應用裝置健全狀況的詳細概觀，以及服務的相關資訊。您可查看所有 VMware Identity Manager 資料庫伺服器、虛擬機器以及每部虛擬機器上可用服務的整體健全狀況。

在 [系統診斷儀表板] 中可以選取您要監控的虛擬機器，並查看該虛擬機器上的服務狀態，包括已安裝的 VMware Identity Manager 版本。如果資料庫或虛擬機器發生問題，標頭列會將機器狀態顯示為紅色。若要查看問題，您可選取顯示為紅色的虛擬機器。

程序

- 使用者密碼到期。顯示 VMware Identity Manager 應用裝置根密碼和遠端登入密碼的到期日期。如果密碼到期，請前往 [設定] 頁面並選取 **VA 組態**。開啟 **系統安全性** 頁面，變更密碼。
- 憑證。顯示憑證簽發者、開始日期和結束日期。若要管理憑證，請前往 [設定] 頁面並選取 **VA 組態**。開啟 **安裝憑證** 頁面。
- 設定程式 - 應用程式部署狀態。顯示 [應用裝置設定程式] 服務資訊。[Web 伺服器狀態] 會顯示 Tomcat 伺服器是否正在執行。[Web 應用程式狀態] 會顯示是否可存取 [應用裝置設定程式] 頁面。應用裝置版本會顯示已安裝的 VMware Identity Manager 應用裝置版本。
- 應用程式管理員 - 應用程式部署狀態。顯示 VMware Identity Manager 應用裝置連線狀態。
- 連接器 - 應用程式部署狀態。顯示 管理主控台 連線狀態。顯示連線成功時，表示您可以存取 管理主控台 頁面。
- VMware Identity Manager FQDN。顯示使用者所輸入用於存取其 VMware Identity Manager 應用程式入口網站的完整網域名稱。如果正在使用負載平衡器，VMware Identity Manager FQDN 會指向該負載平衡器。
- 應用程式管理員 - 整合式元件。顯示 VMware Identity Manager 資料庫連線、稽核服務和分析連線資訊。
- 連接器 - 整合式元件。顯示可從 [連接器服務管理員] 頁面管理之服務的相關資訊。這會顯示 ThinApp、View 和 Citrix 發行的應用程式資源的相關資訊。
- 模組。顯示 VMware Identity Manager 中啟用的資源。按一下 **已啟用** 可前往該資源的 [連接器服務管理員] 頁面。

檢視報告

您可以建立報告來追蹤使用者和群組活動以及資源使用。您可以在管理主控台的 [儀表板] > [報告] 頁面中檢視報告。

您可將報告匯出為逗點分隔值 (csv) 檔案格式。

表格 11-1. 報告類型

報告	說明
最近活動	最近活動是使用者在過去一天、過去一週、過去一個月或過去 12 週內，使用其 Workspace ONE 入口網站時所執行之動作的相關報告。活動可包含使用者資訊，例如多少次唯一使用者登入、多少次一般登入以及資源資訊，例如啟動的資源數量以及新增的資源權利。按一下 顯示事件 可以查看該活動的日期、時間和使用者詳細資料。
資源使用	資源使用是目錄中所有資源的報告，並包含每個資源的使用者數量、啟動及授權等詳細資料。您可選取以檢視在過去一天、過去一週、過去一個月或過去 12 週內的活動。
資源權利	資源權利是依資源顯示的報告，會顯示取得資源授權的使用者數量、啟動次數和使用的授權數量。

表格 11-1. 報告類型 (繼續)

報告	說明
資源活動	資源活動報告可針對所有使用者或特定使用者群組而建立。資源活動資訊會列出使用者名稱、授權給使用者的資源、上次存取資源的日期，以及使用者用來存取資源的裝置類型相關資訊。
群組成員資格	群組成員資格會列出您指定之群組的成員。
角色指派	角色指派會列出身分為僅限 API 管理員或管理員的使用者，以及其電子郵件地址。
使用者	使用者報告會列出所有使用者並提供每位使用者的詳細資料，例如使用者的電子郵件地址、角色和群組關聯。
並行使用者	並行使用者報告會顯示同時開啟的使用者工作階段，以及日期和時間。
裝置使用量	裝置使用量報告可針對所有使用者或特定使用者群組而顯示裝置使用情形。裝置資訊是依照個別使用者而列出，包含使用者名稱、裝置名稱、作業系統資訊，以及上次使用日期。
稽核事件	稽核事件報告會列出與您指定之使用者相關的事件，例如過去 30 天的使用者登入情形。您也可以檢視稽核事件詳細資料。此功能很適合用來進行疑難排解。若要執行稽核事件報告，必須在 [目錄] > [設定] > [稽核] 頁面中啟用稽核。請參閱“產生稽核事件報告,” 第 99 頁。

產生稽核事件報告

您可以產生您所指定之稽核事件的報告。

稽核事件報告適合做為疑難排解的方法。

先決條件

稽核功能必須啟用。若要確認是否已啟用，請在管理主控台中移至 **目錄 > 設定** 頁面，然後選取 **稽核**。

程序

- 1 在管理主控台中，選取 **報告 > 稽核事件**
- 2 選取稽核事件準則。

稽核事件準則	說明
使用者	此文字方塊可讓您將稽核事件的搜尋範圍縮小至特定使用者所產生的事件。
類型	此下拉式清單可讓您將稽核事件的搜尋範圍縮小至特定的稽核事件類型。此下拉式清單不會顯示所有可能的稽核事件類型。此清單只會顯示您的部署中發生的事件類型。全部以大小字母列出的稽核事件類型是存取事件 (例如 LOGIN 和 LAUNCH)，此類事件並不會在資料庫中產生變更。其他稽核事件類型則會在資料庫中產生變更。
動作	此下拉式清單可讓您將搜尋範圍縮小至特定動作。清單中會顯示對資料庫進行特定變更的事件。如果您在 [類型] 下拉式清單中選取了存取事件，由於這是非動作事件，因此請不要在 [動作] 下拉式清單中指定動作。
物件	此文字方塊可讓您將搜尋範圍縮小至特定物件。物件的範例包括群組、使用者和裝置。物件可由名稱或識別碼來識別。
日期範圍	這些文字方塊可讓您將搜尋範圍縮小至「從 ___ 天之前到 ___ 天之前」格式的日期範圍。日期範圍上限為 30 天。例如，從 90 天之前到 60 天之前是有效的範圍，而從 90 天之前到 45 天之前則是無效的範圍，因為已超過 30 天的上限。

- 3 按一下 **顯示**。

稽核事件報告會根據您所指定的準則顯示。

備註 有時候，當稽核子系統重新啟動時，[稽核事件] 頁面可能會顯示錯誤訊息，而未轉譯報告。如果您看見此類關於未轉譯報告的錯誤訊息，請稍候幾分鐘，然後再試一次。

- 4 如須稽核事件的詳細資訊，請對該稽核事件按一下 **檢視詳細資料**。

自訂品牌 VMware Identity Manager 服務

12

您可以自訂顯示在管理主控台、使用者和管理員登入畫面、Workspace ONE 應用程式入口網站的 Web 檢視，以及行動裝置上的 Workspace ONE 應用程式的 Web 檢視等。

您可以使用自訂工具來比對公司的色彩、標誌及設計的外觀和質感。

- 若要自訂瀏覽器網址列和登入頁面，請前往 [身分識別與存取管理] > [設定] > [自訂品牌] 頁面。
- 若要新增標誌及自訂使用者 Web 入口網站行動裝置與平板電腦檢視，請前往 [目錄] > [設定] > [使用者入口網站品牌] 頁面。

本章節討論下列主題：

- “在 VMware Identity Manager 中自訂品牌,” 第 101 頁
- “自訂使用者入口網站的品牌,” 第 102 頁
- “為 VMware Verify 應用程式自訂品牌,” 第 103 頁

在 VMware Identity Manager 中自訂品牌

您可以在管理主控台和使用者入口網站的網址列上新增您的公司名稱、產品名稱和 Favicon。您也可以自訂登入頁面，以設定與公司的色彩和標誌設計相符的背景色彩。

若要新增公司標誌，請前往管理主控台內的 [目錄] > [設定] > [使用者入口網站品牌] 頁面。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取 **設定 > 自訂品牌**。
- 2 視需要編輯表單中的下列設定。

備註 下表未列出的設定代表並不使用且無法自訂的設定。

表單欄位	說明
	名稱與標誌
公司名稱	[公司名稱] 選項適用於桌面平台和行動裝置。您可以將公司名稱新增為顯示在瀏覽器索引標籤中的標題。 輸入新的公司名稱來取代現有名稱即可以變更名稱。
產品名稱	[產品名稱] 選項適用於桌面平台和行動裝置。在瀏覽器索引標籤中，產品名稱會顯示在公司名稱之後。 輸入產品名稱來取代現有名稱即可以變更名稱。

表單欄位	說明
Favicon	Favicon 是一個與瀏覽器網址列中所顯示 URL 相關聯的圖示。 Favicon 影像的大小上限為 16 x 16 像素。可用格式包括 JPEG、PNG、GIF 或 ICO。 按一下 上傳 可藉由上傳新影像來取代目前的 Favicon。系統會提示您確認變更。變更會立即生效。
登入畫面	
標誌	按一下 上傳 可藉由上傳新標誌來取代登入畫面中的現有標誌。當您按一下 確認 時，變更將會立即生效。 建議上傳的影像大小下限為 350 x 100 像素。如果您上傳大於 350 x 100 像素的影像，系統會將影像調整為符合 350 x 100 像素的大小。可用格式包括 JPEG、PNG 或 GIF。
背景色彩	顯示為登入畫面背景的色彩。 輸入六位數十六進位色彩碼來取代現有代碼，即可以變更背景色彩。
方塊背景色彩	您可以自訂登入畫面方塊色彩。 輸入六位數十六進位色彩碼來取代現有代碼。
登入按鈕背景色彩	您可以自訂登入按鈕的色彩。 輸入六位數十六進位色彩碼來取代現有代碼。
登入按鈕文字色彩	您可以自訂顯示在登入按鈕上的文字色彩。 輸入六位數十六進位色彩碼來取代現有代碼。

自訂登入畫面時，您可以先在 [預覽] 窗格中查看變更，之後再予以儲存。

3 按一下**儲存**。

管理主控台和登入頁面的自訂品牌更新會在您按一下 [儲存] 後的五分鐘之內套用。

下一個

在各種介面中檢查品牌變更的外觀。

更新使用者 Workspace ONE 入口網站及行動裝置與平板電腦檢視的外觀。請參閱“[自訂使用者入口網站的品牌](#),” 第 102 頁

自訂使用者入口網站的品牌

您可以新增標誌、變更背景色彩以及新增影像，以自訂 Workspace ONE 入口網站。

程序

- 1 在管理主控台的 [目錄] 索引標籤中，選取**設定 > 使用者入口網站品牌**。
- 2 視需要編輯表單中的設定。

表單項目	說明
標誌	新增要在管理主控台的頂端和 Workspace ONE 入口網站上作為橫幅的報頭標誌。 影像的大小上限為 220 x 40 像素。可用格式包括 JPEG、PNG 或 GIF。
入口網站	
報頭背景色彩	輸入六位數十六進位色彩碼來取代現有色彩碼，即可變更報頭的背景色彩。當您輸入新的色彩代碼時，應用程式入口網站預覽畫面中的背景色彩將會變更。
報頭文字色彩	輸入六位數十六進位色彩碼來取代現有色彩碼，即可變更報頭中顯示的文字色彩。

表單項目	說明
背景色彩	顯示為 Web 入口網站畫面背景的色彩。 輸入新的六位數十六進位色彩碼來取代現有代碼，即可以變更背景色彩。當您輸入新的色彩代碼時，應用程式入口網站預覽畫面中的背景色彩將會變更。 選取 背景反白 可強調背景色彩。如果啟用此項目，支援多重背景影像的瀏覽器會在啟動器和目錄頁面中顯示重疊。 選取 背景圖樣 可設定背景色彩中預先設計的三角形圖樣。
名稱與圖示色彩	您可以為列示在應用程式入口網站頁面之圖示下方的名稱選取文字色彩。 輸入十六進位色彩碼來取代現有代碼，即可以變更字型色彩。
字型效果	選取要用於 Workspace ONE 入口網站畫面之文字的字型類型。
影像 (選用)	若要將影像新增至應用程式入口網站畫面的背景來取代色彩，請上傳影像。

3 按一下**儲存**。

使用者入口網站的自訂品牌更新會每隔 24 小時重新整理一次。若要在較短的時間內推送變更，請以管理員身分開啟新索引標籤並輸入此 URL，同時將 `myco.example.com` 替換成您的網域名稱。

`https://<myco.example.com>/catalog-portal/services/api/branding?refreshCache=true`。

下一個

在各種介面中檢查品牌變更的外觀。

為 VMware Verify 應用程式自訂品牌

如果您已啟用 VMware Verify 以進行雙重要素驗證，您可以使用公司標誌自訂登入頁面。

先決條件

已啟用 VMware Verify。

程序

- 1 在管理主控台的 [目錄] 索引標籤中，選取**設定 > 使用者入口網站品牌**。
- 2 編輯 VMware Verify 區段。

表單項目	說明
標誌	上傳顯示於核准要求頁面上的公司標誌。 影像大小為 540 x 170 像素 (PNG 格式)，128 kB 或更小。
圖示	當 VMware Verify 啟動時上傳顯示於裝置上的圖示。 影像大小為 81 x 81 像素 (PNG 格式)，128 kB 或更小。

3 按一下**儲存**。

整合 AirWatch 與 VMware Identity Manager

13

AirWatch 可為裝置提供企業行動性管理功能，VMware Identity Manager 則可為使用者提供單一登入和身分識別管理功能。

當 AirWatch 與 VMware Identity Manager 整合時，AirWatch 註冊裝置的使用者將可直接安全地登入其已啟用的應用程式，而無須輸入多個密碼。

當 AirWatch 與 VMware Identity Manager 整合時，您可以設定下列與 AirWatch 的整合。

- 一個將 AirWatch 使用者和群組同步至 VMware Identity Manager 服務中的目錄，然後透過 AirWatch Cloud Connector 設定密碼驗證的 AirWatch 目錄。
- 對整合目錄進行單一登入 (目錄中包含同時受到 AirWatch 和 VMware Identity Manager 管理的授權應用程式)。
- 使用 Kerberos 驗證對 iOS 9 裝置進行單一登入。
- 用來檢查 AirWatch 管理的 iOS 9 裝置是否合規的存取原則規則。

本章節討論下列主題：

- [“設定 AirWatch 以便與 VMware Identity Manager 整合,”](#) 第 105 頁
- [“在 VMware Identity Manager 中設定 AirWatch 執行個體,”](#) 第 108 頁
- [“為 AirWatch 啟用整合目錄,”](#) 第 109 頁
- [“使用 AirWatch Cloud Connector 實作驗證,”](#) 第 110 頁
- [“為 AirWatch 管理的 iOS 裝置實作 Mobile Single Sign-in 驗證,”](#) 第 112 頁
- [“實作 Android 裝置的行動單一登入驗證,”](#) 第 118 頁
- [“為 AirWatch 管理的裝置啟用符合性檢查,”](#) 第 124 頁

設定 AirWatch 以便與 VMware Identity Manager 整合

在 VMware Identity Manager 管理主控台中設定 AirWatch 設定前，您需先在 AirWatch 管理主控台中設定與 VMware Identity Manager 的通訊。

若要整合 AirWatch 與 VMware Identity Manager，必須符合下列條件。

- 在 AirWatch 中，您要為其設定 VMware Identity Manager 的組織群組，即為**客戶**。
- 用來與 VMware Identity Manager 服務通訊的 REST API 管理員金鑰，以及 REST 為 AirWatch Cloud Connector 密碼驗證註冊的使用者 API 金鑰，皆會建立於設定 VMware Identity Manager 所在的相同組織群組上。

- 在 VMware Identity Manager 管理主控台中，從 AirWatch 將 API 管理員帳戶設定和管理員驗證憑證新增至 AirWatch 設定。
- 在設定 VMware Identity Manager 所在的相同組織群組上，設定 Active Directory 使用者帳戶。
- 如果在登錄和註冊之後，將使用者放置在從中設定 VMware Identity Manager 的子系組織群組中，則必須使用 AirWatch 註冊組態中的使用者群組對應，將使用者及其各自的裝置篩選至適當的組織群組。

系統會在 AirWatch 管理主控台中設定下列項目。

- 用於與 VMware Identity Manager 服務通訊的 REST 管理員 API 金鑰
- VMware Identity Manager 的 API 管理員帳戶以及從 AirWatch 匯出並新增至 VMware Identity Manager 中 AirWatch 設定的管理員驗證憑證
- 用於 AirWatch Cloud Connector 密碼驗證的 REST 註冊使用者 API 金鑰

在 AirWatch 中建立 REST API 金鑰

您必須在 AirWatch 管理主控台內啟用 REST 管理員 API 存取和註冊使用者存取，才能整合 VMware Identity Manager 與 AirWatch。當您啟用 API 存取時，將會產生 API 金鑰。

程序

- 1 在 AirWatch 管理主控台內，選取 [全域] > [客戶層級組織群組]，接著瀏覽至 **群組和設定 > 所有設定 > 系統 > 進階 > API > REST API**。
- 2 在 [一般] 索引標籤中，按一下 **新增** 以產生用於 VMware Identity Manager 服務的 API 金鑰。帳戶類型應該是 [管理員]。

提供唯一的服務名稱。新增說明，例如 **AirWatchAPI for IDM**。

- 3 若要產生註冊使用者 API 金鑰，請再次按一下 **新增**。
- 4 在 [帳戶類型] 下拉式功能表中選取 **註冊使用者**。

提供唯一的服務名稱。新增說明，例如 **UserAPI for IDM**。

- 5 複製兩個 API 金鑰，並將其儲存至檔案。

您可以在使用 VMware Identity Manager 管理主控台設定 AirWatch 時新增這些金鑰。

Service	Account Type	API Key	Description
AirWatchAPI	Admin	130HA4AAAAG5A7AADQA	
UserAPI	Enrollment User	DrhD17luOMyah1RyaSqkTFEs+2V8NTd ujoEvdDyVyl=	

- 6 按一下 **儲存**。

在 AirWatch 中建立管理員帳戶和憑證

在建立管理員 API 金鑰後，您可以在 AirWatch 管理主控台內新增管理員帳戶及設定憑證驗證。

若要進行 REST API 憑證型驗證，系統會從 AirWatch 管理主控台產生使用者層級憑證。使用的憑證是從 AirWatch 管理員根憑證產生的自我簽署 AirWatch 憑證。

先決條件

已建立 AirWatch REST 管理員 API 金鑰。

程序

- 1 在 AirWatch 管理主控台內選取 [全域] > [客戶層級組織群組]，接著瀏覽至 **帳戶 > 管理員 > 清單檢視**。
- 2 按一下 **新增 > 新增管理員**。
- 3 在 [基本] 索引標籤中，於必要的文字方塊中輸入憑證管理員的使用者名稱和密碼。

- 4 選取 [角色] 索引標籤，並選擇目前的組織群組，接著按一下第二個文字方塊，然後選取 **AirWatch 管理員**。
- 5 選取 [API] 索引標籤，然後在 [驗證] 文字方塊中選取 **憑證**。
- 6 輸入憑證密碼。該密碼與在 [基本] 索引標籤中輸入的管理員密碼相同。
- 7 按一下 **儲存**。
系統隨即會建立新的管理員帳戶和用戶端憑證。
- 8 在 [清單檢視] 頁面中選取您已建立的管理員，然後再次開啟 API 索引標籤。
憑證頁面會顯示憑證的相關資訊。

- 9 輸入您在 [憑證密碼] 文字方塊中設定的密碼，接著按一下 **匯出用戶端憑證** 並儲存檔案。

用戶端憑證會儲存為 .p12 檔案類型。

下一個

在 VMware Identity Manager 管理主控台內設定 AirWatch URL 組態。

在 VMware Identity Manager 中設定 AirWatch 執行個體

在 AirWatch 管理主控台內設定組態後，您可以在 VMware Identity Manager 管理主控台的 [身分識別與存取管理] 頁面中輸入 AirWatch URL、API 金鑰值及憑證。在設定 AirWatch 組態後，您可以啟用 AirWatch 整合賦予的功能選項。

新增 AirWatch 設定至 VMware Identity Manager

在 VMware Identity Manager 中設定 AirWatch 設定，以將 AirWatch 與 VMware Identity Manager 整合，並啟用 AirWatch 功能整合選項。新增 AirWatch API 金鑰和憑證，以便使用 AirWatch 來驗證 VMware Identity Manager。

先決條件

- 管理員用來登入 AirWatch 管理主控台的 AirWatch 伺服器 URL。
- 用來從 VMware Identity Manager 向 AirWatch 伺服器進行 API 要求以設定整合的 AirWatch 管理員 API 金鑰。
- 用來進行 API 呼叫和憑證密碼的 AirWatch 憑證檔案。憑證檔案必須採用 .p12 檔案格式。
- AirWatch 註冊使用者 API 金鑰。
- 您的承租人的 AirWatch 群組識別碼，這是 AirWatch 中的承租人識別碼。

程序

- 1 在 VMware Identity Manager 管理主控台的 [身分識別與存取管理] 索引標籤中，按一下 **設定 > AirWatch**。
- 2 在下列欄位中輸入 AirWatch 整合設定。

欄位	說明
AirWatch API URL	輸入 AirWatch URL。例如， https://myco.airwatch.com
AirWatch API 憑證	上傳用來進行 API 呼叫的憑證檔案。

欄位	說明
憑證密碼	輸入憑證密碼。
AirWatch 管理員 API 金鑰	輸入管理員 API 金鑰值。API 金鑰值 FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc+jveeYs= 的範例
AirWatch 註冊使用者 API 金鑰	輸入註冊使用者 API 金鑰值。
AirWatch 群組識別碼。	輸入建立 API 金鑰和管理員帳戶所在組織群組的 AirWatch 群組識別碼。

3 按一下**儲存**。

AirWatch

AirWatch Configuration Configure AirWatch settings to integrate AirWatch with VMware Identity Manager. After you configure the settings click Save. You can then enable other feature options with AirWatch.

AirWatch API URL*
Enter the URL used to access the AirWatch admin console.

AirWatch API Certificate*
Upload the AirWatch .p12 certificate used for API calls.

Certificate Password*
Enter the certificate password.

AirWatch Admin API Key*
Enter the AirWatch admin API key copied from the AirWatch console.

AirWatch Enrolled User API Key*
Enter the AirWatch enrolled user API key copied from the AirWatch console.

AirWatch Group ID*
Enter the AirWatch Organization Group ID for this integration.

下一個

- 啟用 [整合目錄] 功能選項可將 AirWatch 目錄中的應用程式設定合併至整合目錄。
- 啟用符合性檢查以驗證 AirWatch 管理的裝置遵守 AirWatch 符合性原則。

請參閱“為 AirWatch 管理的裝置啟用符合性檢查,” 第 124 頁。

為 AirWatch 啟用整合目錄

當您對 AirWatch 執行個體設定 VMware Identity Manager 時，您可以啟用整合目錄，讓使用者可從 VMware Identity Manager 和 AirWatch 檢視其有權使用的所有應用程式。

AirWatch 未與整合目錄整合時，使用者從 VMware Identity Manager 服務只能檢視其有權使用的應用程式。

先決條件

已在 VMware Identity Manager 中設定 AirWatch。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，按一下**設定 > AirWatch**。
- 2 在此頁面上的 [整合目錄] 區段中，選取**啟用**。

3 按一下**儲存**。

下一個

通知 AirWatch 使用者，使其瞭解如何透過 VMware Identity Manager 存取整合目錄及檢視其 Workspace ONE 入口網站。

使用 AirWatch Cloud Connector 實作驗證

您可以整合 AirWatch Cloud Connector 與 VMware Identity Manager 服務，以用於使用者密碼驗證。您可以將 VMware Identity Manager 服務設定成從 AirWatch 目錄同步使用者，而不要部署 VMware Identity Manager Connector。

若要實作 AirWatch Cloud Connector 驗證，您可以在 VMware Identity Manager 管理主控台的內建身分識別提供者頁面中啟用 [AirWatch Cloud Connector 密碼驗證]。

備註 針對 VMware Identity Manager 的驗證，必須在 AirWatch 8.3 版和更新版本上設定 AirWatch Cloud Connector。

使用者名稱和密碼驗證會整合到 AirWatch Cloud Connector 部署中。若要使用其他 VMware Identity Manager 支援的驗證方法來驗證使用者，必須設定 VMware Identity Manager Connector。

管理使用者屬性對應

您可設定 AirWatch 目錄和 VMware Identity Manager 目錄之間的使用者屬性對應。

VMware Identity Manager 管理主控台中 [身分識別與存取管理] > [設定] > [使用者屬性] 頁面的 [使用者屬性] 頁面會列出可對應至 AirWatch 目錄屬性的預設目錄屬性。必要的屬性會以星號標示。在設定檔中遺失必要屬性的使用者不會同步至 VMware Identity Manager 服務。

表格 13-1. 預設 AirWatch 目錄屬性對應

VMware Identity Manager 使用者屬性名稱	預設對應至 AirWatch 使用者屬性
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeID	employeeID
網域	網域
已停用 (已停用外部使用者)	已停用
手機	telephoneNumber
lastName	lastname*
firstName	firstname*
電子郵件	Email*
userName	username*

將使用者和群組從 AirWatch 目錄同步到 VMware Identity 目錄

您可以在 AirWatch 管理主控台中設定 VMware Identity Manager 設定，以建立您組織群組之 AirWatch 目錄執行個體與 VMware Identity Manager 之間的連線。此連線可用來將使用者和群組同步至 VMware Identity Manager 服務中所建立的目錄。

VMware Identity Manager 目錄可與 AirWatch Cloud Connector 搭配使用以進行密碼驗證。

使用者和群組最初可手動同步至 VMware Identity Manager 目錄。AirWatch 同步排程會決定使用者和群組與 VMware Identity Manager 目錄同步的時機。

在 AirWatch 伺服器上新增或刪除使用者或群組時，其變更會立即反映在 VMware Identity Manager 服務上。

先決條件

- VMware Identity Manager 本機管理員名稱和密碼。
- 識別要從 AirWatch 目錄對應的屬性值。請參閱“[管理使用者屬性對應](#),” 第 110 頁。

程序

- 1 在 AirWatch 管理主控台中，依序按一下 [群組和設定] 與 [所有頁面]，接著選取 [全域] > [客戶層級組織群組]，並導覽至 **系統 > 企業整合 > VMware Identity Manager**。
- 2 在 [伺服器] 區段中，按一下 **設定**。

備註 組態按鈕僅在目錄服務也針對相同的組織群組設定時才可供使用。如果看不見 [設定] 按鈕，表示您不在正確的組織群組中。您可以在 [全域] 下拉式功能表中變更組織群組。

- 3 輸入 VMware Identity Manager 的設定。

選項	說明
URL	輸入您的承租人 VMware URL。例如， <code>https://myco.identitymanager.com</code> 。
管理員使用者名稱	輸入 VMware Identity Manager 本機管理員使用者名稱。
管理員密碼	輸入 VMware Identity Manager 本機管理員使用者的密碼。

- 4 按**下一步**。
- 5 啟用自訂對應以設定從 AirWatch 到 VMware Identity Manager 服務的使用者屬性對應。
- 6 按一下 **測試連線** 來確認設定均正確。
- 7 按一下 **立即同步** 手動將所有使用者和群組同步到 VMware Identity Manager 服務。

備註 為了控制系統負載，手動同步只能在上一次同步的四小時後執行。

VMware Identity Manager 服務中會建立 AirWatch 目錄，而使用者和群組則會同步到 VMware Identity Manager 中的目錄。

下一個

在 VMware Identity Manager 管理主控台中檢閱 [使用者和群組] 索引標籤，以確認使用者和群組名稱均已同步。

在升級 AirWatch 之後更新 VMware Identity Manager

將 AirWatch 升級至新版本後，您必須透過 VMware Identity Manager 服務中的 AirWatch 組態選項，更新「整合目錄」和「使用者密碼驗證」。

當您在升級 AirWatch 之後儲存這些選項時，VMware Identity Manager 服務中的 AirWatch 設定會使用新版本的 AirWatch 進行更新。

程序

- 1 升級 AirWatch 之後，請登入 VMware Identity Manager 管理主控台。

- 2 在 [身分識別與存取管理] 索引標籤中，按一下**設定 > AirWatch**。
- 3 將頁面向下捲動至**整合目錄**區段，然後按一下**儲存**。
- 4 向下捲動至**透過 AirWatch 驗證使用者密碼**區段，然後按一下**儲存**。

在 VMware Identity Manager 服務中，AirWatch 組態會使用新版本進行更新。

為 AirWatch 管理的 iOS 裝置實作 Mobile Single Sign-in 驗證

在進行 iOS 裝置驗證時，VMware Identity Manager 會使用內建於 Identity Manager 服務中的身分識別提供者，以提供對 Mobile SSO 驗證的存取權。這種驗證方法會使用金鑰發佈中心 (KDC)，而不使用連接器或第三方系統。您必須先啟動 VMware Identity Manager 內建身分識別提供者中的 KDC 服務，然後才能在管理主控台中啟用 Kerberos。

要為 AirWatch 管理的 iOS 9 裝置實作 Mobile SSO 驗證，必須執行下列組態步驟。

備註 執行 iOS 9 和更新版本的 iOS 裝置上支援 Mobile SSO 驗證。

- 在 VMware Identity Manager 應用裝置中初始化金鑰發佈中心 (KDC)。請參閱《安裝指南》中的〈準備在 iOS 裝置上使用 Kerberos 驗證〉章節。
- 如果要使用 Active Directory 憑證服務，請在 Active Directory 憑證服務中針對 Kerberos 憑證發佈設定憑證授權機構範本。然後，設定 AirWatch 以使用 Active Directory 憑證授權機構。在 AirWatch 管理主控台中新增憑證範本。下載發行者憑證以設定 iOS 版 Mobile SSO。
- 如果您使用 AirWatch 憑證授權機構，請在 VMware Identity Manager [整合] 頁面中啟用憑證。下載發行者憑證以設定 iOS 版 Mobile SSO。
- 在 VMware Identity Manager 管理主控台中設定內建身分識別提供者，並啟用及設定 iOS 版 Mobile SSO 驗證。
- 從 AirWatch 管理主控台中設定 iOS 裝置設定檔，並啟用單一登入。

在 AirWatch 中設定 Active Directory 憑證授權機構

若要對 AirWatch 管理的 iOS 9 行動裝置設定單一登入驗證，您可以在 Active Directory 和 AirWatch 之間設定信任關係，並在 VMware Identity Manager 中啟用 iOS 版 Mobile SSO 驗證方法。

在 Active Directory 憑證服務中針對 Kerberos 憑證發佈設定憑證授權機構和憑證範本之後，您會啟用 AirWatch 以要求用於驗證的憑證，並將憑證授權機構新增至 AirWatch 管理主控台。

程序

- 1 在 AirWatch 管理主控台主功能表中，導覽至**裝置 > 憑證 > 憑證授權機構**。
- 2 按一下**新增**。
- 3 在 [憑證授權機構] 頁面中設定下列項目。

備註 確定已選取 [Microsoft AD CS] 做為 [授權單位類型]，之後才開始完成此表單。

選項	說明
名稱	輸入新憑證授權機構的名稱。
授權單位類型	確定已選取 Microsoft AD CS 。
通訊協定	選取 AD CS 做為通訊協定。

選項	說明
伺服器主機名稱	輸入伺服器的 URL。以 <code>https://{servername.com}/certsrv.adcs/</code> 這個格式輸入主機名稱。根據網站的設定方式，網站可以是 <code>http</code> 或 <code>https</code> 。URL 必須包含尾端 <code>/</code> 。 備註 測試 URL 時若連線失敗，請從位址中移除 <code>http://</code> 或 <code>https://</code> ，然後再次測試連線。
授權單位名稱	輸入 AD CS 端點所連線之憑證授權機構的名稱。您可以透過啟動憑證授權機構伺服器上的憑證授權機構應用程式來找到此名稱。
驗證	確定已選取 服務帳戶 。
使用者名稱和密碼	輸入具有足夠存取權，而可讓 AirWatch 要求和簽發憑證之 AD CS 管理員帳戶的使用者名稱和密碼。

4 按一下**儲存**。

下一個

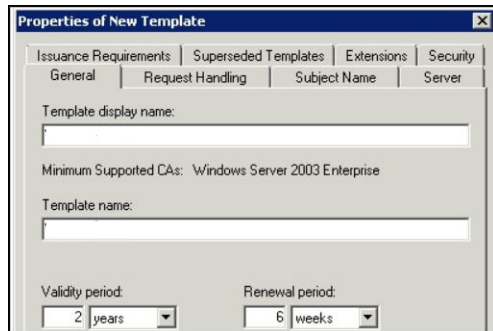
在 AirWatch 中設定憑證範本。

設定 AirWatch 以使用 Active Directory 憑證授權機構

必須正確設定您的憑證授權機構範本，才能進行 Kerberos 憑證發佈。在 Active Directory 憑證服務 (AD CS) 中，您可以複製現有的 Kerberos 驗證範本，以為 iOS Kerberos 驗證設定新的憑證授權機構範本。

從 AD CS 複製 Kerberos 驗證範本時，您必須在 [新增範本] 對話方塊的 [內容] 中設定下列資訊。

圖 13-1 新增範本對話方塊中的 Active Directory 憑證服務內容



- **一般索引標籤**。輸入範本顯示名稱和範本名稱。例如 iOSKerberos。這是 [憑證範本] 嵌入式管理單元、[憑證] 嵌入式管理單元和 [憑證授權機構] 嵌入式管理單元中顯示的顯示名稱。
- **主體名稱索引標籤**。選取**在要求中提供**選項按鈕。主體名稱是由 AirWatch 在 AirWatch 要求憑證時提供。
- **延伸模組索引標籤**。定義應用程式原則。
 - 選取 [應用程式原則]，然後按一下 [編輯] 來新增應用程式原則。將此原則命名為「Kerberos 用戶端驗證」。
 - 如下所示新增物件識別碼 (OID): 1.3.6.1.5.2.3.4。請勿變更。
 - 在 [應用程式原則的描述] 清單中，刪除所列出 Kerberos 用戶端驗證原則和智慧卡驗證原則以外的所有原則。
- **安全性索引標籤**。新增 AirWatch 帳戶至可以使用憑證的使用者清單。設定帳戶的權限。設定「完整控制」以允許安全性主體修改憑證範本的所有屬性，包括憑證範本的權限。否則，請根據組織的需求設定權限。

儲存變更。新增範本至 Active Directory 憑證授權機構所使用範本的清單。

在 AirWatch 中，設定憑證授權機構，並新增憑證範本。

在 AirWatch 中新增憑證範本

您會新增與憑證授權機構相關聯的憑證範本，以便產生使用者的憑證。

先決條件

在 AirWatch 中設定憑證授權機構。

程序

- 1 在 AirWatch 管理主控台中，導覽至**系統 > 企業整合 > 憑證授權機構**。
- 2 選取**要求範本**索引標籤，然後按一下**新增**。
- 3 在憑證範本頁面中設定下列項目。

選項	說明
名稱	在 AirWatch 中輸入新要求範本的名稱。
憑證授權機構	在下拉式功能表中，選取所建立的憑證授權機構。
發行範本	輸入 Microsoft CA 憑證範本名稱 (與您在 AD CS 中所建立的名稱完全相同)。例如 iOSKerberos 。
主體名稱	在 CN= 之後，輸入 {EnrollmentUser} ，其中 {} 文字方塊為 AirWatch 查閱值。此處輸入的文字為憑證的主體，它可以用來判斷收到憑證的人員。
私密金鑰長度	此私密金鑰長度會符合 AD CS 所使用之憑證範本上的設定。它通常為 2048。
私密金鑰類型	選取 簽署和加密 的核取方塊。
SAN 類型	針對主體替代名稱，選取 使用者主體名稱 。值必須為 {EnrollmentUser} 。如果使用 Kerberos 驗證設定了裝置符合性檢查，則必須設定第二個 SAN 類型才能包含 UDID。選取 SAN 類型 DNS 。值必須是 UDID={DeviceUid} 。
自動憑證更新	選取此核取方塊，讓使用此範本的憑證在其到期日之前自動更新。
自動更新期間 (天)	指定自動更新的天數。
啟用憑證撤銷	選取此核取方塊，以便在適用的裝置取消註冊或刪除時，或如果移除了適用的設定檔時自動撤銷憑證。
發佈私密金鑰	選取此核取方塊以發佈私密金鑰。
私密金鑰目的地	目錄服務或自訂 Web 服務

- 4 按一下儲存。

下一個

在 [身分識別提供者] 管理主控台中，設定使用 iOS 版 Mobile SSO 驗證方法的內建身分識別提供者。

在 AirWatch 中使用 Active Directory 憑證授權機構和憑證範本設定 Apple iOS 設定檔

在 AirWatch 中建立及部署 Apple iOS 裝置設定檔，以便將 Identity Provider 設定推送到裝置。該設定檔包含裝置連接 VMware Identity Provider 所需的資訊，以及裝置用來進行驗證的憑證。啟用單一登入以在不需要驗證的情況下登入各個應用程式，實現流暢的存取體驗。

先決條件

- iOS 版 Mobile SSO 會在 VMware Identity Manager 中進行設定。
- 已將 iOS Kerberos 憑證授權機構檔案儲存在可從 AirWatch 管理主控台存取的電腦中。
- 已在 AirWatch 中適當設定憑證授權機構和憑證範本。
- URL 清單和 iOS 裝置上使用 iOS 版 Mobile SSO 驗證的應用程式服務包識別碼。

程序

- 1 在 AirWatch 管理主控台中，導覽至 **裝置 > 設定檔和資源 > 設定檔**。
- 2 選取 **新增 > 新增設定檔**，然後選取 **Apple iOS**。
- 3 輸入 **iOSKerberos** 作為名稱，然後設定一般設定。

- 4 在左側導覽窗格中，選取**認證 > 設定**以設定認證。

選項	說明
認證來源	從下拉式功能表選取 定義的憑證授權機構 。
憑證授權機構	從下拉式功能表中的清單選取憑證授權機構。
憑證範本	從下拉式功能表選取參考憑證授權機構的要求範本。這是在 AirWatch 之「新增憑證範本」中建立的憑證範本。

- 5 再按一下頁面右下角的 **+**，然後建立第二個認證。
- 6 在**認證來源**下拉式功能表中選取**上傳**。
- 7 輸入認證名稱。
- 8 按一下**上傳**以上傳從 [身分識別與存取管理] > [管理] > [身分識別提供者] > [內建身分識別提供者] 頁面下載的 KDC 伺服器根憑證。
- 9 在左側導覽窗格中選取**單一登入**，然後按一下**設定**。
- 10 輸入連線資訊。

選項	說明
帳戶名稱	輸入 Kerberos 。
Kerberos 主要名稱	按一下 + ，接著選取 {EnrollmentUser} 。
領域	輸入在 VMware Identity Manager 應用裝置中初始化 KDC 時使用的領域名稱。例如，EXAMPLE.COM
更新憑證	從下拉式功能表選取 Certificate#1 。這是在認證下設定的 Active Directory CA 憑證。
URL 首碼	輸入必須相符的 URL 首碼，以透過 HTTP 將此帳戶用於 Kerberos 驗證。以 https://myco.example.com 的格式輸入 VMware Identity Manager 伺服器 URL。
應用程式	輸入允許使用此登入的應用程式身分識別清單。若要使用 iOS 內建的 Safari 瀏覽器來執行單一登入，請輸入 com.apple.mobilesafari 以當做第一個應用程式服務包識別碼。繼續輸入應用程式服務包識別碼。列示的應用程式必須支援 SAML 驗證

- 11 按一下**儲存並發佈**。

當 iOS 設定檔成功推送到使用者的裝置時，他們不需要輸入認證，即可使用 iOS 版 Mobile SSO 驗證方法登入 VMware Identity Manager。

下一個

建立另一個設定檔以設定其他任何所需的功能。例如，設定 Web Clips，以針對從 AirWatch 推送到 iOS 裝置首頁或應用程式目錄的 Web 應用程式建立圖示。

將 AirWatch 憑證授權機構用於 Kerberos 驗證

您可使用 AirWatch 憑證授權機構取代 Active Directory 憑證授權機構，對 AirWatch 管理的 iOS 9 行動裝置設定為使用內建 Kerberos 驗證的單一登入。您可在 AirWatch 管理主控台中啟用 AirWatch 憑證授權機構，並匯出 CA 簽發者憑證以便用於 VMware Identity Manager 服務。

AirWatch 憑證授權機構設計為遵守簡單憑證註冊通訊協定 (SCEP)，並可搭配支援 SCEP 的 AirWatch 管理裝置使用。VMware Identity Manager 與 AirWatch 的整合使用 AirWatch 憑證授權機構來簽發憑證給 iOS 9 行動裝置，以做為設定檔的一部分。

AirWatch 憑證授權機構簽發者根憑證也是 OCSP 簽署憑證。

啟用及匯出 AirWatch 憑證授權機構

如果已在 AirWatch 中啟用 VMware Identity Manager，您將可在受管理的 iOS 9 行動裝置上產生 AirWatch 發行者根憑證，並匯出此憑證以用於 iOS 版 Mobile SSO 驗證。

程序

- 1 在 AirWatch 管理主控台中，導覽至 **系統 > 企業整合 > VMware Identity Manager**。
- 2 若要啟用 AirWatch 憑證授權機構，組織群組類型必須是 [客戶]。



Tip 若要檢視或變更群組類型，請導覽至 [群組和設定]、**群組 > 組織群組 > 組織群組詳細資料**。

- 3 在 [憑證] 區段中，按一下 **啟用**。
頁面會顯示發行者根憑證詳細資料。
- 4 按一下 **匯出**，然後儲存檔案。

下一個

在 VMware Identity Manager 管理主控台中，設定 [內建身分識別提供者] 中的 [Kerberos 驗證]，並新增憑證授權機構發行者憑證。

在 AirWatch 中使用 AirWatch 憑證授權機構設定 Apple iOS 設定檔

在 AirWatch 中建立及部署 Apple iOS 裝置設定檔，以便將 Identity Provider 設定推送到裝置。該設定檔包含裝置連線 VMware Identity Provider 所需的資訊，以及裝置用來進行驗證的憑證。

先決條件

- 已在 Identity Manager 中設定內建 Kerberos。
- 已將 VMware Identity Manager KDC 伺服器根憑證檔案儲存在可從 AirWatch 管理主控台存取的電腦中。
- 從 AirWatch 管理主控台 [系統] > [企業整合] > [VMware Identity Manager] 頁面啟用及下載的憑證。
- URL 清單和 iOS 裝置上使用內建 Kerberos 驗證的應用程式服務包識別碼。

程序

- 1 在 AirWatch 管理主控台中，導覽至 **裝置 > 設定檔和資源 > 設定檔 > 新增設定檔**，然後選取 **Apple iOS**。
- 2 進行設定檔的**一般**設定，再輸入 **iOSKerberos** 以做為裝置名稱。

- 3 在左側導覽窗格中，選取 **SCEP > 設定** 以設定認證。

選項	說明
認證來源	從下拉式功能表選取 AirWatch 憑證授權機構 。
憑證授權機構	從下拉式功能表選取 AirWatch 憑證授權機構 。
憑證範本	選取 單一登入 以設定 AirWatch 憑證授權機構發出的憑證類型。

- 4 按一下**認證 > 設定**，然後建立第二個認證。
- 5 在**認證來源**下拉式功能表中選取**上傳**。
- 6 輸入 iOS Kerberos 認證名稱。
- 7 按一下**上傳**以上傳從 [身分識別與存取管理] > [管理] > [身分識別提供者] > [內建身分識別提供者] 頁面下載的 VMware Identity Manager KDC 伺服器根憑證。
- 8 在左側導覽窗格中選取**單一登入**。
- 9 輸入連線資訊。

選項	說明
帳戶名稱	輸入 Kerberos 。
Kerberos 主要名稱	按一下 +，接著選取 {EnrollmentUser}。
領域	輸入在 VMware Identity Manager 應用裝置中初始化 KDC 時使用的領域名稱。例如 EXAMPLE.COM 。
更新憑證	在 iOS 8 和更新版本裝置上，選取在使用者的單一登入工作階段到期時，用來自動重新驗證使用者、而不需要任何使用者互動的憑證。
URL 首碼	輸入必須相符的 URL 首碼，以透過 HTTP 將此帳戶用於 Kerberos 驗證。 以 https://myco.example.com 的格式輸入 VMware Identity Manager 伺服器 URL。
應用程式	輸入允許使用此登入的應用程式身分識別清單。若要使用 iOS 內建的 Safari 瀏覽器來執行單一登入，請輸入 com.apple.mobilesafari 作為第一個應用程式服務包識別碼。繼續輸入應用程式服務包識別碼。列示的應用程式必須支援 SAML 驗證

- 10 按一下**儲存並發佈**。

當 iOS 設定檔成功推送到使用者的裝置時，他們不需要輸入認證即可使用內建 Kerberos 驗證方法登入 VMware Identity Manager。

下一個

建立另一個設定檔以設定其他任何需要的 iOS Kerberos 功能。例如，設定 Web Clips 以針對從 AirWatch 推送到 iOS 裝置首頁或應用程式目錄的 Web 應用程式建立圖示。

實作 Android 裝置的行動單一登入驗證

Android 版 Mobile SSO 為 AirWatch 管理的 Android 裝置憑證驗證方法的實作。

AirWatch Tunnel 行動應用程式會安裝於 Android 裝置上。AirWatch Tunnel 用戶端已設定為存取 VMware Identity Manager 服務以進行驗證。通道用戶端會使用用戶端憑證建立相互驗證的 SSL 工作階段，而 VMware Identity Manager 服務會擷取用戶端憑證以進行驗證。

備註 Android 裝置 4.4 和更新版本可支援 Android 版 Mobile SSO 驗證。

無 VPN 存取的行動單一登入

當不需要 VPN 存取時，您可以設定 Android 裝置的行動單一登入驗證，以略過 Tunnel 伺服器。實作未使用 VPN 的 Android 版 Mobile SSO 驗證時，會使用與用於設定 AirWatch Tunnel 相同的組態頁面，但因為不是在安裝 Tunnel 伺服器，您不會輸入 AirWatch Tunnel 伺服器主機名稱和連接埠。您仍會使用 AirWatch Tunnel 設定檔表單來設定設定檔，但系統不會將流量導向 Tunnel 伺服器。Tunnel 用戶端只會用於單一登入。

在 AirWatch 管理主控台中，您可以進行下列設定。

- AirWatch Tunnel 中的「個別應用程式通道」元件。此組態可讓 Android 裝置透過 AirWatch Tunnel 行動應用程式用戶端存取內部和受管理的公用應用程式。
- 個別應用程式通道設定檔。此設定檔可用來為 Android 啟用個別應用程式通道功能。
- 在 [網路流量規則] 頁面中，因為未設定 Tunnel 伺服器，您會選取 [略過]，讓系統不會將任何流量導向 Tunnel 伺服器。

有 VPN 存取的行動單一登入

當設定了單一登入的應用程式也用來存取防火牆後的內部網路資源時，請設定 VPN 存取並設定 Tunnel 伺服器。對 VPN 設定了單一登入時，Tunnel 用戶端可以選擇性地透過 Tunnel 伺服器路由應用程式流量和登入要求。不要將預設組態用於主控台中處於單一登入模式的 Tunnel 用戶端，組態應該指向 Tunnel 伺服器才對。

要為 AirWatch 管理的 Android 裝置實作 Android 版 Mobile SSO 驗證，必須先在 AirWatch 管理主控台中設定 AirWatch Tunnel 並安裝 AirWatch Tunnel 伺服器，再於 VMware Identity Manager 的管理主控台中設定 Android 版 Mobile SSO。AirWatch Tunnel 服務可讓使用者透過「個別應用程式 VPN」存取 AirWatch 管理的應用程式。AirWatch Tunnel 也提供將來自行動應用程式的 Proxy 流量處理至 VMware Identity Manager 以進行單一登入的能力。

在 AirWatch 管理主控台中，您可以進行下列設定。

- AirWatch Tunnel 中的「個別應用程式通道」元件。此組態可讓 Android 裝置透過 AirWatch Tunnel 行動應用程式用戶端存取內部和受管理的公用應用程式。

在管理主控台中設定 AirWatch Tunnel 設定後，您可以下載 AirWatch Tunnel 安裝程式，並繼續執行 AirWatch Tunnel 伺服器的安裝。

- Android VPN 設定檔。此設定檔可用來為 Android 啟用個別應用程式通道功能。
- 透過管理主控台，為每個使用應用程式通道功能的應用程式啟用 VPN。
- 使用為「個別應用程式 VPN」所設定的所有應用程式的清單、Proxy 伺服器詳細資料以及 VMware Identity Manager URL 來建立裝置流量規則。

如需關於安裝及設定 AirWatch Tunnel 的詳細資訊，請參閱 AirWatch Resources 網站上的《VMware AirWatch Tunnel 指南》。

從 AirWatch 管理主控台設定 Android 裝置的單一登入

設定 Android 裝置的單一登入，以允許使用者安全地登入企業應用程式，而不需輸入其密碼。

若要設定 Android 裝置的單一登入，您不需設定 AirWatch Tunnel，但會使用許多相同的欄位設定單一登入

先決條件

- Android 4.4 或更新版本
- 應用程式必須支援 SAML 或其他支援的聯盟標準

程序

- 1 在 AirWatch 管理主控台中，導覽至**系統 > 企業整合 > AirWatch Tunnel**。
- 2 第一次設定 AirWatch Tunnel 時，請選取**組態**，並遵循設定精靈進行操作。否則，請選取**覆寫**，然後選取**啟用 AirWatch Tunnel** 核取方塊。然後，按一下**設定**。
- 3 在 [組態類型] 頁面中，啟用**個別應用程式通道 (僅限 Linux)**。按**下一步**。
將部署模式保留為**基本**。
- 4 在 [詳細資料] 頁面中，於文字方塊中輸入虛設值，因為此欄位對單一登入組態而言並非必要。按**下一步**。
- 5 在 [SSL] 頁面中，設定「個別應用程式通道」的 SSL 憑證。若要使用公用 SSL，請選取**使用公用 SSL 憑證**核取方塊。按**下一步**。
通道裝置根憑證會自動產生。

備註 不支援 SAN 憑證。請確定您的憑證是為對應的伺服器主機名稱核發的，或者是適用於對應網域的有效萬用字元憑證。

- 6 在 [驗證] 頁面中，選取所要使用的憑證驗證類型。按**下一步**。

選項	說明
預設值	選取 [預設] 以使用 AirWatch 核發的憑證。
企業 CA	系統會顯示一個下拉式功能表，其中列出您在 AirWatch 中設定的憑證授權機構和憑證範本。您也可以上傳 CA 的根憑證。

如果您選取 [企業 CA]，請確保 CA 範本中包含主體名稱 **CN=UDID**。您可以從 AirWatch Tunnel 組態頁面下載 CA 憑證。

- 7 按**下一步**。
- 8 在 [設定檔關聯] 頁面中，關聯至 Android 的現有 AirWatch Tunnel VPN 設定檔，或建立新的設定檔。
如果您在此步驟中建立設定檔，您仍須發佈設定檔。請參閱〈在 AirWatch 中設定 Android 設定檔〉。
- 9 檢閱組態的摘要，然後按一下**儲存**。
系統會將您重新導向至系統設定組態頁面。

從 AirWatch 管理主控台設定 AirWatch Tunnel VPN 存取設定

您可以在 AirWatch Tunnel 設定中啟用「個別應用程式通道」元件，為 Android 裝置設定個別應用程式的通道功能。「個別應用程式通道」可讓您的內部和受管理的公用應用程式依個別的應用程式存取您的公司資源。指定的應用程式啟動時，VPN 可自動連線。如需詳細的 AirWatch Tunnel 組態指示，請參閱 AirWatch Resources 網站上的《VMware AirWatch Tunnel 指南》。

程序

- 1 在 AirWatch 管理主控台中，導覽至**系統 > 企業整合 > AirWatch Tunnel**。
- 2 第一次設定 AirWatch Tunnel 時，請選取**組態**，並遵循設定精靈進行操作。否則，請選取**覆寫**，然後選取**啟用 AirWatch Tunnel** 核取方塊。然後，按一下**設定**。
- 3 在 [組態類型] 頁面中，啟用**個別應用程式通道 (僅限 Linux)**。按**下一步**。
將部署模式保留為**基本**。
- 4 在 [詳細資料] 頁面中，為「個別應用程式通道」設定輸入 AirWatch Tunnel 伺服器的主機名稱和連接埠。例如，您可以輸入 `tunnel.example.com`。按**下一步**。

- 5 在 [SSL] 頁面中，設定「個別應用程式通道」的 SSL 憑證。若要使用公用 SSL，請選取**使用公用 SSL 憑證**核取方塊。按**下一步**。
通道裝置根憑證會自動產生。

備註 不支援 SAN 憑證。請確定您的憑證是為對應的伺服器主機名稱核發的，或者是適用於對應網域的有效萬用字元憑證。

- 6 在 [驗證] 頁面中，選取所要使用的憑證驗證類型。按**下一步**。

選項	說明
預設值	選取 [預設] 以使用 AirWatch 核發的憑證。
企業 CA	系統會顯示一個下拉式功能表，其中列出您在 AirWatch 中設定的憑證授權機構和憑證範本。您也可以上傳 CA 的根憑證。

如果您選取 [企業 CA]，請確保 CA 範本中包含主體名稱 **CN=UDID**。您可以從 AirWatch Tunnel 組態頁面下載 CA 憑證。

如果已對 Android 設定裝置符合性檢查，請確保 CA 範本中包含主體名稱 **CN=UDID**，或設定 SAN 類型以納入 UDID。選取 SAN 類型 DNS。值必須是 **UDID={DeviceUid}**。

- 7 按**下一步**。
- 8 在 [設定檔關聯] 頁面中，關聯至 Android 的現有 AirWatch Tunnel VPN 設定檔，或建立新的設定檔。
如果您在此步驟中建立設定檔，您仍須發佈設定檔。請參閱〈在 AirWatch 中設定 Android 設定檔〉。
- 9 (選用) 在 [其他] 頁面中，為「個別應用程式通道」元件啟用存取記錄。按**下一步**。
您必須在安裝 AirWatch Tunnel 伺服器之前啟用這些記錄。
- 10 檢閱組態的摘要，然後按一下**儲存**。
系統會將您重新導向至系統設定組態頁面。
- 11 選取**一般**索引標籤並下載 **Tunnel 虛擬應用裝置**。
您可以使用 VMware Access Point 來部署 Tunnel 伺服器。

下一個

安裝 AirWatch Tunnel 伺服器。如需相關指示，請參閱 AirWatch Resources 網站上的《VMware AirWatch Tunnel 指南》。

設定 Android 的個別應用程式通道設定檔

在您設定並安裝 AirWatch Tunnel 的「個別應用程式通道」元件後，您可以設定 Android VPN 設定檔，並在設定檔中新增版本。

程序

- 1 在 AirWatch 管理主控台中，導覽至**裝置 > 設定檔 > 新增設定檔**，然後選取 **Android** 或 **Android for Work**。
- 2 設定 Android 的 [一般] 設定 (如果尚未設定)。
- 3 在左側的資料行中選取 **VPN**，然後按一下**設定**。

- 4 完成 VPN 連線資訊。

選項	說明
連線類型	選取 AirWatch Tunnel 。
連線名稱	輸入此連線的名稱。例如 AndroidSSO Configuration 。
Server	AirWatch Tunnel 伺服器 URL 會自動輸入。
個別應用程式 VPN 規則	選取 個別應用程式 VPN 規則 核取方塊。

- 5 按一下**新增版本**。
- 6 按一下**儲存並發佈**。

下一個

為能夠使用 Android 版 Mobile SSO 來存取的 Android 應用程式啟用個別應用程式 VPN。請參閱“[為 Android 應用程式啟用個別應用程式 VPN](#),” 第 122 頁。

為 Android 應用程式啟用個別應用程式 VPN

對於使用 VMware Identity Manager Mobile Android 版 Mobile SSO 存取的 Android 應用程式，系統會啟用 [個別應用程式 VPN 設定檔] 設定。

先決條件

- 已安裝使用個別應用程式通道元件進行設定的 AirWatch Tunnel。
- 已建立 Android VPN 設定檔。

程序

- 1 在 AirWatch 管理主控台中，導覽至**應用程式和書籍 > 應用程式 > 清單檢視**。
- 2 選取 [內部] 索引標籤。
- 3 選取**新增應用程式**，然後新增一個應用程式。
- 4 按一下**儲存並指派**。
- 5 在 [指派] 頁面中選取**新增指派**，然後在 [進階] 區段的**個別應用程式 VPN 設定檔**下拉式功能表中，選取您所建立的 Android VPN 設定檔。
- 6 按一下**儲存並發佈**。

為使用 Android 版 Mobile SSO 來存取的每個 Android 應用程式啟用個別應用程式 VPN。如需關於新增或編輯應用程式的詳細資訊，請參閱 AirWatch 資源網站上的《VMware AirWatch Mobile Application Management 指南》。

下一個

建立網路流量規則。請參閱“[在 AirWatch 中設定網路流量規則](#),” 第 122 頁。

在 AirWatch 中設定網路流量規則

設定網路流量規則，讓 AirWatch Tunnel 用戶端得以將流量路由到 Android 裝置的 HTTPS Proxy。您將列出已設定流量規則之個別應用程式 VPN 選項的 Android 應用程式，接著設定 Proxy 伺服器位址和 destination 主機名稱。

如需關於建立網路流量規則的詳細資訊，請參閱 AirWatch Resources 網站上的《VMware AirWatch Tunnel 指南》。

先決條件

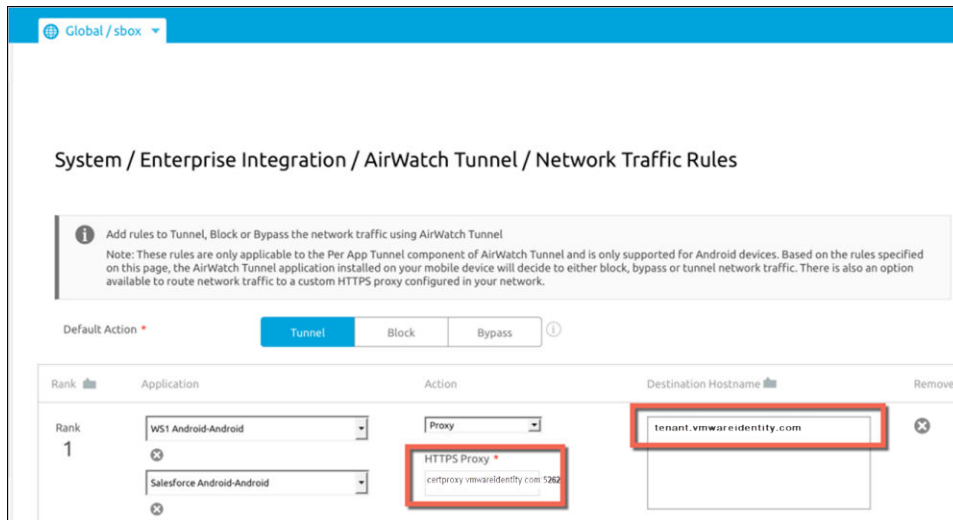
- 已安裝使用個別應用程式通道元件進行設定的 AirWatch Tunnel 選項。
- 已建立 Android VPN 設定檔。
- 已為每個新增至網路流量規則的 Android 應用程式啟用個別應用程式 VPN。

程序

- 1 在 AirWatch 管理主控台中，導覽至 **系統 > 企業整合 > AirWatch Tunnel > 網路流量規則**。
- 2 依照《AirWatch Tunnel 指南》中的說明，設定網路流量規則設定。特別是針對 Android 版 Mobile SSO 組態，必須在 [網路流量規則] 頁面中進行下列設定。
 - a 在 [應用程式] 資料行中，新增使用個別應用程式 VPN 設定檔的 Android 應用程式。
 - b 在 [動作] 資料行中，選取 Proxy 並指定 HTTPS Proxy 資訊。輸入 VMware Identity Manager 主機名稱和連接埠。例如，**login.example.com:5262**。

備註 如果您提供 VMware Identity Manager 主機的外部存取權限，則必須開啟防火牆連接埠 5262，或透過 DMZ 中的反向 Proxy 來代理連接埠 5262 流量。

- c 在 [目的地主機名稱] 資料行中，輸入目的地 VMware Identity Manager 主機名稱。例如 **myco.example.com**。AirWatch Tunnel 用戶端會將流量從 VMware Identity Manager 主機名稱路由到 HTTPS Proxy。
- 3 按一下 **儲存**。



下一個

發佈這些規則。發佈規則後，裝置會收到更新 VPN 設定檔，並將 AirWatch Tunnel 應用程式設定為啟用 SSO。

移至 VMware Identity Manager 管理主控台，然後在 [內建的身分識別提供者] 頁面中設定 Android 版 Mobile SSO。請參閱 [GUID-3D7A6C83-9644-42AE-94BD-003EAF3718CD#GUID-3D7A6C83-9644-42AE-94BD-003EAF3718CD](#)。

為 AirWatch 管理的裝置啟用符合性檢查

當使用者透過 AirWatch Agent 應用程式註冊其裝置時，系統將會根據排程傳送範例，其中包含用來評估符合性的資料。此範例資料的評估，可確保裝置符合管理員在 AirWatch 主控台中設定的符合性規則。如果裝置不合規，則會採取在 AirWatch 主控台中設定的對應動作。

VMware Identity Manager 包含存取原則選項，經設定可在使用者從裝置登入時用來檢查 AirWatch 伺服器中的裝置合規狀態。符合性檢查可確保在裝置不合規時，使用者將無法登入應用程式或對 VMware Identity Manager 入口網站使用單一登入。當裝置再次合規後，登入功能隨即恢復。

Workspace ONE 應用程式會在裝置遭到破解時自動登出，並封鎖對應用程式的存取。如果裝置是透過調適性管理進行註冊，則透過 AirWatch 主控台發出的企業抹除命令將會取消註冊裝置，並從裝置中移除受管理的應用程式。未受管理的應用程式不會移除。

如需關於 AirWatch 符合性原則的詳細資訊，請參閱 AirWatch 資源網站上提供的《VMware AirWatch Mobile Device Management 指南》。

設定符合性檢查的存取原則規則

設定需要符合性檢查的存取原則規則，讓 VMware Identity Manager 能夠驗證 AirWatch 管理的裝置是否遵循 AirWatch 裝置符合性原則。您可以在內建身分識別提供者中啟用符合性檢查。符合性檢查啟用時，您可以建立必須對 AirWatch 所管理的裝置進行驗證和裝置符合性驗證的存取原則規則。

符合性檢查原則規則能在搭配 iOS 版 Mobile SSO、Android 版 Mobile SSO 及憑證雲端部署的驗證鏈結中運作。使用驗證方法的優先順序必須高於原則規則組態中的裝置符合性選項。

先決條件

已在內建身分識別提供者中設定驗證方法。

程序

- 1 在管理主控台的 [身分識別與存取管理] 索引標籤中，選取**設定 > AirWatch**。
- 2 在 [AirWatch] 頁面的 [符合性檢查] 區段中，選取**啟用**。
- 3 按一下**儲存**。
- 4 在 [身分識別與存取管理] 索引標籤中，移至**管理 > 原則**。
- 5 選取要編輯的存取原則。
- 6 在 [原則規則] 區段中，選取要編輯的原則規格。
- 7 在**則使用者必須使用下列方法進行驗證**的下拉式功能表中，按一下 **+** 並選取要使用的驗證方法。
- 8 在**則使用者必須使用下列方法進行驗證**的第二個下拉式功能表中，選取**裝置符合性 (針對 AirWatch)**。
- 9 (選擇性) 在 [自訂錯誤] 的**訊息文字**文字方塊中，建立在使用者驗證因裝置不合規而失敗時所顯示的自訂訊息。在**自訂錯誤連結**文字方塊中，您可以在訊息中新增連結。

10 按一下儲存。

Add a Policy Rule

If a user's Network Range is...

and the user is trying to access content from...

then the user must authenticate using the following method...

and

If preceding Authentication Method fails, then:

only

Re-authenticate after: hours

Custom Error Message Create an custom access denied error message that displays when user authentication fails.

Message Text

索引

字母

Active Directory

部署 64

整合 15

整合式 Windows 驗證 13

屬性對應 21

Active Directory over LDAP 13, 22

Active Directory 全域目錄 15

Active Directory 憑證授權機構 113

AirWatch

啟用整合目錄 109

設定 iOS 設定檔 115, 117

裝置符合性檢查 124

管理員帳戶 107

憑證 107

AirWatch API 金鑰 106

AirWatch Cloud Connector 驗證 110

AirWatch Cloud 密碼驗證 63

AirWatch Tunnel, 設定 120

AirWatch 中的 Apple iOS 設定檔 117

AirWatch 中的合規檢查 124

AirWatch 升級, 更新服務 111

AirWatch 目錄, 使用者屬性 110

AirWatch 的符合性檢查 124

AirWatch 的憑證授權機構, Kerberos 驗證 112

AirWatch 的憑證範本, Kerberos 114

AirWatch 憑證授權機構, OCSP 117

AirWatch 憑證授權機構, 啟用 117

AirWatch, 設定 105

AirWatch, 網路流量規則 122

AirWatch, 與 Identity Manager 整合 105

AirWatch, 在 VMware Identity Manager 中設定 108

Android 版 Mobile SSO, 實作 118

Android 的個別應用程式通道設定檔 121

Android 驗證, 網路流量規則 122

android, 個別應用程式 VPN 122

Android, 單一登入 119

API 金鑰 105, 106

AWCA 117

Chrome 51

Citrix 發行的應用程式, 啟用 90

Cookie, 持續性 75

DNS 服務位置查閱 17-19

domain_krb.properties 檔案 17-19

Firefox 51

ICA 內容 95

Internet Explorer 50

iOS Kerberos 驗證 48

iOS 版 Mobile SSO 112

IP 範圍 66

Just-in-Time 目錄 41, 45

Just-in-Time 使用者佈建

SAML 宣告 44

本機群組 42

刪除目錄 45

使用者屬性 42

停用 45

設定 43

概觀 41

準備 42

錯誤訊息 46

Kerberos

Windows 驗證 48

內建 112

要設定的瀏覽器 49

符合性檢查 124

設定 49

設定 AirWatch 113

Kerberos, 使用 IWA 實作 48

LDAP 目錄

限制 29

整合 29, 30

OneTouch 通知 60

RADIUS 伺服器 54

RADIUS 組態 54

RADIUS 驗證 54

REST API 95

REST API 金鑰 106

RSA SecurID 伺服器 52

RSA 調適性驗證, 註冊使用者 56

RSA 調適性驗證, 設定 56

runtime-config.properties 檔案 18

SAML

中繼資料 92

- 第三方身分識別提供者 64
- 憑證 92
- SAML 宣告, Just-in-Time 44
- SecurID, 設定 53
- siteaware.subnet 內容 18
- SMS 60
- SRV 查閱 17–19
- ThinApp 套件, 啟用 90
- ThinApp 警示 95
- TOTP 60
- UPN 58
- userName 78
- View, 啟用 90
- VMware Verify
 - 安全性權杖 60
 - 重設 79
- VMware Verify, 品牌 103
- VMware Verify, 雙重要素驗證 60
- VMware Verify, 啟用 60
- VMware Verify, 登錄使用者 61
- VMware Verify, 解除登錄 61
- Web 應用程式 87, 88
- Worker 13
- Workspace IDP 64

兩劃

- 入口網站頁面, 自訂 102

三劃

- 工作區映像 87

四劃

- 內建身分識別提供者, 啟用 62
- 內建的身分識別提供者, 設定 62
- 內建的身分識別提供者, 設定 63
- 升級 AirWatch Cloud Connector 111

五劃

- 主要對象 7
- 加入網域, kerberos 49
- 平板電腦檢視, 自訂 102
- 本機目錄
 - 刪除 39
 - 刪除網域 38
 - 使用者屬性 38
 - 建立 34, 35
 - 建立與身分識別提供者的關聯 37
 - 新增網域 38
 - 編輯 38
 - 變更名稱 38
 - 變更網域名稱 38
- 本機目錄的使用者屬性 34

- 本機目錄設定 38

- 本機使用者

- 刪除 84

- 停用 83

- 新增 83

- 本機使用者, 新增 82

- 目錄

- 同步化保護 27

- 同步保護 27

- 新增 10, 13, 22

- 新增 Web 應用程式 89

- 管理 87

- 目錄, AirWatch 110

- 目錄, ThinApp 套件 90

- 目錄, View 90

- 目錄, Citrix 發行的應用程式 90

- 目錄伺服器群組 77

- 目錄設定, Citrix 發佈的應用程式 95

- 目錄整合 13

六劃

- 全域設定, 停用協助程式應用程式 93

- 同步保護, 忽略 28

- 同步設定 21

- 同步網域, 使用者 79

- 在 VMware Verify 中登錄使用者 61

- 多網域 15

- 存取事件 99

- 存取原則

- TTL 67, 69, 71

- Web 應用程式特定 71, 73, 74

- 用戶端類型 67

- 最小驗證分數 69, 71

- 網路 67, 69, 71

- 與身分識別提供者的關係 69, 73, 74

- 驗證強度 67

- 存取原則集

- Web 應用程式特定 71, 73, 74

- 入口網站 69, 73

- 建立 73

- 預設 74

- 預設值 67, 69, 73

- 存取遭拒訊息, 設定 67

- 自訂入口網站頁面 102

- 自訂品牌, 設定 10

- 自訂錯誤訊息 74

- 自訂屬性名稱, 請勿使用 20

- 行動應用程式, 資源類型 87

- 行動檢視, 自訂 102

七劃

- 刪除本機使用者 84
- 系統目錄 33
- 系統身分識別提供者 33
- 系統診斷儀表板 98
- 系統資訊 98
- 系統網域 33
- 角色, 使用者 79
- 角色指派報告 98
- 身分識別和存取管理設定 10
- 身分識別提供者
 - Workspace 64
 - 內建 62
 - 第三方 47, 64, 66, 92
 - 連接器 47, 66
 - 單一登出 64
 - 與存取原則的關係 69
- 身分識別提供者執行個體, 選取 66
- 身分識別提供者選項, 設定 64

八劃

- 使用者
 - Active Directory 77
 - 使用者屬性 21
 - 權利 79
- 使用者, Workspace ONE 9
- 使用者入口網站, 自訂 101
- 使用者名稱 78, 79
- 使用者設定檔 79
- 使用者報告 98
- 使用者儲存區 64
- 使用者屬性, 設定 10
- 使用者屬性, AirWatch 目錄 110
- 使用者屬性頁面 20
- 其他目錄 110
- 到期的 Active Directory 密碼 26
- 協助程式應用程式 93
- 版本 98
- 金鑰發佈中心 48

九劃

- 保護, 目錄同步化 27
- 保護, 臨界值 27
- 保護設定, 忽略 28
- 品牌, VMware Verify 103
- 客體使用者 77
- 持續性 Cookie, 啟用 75
- 挑戰問題 56
- 重設 Active Directory 密碼 26
- 重設 VMware Verify 61
- 重新驗證工作階段時間, 設定 67

十劃

- 原則, 編輯 74
- 原則規則
 - 符合性檢查 124
 - 驗證鏈結 69
- 核准 95

十一劃

- 停用
 - Citrix Receiver 下載 93
 - Horizon Client 下載 93
- 停用本機使用者 83
- 停用帳戶 20
- 偏好設定, 持續性 Cookie 75
- 密碼, 到期的 26
- 密碼 (本機目錄), 管理員 39
- 密碼長度下限 84
- 密碼原則 84
- 密碼提醒通知 84
- 密碼歷程記錄, 設定 84
- 授權核准 95
- 啟用 AirWatch 憑證授權機構 117
- 啟用合規檢查 124
- 啟用持續性 Cookie 75
- 啟用授權核准 95
- 啟用整合目錄 108
- 第三方身分識別提供者 64
- 規則 74
- 設定, 目錄 92
- 設定 AirWatch 105
- 設定 AirWatch 整合 108
- 設定 iOS 裝置設定檔 115
- 設定 RSA 調適性驗證 56
- 通道, AirWatch 119
- 連接器, 啟動代碼 10

十二劃

- 單一登出, 身分識別提供者 64
- 單一樹系 Active Directory 15
- 報告
 - 角色 98
 - 裝置使用量 98
 - 資源活動 98
- 智慧卡, 設定 59
- 智慧卡憑證授權機構 58
- 智慧卡憑證撤銷 58
- 智慧卡驗證 58
- 登入的使用者, 數目 97
- 登入頁面, 自訂 101

十三劃

- 匯出 AirWatch 憑證授權機構 117
- 新增 Web 應用程式 89
- 新增本機使用者 82, 83
- 新增至 Active Directory 22
- 新增身分識別提供者按鈕 64
- 新增群組 80
- 概念證明 64
- 概觀, 身分識別和存取管理設定 10
- 群組
 - Active Directory 77
 - 工作區 80
 - 成員資格報告 98
 - 授權資源 80, 82
 - 新增 80
 - 新增使用者 80
- 群組名稱 78, 79
- 群組成員資格報告 98
- 群組關聯, 使用者 79
- 裝置使用量報告 98
- 資料庫, 監控 98
- 資源
 - 使用中的類型百分比 97
 - 授權 82
 - 授權核准 95
 - 授權給群組 80
 - 類別 90, 91
- 資源使用報告 98
- 資源活動報告 98
- 資源權利報告 98

十四劃

- 撤銷檢查, 智慧卡 58
- 疑難排解 domain_krb.properties 20
- 監控工作區健全狀況 98
- 管理主控台 9
- 管理員, 驗證 39
- 管理索引標籤說明 9
- 網域 21
- 網路範圍, 與存取原則的關係 69, 73, 74
- 與 Active Directory 整合 15
- 遠端應用程式存取, 用戶端 93

十五劃

- 儀表板 97
- 標誌, 新增 101
- 稽核事件報告 99
- 適用於 Kerberos 的瀏覽器 49

十六劃

- 憑證授權機構, 智慧卡 58

整合 AirWatch 105

整合目錄, 為 AirWatch 啟用 109

整合式 Windows 驗證 22

頻外驗證 56

應用程式

- Web 88

- 行動 88

- 類別 92

應用程式受歡迎度 97

應用裝置狀態 98

十七劃

檢視使用者資訊 79

十八劃

瀏覽管理主控台 9

瀏覽器, 支援的 9

雙因素驗證 60

十九劃

類別

- 刪除 92

- 建立 91

- 套用 91

- 移除 91, 92

二十一劃

屬性

- 預設值 20

- 對應 21

二十二劃

權利, 使用者 79

二十三劃

變更 Active Directory 密碼 26

變更 AD 密碼 26

驗證

- RADIUS 54

- 為 Android 應用程式啟用個別應用程式
VPN 122

驗證, Android 版 Mobile SSO 118

驗證, Android 設定檔 121

驗證, AirWatch 密碼 63

驗證; AirWatch Cloud Connector 110

驗證方法

- RSA 調適性驗證 56

- 新增至原則 67

- 與存取原則的關係 69, 73, 74

驗證方法順序 67

驗證錯誤訊息 74

驗證鏈結 69