VMware Identity Manager 管理指南 (雲端)

2019 年 4 月

VMware Identity Manager

vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

VMware 網站也提供最新的產品更新。

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

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

Copyright © 2015 – 2019 VMware, Inc. 保留所有權利。 版權與商標資訊。

目錄

VMware Identity Manager 管理 (雲端)

《VMware Identity Manager 管理指南》提供如何透過 VMware Identity Manager™ 服務來使用及維護承租人的相關資訊和指示。

您在 VMware Identity Manager 主控台中執行的初始工作，即設定與 Active Directory 的目錄同步、設定使用者用來登入其 Workspace ONE 應用程式入口網站的驗證方法，以及將您的自訂品牌套用至站台。初始設定完成後，您所執行的主要工作將是授權使用者使用資源。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。

您所管理的實際資源類型會根據組織的需求而有所不同。若要授權某個資源類型，您必須先依照《設定資源指南》中的說明執行預先設定工作。

主要對象

這些資訊適用於要設定和管理其 VMware Identity Manager 承租人的任何人。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。若您計劃實作這些功能，瞭解 VMware Horizon® 7、Horizon® Cloud 和 Citrix 應用程式虛擬化等其他技術，以及 RSA SecurID 之類的驗證方法也將有所幫助。

在 VMware Identity Manager 主控台中工作 1

VMware Identity Manager™ 主控台為您提供了集中的管理主控台，讓您可在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 Workspace ONE UEM 整合，以及設定和管理驗證與存取原則。

您在 VMware Identity Manager 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。

本章包含以下主題：

在 VMware Identity Manager 主控台中導覽

VMware Identity Manager 主控台中的工作會依索引標籤進行整理。

如果您擁有管理員權限。您可以從 Workspace ONE 入口網站頁面登入 VMware Identity Manger 主控台。若要直接登入至主控台，VMware Identity Manager 管理員使用者可以輸入下列 URL `<example.com>/SAAS/login/0`。此時會顯示使用者名稱和密碼畫面。

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活動和使用的資源。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。 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 應用程式及管理現有的資源。在 [虛擬應用程式集合] 頁面中，您可以管理 Horizon、Citrix、Horizon Cloud 和 ThinApp 桌面平台與應用程式整合。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。

索引標籤	說明
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 Workspace ONE UEM 整合、設定驗證方法，以及將自訂品牌套用至登入頁面和 VMware Identity Manager 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。
角色	在 [角色] 索引標籤中，您可以管理「管理員」角色。使用者可指派為三個預先定義之管理員角色的管理員，您也可以在 VMware Identity Manager 主控台中建立自訂管理員角色，以給予特定服務的有限權限。

支援存取 VMware Identity Manager 主控台的網頁瀏覽器

VMware Identity Manager 主控台是可讓您用來管理承租人的 Web 型應用程式。您可以從最新版本的 Mozilla Firefox、Google Chrome、Safari、Microsoft Edge 和 Internet Explorer 11 存取 VMware Identity Manager 主控台。

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。

使用者的 Workspace ONE

使用者可從其 Workspace ONE 入口網站存取其有權使用的資源。Workspace ONE 是使用者透過瀏覽器存取及使用其有權使用的資源時所使用的預設介面。

Workspace ONE UEM 與 VMware Identity Manager 整合後，使用者將可看見他們有權使用的所有應用程式。內部開發或在應用程式商店中公開提供的原生應用程式，將可透過 Workspace ONE 入口網站提供給您的使用者使用。

身分識別與存取管理設定概觀

在 VMware Identity Manager 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 VMware Identity Manager 主控台的品牌。

以下將說明 [身分識別與存取管理] 索引標籤中的設定。

表格 1-1. 身分識別與存取管理設定

設定	說明
設定 > 連接器	[連接器] 頁面會列出您的企業網路內所部署的連接器。連接器可用來在您的企業目錄與服務之間同步使用者和群組資料。連接器在用作身分識別提供者時會向服務驗證使用者。 當您將某個目錄與連接器執行個體建立關聯時，連接器會為稱為 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。 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。 ■ 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 6 章，在 VMware Identity Manager 中設定使用者驗證。 ■ 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。 ■ 在 [關聯的目錄] 資料行中，存取與此 Worker 相關聯的目錄。 您必須先按一下 [新增連接器] 來產生啟動碼才能新增連接器。您必須在安裝精靈中貼上此啟動碼，以建立與連接器的通訊。
設定 > 自訂品牌	在 [自訂品牌] 頁面中，您可以自訂 VMware Identity Manager 主控台標頭和登入畫面的外觀。請參閱在 VMware Identity Manager 服務中自訂品牌。 若要自訂使用者 Web 入口網站、行動裝置和平板電腦等視圖，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。
設定 > 使用者屬性	[使用者屬性] 頁面會列出目錄中同步的預設使用者屬性。您可以新增與 Active Directory 屬性對應的其他屬性。請參閱《目錄與 VMware Identity Manager 的整合》指南。
設定 > 自動探索	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。
設定 > AirWatch	在此頁面上，您可以設定與 Workspace ONE UEM 的整合。在整合設定並儲存後，您可以啟用整合目錄，將設定於 Workspace ONE 目錄中的應用程式合併到整合目錄，您也可以啟用符合性檢查，以確認受管理的裝置符合 Workspace ONE UEM 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 VMware Workspace ONE 部署指南。
設定 > 喜好設定	[喜好設定] 頁面會顯示管理員可啟用的功能。此頁面包括下列喜好設定。 ■ 可以啟用 [在登入頁面顯示系統網域]。 ■ 持續性 Cookie 可從這個頁面啟用。請參閱啟用持續性 Cookie。 ■ 當您不想要求使用者在登入前選取其網域時，請啟用 [隱藏網域下拉式功能表]。 ■ 選取 [使用者登入唯一識別碼] 選項，以顯示以識別碼為基礎的登入頁面。請參閱第 5 章，管理使用者登入體驗 ■ [自訂登入輸入提示] 可用來自訂登入畫面上使用者文字方塊中的提示。
[設定] > [使用條款]	在此頁面上，您可以設定 Workspace ONE 使用條款，並確定使用者必須接受這些使用條款才能使用 Workspace ONE 入口網站。

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。

表格 1-2. 身分識別與存取管理的管理設定

設定	說明
管理 > 目錄	[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。 請參閱《目錄與 VMware Identity Manager 的整合》指南。 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。 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。
管理 > 身分識別提供者	[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。VMware Identity Manager 內建身分識別提供者可設定為用於驗證。 請參閱新增和設定身分識別提供者執行個體。
管理 > 密碼恢復助理	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。
[管理] > [驗證方法]	[驗證方法] 頁面可用來設定能夠與內建身分識別提供者建立關聯的驗證方法。在此頁面上設定驗證方法後，您可以在內建身分識別提供者頁面中建立驗證方法的關聯。
管理 > 原則	[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。您可以設定要用來允許使用者透過 IP 位址進行存取的網路範圍。 原則是一組規則集，用於指定使用者存取其 Workspace ONE 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 7 章，管理存取原則。

管理管理員角色

2

VMware Identity Manager 會使用角色型存取控制來管理「管理員」角色。透過角色型存取控制，您可以建立功能角色，用以控制管理員對 VMware Identity Manager 主控台中各項工作的存取，以及將角色指派給一或多個使用者和群組。

VMware Identity Manager 服務中會內建三個預先定義的管理員角色。您可以將這些預先定義的角色指派給服務中的使用者和群組。您無法修改或刪除這些角色。

您也可以在 VMware Identity Manager 主控台中建立自訂管理員角色，以給予特定服務的有限權限。在服務中，可選取特定作業作為可在角色中執行的動作類型。

本章包含以下主題：

關於角色型存取角色

在 VMware Identity Manager 伺服器中可授與下列類型的角色

三個預先定義的管理員角色說明如下。

- 超級管理員角色可存取及管理 VMware Identity Manager 服務中的所有特性和功能。

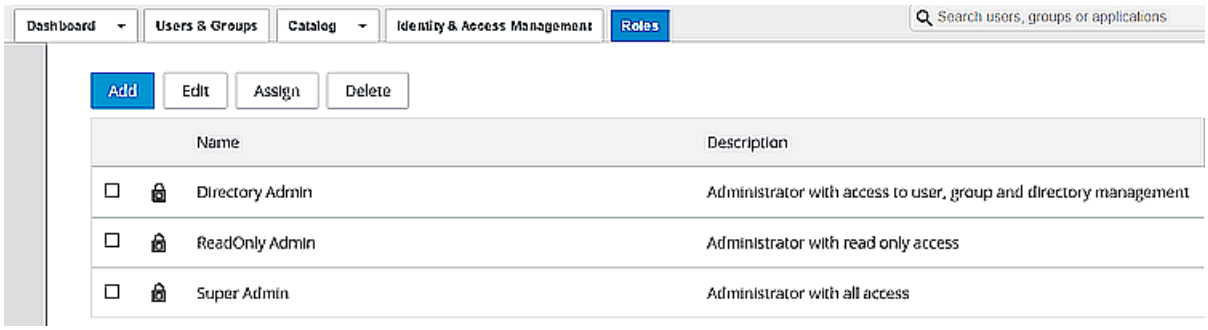
  第一個超級管理員是 VMware Identity Manager 在您第一次設定服務時所建立的本機管理員使用者。服務會在系統目錄的系統網域中建立管理員。您可以在系統目錄中將其他使用者指派給超級管理員角色。最佳做法是為選定的少數幾人授與超級管理員角色。

- 唯讀管理員角色可檢視 VMware Identity Manager 主控台頁面中的詳細資料 (包括儀表板和報告)，但無法進行變更。所有管理員角色皆會自動指派唯讀角色。

  備註 僅具備唯讀角色權利的管理員無法檢視部分 Identity Manager 主控台頁面。當唯讀管理員嘗試檢視這些頁面時，系統會將其重新導向至儀表板。

- 目錄管理員角色可管理使用者、群組和目錄。目錄管理員可管理組織中企業目錄與與本機目錄的目錄整合。目錄管理員也可管理本機使用者和群組。

圖 2-1：VMware Identity Manager 主控台中的 [角色] 索引標籤



您可以將這些預先定義的角色指派給服務中的使用者和群組。您無法修改或刪除這些角色。

您也可以在 VMware Identity Manager 主控台中建立自訂管理員角色，以給予特定服務的有限權限。在服務中，可選取特定作業作為可在角色中執行的動作類型。

多個角色可指派給相同的使用者和群組。一個使用者被指派多個角色時，套用的角色行為會累加。例如，如果有一個管理員被指派兩個角色，一個具有原則管理的寫入權限，而另一個則無，則該管理員將有權修改原則。

您可以設定角色型存取控制，以便在管理員主控台中管理下列服務。

服務類型	服務說明
目錄	「目錄」是可授權給使用者之所有 Workspace ONE 資源的存放庫。 「目錄」服務可管理下列類型的動作。 ■ Web 應用程式 ■ 應用程式來源 ■ 第三方應用程式 ■ ThinApp 虛擬應用程式集合 ■ 包含 Horizon、Horizon Cloud 和 Citrix 型應用程式的虛擬應用程式集合。 **備註** 「開始使用」流程必須由超級管理員在 [目錄] 中的 [虛擬應用程式集合] 頁面中起始。在初始的「開始使用」流程之後，擁有「目錄」服務的管理員角色即可管理 ThinApp 套件和桌面平台應用程式。請參閱《在 VMware Identity Manager 3.2 中設定資源》指南中的〈使用虛擬應用程式集合進行桌面平台整合〉。
目錄管理	「目錄管理」服務可為組織或組織中的特定目錄管理下列類型的動作。 ■ 企業目錄。管理員可新增、編輯及刪除服務中的目錄。目錄的編輯包括管理目錄設定，其中包括同步設定。 ■ 本機目錄。管理員可建立、編輯及刪除本機目錄。目錄的編輯包括管理設定，以及建立、編輯和刪除本機使用者和群組。 當角色中包含「目錄管理」服務時，您也必須在該角色中設定「身分識別與存取管理」服務。
使用者和群組	「使用者和群組」服務可為整個組織或組織中的特定網域管理下列類型的動作。 ■ 群組 ■ 使用者 ■ 本機使用者的密碼重設

服務類型	服務說明
權利	「權利」服務可將使用者指派給 Web 和虛擬應用程式。 可管理的權利動作類型如下。對於以下每個動作，您都可以設定角色，以便將使用者和群組指派給組織中的所有資源，或指派給特定應用程式。您也可以為特定網域內的使用者和群組賦予應用程式的權利。 ■ Web 權利 ■ 第三方權利
角色管理	「角色管理」服務可管理對使用者的管理員角色指派。 當您建立具有「角色管理」服務的角色時，必須設定「使用者和群組」服務，並選取「管理使用者」和「管理群組」動作。 受指派此角色的管理員可將使用者和群組升階為管理員角色，並且可從使用者或群組中移除管理員角色。
身分識別與存取管理	「身分識別與存取管理」服務可管理 [身分識別與存取管理] 索引標籤中的設定。若要管理目錄設定，則也需要「目錄管理」服務。 **備註** 具有身分識別與存取管理角色的管理員可以整合 VMware Identity Manager 與 Workspace ONE UEM，以及從 Workspace ONE UEM Console 建立目錄。

當您新增角色時，可以選取服務，並定義可在服務中執行的動作。在某些服務中，您可以為選定的動作選取要管理所有資源，或管理部分資源。

管理唯讀存取權

每個指派給管理員的角色都會被授與唯讀存取權。您也可以從 [唯讀管理員角色] 頁面將使用者和群組指派給唯讀角色。

唯讀管理員角色可為使用者管理員提供檢視 VMware Identity Manager 主控台的存取權，但除非管理員被指派了擁有額外存取權的其他角色，否則他們僅能檢視 VMware Identity Manager 主控台中的內容。

如果您是以個別角色的形式指派唯讀角色，則可以從 [唯讀管理員角色指派] 頁面或從使用者或群組設定檔頁面中移除該角色。

新增管理員角色

透過角色型存取控制，您可以建立用來管理一個動作或多個動作的角色。

當您建立角色時，可以將一或多個服務新增至該角色。您可以為角色命名、選取服務的類型，並選取角色可在服務中管理的特定動作。

- 當您建立具有「目錄管理」服務的角色時，也必須在該角色中設定「身分識別與存取管理」服務。
- 當您建立具有「角色管理」服務的角色時，也必須使用動作來設定「使用者和群組」服務，以便管理使用者和選取的群組。

先決條件

若要建立角色，您必須是超級管理員，或是已被指派角色、且該角色設定了「角色管理」服務的管理員。

程序

1 在 VMware Identity Manager 主控台的**角色**索引標籤中，按一下**新增**。

2 在**角色名稱**文字方塊中輸入描述性的角色名稱，並新增說明。

您的環境中的每個角色名稱皆必須是唯一的。

3 按**下一步**。

4 選取要由此角色管理的服務。

5 在**動作**下拉式功能表中，選取可管理的動作類型。

6 選取**所有**資源以管理動作內的所有資源，或選取**部分**，然後從 [條件] 下拉式功能表中選取可管理的條件。

7 若要新增要由此角色管理的其他動作，請按一下 **+** 並完成設定動作。

8 按一下**儲存**。

[服務] 頁面會顯示您設定的組態。

9 如果您想要將其他服務新增至此角色，請選取服務，然後完成設定步驟 5 至 8。

10 完成後，請按一下 [組態] 頁面上的**儲存**。

後續步驟

將此角色指派給使用者，使其成為此服務的管理員。

將使用者和群組指派給 VMware Identity Manager 管理員角色

VMware Identity Manager 超級管理員或是包含角色管理員服務以及使用者和群組服務的角色，可以將角色指派給使用者和群組，以將其提升為該角色的管理員。

先決條件

- 在將 Identity Manager 管理員角色新增至從 Workspace ONE UEM 目錄同步的使用者之前，請務必在 Workspace ONE UEM 主控台中使用**管理員使用者升級**帳戶來設定使用者設定檔。

  擁有「管理員使用者升級」帳戶的使用者同步至 VMware Identity Manager 時會被識別為管理員，並且可在 VMware Identity Manager 中被指派角色。如果管理員不在 UEM 主控台的此帳戶中，則在 Workspace ONE UEM 目錄與 VMware Identity Manager 目錄同步時，管理員角色將會從使用者設定檔中移除。

程序

1 在 VMware Identity Manager 主控台的**角色**索引標籤中選取角色，然後按一下**指派**。

2 在搜尋方塊中輸入名稱，然後選取使用者或群組。

只有群組中的使用者數目不到 500 人的群組可以升級至管理員角色。

3 按一下**儲存**。

使用者或群組會成為該角色的管理員。使用者設定檔頁面會更新以顯示該角色。

移除管理員角色

管理員角色可從特定角色的 [指派] 頁面撤銷。您可以從使用者的設定檔頁面撤銷所有指派給該使用者的角色。

您可以從角色移除群組，以及為所有群組成員撤銷該角色。您無法從特定群組的成員移除角色。若只要從角色移除使用者，您可以從群組中移除使用者。

移除個別使用者的管理員角色

超級管理員或角色管理員可從角色移除管理員使用者。

您可以從 [使用者和群組] 索引標籤中的使用者設定檔頁面開始撤銷角色。從設定檔頁面開始作業時，您會在按一下連結以移除角色後重新導向至 [角色] 頁面。

備註 管理員角色可以直接從角色的 [指派] 頁面撤銷。

程序

1 在 VMware Identity Manager 主控台的 **使用者和群組**索引標籤中選取**使用者**，然後選取使用者名稱。

在 [設定檔] 頁面中，[角色] 資料列會列出所有指派給此使用者的角色。

2 在**角色**資料列中，按一下**這裡**。

您會重新導向至 [角色] 頁面。

3 選取角色，然後按一下**指派**。

4 按一下名稱旁的 **X**。

5 按一下**儲存**。

使用者會從角色移除，而角色會從使用者設定檔中移除。

從角色移除群組

當您從角色移除群組時，該群組所有成員的存取權都會被撤銷。使用者和群組設定檔頁面的 [角色] 區段會隨之更新以移除角色。

您無法從角色移除群組的個別成員。若要從角色移除群組的成員，請從群組中移除使用者。

如果群組中的使用者已直接指派給角色，則在從角色移除該群組時，該使用者將維持管理員角色。

備註 群組管理員角色可以直接從角色的 [指派] 頁面撤銷。

程序

1 在 VMware Identity Manager 主控台的 **使用者和群組**索引標籤中選取**群組**，然後選取群組名稱。

在 [設定檔] 頁面中，[角色] 資料列會列出所有指派給此群組的角色。

2 在**角色**資料列中，按一下**這裡**。

您會重新導向至 [角色] 頁面。

3 選取角色，然後按一下**指派**。

4 按一下群組名稱旁的 **X**。

5 按一下**儲存**。

該群組會從角色中移除。角色會從群組設定檔和每個成員設定檔中移除。

範例：從角色移除群組的範例

包含 User1、User2 和 User3 的群組 A 會指派給目錄管理員角色。群組 A、User1、User2 和 User3 設定檔隨即更新，以反映其設定檔頁面中的目錄管理員角色。

User2 也會直接指派給目錄管理員角色。

您撤銷了對群組 A 的存取。群組 A、User1 和 User3 都會從該角色中移除，而該角色則會從這些設定檔頁面中移除。

由於 User2 已直接指派給目錄管理員角色，因此 User2 仍會指派給目錄管理員角色。

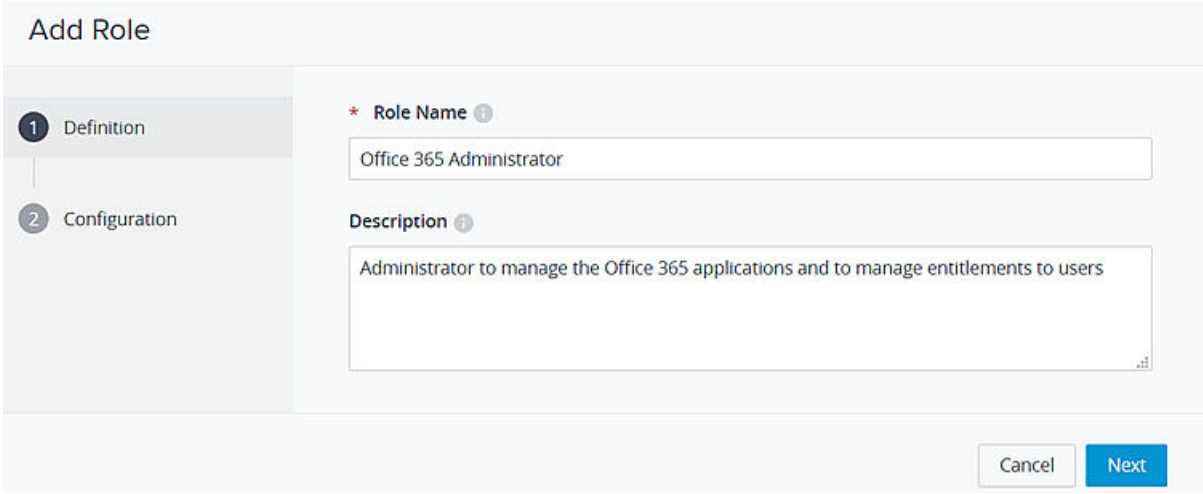
範例 1.建立用來管理 Office 365 應用程式和權利的角色

透過角色型存取控制，您可以為使用者和群組授與管理員存取權，讓他們能夠管理特定的應用程式。

例如，超級管理員可以將在 Workspace ONE 中管理 Office 365 應用程式的日常工作委派給其他管理員。您需要建立一個管理員角色來管理 Workspace ONE 中的 Office 365，以及管理應用程式權利。

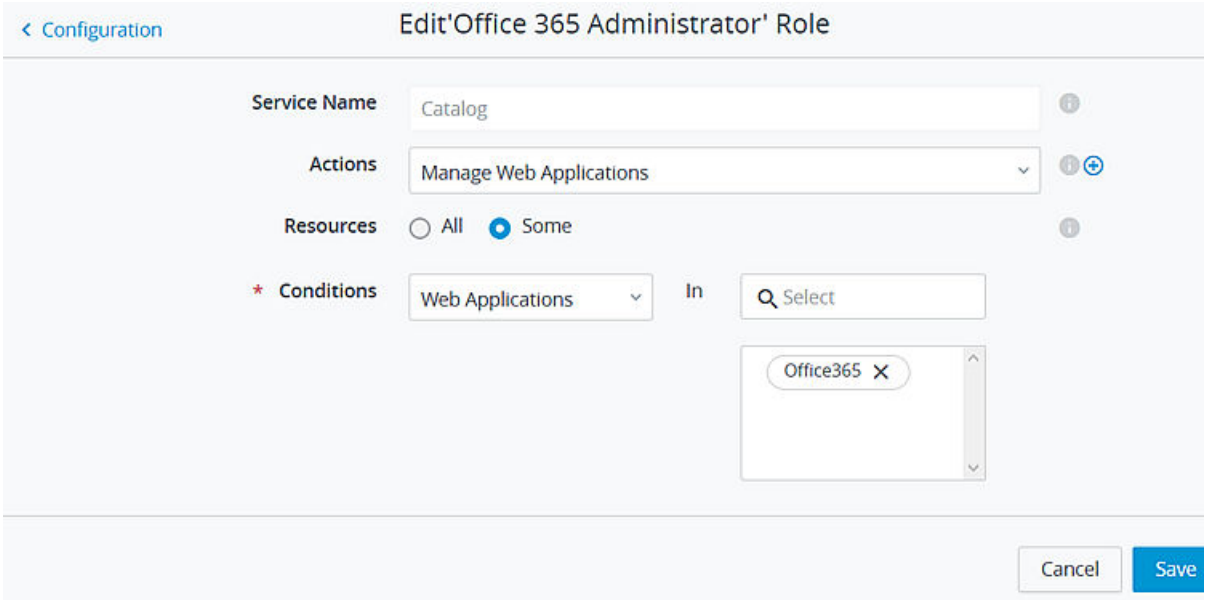
程序

1 在 VMware Identity Manager 主控台的 [角色] 頁面中，按一下**新增**。建立描述性的角色名稱，並說明角色的用途。按**下一步**。



2 在 [組態] 頁面中，選取「目錄」服務。針對**動作**，選取**管理 Web 應用程式**。針對**資源**，選取**部分**。針對**條件**，選取 **Web 應用程式**，然後在搜尋方塊中輸入 **Office 365**。**儲存**組態。

您可以新增其他要管理的應用程式。例如，您可以搜尋 SalesForce，並將其新增至要在此角色中管理的 Web 應用程式清單。



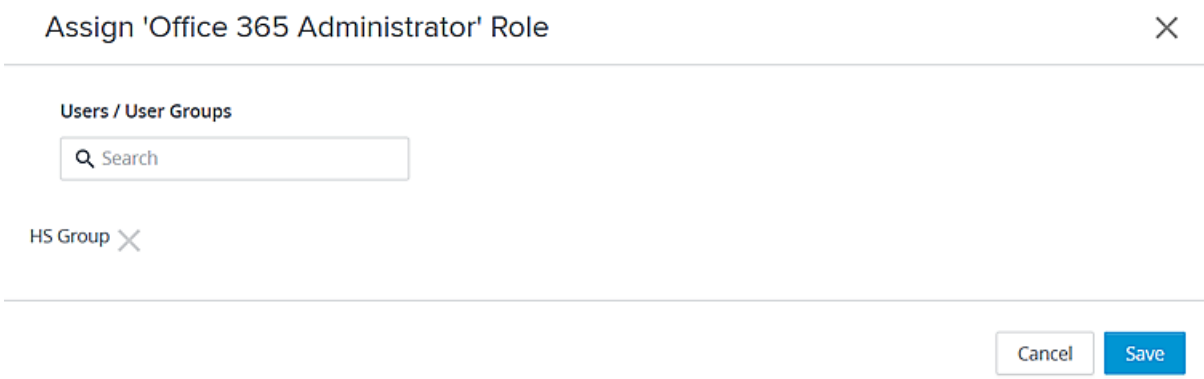
3 同樣地，在 [組態] 頁面上選取**權利**服務。針對**動作**，選取**管理 Web 權利**。針對**資源**，選取**部分**。針對**條件**，選取**應用程式**，然後在搜尋方塊中輸入 **Office 365**，以選取相同的應用程式。**儲存**組態。

如果您已在「目錄服務」中新增另一個應用程式，而想要讓管理員管理權利，請確保將該應用程式新增至此處。

4 在 [組態] 頁面上，再按一次**儲存**。

管理 Office 365 應用程式的角色隨即建立，且會在 [角色] 頁面上列出。

5 選取您所建立的角色，然後按一下**指派**。在**搜尋**文字方塊中，輸入應被授與存取權的使用者或群組名稱。選取使用者或群組，然後按一下**儲存**。



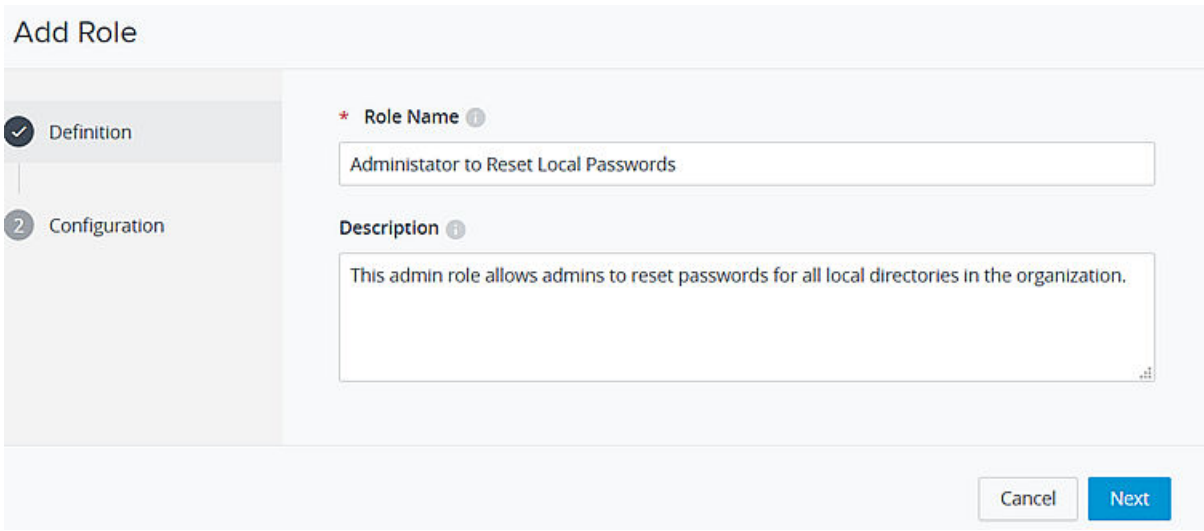
使用者或群組現在已是此角色的管理員。設定檔頁面會更新以顯示已指派的管理員角色。

範例 2.建立角色以管理本機目錄中的密碼重設

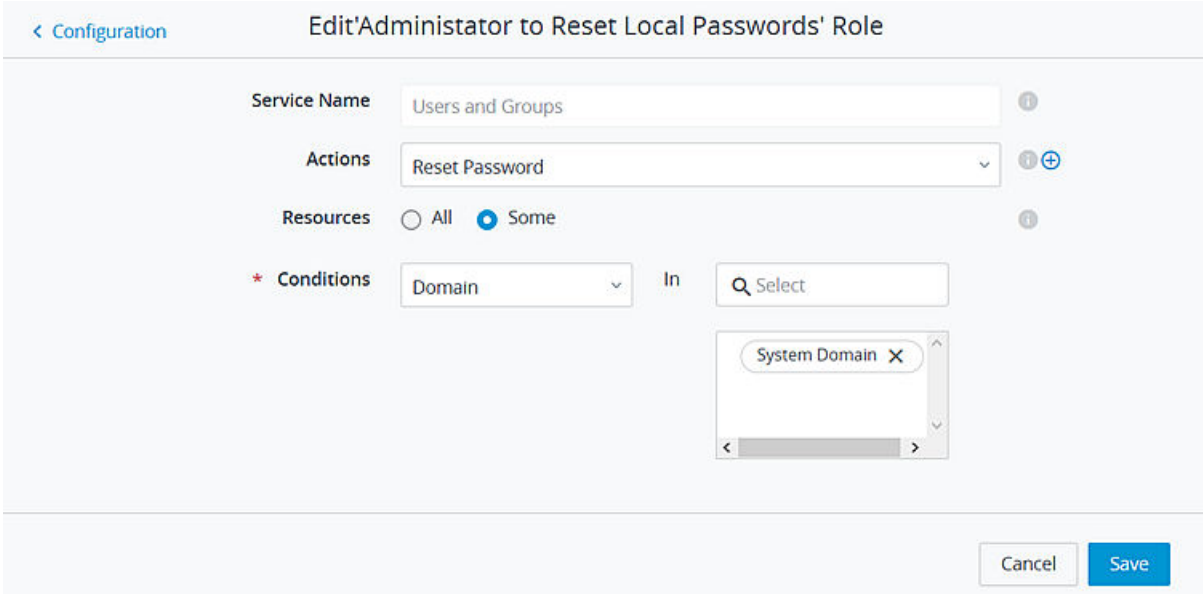
您可以建立簡單的管理員角色，以管理特定網域的密碼重設。

程序

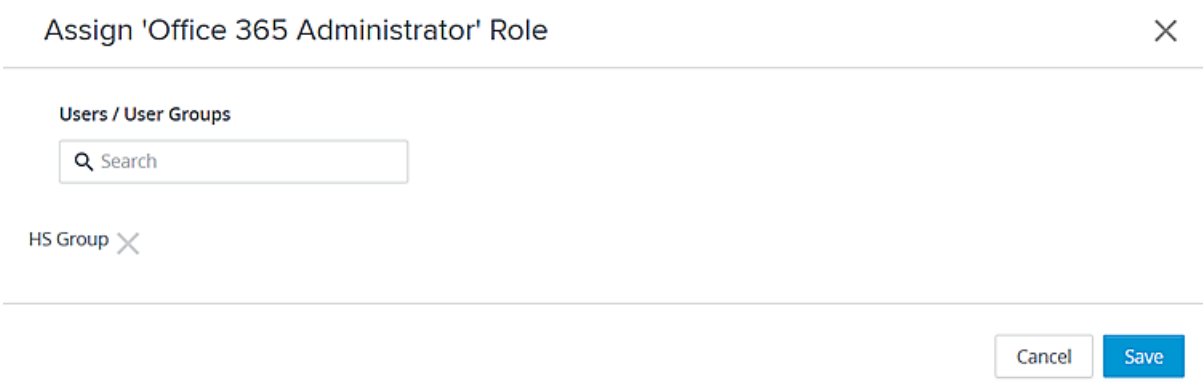
1 在 VMware Identity Manager 主控台的 [角色] 頁面中按一下**新增**、輸入描述性的角色名稱，並說明角色的用途。按**下一步**。



2 在 [組態] 頁面中，選取**使用者和群組**服務。針對**動作**，選取**重設密碼**。針對資源，選取**部分**。針對**條件**，選取本機網域，然後在搜尋方塊中輸入本機目錄名稱以選取本機目錄。**儲存**組態。



3 選取您所建立的角色，然後按一下**指派**。在**搜尋**文字方塊中，輸入使用者或使用者群組名稱。選取使用者或群組，然後按一下**儲存**。



使用者或群組現在已是此角色的管理員。設定檔頁面會更新以顯示已指派的管理員角色。

使用本機目錄

3

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」。您也可以建立其他本機目錄。

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。此目錄會使用名為「系統網域」的網域。您無法變更系統目錄的目錄或網域名稱，或是為其新增網域。您也無法刪除系統目錄或系統網域。

第一次設定承租人時，會在系統目錄的系統網域中建立本機管理員使用者。您在取得新承租人時所收到的認證，即屬於此本機管理員使用者。

您可以將其他本機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

除了系統目錄以外，您也可以建立其他本機目錄。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。

您可以選取本機使用者所需的使用者屬性。userName、lastName、firstName 和 email 等使用者屬性會指定於 VMware Identity Manager 服務的全域層級上，且皆為必要屬性。全域使用者屬性會套用至服務中的所有目錄。在本機目錄層級上，您可以選取目錄所需的其他屬性。選取其他屬性可讓您為每個本機目錄建立一組自訂屬性。

在下列情況下，使用自訂的對應屬性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，您可以為合作夥伴建立本機目錄，並僅為合作夥伴提供其所需之特定應用程式的存取權。
- 如果您想將不同的使用者屬性或驗證方法用於不同組的使用者，可以建立不同的本機目錄。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。在建立本機目錄之後，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多個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都可在使用者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〉。

本章包含以下主題：

- 建立本機目錄
- 變更本機目錄設定
- 刪除本機目錄
- 設定系統管理員使用者的驗證方法

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 3-1. 無法用作自訂屬性名稱的文字

active	addresses	costCenter
department	displayName	division
emails	employeeNumber	entitlements
externalId	groups	id
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 VMware Identity Manager 主控台中，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**。

後續步驟

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

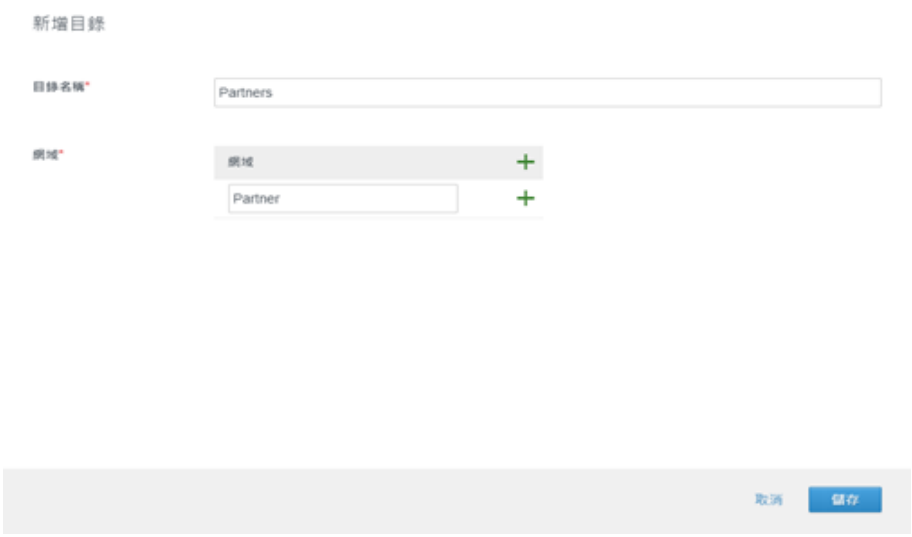
1 在 VMware Identity Manager 主控台中，按一下**身分識別與存取管理**索引標籤，然後按一下**目錄**索引標籤。

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：



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。

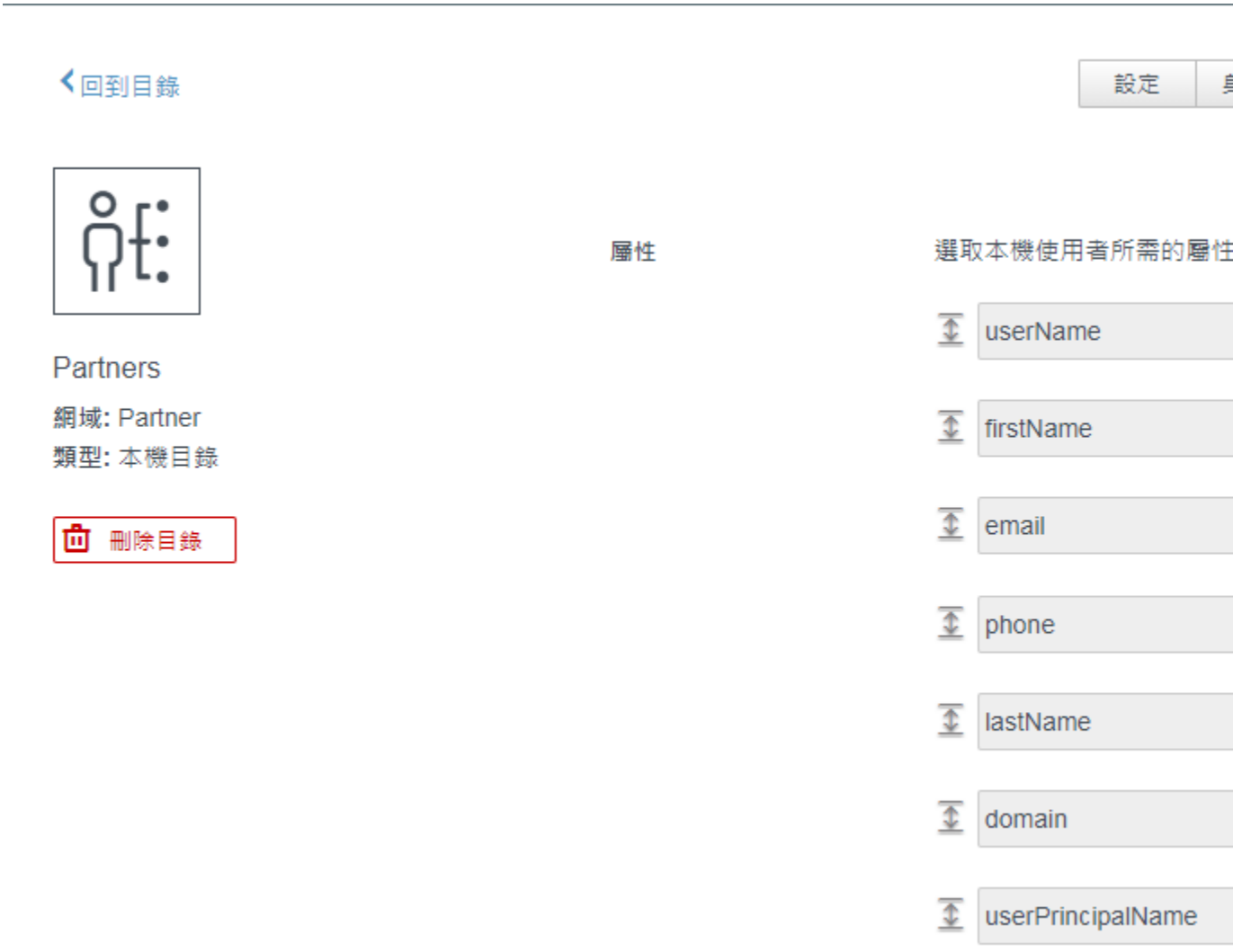
您可以指定哪些屬性是必要的，而哪些屬性是選用的。您也可以變更屬性的顯示順序。

重要 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：



8 按一下**儲存**。

後續步驟

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。

先決條件

必須在 [身分識別與存取管理] > [驗證方法] 頁面中設定密碼 (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 Workspace ONE UEM 管理的 iOS 裝置設定行動 SSO，否則不需要下載憑證。

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。

後續步驟

建立本機使用者和群組。您可以在 Identity Manager 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	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	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	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**。

選項	動作
使屬性成為目錄的必要或選用屬性	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	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。

注意　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所輸入的預設驗證方法為「密碼 (本機目錄)」。預設存取原則包含將「密碼 (本機目錄)」設定為後援方法的原則規則，讓管理員可登入 VMware Identity Manager 主控台和 Workspace ONE 入口網站。

當您為系統管理員角色有權使用的特定 Web 和桌面平台應用程式建立存取原則時，請在原則中設定規則，將「密碼 (本機目錄)」納入為後援驗證方法。否則，管理員將無法登入應用程式。

Just-in-Time 使用者佈建

4

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。

本章包含以下主題：

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。

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 VMware Identity Manager 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。

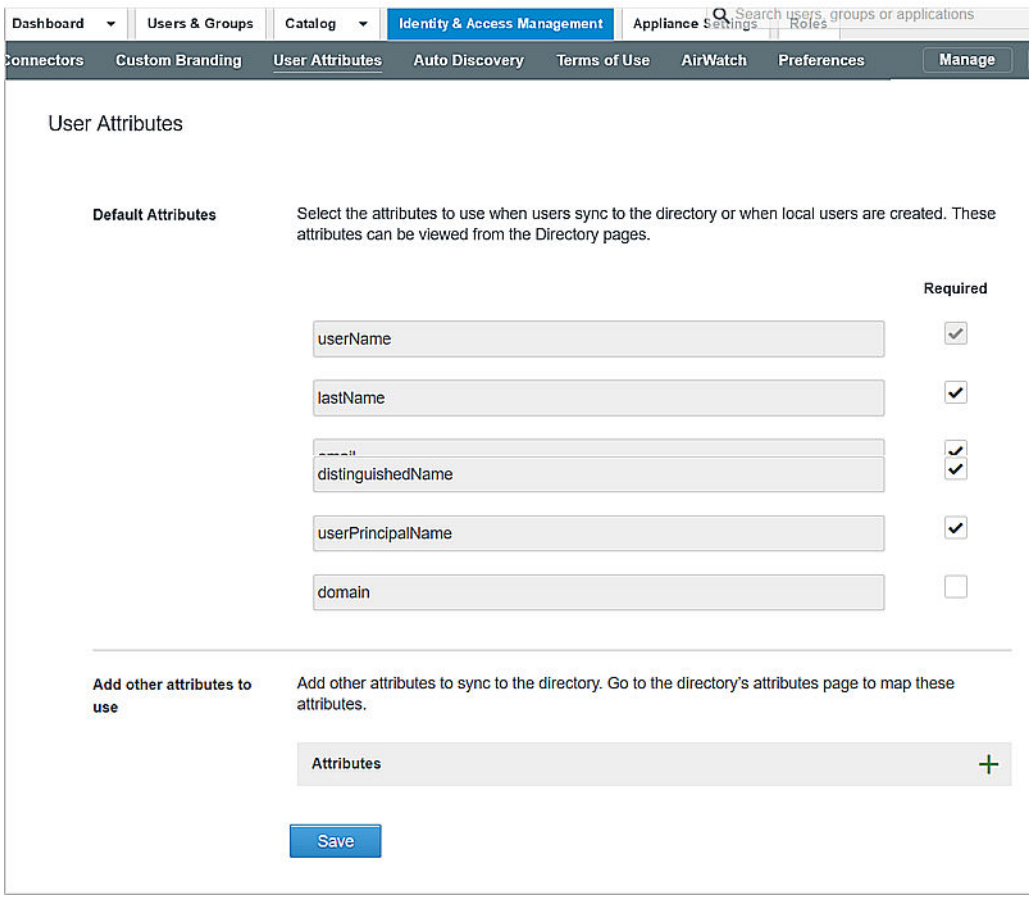
重要 如果屬性在 [使用者屬性] 頁面上標示為必要，SAML 宣告必須包含該屬性，否則登入會失敗。

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。



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 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 網域名稱在承租人中所有目錄間必須是唯一的。

  例如：

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。

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 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 VMware Identity Manager 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 VMware Identity Manager 主控台中，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 VMware Identity Manager 主控台可能出現的錯誤。

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。	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。 1 在 VMware Identity Manager 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**。 Just-in-Time 目錄隨即建立。

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：*name*。	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。
網域遺漏且無法推斷。	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： ■ 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。 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。 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。
屬性名稱：*name*、值：*value*。	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。
無法建立或更新 `JIT` 使用者。	使用者無法建立於服務中。可能的原因包括： ■ SAML 判斷提示中遺漏必要屬性。 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。 ■ 無法判斷使用者的網域。 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。

管理使用者登入體驗

5

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。從 VMware Identity Manager 登入 Workspace ONE 入口網站之使用者的預設體驗，即為在顯示的第一個登入頁面上選取他們所屬的網域。

由於使用者會先選取其網域，因此具有相同使用者名稱但位於不同網域的使用者可以成功登入。例如，您可以在網域 eng.example.com 中擁有使用者 jane，且在網域 sales.example.com 中擁有另一個使用者 jane

VMware Identity Manager 會根據為該網域設定的存取原則規則顯示驗證頁面。

本章包含以下主題：

登入時選取網域

依預設會在 [身分識別與存取管理] > [設定] > [喜好設定] 頁面上啟用**在登入頁面上顯示系統網域**設定。使用者會看見網域下拉式選取項目功能表，其中會列出所有與 VMware Identity Manager 伺服器和本機系統網域整合的 Active Directory 網域。

如果您取消 [在登入頁面上顯示系統網域] 設定，則會從網域下拉式功能表中移除 [系統網域] 項目。當 VMware Identity Manager 服務中包含單一 Active Directory 網域時，使用者將不會看見下拉式功能表。系統會提示使用輸入認證以進行登入。

當系統網域未顯示於下拉式功能表中時，VMware Identity Manager 管理員使用者可輸入下列 URL 來登入 VMware Identity Manager 主控台：**<example.com>/SAAS/login/0**。此時會顯示使用者名稱和密碼畫面。

使用唯一識別碼的登入體驗

如果您不想要求使用者在登入之前選取其網域，您可以隱藏網域要求頁面。您稍後需要選取唯一識別碼才能區分組織中的使用者。

使用者登入時，系統會顯示一個頁面以提示使用者輸入其唯一識別碼。VMware Identity Manager 會嘗試在內部資料庫中尋找使用者。當 VMware Identity Manager 服務查閱識別碼時，找到的資訊會包含使用者所屬的網域。顯示的驗證頁面會以該網域的存取原則規則為準。

唯一識別碼可以是使用者名稱、電子郵件地址、UPN 或員工識別碼。您可以在 [身分識別與存取管理] > [喜好設定] 頁面中選取所要使用的識別碼。唯一識別碼屬性必須對應於 [使用者屬性] 頁面，且必須從 Active Directory 進行同步。

如果找到多個符合識別碼的使用者，且無法判斷唯一使用者，則會顯示錯誤訊息。若未找到任何使用者，則會顯示本機使用者登入頁面，以避免可能的使用者名稱列舉攻擊。

設定以唯一識別碼為基礎的登入

當使用者採用使用者名稱和密碼驗證方法時，您可以啟用唯一識別碼選項，以顯示以識別碼為基礎的登入頁面。系統會要求使用者輸入其唯一識別碼，接著要求根據設定的存取原則規則輸入適當的驗證。

支援以唯一識別碼為基礎之登入的驗證方法，包括密碼驗證方法、RSA SecurID 和 RADIUS。

先決條件

- 在 [身分識別與存取管理] > [使用者屬性] 頁面中，選取要使用的唯一識別碼使用者屬性。確定該屬性僅用來識別唯一物件。
- 確定選取的屬性已同步至目錄。
- 確認以識別碼為基礎的登入可供使用時，使用者網域的預設存取原則規則會反映出要使用的驗證類型。

程序

1. 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，按一下**喜好設定**。
2. 如果您要在單一網域環境中設定以唯一識別碼為基礎的登入，請啟用**在登入頁面上顯示系統網域**。

   僅在 VMware Identity Manager 中設定單一網域時才需要啟用此功能。
3. 若要隱藏網域選擇登入頁面，請選取**啟用**核取方塊。
4. 從下拉式功能表中選取要使用的唯一識別碼。選項為 VMware Identity Manager 雲端部署版本承租人的**使用者名稱**或**電子郵件**。內部部署服務也包含 **userPrincipalName** 和 **employeeID** 唯一識別碼選項。
5. 在**自訂登入輸入提示**文字方塊中，輸入要在登入畫面上使用者文字方塊中顯示的提示。

   如果此文字方塊為空白，則會顯示登入的唯一識別碼值。
6. 按一下**儲存**。

需要使用條款才能存取 Workspace ONE 目錄

您可以撰寫組織自有的 Workspace ONE 使用條款，並確定使用者必須接受此使用條款才能使用 Workspace ONE。

當使用者登入 Workspace ONE 後，即會顯示使用條款。使用者必須接受使用條款，才能繼續使用其 Workspace ONE 目錄。

使用條款功能包含下列組態選項。

- 建立現有使用條款的版本。
- 編輯使用條款。
- 建立可根據裝置類型來顯示的多個使用條款。
- 建立使用條款的語言特定複本。

您所設定的使用條款原則會在 [身分識別與存取管理] 索引標籤中列出。您可以編輯使用條款原則以修正現有原則或建立新版的原則。新增新版的使用條款即會取代現有的使用條款。編輯原則不會改變使用條款的版本。

您可以在使用條款頁面中檢視已接受或拒絕使用條款的使用者數量。按一下已接受或拒絕的數量以檢視使用者的清單及其狀態。

設定和啟用使用條款

在 [使用條款] 頁面中，您可以新增使用條款原則，以及設定使用量參數。新增使用條款後，您可以啟用 [使用條款] 選項。使用者登入 Workspace ONE 時必須接受使用條款才能存取其目錄。

先決條件

要複製並貼上至 [使用條款] 內容文字方塊中且以 HTML 格式化的使用條款原則文字。您可以新增英文、德文、西班牙文、法文、義大利文和荷蘭文的使用條款。

程序

1 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，選取**設定 > 使用條款**。

2 按一下**新增使用條款**。

3 輸入使用條款的描述性名稱。

4 如果使用條款原則適用於所有使用者，請選取**任何**。若要依裝置類型使用使用條款原則，請選取**選取裝置平台**，然後選取顯示此使用條款原則的裝置類型。

5 依預設，第一次顯示的使用條款會根據瀏覽器語言喜好設定來決定其語言。在文字方塊中輸入預設語言的使用條款內容。

6 按一下**儲存**。

若要新增其他語言的使用條款原則，請按一下**新增語言**，然後選取其他語言。[使用條款] 內容文字方塊會重新整理，然後您可以在文字方塊中新增文字。

您可以拖曳語言名稱以建立使用條款的顯示順序。

7 若要開始使用使用條款，請在顯示的頁面上按一下**啟用使用條款**。

後續步驟

如果您已針對使用條款選取特定的裝置類型，則可以為其他裝置類型建立額外的使用條款。

檢視使用條款的接受狀態

[身分識別與管理] > [使用條款] 頁面中所列出的使用條款原則會顯示已接受或拒絕原則的使用者數量。

程序

1 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，選取**設定 > 使用條款**。

2 在 [已接受]/[已拒絕] 資料行中，按一下左側的 [已接受] 數量，或右側的 [已拒絕] 數量。

狀態頁面會顯示採取的動作 (即已接受或已拒絕)，以及使用者名稱、裝置識別碼、檢視的原則版本、使用的平台以及日期。

3 按一下**取消**以關閉檢視。

在 VMware Identity Manager 中設定使用者驗證

6

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 服務搭配使用的身分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分識別提供者。您現有的 Active Directory 基礎結構會用於使用者驗證和管理。

在部署於僅限輸出連線模式的連接器中設定的驗證方法，可透過 VMware Identity Manager 主控台在內建的身分識別提供者中啟用。在內建的身分識別提供者中啟用驗證方法時，VMware Identity Manager 服務會透過 Websocket 型通訊通道與連接器通訊以驗證使用者。若要在內建的身分識別提供者中啟用驗證方法，請參閱使用內建身分識別提供者。

下列在連接器中設定的驗證方法，可以在內建的身分識別提供者中啟用。

驗證方法	說明
密碼 (雲端部署)	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。
RSA SecurID (雲端部署)	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 (雲端部署)	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 (雲端部署)	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。

桌面平台的 Kerberos 驗證會在連接器上設定並啟用。

以下是不使用連接器、直接在內建的身分識別提供者頁面中設定的驗證方法。

驗證方法	說明
憑證 (雲端部署)	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。
行動 SSO (Android 版)	Android 版行動 SSO 是一種憑證 Proxy 驗證，可用於 Workspace ONE UEM 管理的 Android 裝置的單一登入驗證。系統會在 VMware Identity Manager 服務與 Workspace ONE UEM 之間設定 Proxy 服務，以從 Workspace ONE UEM 擷取憑證並進行驗證。
行動 SSO (iOS 版)	iOS 版行動 SSO 驗證可用於 Workspace ONE UEM 管理的 iOS 裝置的單一登入驗證。iOS 版行動 SSO 驗證會使用 Identity Manager 服務中的金鑰發佈中心 (KDC)。
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 Workspace ONE UEM 目錄同步使用者。
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。

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。請參閱管理要套用至使用者的驗證方法。

本章包含以下主題：

- 為 VMware Identity Manager 設定 Kerberos
- 為 VMware Identity Manager 設定 SecurID
- 針對 VMware Identity Manager 設定 RADIUS
- 在 VMware Identity Manager 中設定 RSA 調適性驗證
- 設定憑證或智慧卡介面卡以搭配 VMware Identity Manager 使用
- 設定雙重要素驗證適用的 VMware Verify
- 使用內建身分識別提供者
- 在 Dell Windows 10 裝置上啟用 Workspace ONE 的全新體驗
- 設定其他 Workspace 身分識別提供者
- 將第三方身分識別提供者執行個體設定為驗證使用者
- 管理要套用至使用者的驗證方法

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。

無論您在 VMware Identity Manager、Active Directory over LDAP 或 Active Directory (整合式 Windows 驗證) 中設定任何類型的目錄，都可以設定 Kerberos 驗證。

在 Identity Manager 服務中設定 Kerberos 驗證通訊協定，可讓您保護使用者瀏覽器和 Identity Manager 服務之間的互動。此外，您可針對在 Workspace ONE UEM 服務中管理的 iOS 9 或更新版本行動裝置，設定通訊協定以實現輕觸一下即可單一登入。如需與 iOS 裝置上的 Kerberos 驗證有關的資訊，請參閱使用雲端主控的 KDC 服務。

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。

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 服務以提供桌面平台的 Kerberos 驗證，您必須加入網域，並在連接器上啟用 Kerberos 驗證。

程序

1 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，選取**設定**。

2 在連接器的 [工作執行緒] 資料行中，按一下**驗證配接器**。

3 按一下 **KerberosIdpAdapter**

系統會將您重新導向至 [Identity Manager 登入] 頁面。

4 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**啟用 Windows 驗證**，以延伸使用者瀏覽器和 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，針對 NT LAN Manager (NTLM) 通訊協定式驗證選取**啟用 NTLM**。 **備註** 僅 Linux 型 VMware Identity Manager 支援此選項。
啟用重新導向	如果在叢集中設定多個連接器，且在負載平衡器後方設定 Kerberos 以實現高可用性，請選取**啟用重新導向**，並指定 [重新導向主機名稱] 的值。 如果僅部署一個連接器，則不需使用 [啟用重新導向] 和 [重新導向主機名稱] 選項。
重新導向主機名稱	如果選取 [啟用重新導向] 選項，則必須提供值。輸入連接器的主機名稱。例如，如果連接器的主機名稱為 connector1.example.com，請在文字方塊中輸入 **`connector1.example.com`**。

5 按一下**儲存**。

後續步驟

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

如果您為部署設定了 Kerberos，並且想為使用者授與使用 Internet Explorer 存取 Web 介面的權限，則必須設定 Internet Explorer 瀏覽器。

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

程序

1 確認您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 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 設定完成。

4 如果區域不是近端內部網路，請將 VMware Identity Manager 連接器 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 > 網站**。

   b 選取**自動偵測內部網路**。

   如果未選取此選項，選取它即可將連接器新增至內部網路區域。

   c (選用) 如果您選取了**自動偵測內部網路**，請按一下**確定**直到所有對話方塊皆關閉為止。

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**將這個網站新增到區域**文字方塊中輸入 VMware Identity Manager 連接器 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網站。

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**啟用整合式 Windows 驗證**。

此選項將在您重新啟動 Internet Explorer 後生效。

c 按一下**確定**。

6 登入 Web 介面以確認存取。

如果 Kerberos 驗證成功，則測試 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

1 在 Firefox 瀏覽器的 URL 文字方塊中，輸入 `about:config` 以存取進階設定。

2 按一下**我保證會小心**。

3 在 [喜好設定名稱] 資料行中按兩下 **network.negotiate-auth.trusted-uris**。

4 在文字方塊中輸入 連接器 URL。

https://myconnectorhost.domain.com

5 按一下**確定**。

6 在 [喜好設定名稱] 資料行中按兩下 **network.negotiate-auth.delegation-uris**。

7 在文字方塊中輸入 連接器 URL。

https://myconnectorhost.domain.com/authenticate/

8 按一下**確定**。

9 使用 Firefox 瀏覽器登入連接器登入 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 連接器。

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 連接器 服務資訊新增為驗證代理程式，並在 連接器 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 連接器 安裝精靈並設定 Active Directory 連線之後，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 VMware Identity Manager 主控台中啟用 SecurID。

- 準備 RSA SecurID 伺服器

  必須藉由 連接器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

  在 RSA SecurID 伺服器中將 連接器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 連接器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。 連接器伺服器使用 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 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	的主機名稱。
IP 位址	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。

後續步驟

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 連接器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) 已安裝且正確設定。
- 從 RSA SecurID 伺服器下載壓縮檔並擷取伺服器組態檔。

程序

1 在 VMware Identity Manager 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 [工作執行緒] 連結。

3 按一下**驗證配接器**，然後按一下 **SecurIDIdpAdapter**。

系統會將您重新導向至 [Identity Manager 登入] 頁面。

4 在 [驗證配接器] 頁面的 [SecurIDIdpAdapter] 資料列中，按一下**編輯**。

5 設定 [SecurID 驗證配接器] 頁面。

設定 SecurID 頁面時需要在 RSA SecurID 伺服器上使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 `sdconf.rec`)。
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**。

後續步驟

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 RSASecurID 驗證方法。請參閱使用內建身分識別提供者。

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。

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，或使用一些其他頻外機制的文字，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。

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 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 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 VMware Identity Manager 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 [工作執行緒] 連結。
3. 按一下**驗證配接器**，然後按一下 **RadiusAuthAdapter**。

   系統會將您重新導向至 [Identity Manager 登入] 頁面。

4 按一下**編輯**以在 [驗證配接器] 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 配接器	選取此方塊以啟用 RADIUS 驗證。
允許嘗試的驗證次數	輸入使用 RADIUS 登入時，登入嘗試失敗的次數上限。預設為五次嘗試。
登入頁面複雜密碼提示	輸入要在使用者登入頁面的訊息中顯示的文字字串，以引導使用者輸入正確的 RADIUS 通行碼。例如，如果將此文字方塊設定為**先 AD 密碼然後 SMS 通行碼**，登入頁面訊息會顯示**先輸入您的 AD 密碼然後輸入 SMS 通行碼。**預設的文字字串為 **RADIUS 通行碼**。
在驗證鏈結期間啟用 Radius 伺服器的直接驗證	選取此方塊以啟用導向使用者驗證。使用者不需要重新輸入其認證。
Radius 伺服器的嘗試次數	輸入重試嘗試的總數。如果主要伺服器未回應，服務會等待設定的時間經過後再次進行重試。
伺服器逾時 (以秒為單位)	輸入 RADIUS 伺服器逾時 (以秒為單位)，在此時間之後，如果 RADIUS 伺服器未回應，即會傳送重試。
Radius 伺服器主機名稱/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。連接埠通常為 1812。
帳戶處理連接埠	輸入 0 做為連接埠號碼。目前未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 服務之間使用的共用密碼。
領域首碼	(選用) 使用者帳戶位置稱為領域。 如果您輸入領域首碼字串，則該名稱傳送至 RADIUS 伺服器時會放置在使用者名稱的開頭。例如，如果輸入的使用者名稱為 jdoe，並指定領域首碼 DOMAIN-A\，則會將使用者名稱 DOMAIN-A\jdoe 傳送至 RADIUS 伺服器。如果不設定這些文字方塊，則只會傳送所輸入的使用者名稱。
領域尾碼	(選用) 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。

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**。

後續步驟

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 RADIUS 驗證方法。請參閱使用內建身分識別提供者。

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。

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頻外驗證。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。

頻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位元組字元，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 VMware Identity Manager 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 **RSAAAIdpAdapter**。

系統會將您重新導向到 Identity Manager 驗證配接器頁面。

4 按一下 RSAAAIdpAdapter 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 RSAAAIdpAdapter。您可以變更此名稱。
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**。

後續步驟

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。請參閱使用內建身分識別提供者。

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。

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平台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。憑證式驗證的運作基礎是使用者所擁有的驗證工具 (私密金鑰或智慧卡)，以及使用者所知道的驗證資訊 (私密金鑰的密碼或智慧卡 PIN)。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。使用智慧卡驗證時，使用者必須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。

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 連接器 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 連接器。

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，以防止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) 和線上憑證狀態通訊協定 (OCSP) 的憑證撤銷檢查。CRL 是核發憑證的 CA 所發佈的撤銷憑證清單。OCSP 是用來取得憑證撤銷狀態的憑證驗證通訊協定。

您可以在相同的憑證驗證配接器組態中同時設定 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，撤銷檢查不會回復使用 OCSP。

透過 CRL 檢查登入

當您啟用憑證撤銷時， 連接器 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

線上憑證狀態通訊協定 (OCSP) 是憑證撤銷清單 (CRL) 的替代功能，用於執行憑證撤銷檢查。

設定憑證型驗證時，如果同時啟用「啟用憑證撤銷」和「啟用 OCSP 撤銷」，則 VMware Identity Manager 會驗證整個憑證鏈結，包括主要、中繼和根憑證。如果鏈結中的任何憑證檢查失敗或 OCSP URL 呼叫失敗，則撤銷檢查將會失敗。

您可以在文字方塊中手動設定 OCSP URL，或從正在驗證之憑證的授權機構資訊存取 (AIA) 延伸中擷取。

設定憑證驗證時，您選取的 OCSP 選項會決定 VMware Identity Manager 如何使用 OCSP URL。

- **僅組態**。使用文字方塊中提供的 OCSP URL 執行憑證撤銷檢查，以驗證整個憑證鏈結。忽略憑證 AIA 延伸中的資訊。您也必須使用 OCSP 伺服器位址設定 OCSP URL 文字方塊才能進行撤銷檢查。
- **僅憑證 (必要)**。使用鏈結中存在於每個憑證 AIA 延伸的 OCSP URL 執行憑證撤銷檢查。系統會忽略 OCSP URL 文字方塊中的設定。鏈結中的每個憑證必須已定義 OCSP URL，否則憑證撤銷檢查將會失敗。
- **僅憑證 (選擇性)**。僅使用憑證 AIA 延伸中存在的 OCSP URL 執行憑證撤銷檢查。如果憑證 AIA 延伸中不存在 OCSP URL，則請勿檢查撤銷。系統會忽略 OCSP URL 文字方塊中的設定。當需要撤銷檢查，但部分中繼或根憑證不包含 AIA 延伸中的 OCSP URL 時，此組態非常實用。
- **具有容錯回復至組態的憑證**。當 OCSP URL 可用時，使用從鏈結中每個憑證 AIA 延伸所擷取的 OCSP URL 執行憑證撤銷檢查。如果 AIA 延伸中不存在 OCSP URL，則使用 OCSP URL 文字方塊中設定的 OCSP URL 來檢查撤銷。您必須使用 OCSP 伺服器位址設定 OCSP URL 文字方塊。

設定憑證型驗證

您可以從 VMware Identity Manager 主控台中的 [驗證方法] 頁面設定「憑證 (雲端部署)」驗證方法，然後選取此驗證方法以便在內建身分識別提供者中使用。

您可以設定 x509 憑證驗證，讓用戶端能夠在其桌面平台和行動裝置上使用憑證進行驗證。請參閱設定憑證或智慧卡介面卡以搭配 VMware Identity Manager 使用。

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。
- (選用) 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 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，選取**管理 > 驗證方法**。

2 在 [驗證方法] 區段中，按一下**憑證 (雲端部署)** 圖示。

3 設定 [憑證服務驗證配接器] 頁面。

備註 星號表示必填欄位。其他欄位為選填。

選項	說明
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。您可以選取多個已編碼為 DER 或 PEM 的根 CA 和中繼 CA 憑證。
已上傳的 CA 憑證	已上傳的憑證檔案會列在表單的 [已上傳的 CA 憑證] 區段中。
識別碼搜尋順序	選取搜尋順序以找到憑證內的使用者識別碼。 ■ **upn**。主體別名的 UserPrincipalName 值 ■ **電子郵件**。來自主體別名的電子郵件地址。 ■ **主體**。來自主體的 UID 值。
驗證 UPN 格式	勾選此核取方塊，以驗證 UserPrincipalName 欄位的格式。
要求逾時	輸入等待回應時間 (以秒為單位)。若值為零 (0)，表示等待回應時間無限期。
已接受的憑證原則	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 所發佈的憑證撤銷清單 (CRL) 來驗證憑證的狀態 (已撤銷或未撤銷)。
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 檢查無法使用時回復為使用 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。

選項	說明
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 URL 來源	選取用於撤銷檢查的來源。 ■ **僅組態**。使用文字方塊中提供的 OCSP URL 執行憑證撤銷檢查，以驗證整個憑證鏈結。 ■ **僅憑證 (必要)**。使用鏈結中存在於每個憑證 AIA 延伸的 OCSP URL 執行憑證撤銷檢查。鏈結中的每個憑證必須已定義 OCSP URL，否則憑證撤銷檢查將會失敗。 ■ **僅憑證 (選擇性)**。僅使用憑證 AIA 延伸中存在的 OCSP URL 執行憑證撤銷檢查。如果憑證 AIA 延伸中不存在 OCSP URL，則請勿檢查撤銷。 ■ **具有容錯回復至組態的憑證**。當 OCSP URL 可用時，使用從鏈結中每個憑證 AIA 延伸所擷取的 OCSP URL 執行憑證撤銷檢查。如果 AIA 延伸中不存在 OCSP URL，則使用 OCSP URL 文字方塊中設定的 OCSP URL 來檢查撤銷。您必須使用 OCSP 伺服器位址設定 OCSP URL 文字方塊。
OCSP 回應程式的簽署憑證	輸入回應程式 OCSP 憑證的路徑 */path/to/file.cer*。
上傳 OCSP 簽署憑證	上傳的憑證檔案會在此區段中列出。
驗證之前啟用同意表	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。
同意表內容	在此文字方塊中輸入要顯示在同意表單中的文字。

4 按一下**儲存**。

後續步驟

- 在內建身分識別提供者中建立「憑證 (雲端部署)」驗證方法的關聯。請參閱設定內建身分識別提供者。
- 將憑證驗證方法新增至預設存取原則。請參閱管理要套用至使用者的驗證方法。

設定雙重要素驗證適用的 VMware Verify

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

您可以透過 VMware Identity Manager 主控台，在內建身分識別提供者中啟用 VMware Verify。

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 VMware Identity Manager 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。

啟用 VMware Verify

針對 VMware Verify 服務的雙重要素驗證，請啟用 VMware Verify，然後將其新增為內建身分識別提供者中的驗證方法。

先決條件

VMware Verify 無法使用透過全域目錄選項設定的目錄。請務必在目錄組態的 [身分識別與存取管理] > [目錄] > [特定目錄] 頁面中，取消選取**此目錄支援 DNS 服務位置**核取方塊。

(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。

程序

1 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，移至**管理 > 驗證方法**。

2 在 **VMware Verify** 的 [設定] 資料行中，按一下圖示。

3 選取**啟用 VMware Verify** 核取方塊。

4 按一下**儲存**。

後續步驟

啟用 VMware Verify 作為內建身分識別提供者中的驗證方法。設定內建身分識別提供者。

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。

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。

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 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 VMware Identity Manager 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。

VMware Verify 防火牆 IP 位址清單

若要進行 VMware Verify 驗證，請將 IP 位址新增至防火牆上的存取控制白名單。VMware Verify 必須能夠透過連接埠 443 連接所有 IP 位址。

您可以在 `vmware.authy.com` 和 `api.authy.com` 上查閱白名單中的 IP 位址。

使用 **nslookup** 命令或其他命令列工具，以取得要新增至外部防火牆白名單的 IP 位址。

使用內建身分識別提供者

內建身分識別提供者可以設定為搭配不需要使用內部部署連接器的驗證方法。VMware Identity Manager 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。

您可以在 [身分識別與存取管理] 的 [管理] > [驗證方法] 頁面中設定驗證方法。設定內建身分識別提供者時，您必須為要在內建身分識別提供者中使用的驗證方法建立關聯。

您也可以設定內建身分識別提供者，以便使用在透過僅限輸出連線模式所部署之連接器上設定的驗證方法。使用僅限輸出連接器時，不需要開啟輸入防火牆連接埠 443。連接器會建立雲端服務的僅限輸出連線 (使用 WebSocket)，並透過此通道接收驗證要求。如需關於部署僅限輸出連接器的詳細資訊，請參閱《VMware Identity Manager 雲端部署指南》中的〈部署模型〉。

針對內建身分識別提供者中的驗證方法建立關聯後，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的驗證方法

您可以在內建身分識別提供者的服務中設定驗證方法。

下列驗證方法不需要使用連接器。您可以在 [身分識別與存取管理] 的 [管理] > [驗證方法] 頁面中啟用並設定驗證方法，並將此驗證方法與內建身分識別提供者建立關聯。

- Workspace ONE UEM 外部存取權杖

- iOS 版行動 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 版行動 SSO
- 裝置符合性 (與 Workspace ONE UEM)
- 密碼 (本機目錄)

啟用驗證方法後，您可以建立套用至這些驗證方法的存取原則。

停用與內建身分識別提供者相關聯的驗證方法

您可以停用從 [驗證方法] 頁面中設定的驗證方法。當您停用某個驗證方法時，如果該驗證方法與任何身分識別提供者相關聯，則系統會在該身分識別提供者中停用驗證方法。在所有存取原則規則中，您也可以透過選項來移除驗證方法。

重要 如果您所停用的驗證方法設定於存取原則規則中，則必須更新該存取原則規則才能選取其他驗證方法。如果未更新存取原則規則，則使用者將可能無法登入其應用程式入口網站或存取其資源。

若要停用特定內建身分識別提供者的驗證，請在內建身分識別提供者 [組態] 頁面中取消選取相關聯驗證方法的方塊。

管理 Workspace ONE UEM 的密碼驗證組態

您可以檢閱及管理您在安裝 Workspace ONE UEM 及新增 VMware Identity Manager 服務時所設定的 [密碼 (AirWatch Connector)] 組態。

「密碼 (AirWatch Connector)」驗證方法可從 [身分識別與存取管理] > [驗證方法] 頁面進行管理，並且會與 [身分識別提供者] 頁面中的內建身分識別提供者相關聯。

重要 升級 AirWatch Cloud Connector 軟體時，請確保在 VMware Identity Manager 主控台的 AirWatch 頁面中更新 Workspace ONE UEM 組態。

程序

1. 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，選取**驗證方法**。
2. 在**密碼 (AirWatch Connector)** 的 [設定] 資料行中，按一下鉛筆圖示。
3. 檢閱組態。

選項	說明
啟動 AirWatch 密碼驗證	此核取方塊會啟用 Workspace ONE UEM 密碼驗證。
AirWatch 管理主控台 URL	已預先填入 Workspace ONE UEM URL。
AirWatch API 金鑰	已預先填入 Workspace ONE UEM 管理員 API 金鑰。
用於驗證的憑證	已預先填入 Workspace ONE UEM Cloud Connector 憑證。

選項	說明
憑證的密碼	已預先填入 Workspace ONE UEM Cloud Connector 憑證的密碼。
AirWatch 群組識別碼	已預先填入組織群組識別碼。
允許嘗試的驗證次數	使用 Workspace ONE UEM 密碼驗證時的登入失敗嘗試次數上限。失敗的登入次數到達此數目後，即不再允許登入嘗試。VMware Identity Manager 服務會嘗試使用後援驗證方法 (如果已設定)。預設為五次嘗試。
已啟用 JIT	若未啟用 JIT，則選取此核取方塊以在使用者第一次登入時，動態啟用使用者在 VMware Identity Manager 服務中的 Just-in-Time 佈建。

4 按一下**儲存**。

為 Workspace ONE UEM 管理的裝置啟用符合性檢查

當使用者註冊其裝置時，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 Workspace ONE UEM (UEM) 主控台中設定的符合性規則。如果裝置不合規，則會採取在 UEM 主控台中設定的對應動作。

VMware Identity Manager 服務包含存取原則選項，經設定可在使用者從裝置登入時用來檢查 Workspace ONE UEM 伺服器中的裝置符合性狀態。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 Workspace ONE 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 Intelligent Hub 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 UEM 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。

如需有關 Workspace ONE UEM 符合性原則的詳細資訊，請參閱 VMware Workspace ONE UEM 說明文件頁面中的《VMware Workspace ONE UEM Mobile Device Management 指南》。

啟用符合性檢查

在 VMware Identity Manager 的 Workspace ONE UEM 組態頁面中啟用裝置符合性，並在 [管理] > [驗證方法] 頁面中設定 [裝置符合性]。

設定 [裝置符合性] 後，您可以設定存取原則規則，以在使用者從其裝置登入 Workspace ONE UEM 伺服器時檢查裝置的符合性狀態。請參閱為 Workspace ONE UEM 管理的裝置啟用符合性檢查。

程序

1 在 VMware Identity Manager 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 [裝置符合性] 區段中選取**啟用**，然後按一下**儲存**。

3 在 [身分識別與存取管理] 索引標籤中，移至**管理 > 驗證方法**。

4 在**裝置符合性 (與 AirWatch)** 的 [設定] 資料行中，按一下圖示。

5 啟用「裝置符合性」驗證，並設定登入失敗嘗試次數上限。其他文字方塊會預先填入已設定的 Workspace ONE UEM 值。

選項	說明
啟用裝置符合性配接器	選取此核取方塊以啟用 Workspace ON UEM 密碼驗證。
AirWatch 管理主控台 URL	已預先填入您在 AirWatch 組態頁面中設定的 Workspace ONE UEM URL。

選項	說明
AirWatch API 金鑰	已預先填入 Workspace ONE UEM 管理員 API 金鑰。
用於驗證的憑證	已預先填入 AirWatch Cloud Connector 憑證
憑證的密碼	已預先填入 AirWatch Cloud Connector 憑證的密碼。

6 按一下**儲存**。

後續步驟

在內建身分識別提供者中建立「裝置符合性」驗證方法的關聯。請參閱設定內建身分識別提供者。

設定預設存取原則，以建立使用裝置符合性 (與 Workspace ONE UEM) 的規則。請參閱設定符合性檢查規則。

設定本機目錄密碼驗證方法

在 [身分識別與存取管理] 的 [管理] > [驗證方法] 頁面中，設定本機目錄的密碼驗證。

設定驗證方法後，您可以在與本機目錄相關聯的內建身分識別提供者中，建立密碼 (本機目錄) 驗證方法的關聯。

程序

1 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，移至**管理 > 驗證方法**。

2 在**密碼 (本機目錄)** 的 [設定] 資料行中，按一下圖示。

3 選取**啟用本機目錄密碼驗證**核取方塊。

4 在**密碼嘗試次數**文字方塊中，輸入登入失敗嘗試次數上限。當失敗的登入嘗試次數達到此數值後，即不允許再次登入。預設為五次嘗試。

5 按一下**儲存**。

後續步驟

- 在內建身分識別提供者中建立「密碼 (本機目錄)」驗證方法的關聯。

設定憑證型驗證

您可以從 VMware Identity Manager 主控台中的 [驗證方法] 頁面設定「憑證 (雲端部署)」驗證方法，然後選取此驗證方法以便在內建身分識別提供者中使用。

您可以設定 x509 憑證驗證，讓用戶端能夠在其桌面平台和行動裝置上使用憑證進行驗證。請參閱設定憑證或智慧卡介面卡以搭配 VMware Identity Manager 使用。

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。
- (選用) 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 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，選取**管理 > 驗證方法**。

2 在 [驗證方法] 區段中，按一下**憑證 (雲端部署)** 圖示。

3 設定 [憑證服務驗證配接器] 頁面。

備註 星號表示必填欄位。其他欄位為選填。

選項	說明
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。您可以選取多個已編碼為 DER 或 PEM 的根 CA 和中繼 CA 憑證。
已上傳的 CA 憑證	已上傳的憑證檔案會列在表單的 [已上傳的 CA 憑證] 區段中。
識別碼搜尋順序	選取搜尋順序以找到憑證內的使用者識別碼。 ■ **upn**。主體別名的 UserPrincipalName 值 ■ **電子郵件**。來自主體別名的電子郵件地址。 ■ **主體**。來自主體的 UID 值。
驗證 UPN 格式	勾選此核取方塊，以驗證 UserPrincipalName 欄位的格式。
要求逾時	輸入等待回應時間 (以秒為單位)。若值為零 (0)，表示等待回應時間無限期。
已接受的憑證原則	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 所發佈的憑證撤銷清單 (CRL) 來驗證憑證的狀態 (已撤銷或未撤銷)。
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 檢查無法使用時回復為使用 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。

選項	說明
OCSP URL 來源	選取用於撤銷檢查的來源。 ■ **僅組態**。使用文字方塊中提供的 OCSP URL 執行憑證撤銷檢查，以驗證整個憑證鏈結。 ■ **僅憑證 (必要)**。使用鏈結中存在於每個憑證 AIA 延伸的 OCSP URL 執行憑證撤銷檢查。鏈結中的每個憑證必須已定義 OCSP URL，否則憑證撤銷檢查將會失敗。 ■ **僅憑證 (選擇性)**。僅使用憑證 AIA 延伸中存在的 OCSP URL 執行憑證撤銷檢查。如果憑證 AIA 延伸中不存在 OCSP URL，則請勿檢查撤銷。 ■ **具有容錯回復至組態的憑證**。當 OCSP URL 可用時，使用從鏈結中每個憑證 AIA 延伸所擷取的 OCSP URL 執行憑證撤銷檢查。如果 AIA 延伸中不存在 OCSP URL，則使用 OCSP URL 文字方塊中設定的 OCSP URL 來檢查撤銷。您必須使用 OCSP 伺服器位址設定 OCSP URL 文字方塊。
OCSP 回應程式的簽署憑證	輸入回應程式 OCSP 憑證的路徑 */path/to/file.cer*。
上傳 OCSP 簽署憑證	上傳的憑證檔案會在此區段中列出。
驗證之前啟用同意表	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。
同意表內容	在此文字方塊中輸入要顯示在同意表單中的文字。

4 按一下**儲存**。

後續步驟

- 在內建身分識別提供者中建立「憑證 (雲端部署)」驗證方法的關聯。請參閱設定內建身分識別提供者。
- 將憑證驗證方法新增至預設存取原則。請參閱管理要套用至使用者的驗證方法。

在 VMware Identity Manager 中設定 iOS 版行動 SSO 驗證

您可以在 VMware Identity Manager 主控台的 [驗證方法] 頁面中設定 iOS 版行動 SSO 驗證方法。建立行動 SSO 驗證方法與內建身分識別提供者的關聯。

使用雲端主控的 KDC 服務

為了支援對 iOS 版行動 SSO 使用 Kerberos 驗證，VMware Identity Manager 提供了雲端主控的 KDC 服務。

使用 Workspace ONE UEM 將 VMware Identity Manager 服務部署在 Windows 環境中時，必須使用在雲端中主控的 KDC 服務。

若要使用 VMware Identity Manager 應用裝置中管理的 KDC，請參閱《VMware Identity Manager 安裝和設定》指南中的〈準備在 iOS 裝置上使用 Kerberos 驗證〉。

當您設定 iOS 版行動 SSO 驗證時，您需要為雲端主控的 KDC 服務設定領域名稱。領域是負責維護驗證資料之管理實體的名稱。當您按一下 [儲存] 時，VMware Identity Manager 服務將會登錄至雲端主控的 KDC 服務。儲存在 KDC 服務中的資料會以 iOS 版行動 SSO 驗證方法的組態為基礎，其中包含 CA 憑證、OCSP 簽署憑證，以及 OCSP 要求組態詳細資料。

記錄會儲存在雲端服務中。記錄中的個人識別資訊 (PII) 包含使用者設定檔中的 Kerberos 主體名稱、主體 DN 和 UPN 以及 EMAIL SAN 值、使用者憑證中的裝置識別碼，以及使用者所存取之 IDM 服務的 FQDN。

若要使用雲端主控的 KDC 服務，VMware Identity Manager 必須根據下述進行設定。

- VMware Identity Manager 服務的 FQDN 必須可從網際網路存取。VMware Identity Manager 使用的 SSL/TLS 憑證必須公開簽署。
- 輸出要求/回應連接埠 88 (UDP) 和連接埠 443 (HTTPS/TCP) 必須可從 VMware Identity Manager 服務存取。
- 如果您啟用 OCSP，則 OCSP 回應程式必須可從網際網路存取。

設定 iOS 版行動 SSO 驗證

您可以在 VMware Identity Manager 主控台的 [驗證方法] 頁面中設定 iOS 版行動 SSO 驗證方法。選取要在內建身分識別提供者中使用的行動 SSO (適用於 iOS) 驗證方法。

先決條件

- 用來簽發憑證給 Workspace ONE UEM 承租人之使用者的憑證授權機構 PEM 或 DER 檔案。
- 若要進行撤銷檢查，需要 OCSP 回應程式的簽署憑證。
- 針對 KDC 服務，選取 KDC 服務的領域名稱。如果使用的是內建 KDC 服務，則必須初始化 KDC。如需內建 KDC 的詳細資訊，請參閱《安裝和設定 VMware Identity Manager》。

程序

1 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，移至**管理 > 驗證方法**。

2 在**行動 SSO (適用於 iOS)** 的 [設定] 資料行中，按一下鉛筆圖示。

3 設定 Kerberos 驗證方法。

選項	說明
啟用 KDC 驗證	選取此核取方塊，可讓使用者使用支援 Kerberos 驗證的 iOS 裝置登入。
領域	對於雲端中的承租人部署，領域值為唯讀。此處顯示的領域名稱即為您承租人的 Identity Manager 領域名稱。 在內部部署中，如果您使用雲端主控的 KDC，請輸入提供給您的預先定義支援領域名稱。此參數中的文字必須全部以大寫輸入。例如 OP.VMWAREIDENTITY.COM。如果您使用內建 KDC，則系統會顯示您在初始化 KDC 時設定的領域名稱。 **備註** 您無法編輯此頁面的領域值。如果您使用內建 KDC，則必須重新初始化 KDC 服務。請參閱在應用裝置中初始化金鑰發佈中心。
根和中繼 CA 憑證	上傳憑證授權機構發行者憑證檔案。可用的檔案格式為 PEM 或 DER。
已上傳的 CA 憑證主體 DN	已上傳之憑證檔案的內容會顯示於此處。您可以上傳多個檔案；系統會將檔案包含的所有憑證新增至清單中。
啟用 OCSP	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。
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 回應程式的簽署憑證	上傳回應程式的 OCSP 憑證。 當您使用 Workspace ONE UEM 憑證授權機構時，系統會將簽發者憑證當做 OCSP 憑證。請在此處一併上傳 Workspace ONE UEM 憑證。

選項	說明
OCSP 回應程式的簽署憑證主體 DN	已上傳的 OCSP 憑證檔案會列示於此。
取消訊息	建立會在驗證花費太長時間時顯示的自訂登入訊息。如果您未建立自訂訊息，預設訊息為「`Attempting to authenticate your credentials`」。
啟動取消連結	如果驗證花費太長的時間，則使用者可以按一下 [取消] 以停止驗證嘗試並取消登入。 當您啟用 [取消] 連結時，文字「取消」會出現在顯示的驗證錯誤訊息結尾處。
企業裝置管理伺服器 URL	輸入行動裝置管理 (MDM) 伺服器 URL，以在使用者的存取因裝置尚未註冊至 Workspace ONE UEM 而遭到拒絕時，將使用者重新導向以進行 MDM 管理。此 URL 會顯示在驗證失敗錯誤訊息中。如果您未輸入 URL，則會顯示一般的「存取遭拒」訊息。

4 按一下**儲存**。

後續步驟

- 在內建身分識別提供者中建立行動 SSO (適用於 iOS) 驗證方法的關聯。

在內建的身分識別提供者中設定 Android 版行動 SSO 驗證

若要提供從 AirWatch 管理的 Android 裝置進行單一登入的功能，您必須在 VMware Identity Manager 內建的身分識別提供者中設定 Android 版行動 SSO 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。
- 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。
- (選用) OCSP 回應簽署憑證檔案位置。

程序

1 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，選取**管理 > 驗證方法**。

2 若要啟用和設定 CertProxyAuthAdapter，按一下**行動 SSO (適用於 Android 裝置)** 鉛筆圖示。

選項	說明
啟用憑證配接器	選取此核取方塊以啟用 Android 版行動 SSO。
根和中繼 CA 憑證	選取要上傳的憑證檔案。您可選取多個已編碼的根 CA 和中繼 CA 憑證。可用的檔案格式為 PEM 或 DER。
已上傳的 CA 憑證	已上傳之憑證檔案的內容會顯示於此。
使用者識別碼搜尋順序	選取搜尋順序以找到憑證內的使用者識別碼。 ■ **upn**。主體別名的 UserPrincipalName 值 ■ **電子郵件**。來自主體別名的電子郵件地址。 ■ **主體**。來自主體的 UID 值。
驗證 UPN 格式	勾選此核取方塊，以驗證 UserPrincipalName 欄位的格式。
已接受的憑證原則	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**新增其他值**來新增其他 OID。

選項	說明
啟用憑證撤銷	選取此核取方塊可啟用憑證撤銷檢查。這樣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 所發佈的憑證撤銷清單 (CRL) 來驗證憑證的狀態 (已撤銷或未撤銷)。
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，可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 故障時使用 CRL	如果您同時設定 CRL 和 OCSP，您可以選取此方塊，以在 OCSP 檢查無法使用時回復為使用 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。
OSCP URL 來源	選取用於撤銷檢查的來源。 ■ **僅組態**。使用文字方塊中提供的 OCSP URL 執行憑證撤銷檢查，以驗證整個憑證鏈結。 ■ **僅憑證 (必要)**。使用鏈結中存在於每個憑證 AIA 延伸的 OCSP URL 執行憑證撤銷檢查。鏈結中的每個憑證必須已定義 OCSP URL，否則憑證撤銷檢查將會失敗。 ■ **僅憑證 (選擇性)**。僅使用憑證 AIA 延伸中存在的 OCSP URL 執行憑證撤銷檢查。如果憑證 AIA 延伸中不存在 OCSP URL，則請勿檢查撤銷。 ■ **具有容錯回復至組態的憑證**。當 OCSP URL 可用時，使用從鏈結中每個憑證 AIA 延伸所擷取的 OCSP URL 執行憑證撤銷檢查。如果 AIA 延伸中不存在 OCSP URL，則使用 OCSP URL 文字方塊中設定的 OCSP URL 來檢查撤銷。您必須使用 OCSP 伺服器位址設定 OCSP URL 文字方塊。
OCSP 回應程式的簽署憑證	輸入回應程式的 OCSP 憑證路徑。輸入為 `/path/to/file.cer`
已上傳的 OCSP 簽署憑證	上傳的憑證檔案會在此區段中列出。
啟動取消連結	當驗證花費太長的時間時，如果此連結已啟用，則使用者可以按一下 [取消] 來停止驗證嘗試並取消登入。
取消訊息	建立會在驗證花費太長時間時顯示的自訂訊息。如果您未建立自訂訊息，預設訊息為「`Attempting to authenticate your credentials`」。

3 按一下**儲存**。

4 選取**管理 > 身分識別提供者**，然後按一下**新增身分識別提供者**。

5 選取**建立內建 IDP**，或選取現有的內建身分識別提供者。

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	系統會列出已設定的目錄。選取要驗證的使用者目錄。
網路	列出了服務中設定的現有網路範圍。您在 Android 版行動 SSO 的原則規則中使用的網路範圍，必須僅包含用以接收來自於 VMware Tunnel Proxy 伺服器所要求的 IP 位址。
驗證方法	選取**行動 SSO (適用於 Android)**。
KDC 憑證匯出	不適用

6 在內建身分識別提供者頁面上按一下**新增**。

後續步驟

設定 Android 版行動 SSO 的預設存取原則規則。

設定內建身分識別提供者

您可以設定多個內建身分識別提供者，並將內建身分識別提供者與已在 [身分識別與存取管理] 的 [管理] > [驗證方法] 頁面中設定的驗證方法建立關聯。

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 按一下**新增身分識別提供者**，然後選取**建立內建 IDP**。

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	系統會顯示在服務上設定的驗證方法。請選取驗證方法的核取方塊以便與此內建身分識別提供者建立關聯。 針對 [裝置符合性 (與 Workspace ONE UEM)] 和 [密碼 (AirWatch Connector)]，請確定選項已在 AirWatch 組態頁面中啟用。

3 按一下**新增**。

後續步驟

設定預設存取原則規則以將驗證原則新增至規則。請參閱管理預設存取原則。

使用輸出連接器在內建身分識別提供者中進行驗證

內建身分識別提供者可以設定為搭配不需要安裝在防火牆後方之連接器的驗證方法。連接器會以輸出連線模式安裝，且不需要開啟輸入防火牆連接埠 443。

連接器會建立雲端服務的僅限輸出連線 (使用 WebSocket)，並透過此通道接收驗證要求。

設定內建身分識別提供者時，您可以使用僅限輸出連線模式，將部署在 DMZ 後方之連接器上所設定的驗證方法與身分識別提供者建立關聯。

您可以設定下列連接器驗證方法。

- 密碼 (雲端部署)
- RSA 調適性驗證 (雲端部署)
- RSA SecurID (雲端部署)
- RADIUS (雲端部署)

設定驗證方法後，接下來您必須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以及在僅限輸出連接器上設定的驗證方法

設定內建身分識別提供者時，您可以使用僅限輸出連線模式，將部署在 DMZ 後方之連接器上所設定的驗證方法與內建身分識別提供者建立關聯。

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 VMware Identity Manager 主控台的 [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	系統會顯示 [身分識別與存取管理] 的 [管理] > [驗證方法] 頁面中設定的驗證方法。請選取驗證方法的核取方塊以便與身分識別提供者建立關聯。 針對 [裝置符合性 (與 Workspace ONE UEM))] 和 [密碼 (AirWatch Connector)]，請確定選項已在 AirWatch 組態頁面中啟用。
連接器	在僅限輸出連線模式中，選取設定的連接器。
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。選取此核取方塊可與驗證方法建立關聯。

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 Workspace ONE UEM 組態中使用。

4 按一下**儲存**。

在 Dell Windows 10 裝置上啟用 Workspace ONE 的全新體驗

當使用者收到已在 Workspace ONE UEM Windows 10 佈建服務中啟用全新 (OOBE) 佈建功能的新 Dell® Windows 10 裝置時，可以將 Workspace ONE 應用程式設定為自動開啟，並將應用程式傳遞至裝置。

若要透過 Workspace ONE 應用程式傳遞此 OOBE，您必須在 Workspace ONE UEM 整合的過程中啟用外部存取權杖驗證方法。接著在內建提供者中啟用此驗證方法，並建立使用外部存取權杖驗證方法的存取原則規則。

使用者無須再次輸入其登入認證，Workspace ONE OOBE 即會執行 Workspace ONE 應用程式。若未啟用此驗證方法，則使用者除了必須在 Windows 登錄程序期間登入裝置，也必須再登入 Workspace ONE。

啟動外部存取權杖作為驗證方法

在 VMware Identity Manager 中，外部存取權杖驗證方法對 Workspace ONE UEM 整合而言是為一的，且進行單一登入 (SSO) 以及在 Windows 10 裝置上觸發 Workspace ONE 的全新體驗 (OOBE) 時，皆需要此驗證方法。

先決條件

使用外部存取權杖驗證時，必須部署和設定 AirWatch Cloud Connector 元件。

- 外部存取權杖驗證可在 [身分識別與存取管理] 索引標籤中 [AirWatch] 頁面上啟用。
- 已為 Windows 10 裝置設定 AirWatch 佈建服務。

外部存取權杖的組態是唯讀的，而其基礎來自於 VMware Identity Manager 中的 Workspace ONE UEM (AirWatch) 組態。權杖存留期欄位是例外狀況。

程序

1 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，選取**驗證方法**。

2 在 **Airwatch 外部存取權杖設定**資料行中，按一下鉛筆圖示。

3 檢閱組態。

選項	說明
啟用 AirWatch 外部存取權杖	在 [AirWatch] 頁面上會啟用此核取方塊。
AirWatch 管理主控台 URL	已預先填入 AirWatch URL。
AirWatch API 金鑰	預先填入 AirWatch 管理員 API 金鑰。
用於驗證的憑證	已預先填入 AirWatch Cloud Connector 憑證。
憑證的密碼	已預先填入 AirWatch Cloud Connector 憑證的密碼。
AirWatch 外部存取權杖存留期 (以秒為單位)	存取權杖會用來驗證對 VMware Identity Manager 的驗證。存取權杖具有有限的存留期。設定的時間即為有效存取權杖的時間上限。權杖存留期可供編輯，而其預設值為 600 秒，即 10 分鐘。 存取權杖到期時，系統會提示使用者在 Workspace ONE 應用程式中重新驗證。

4 按一下**儲存**。

後續步驟

在內建身分識別提供者中建立 AirWatch 外部存取權杖驗證方法的關聯。請參閱設定內建身分識別提供者

AirWatch 外部存取權杖與內建身分識別提供者建立關聯後，請建立要使用此驗證方法的存取原則規則。請參閱為 Workspace ONE 全新體驗程序建立存取原則。

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 VMware Identity Manager 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/新增第三方身分識別提供者執行個體之前，請先完成下列工作。

- 確認第三方執行個體與 SAML 2.0 相容，且 VMware Identity Manage 服務可以連線至第三方執行個體。
- 在 VMware Identity Manager 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。

新增和設定身分識別提供者執行個體

為您的 VMware Identity Manager 部署新增和設定新的身分識別提供者執行個體時，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

- 對第三方中繼資料文件的存取權。存取權可以是中繼資料的 URL 或是實際的中繼資料。

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，選取**身分識別提供者**。

2 按一下**新增身分識別提供者**。

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	新增第三方身分識別提供者 XML 式中繼資料文件，以建立與身分識別提供者的信任關係。 1 在文字方塊中輸入 SAML 中繼資料 URL 或 xml 內容。按一下**處理 IdP 中繼資料**。 2 選取識別使用者的方式。在輸入 SAML 判斷提示中傳送的識別碼，可透過主體或屬性陳述式來傳送。 ■ **NameID 元素**。NameID 元素可透過 SAML 屬性陳述式來擷取。 ■ **SAML 屬性**。 3 如果您選取 SAML 屬性，則會從中繼資料擷取身分識別提供者支援的 NameID 格式，並新增至 [名稱識別碼格式] 表格。 ■ 在**名稱識別碼值**資料行中，選取服務中的使用者屬性以對應至顯示的識別碼格式。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。 ■ (選用) 選取「NameID 原則」回應識別碼字串格式。
Just-in-Time 佈建	不適用
使用者	選取**其他目錄**以納入可使用此身分識別提供者進行驗證的使用者。
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。

表單項目	說明
單一登出組態	當使用者從第三方身分識別提供者 (IDP) 登入 Workspace ONE 時，系統會開啟兩個工作階段，其中一個適用於第三方身分識別提供者，另一個則適用於 Workspace ONE 的 Identity Manager 服務提供者。您可以分別管理這些工作階段的存留期。當使用者登出 Workspace ONE 時，隨即會關閉 Workspace ONE 工作階段，但第三方 IDP 工作階段仍可能處於開啟狀態。視您的安全性需求而定，您可以啟用單一登出並設定單一登出以同時登出兩個工作階段，或者可以讓第三方 IDP 工作階段保持不變。 組態選項 1 ■ 當您設定第三方身分識別提供者時，可以啟用單一登出。如果第三方身分識別提供者支援 SAML 式單一登出通訊協定 (SLO)，則使用者登出 Workspace ONE 入口網站時，即會同時登出兩個工作階段。未設定 [重新導向 URL] 文字方塊。 ■ 如果第三方 IDP 不支援 SAML 式單一登出，您可以啟用單一登出，並在 [重新導向 URL] 文字方塊中指定 IDP 單一登出端點 URL。您也可以新增重新導向參數，以附加至將使用者傳送至特定端點的 URL。當使用者登出 Workspace ONE 入口網站且從 IDP 登出時，系統會將使用者重新導向至此 URL。 組態選項 2 ■ 另一個單一登出選項是讓使用者登出 Workspace ONE 入口網站，並將其重新導向至自訂的端點 URL。您可以啟用單一登出、在 [重新導向 URL] 文字方塊中指定 URL，以及自訂端點的重新導向參數。當使用者登出 Workspace ONE 入口網站時，系統會將其導向這個可以顯示自訂訊息的頁面。第三方 IDP 工作階段仍可能處於開啟狀態。URL 輸入的形式為 **`https://<vidm-access-url>/SAAS/auth/federation/slo`**。 如果未啟用 [啟用單一登出]，則當使用者登出時，VMware Identity Manager 服務中的預設組態會將使用者導向至 Workspace ONE 入口網站登入頁面。第三方 IDP 工作階段仍可能處於開啟狀態。
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**。

後續步驟

■ 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。

此外也可設定原則規則，以依網路範圍和裝置類型拒絕使用者存取。

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。

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。

管理存取原則

7

若要能夠安全地存取 Workspace ONE 入口網站並啟動應用程式，您需要設定存取原則。存取原則所包含的規則，可用來指定讓使用者登入其應用程式入口網站並使用其資源所需符合的條件。

存取原則可讓管理員設定如下的功能：行動單一登入，根據註冊、符合性狀態、多重要素驗證的應用程式條件式存取，以及逐步驗證。

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。您可以選取一或多個要與存取規則建立關聯的群組，或將規則套用於所有人。

VMware Identity Manager 服務包含預設存取原則集，其中包含控制整體存取的基本存取原則規則。基本存取原則規則初始設定為允許所有使用者透過網頁瀏覽器或 Workspace ONE 應用程式從所有網路範圍進行存取。您可以編輯預設原則集，以針對特定類型的裝置建立更多規則，並使用各種類型的驗證。

您也可以建立應用程式特定的存取原則規則，以管理特定 Web 和桌面平台應用程式的存取權。應用程式特定存取原則規則可用於建立要求對更加機密資源進行強化驗證的逐步驗證。

本章包含以下主題：

存取原則設定

您可以建立存取原則規則，並指定存取整體 Workspace ONE 入口網站和已授權應用程式必須符合的準則。您也可以建立應用程式特定的存取原則與規則，以管理使用者對於特定 Web 和桌面平台應用程式的存取。

網路範圍

您可以將網路位址指派給存取原則規則，以根據登入和存取應用程式所使用的 IP 位址來管理使用者存取。在以內部部署方式設定 VMware Identity Manager 服務時，您可以針對內部網路存取和外部網路存取設定網路 IP 位址的範圍。然後，您可以根據規則中設定的網路範圍建立不同的規則。

備註 當設定 VMware Identity Manager 雲端服務的網路位址時，請指定用於存取內部網路的 VMware Identity Manager 承租人公用位址。

在設定存取原則規則之前，您可以從 [身分識別與存取管理] 索引標籤的 [管理] > [原則] > [網路範圍] 頁面設定網路範圍。

部署中的每個身分識別提供者執行個體已設定為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您選取的網路範圍。

裝置類型

存取原則規則會設定為管理用於存取入口網站和資源的裝置類型。您可以指定的裝置包括 iOS 和 Android 行動裝置、執行 Windows 10 或 macOS 作業系統的電腦、網頁瀏覽器、Workspace ONE 應用程式，以及所有裝置類型。

裝置類型為「Workspace ONE 應用程式」的原則規則會定義從裝置登入後，用於從 Workspace ONE 應用程式啟動應用程式的存取原則。若此規則為原則清單中的第一個規則，當使用者完成驗證後，他們可以在 Workspace ONE 應用程式保持登入狀態，並根據預設設定存取其資源長達 90 天。

無論裝置硬體類型和作業系統為何，裝置類型為「網頁瀏覽器」的原則規則會定義使用任何類型網頁瀏覽器的存取原則。

裝置類型為「所有裝置類型」的原則規則會比對所有存取案例。

當使用 Workspace ONE 應用程式來存取應用程式時，原則集會將裝置類型分門別類，其中 Workspace ONE 應用程式為第一個規則，隨後是行動裝置、Windows 和 macOS、網頁瀏覽器裝置類型，最後是所有裝置類型。規則的列出順序表示規則的套用順序。當裝置類型符合驗證方法時，系統會忽略後續的規則。如果裝置類型 Workspace ONE 應用程式規則不是原則清單中的第一個規則，則使用者無法延長登入 Workspace ONE 應用程式的時間。請參閱將 Workspace ONE 應用程式規則套用至存取原則

新增群組

您可以根據使用者的群組成員資格套用不同的驗證規則。群組可以是從企業目錄同步的群組，以及您在 VMware Identity Manager 主控台中建立的本機群組。

當群組指派給存取原則規則時，系統會要求使用者輸入其唯一識別碼，接著要求根據存取原則規則來輸入驗證。請參閱 使用唯一識別碼的登入體驗。依預設，唯一識別碼是**使用者名稱**。前往 [身分識別與存取管理] > [設定] > [喜好設定] 頁面，即可查看已設定的唯一識別碼值，或變更識別碼。

備註 若未在規則中識別群組，則該規則將套用至所有使用者。當您設定包含群組規則和非群組規則的存取原則時，使用群組設定之規則的順序必須高於未使用群組設定的規則。

由規則管理的動作

您可以設定存取原則規則，以允許或拒絕存取工作區和資源。當原則設定為提供特定應用程式的存取權時，您也可以指定允許存取應用程式的動作，而無需進一步驗證。若要套用此動作，使用者需已準備好透過預設存取原則進行驗證。

您可以在套用至動作的規則中選擇性套用條件，例如要包含的網路、裝置類型和群組，以及裝置註冊和符合性狀態。採取拒絕存取動作時，使用者將無法從規則中設定的裝置類型和網路範圍來登入或啟動應用程式。

驗證方法

VMware Identity Manager 服務中設定的驗證方法會套用至存取原則規則。對於每個規則，您可以選取要使用的驗證方法，以驗證登入 Workspace ONE 或存取應用程式的使用者身分。您可以在規則中選取多個驗證方法。

驗證方法將按照在規則中列出的順序進行套用。系統會選取規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。

您可以在存取原則規則中設定驗證鏈結，以要求使用者必須透過多個驗證方法完成認證才能進行登入。系統會在單一規則中設定兩個驗證條件，而使用者必須正確回應這兩個驗證要求。例如，如果您將驗證設定為使用「密碼」和「VMware Verify」，則使用者必須輸入其密碼和 VMware Verify 通行碼才能進行驗證。

您可以設定後援驗證，讓先前於驗證要求時失敗的使用者有機會重新登入。如果使用者無法使用驗證方法進行驗證，且已設定後援方法，則系統會提示使用者輸入其認證，以使用已設定的其他驗證方法。下列兩個案例說明此後援的運作方式。

- 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 VMware Verify 通行碼進行驗證。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 VMware Verify 通行碼。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 VMware Verify 通行碼進行驗證。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 VMware Verify 通行碼。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。

若要設定需要對 Workspace ONE UEM 管理裝置進行驗證和裝置符合性驗證的存取原則規則，則必須在內建身分識別提供者頁面中啟用 [裝置符合性與 (AirWatch)]。請參閱 為 Workspace ONE UEM 管理的裝置啟用符合性檢查。可和使用裝置符合性 (與 AirWatch) 之鏈結的內建身分識別提供者驗證方法為行動 SSO (適用於 iOS)、行動 SSO (適用於 Android) 或憑證 (雲端部署)。

當 VMware Verify 用於雙因素驗證時，VMware Verify 為驗證鏈結中的第二個驗證方法。必須在內建身分識別提供者頁面中啟用 [VMware Verify]。請參閱設定雙重要素驗證適用的 VMware Verify。

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，或開啟特定應用程式之間所擁有的時間上限。例如，Web 應用程式規則中的值「8」表示完成驗證後，使用者在 8 小時內不需再次重新進行驗證。

原則規則設定**在以下時間之後重新驗證**不會控制應用程式工作階段。此設定可控制時間，之後使用者必須重新驗證。

自訂存取遭拒錯誤訊息

當使用者嘗試登入，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。

您可以建立自訂錯誤訊息，以覆寫每個存取原則規則的預設訊息。自訂訊息可包含文字和呼叫動作訊息的連結。例如，在限制存取已註冊裝置的原則規則中，如果使用者嘗試從未註冊的裝置登入，則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。

將 Workspace ONE 應用程式規則套用至存取原則

在裝置上安裝 Workspace ONE 應用程式時，使用者可以透過 VMware Identity Manager 使用單一登入功能來存取其有權使用的應用程式。

Workspace ONE 應用程式是一種 OAuth 用戶端，可使用 GreenBox-TemplatedId OAuth 範本來管理應用程序存取。此範本已登錄於 VMware Identity Manager 主控台中的 [目錄] > [設定] > [遠端存取] 頁面。

當使用者第一次成功登入 Workspace ONE 應用程式時，系統會將 OAuth 存取權杖套用至該應用程式。此存取權杖會使用存留時間 (TTL) 進行設定。TTL 值為使用者不需再次登入即可存取 Workspace ONE 的時間上限。

系統會設定重新整理權杖，以便 Workspace ONE 在存取權杖到期時要求新的存取權杖。透過此方式，使用者可以延長不需再次登入即可延長登入 Workspace ONE 應用程式的期間。

請根據下述設定 Workspace ONE 存取權杖的存留時間。

- 存取權杖的存留時間為 3 小時。
- 重新整理權杖的存留時間為 90 天。
- 閒置權杖的存留時間為 10 天。

如果使用者每天使用 Workspace ONE 應用程式，則根據重新整理權杖 TTL 值，使用者在 90 天內皆不需再次登入。不過，如果使用者處於閒置狀態，且連續 10 天未使用 Workspace ONE 應用程式，則使用者必須再次登入 Workspace ONE。

若要登入 Workspace ONE 並將存取權杖套用至該應用程式，則裝置類型 **Workspace ONE 應用程式**應為預設存取原則中的第一個規則，以強制執行 OAuth TTL。驗證使用者後，存取權杖會根據重新整理權杖和閒置權杖值，來管理工作階段的有效期間。

您可以設定存取原則規則中的工作階段重新驗證值，使其與重新整理權杖的存留時間值相同，即 90 天或 2160 小時。如果您將工作階段重新驗證值設定為小於重新整理權杖存留時間，則系統會在工作階段重新驗證達到臨界值時，提示使用者登入 Workspace ONE。

如果 Workspace ONE 應用程式不是第一個規則，則 OAuth 存取權杖不會套用至 Workspace ONE 應用程式，且無法對其他資源使用單一登入。使用者每次透過裝置存取 Workspace ONE 時，必須在其入口網站中登入應用程式 。

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。

備註 不支援網際網路通訊協定第 6 版 (IPv6) 位址。

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。您可以建立具有適用於特定用途之特定 IP 位址的其他網路範圍。

預設網路範圍 ALL RANGES 及其說明「所有範圍的網路」均可供編輯。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。您可以根據內部和外部存取來設定網路範圍。
- 針對 VMware Identity Manager 雲端服務，請確認用於內部網路範圍的承租人公用位址。雲端服務的內部網路識別碼並非 10.x.x.x。
- 在服務中啟用 Horizon 時，您可以根據網路範圍來指定 Horizon URL。若要在啟用 Horizon 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。請參閱在 VMware Identity Manager 中設定資源指南中的〈提供 View 桌面平台集區和應用程式的存取權〉一節。

程序

1. 在 VMware Identity Manager 主控台的 [原則] 索引標籤中，選取**網路範圍**。
2. 編輯現有的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進行編輯。
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。
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。

後續步驟

- 將每個網路範圍與身分識別提供者執行個體建立關聯。
- 視情況將網路範圍與存取原則規則建立關聯。

管理預設存取原則

VMware Identity Manager 服務包含一個預設存取原則集，可控制使用者對其 Workspace ONE 入口網站和 Web 應用程式的存取。

預設存取原則已設定為允許從所有裝置類型存取所有網路範圍。工作階段逾時為八小時。您可以在必要時編輯原則集以變更原則規則。

在 VMware Identity Manager 服務中啟用密碼驗證以外的驗證方法時，您必須編輯預設原則，以將這些驗證方法新增至原則規則。

您可以在預設存取原則中建立存取規則，以管理 iOS、Android 和 Windows 10 裝置的行動單一登入機制。

使用者嘗試登入時，VMware Identity Manager 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。

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，將會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依預設為五次。當使用者嘗試登入失敗五次後，服務會嘗試使用清單中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。

編輯預設存取原則

您必須編輯原則規則才能選取您在 VMware Identity Manager 中設定的驗證方法，並設定驗證方法用於驗證的順序。

先決條件

- 已設定並啟用您組織所支援的驗證方法。請參閱第 6 章，在 VMware Identity Manager 中設定使用者驗證
- 已建立定義的 IP 位址網路範圍，並指派給身分識別提供者。

密碼 (本機目錄) 驗證方法已套用至系統目錄。預設存取原則包含將「密碼 (本機目錄)」設定為後援方法的原則規則，讓管理員可登入 VMware Identity Manager 主控台。請參閱設定系統管理員使用者的驗證方法。

建立原則規則並套用至每個目錄中設定的所有驗證方法。如果目錄使用未在原則規則中設定的驗證方法，則該目錄中的使用者將無法登入。

程序

1 在 VMware Identity Manager 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**編輯預設原則**。

3 您可以變更原則名稱，使其更為明確。例如，公司基本存取原則。

除非應用程式已指派給 Web 特定存取原則，否則此原則將套用至目錄中的所有應用程式。

4 按**下一步**以開啟 [組態] 頁面。

5 選取要編輯的規則名稱，或按一下**新增原則規則**來新增原則規則。

選項	說明
如果使用者的網路範圍為	確認網路範圍是否正確，如果新增規則，請選取網路範圍。
且使用者正在存取來自下列裝置的內容	選取此規則所要管理的裝置類型。當使用 Workspace ONE 應用程式來存取 Workspace ONE 和資源時，請建立第一個規則，並將 Workspace ONE 應用程式設為裝置類型。
且使用者屬於群組	如果此存取規則將套用至特定群組，請在搜尋方塊中搜尋群組。 若未選取任何群組，則存取原則規則會套用至所有使用者。
則執行此動作	選取**使用下列方法進行驗證...**。
則使用者可使用下列方法進行驗證	設定驗證方法的順序。選取要優先套用的驗證方法。 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。
如果前述方法失敗或不適用，則	設定後援驗證方法。
在以下時間之後重新驗證	選取工作階段的長度之後，使用者必須重新進行驗證。

6 (選用) 在**進階內容**中，建立使用者驗證失敗時所顯示的自訂存取遭拒錯誤訊息。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其他頁面，請在 [自訂錯誤連結 URL] 文字方塊中輸入 URL 連結位址。在 [自訂錯誤連結] 文字方塊中，輸入說明自訂錯誤連結的文字。此文字即為連結。如果您將此文字方塊保留為空白，則會將文字「繼續」顯示為連結。

7 按**下一步**以檢閱規則，然後按一下**儲存**。

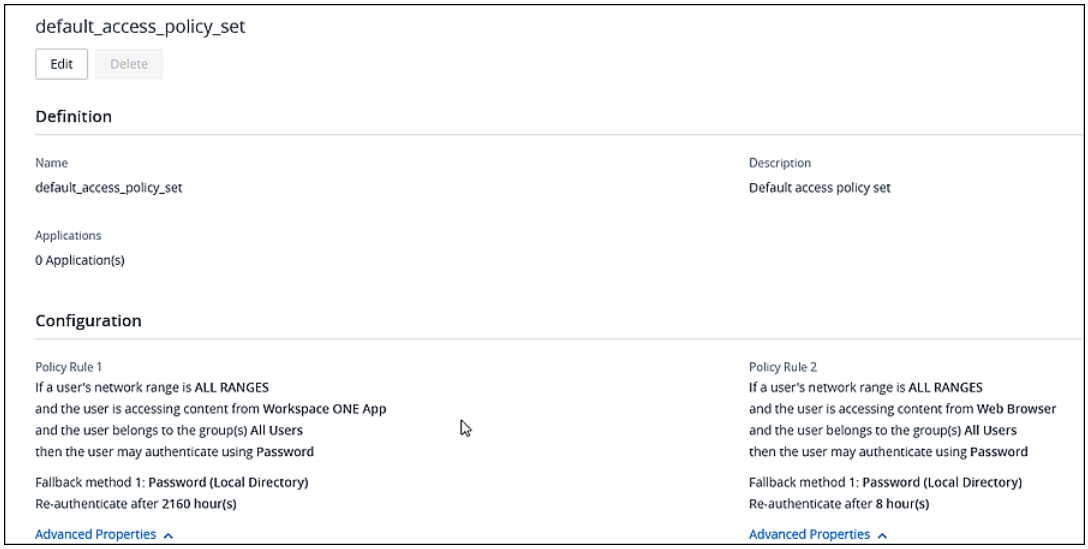
後續步驟

如有必要，請建立其他規則。

所有規則建立之後，請在清單中排序規則，系統會依此順序來進行套用。如果使用 Workspace ONE 應用程式來存取 Workspace ONE 和其他資源，請務必將 Workspace ONE 應用程式設為清單中的第一個規則。

編輯後的原則規則會立即生效。

圖 7-1：預設存取原則組態



裝置類型 Workspace ONE 應用程式預設存取原則的範例

當使用者從 Workspace ONE 應用程式存取資源時，為了實現單一登入體驗，預設的存取原則已針對您環境 (Android、iOS、Mac OS 或 Windows 10) 中所使用每個裝置類型的規則進行設定。您也可以為裝置類型 Workspace ONE 應用程式建立規則。

在此範例的預設存取原則組態中會建立預設的存取原則，其中的規則可涵蓋從所有網路範圍登入的使用者。下列規則已建立。

- 此規則適用於可用來存取 Workspace ONE 應用程式的每個裝置。
- 此規則適用於來自 Workspace ONE 應用程式裝置類型的使用者存取。必須在規則中包含為每個裝置設定的驗證方法。
- 此規則適用於來自 Web 瀏覽器裝置類型之使用者存取的規則，以便從任何 Web 瀏覽器存取 Workspace ONE。

裝置類型 Workspace ONE 應用程式的規則已設定為使用可用來存取 Workspace ONE 應用程式的所有驗證方法。系統會先指派一個驗證方法，並將其他驗證方法設定為後援驗證類型。當使用者使用其中一個裝置來登入 Workspace ONE 應用程式時，將根據為裝置類型設定的驗證方法進行驗證。成功驗證使用者之後，當他們從 Workspace ONE 應用程式畫面啟動其他資源時，系統會識別該驗證方法且不會提示使用者重新驗證。如果用來向 Workspace ONE 驗證的驗證方法無法識別，則當使用者從 Workspace ONE 應用程式啟動資源時，即會根據 Workspace ONE 應用程式規則提示使用者進行驗證。

為獲得最佳使用者經驗，請將裝置類型 Workspace ONE 應用程式列為預設存取原則中的第一個規則。當該規則為第一個時，使用者會登入應用程式，且可以啟動資源而不需重新驗證，直到工作階段到期為止。

1. 針對可用來存取 Workspace ONE 應用程式的每個裝置建立一個規則。此範例適用於允許來自裝置類型 iOS 存取的規則。

- 網路範圍為 **ALL RANGES**。
- 使用者可存取來自 **iOS** 的內容。

- 系統不會將群組新增至原則規則。支援**所有使用者**。
- 設定所有支援的驗證方法。
  - 使用**行動 SSO (適用於 iOS)** 進行驗證。
  - 後援方法 1：**密碼 (雲端部署)**。
  - 後援方法 2：**裝置符合性 (與 AirWatch)**。
- 系統會在 **8 小時**後重新驗證工作階段。

2. 針對裝置類型 Workspace ONE 應用程式建立規則。必須在規則中包含為每個裝置設定的驗證方法。

- 網路範圍為 **ALL RANGES**。
- 使用者可從 **Workspace ONE 應用程式**存取內容。
- 系統不會將群組新增至原則規則。支援**所有使用者**。
- 設定所有支援的驗證方法。
  - 使用**行動 SSO (適用於 iOS)** 進行驗證。
  - 後援方法 1：**行動 SSO (適用於 Android)**。
  - 後援方法 2：**密碼 (雲端部署)**。
  - 後援方法 3：**裝置符合性 (與 AirWatch)**。
- 系統會在 **2160 小時**後重新驗證工作階段。

2160 小時等於 90 天，這是 Workspace ONE 應用程式 OAuth 權杖重新整理權杖的存留時間。請參閱將 Workspace ONE 應用程式規則套用至存取原則。

3. 針對裝置類型網頁瀏覽器建立規則，以便從任何 Web 瀏覽器存取 Workspace ONE。包含此範例可作為「密碼 (本機目錄)」驗證方法的後援。若要驗證登入的系統管理員身分，至少必須設定一個規則以使用密碼 (本機目錄) 以進行驗證。工作階段會在 24 小時之後逾時。

- 網路範圍為 **ALL RANGES**。
- 使用者可從 **Web 瀏覽器**存取內容。
- 系統不會將群組新增至原則規則。支援**所有使用者**。
- 設定所有支援的驗證方法。
  - 使用**密碼 (雲端部署)** 進行驗證。
  - 後援方法 2：**密碼**。
  - 後援方法 3：**密碼 (本機目錄)**。
- 系統會在 **8 小時**後重新驗證工作階段。

針對所有裝置、Workspace ONE 應用程式和 Web 瀏覽器建立規則時，您的預設原則集看起來類似下列的螢幕擷取畫面。

圖 7-2：Workspace ONE 應用程式的預設原則集會先列出

設定此預設存取原則的流程。

1 UserA 從其 iOS 裝置登入 Workspace ONE 應用程式，且系統要求其使用行動 SSO (適用於 iOS) 進行驗證。驗證成功。

2 UserA 啟動 Workspace ONE 應用程式中列出的資源，且因為 Workspace ONE 應用程式規則中包含行動 SSO (適用於 iOS) 驗證方法作為後援驗證方法，因此系統會啟動資源而無需再次要求驗證。在 2160 小時內，使用者可以啟動資源，而不需再次登入 Workspace ONE。

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

- 為您的部署設定適當的驗證方法。
- 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。

當 WS-Fed Web 應用程式 (Office 365) 用戶端 (VMware Boxer、iOS 和 Android 原生電子郵件用戶端) 使用舊版驗證流程的使用者名稱和密碼驗證時，您可以從 [目錄] 頁面設定 Office 365 應用程式中的用戶端存取原則。請參閱 VMware Identity Manager 與 Office 365 的整合指南。

備註 對於由應用程式來源或 Web 連結管理的應用程式，系統不會為其建立存取原則。

程序

1 在 VMware Identity Manager 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**。

3 在各自的文字方塊中新增原則名稱和說明。

4 在**套用至**區段的 [搜尋] 文字方塊中輸入應用程式，然後選取要與此原則建立關聯的應用程式。

5 按**下一步**。

6 按一下**新增原則規則**以新增規則。

選項	說明
如果使用者的網路範圍為	確認網路範圍是否正確，如果新增規則，請選取網路範圍。
且使用者正在存取來自下列裝置的內容	選取此規則所要管理的裝置類型。
且使用者屬於群組	如果此存取規則將套用至特定群組，請在搜尋方塊中搜尋群組。 若未選取任何群組，則存取原則規則會套用至所有使用者。
則執行此動作	選取**使用下列方法進行驗證...**。
則使用者可使用下列方法進行驗證	設定驗證方法的順序。選取要優先套用的驗證方法。 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。
如果前述方法失敗或不適用，則	設定後援驗證方法。
在以下時間之後重新驗證	選取工作階段的長度之後，使用者必須重新進行驗證。

7 如有必要，請設定其他規則。

8 按一下**儲存**。

套用 Web 和桌面平台應用程式特定的原則

您可以為目錄中的個別 Web 和桌面平台應用程式建立自訂存取原則。這些存取原則可以根據位置、裝置類型，驗證方法和工作階段長度來限制存取。若要限制存取，您可以將一組特定群組與應用程式規則建立關聯。

以下是您可以建立的 Web 應用程式特定原則範例，用於控制對指定 Web 應用程式的存取。

範例 1 指派給群組的基本 Web 應用程式特定原則

在此範例中，您將建立新的應用程式特定存取原則，並套用至銷售團隊群組可以存取的 Web 應用程式。此範例將套用兩個規則。第一個規則專屬於銷售團隊群組中可從內部網路存取應用程式的使用者。

從內部網路存取的規則設定如下。

- 網路範圍為 **INTERNAL NETWORK**。
- 使用者可從**網頁瀏覽器**存取內容。
- 使用者屬於**銷售團隊**群組。
- 第一個驗證方法為 **Kerberos**。
- 後援為**密碼**。
- 系統會在 **8 小時**後重新驗證工作階段。

若要從內部網路存取銷售團隊應用程式，銷售團隊群組成員需要從網頁瀏覽器啟動應用程式，而系統會要求輸入名稱和 Kerberos 密碼。如果 Kerberos 驗證失敗，則系統會要求使用者輸入 Active Directory 密碼。工作階段持續時間為八小時。八個小時後，系統會提示使用者再次登入。

如果銷售團隊群組中的使用者從外部網路透過網頁瀏覽器存取應用程式，則系統會套用第二個規則。

從外部網站存取的規則設定如下。

- 網路範圍為 **ALL RANGES**。
- 使用者可從**網頁瀏覽器**存取內容。
- 使用者屬於**銷售團隊**群組。
- 實作的驗證方法包括使用行動裝置和電腦登入的功能。
  - 使用**行動 SSO (適用於 iOS)** 進行驗證。
  - 回復至**行動 SSO (適用於 Android)**。
  - 回復至 **RSA SecurID**。
- 系統會在 **4 小時**後重新驗證工作階段。

若要從企業網路外部存取這些應用程式，視裝置類型而定，外部使用者需要使用行動裝置通行碼或 RSA SecurID 通行碼才能登入應用程式。工作階段隨即開始，且持續時間為四小時。四小時後，系統會提示使用者再次登入。

範例 2 為指派給群組的嚴格 Web 應用程式特定原則

在此範例中，您將建立應用程式特定的存取原則，並套用至高度機密的 Web 應用程式。銷售團隊群組成員可以從任何類型的裝置存取此應用程式，但 1 小時後系統會要求再次驗證。

- 網路範圍為 **ALL RANGES**。
- 使用者可從**所有裝置類型**存取內容。
- 使用者屬於**銷售團隊**群組。
- 驗證方法為 **RSA SecurID**。
- 系統會在 **1 小時**後重新驗證工作階段。

銷售團隊使用者登入後，將根據預設存取原則規則進行驗證，且能存取應用程式入口網站和資源。使用者按一下由嚴格存取原則規則管理的應用程式，如範例 2 所述。系統會將使用者重新導向至 RSA SecurID 驗證登入畫面。

使用者成功登入後，服務會啟動應用程式並儲存驗證事件。使用者可繼續啟動應用程式，且一小時內不需登入。1 小時後，系統會提示使用者透過 RSA SecurID 重新驗證。

新增拒絕存取原則

您可以建立拒絕存取規則，以根據網路範圍和裝置類型來拒絕應用程式存取。

程序

1 在 VMware Identity Manager 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**。

3 在各自的文字方塊中新增原則名稱和說明。

4 在**套用至**區段的 [搜尋] 文字方塊中輸入應用程式，然後選取要與此原則建立關聯的應用程式。

5 按**下一步**。

6 按一下**新增原則規則**以新增規則。

選項	說明
如果使用者的網路範圍為	選取網路範圍。
且使用者正在存取來自下列裝置的內容	選取此規則所要管理的裝置類型。
且使用者屬於群組	如果此存取規則將套用至特定群組，請在搜尋方塊中搜尋群組。 若未選取任何群組，則存取原則規則會套用至所有使用者。
則執行此動作	選取**拒絕存取**。

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。

自訂訊息可包含訊息和連往其他 URL 的連結，以協助使用者解決問題。您可以使用最多 4000 個字元，大約為 650 字。

程序

1 在 VMware Identity Manager 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 選取要編輯的存取原則。

3 按一下**編輯**，然後按**下一步**。

4 選取要編輯的規則。

5 按一下**進階屬性**，然後在**自訂錯誤訊息**文字方塊中輸入錯誤訊息。

6 若要新增 URL 的連結，請在**自訂錯誤連結文字**文字方塊中輸入顯示為連結、以在驗證失敗時將使用者傳送至另一個畫面的訊息。

   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] 文字方塊中新增訊息，顯示的連結將會是

   ```
   繼續。
   ```

7 在**自訂錯誤連結 URL** 文字方塊中，輸入 URL。

8 按一下**儲存**、按**下一步**，然後再按一下**儲存**。

後續步驟

為其他原則規則建立自訂錯誤訊息。

為 Workspace ONE UEM 管理的裝置啟用符合性檢查

當使用者註冊其裝置時，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 Workspace ONE UEM (UEM) 主控台中設定的符合性規則。如果裝置不合規，則會採取在 UEM 主控台中設定的對應動作。

VMware Identity Manager 服務包含存取原則選項，經設定可在使用者從裝置登入時用來檢查 Workspace ONE UEM 伺服器中的裝置符合性狀態。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 Workspace ONE 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 Intelligent Hub 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 UEM 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。

如需有關 Workspace ONE UEM 符合性原則的詳細資訊，請參閱 VMware Workspace ONE UEM 說明文件頁面中的《VMware Workspace ONE UEM Mobile Device Management 指南》。

設定符合性檢查規則

符合性檢查啟用時，您可以建立必須對 Workspace ONE UEM 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 版行動 SSO、Android 版行動 SSO 及憑證雲端部署的驗證鏈結中運作。設定規則時，所使用的驗證方法必須優先於裝置符合性方法。

先決條件

已設定驗證方法，並使其與內建身分識別提供者建立關聯。

在 VMware Identity Manager AirWatch 頁面中已啟用符合性檢查。

程序

1 在 VMware Identity Manager 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**編輯預設原則**。

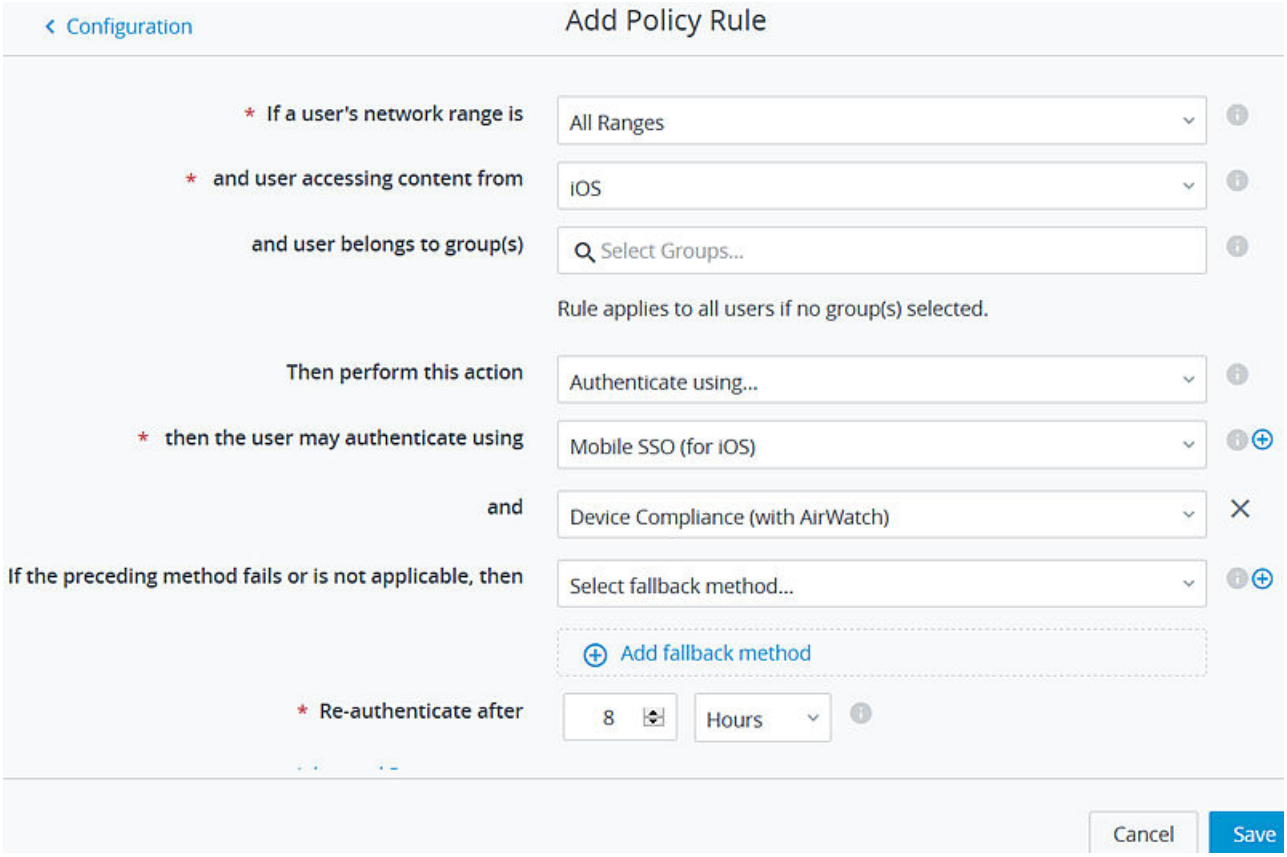
3 按**下一步**。

4 按一下**新增原則規則**以新增規則，或選取要編輯的規則。

選項	說明
如果使用者的網路範圍為	確認網路範圍是否正確，如果新增規則，請選取網路範圍。
且使用者正在存取來自下列裝置的內容	選取行動裝置類型。
且使用者屬於群組	如果此存取規則將套用至特定群組，請在搜尋方塊中搜尋群組。 若未選取任何群組，則存取原則會套用至所有使用者。
則執行此動作	選取**使用下列方法進行驗證...**。
則使用者可使用下列方法進行驗證	選取要套用的行動裝置驗證方法。 按一下 **[+]**，然後在下拉式功能表中選取**裝置符合性 (與 AirWatch)**。

選項	說明
如果前述方法失敗或不適用，則	如有必要，請設定後援驗證方法。
在以下時間之後重新驗證	選取工作階段的長度之後，使用者必須重新進行驗證。

5 按一下儲存。



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，啟用使用者工作階段的持續性 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 VMware Identity Manager 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**。

後續步驟

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。

為 Workspace ONE 全新體驗程序建立存取原則

若要在外部存取權杖已啟用並新增至內建身分識別提供者之後建立 Workspace ONE 全新體驗 (OOBE)，您必須將外部存取權杖驗證方法新增至預設存取原則集。

先決條件

在 [身分識別與存取管理] > [驗證方法] 頁面中，將外部存取權杖驗證啟用為內建身分識別提供者的驗證方法。

程序

1 在 VMware Identity Manager 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**編輯預設原則**，然後按**下一步**。

3 選取在 [裝置類型] 資料行中列出 **Workspace ONE 應用程式**的資料列。

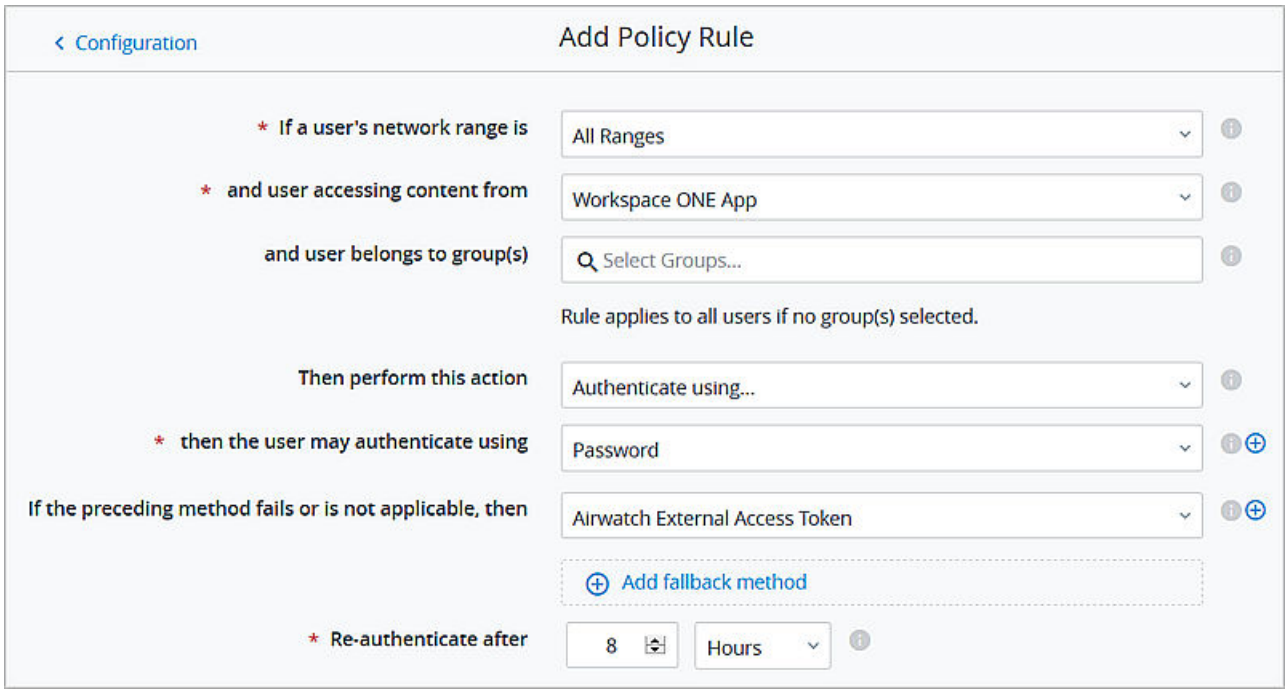
如果未列出 Workspace ONE 應用程式規則，請按一下**新增原則規則**，然後建立以 Workspace ONE 應用程式作為裝置類型的規則。

4 選取要用來存取 Workspace ONE 應用程式之內容的驗證方法。

將外部存取權杖驗證方法列為規則中的最後一個後援方法。在驗證要求中偵測到外部存取權杖時，即會採用該驗證方法。系統不會偵測到任何在外部存取權杖之後列出的其他驗證方法。

5 按**下一步**以檢閱組態。

6 按一下**儲存**。



7 在 [組態] 頁面上，檢閱規則清單中的規則順序。如果 Workspace ONE 應用程式規則不是預設存取原則清單中的第一個規則，請將該規則拖曳至清單中的第一列。

Workspace ONE 應用程式必須是預設存取原則規則清單中的第一個規則。

8 按**下一步**。

9 檢閱 [摘要] 頁面，然後按一下**儲存**。

管理使用者和群組

8

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。

VMware Identity Manager 服務中的使用者可以是從您的企業目錄同步的使用者、您在 VMware Identity Manager 主控台中佈建的本機使用者，或是使用 Just-in-Time 佈建新增的使用者。

從您的企業目錄匯入的使用者，會根據您的伺服器同步化排程在 VMware Identity Manager 目錄中更新。您無法編輯或刪除從 Active Directory 同步的使用者。

您可以建立本機使用者和群組。本機使用者可新增至服務的本機目錄。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 佈建新增的使用者，會在使用者登入時根據身分識別提供者所傳送的 SAML 判斷提示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 4 章，Just-in-Time 使用者佈建。

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 VMware Identity Manager 主控台中建立的本機群組。Active Directory 群組名稱會根據您的同步排程同步至目錄。在群組有權使用資源或群組新增至存取原則規則之前，這些群組中的使用者不會同步至目錄。您無法編輯或刪除從 Active Directory 同步的群組。

在 VMware Identity Manager 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，以及監控資源權利、群組關係和 VMware Verify 電話號碼。針對本機使用者，您也可以管理密碼原則。

本章包含以下主題：

管理使用者

在 VMware Identity Manager 服務中，使用者可依其名稱和網域精確識別出來。這可讓您在不同 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。

在 VMware Identity Manager 中設定目錄之前，您需要指定哪些是必要的預設使用者屬性，並新增要對應至 Active Directory 屬性的其他屬性。您在 Active Directory 中選取要對應至這些屬性的屬性和篩選器，將決定哪些 Active Directory 使用者會在 VMware Identity Manager 目錄中進行同步。如需關於如何整合 Active Directory 與 VMware Identity Manager 的詳細資訊，請參閱《目錄與 VMware Identity Manager 的整合》文件。

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。

提示 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。

在 VMware Identity Manager 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 4 章，Just-in-Time 使用者佈建以取得相關資訊。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。

從 Active Directory 中選取要新增至目錄的使用者

當使用者設定檔從 Active Directory 同步至 VMware Identity Manager 目錄時，系統會新增 Active Directory 使用者。

由於群組成員在群組具有權利之前不會進行同步，因此請在最初設定 VMware Identity Manager 時新增所有需要存取 VMware Identity Manager 服務的使用者。

先決條件

Active Directory 屬性已對應至 [身分識別與存取管理] > [設定] > [使用者屬性] 頁面中的使用者屬性。如需關於如何整合 Active Directory 與 VMware Identity Manager 的詳細資訊，請參閱《目錄與 VMware Identity Manager 的整合》出版品。

程序

1 在 VMware Identity Manager 主控台的 [身分識別與存取管理] 索引標籤中，按一下**管理員 > 目錄**。

2 選取要更新使用者篩選器的目錄。

3 按一下**同步設定**，然後選取**使用者**。

4 在**指定使用者 DN** 資料列中按一下 **+**，並輸入使用者 DN。

輸入針對 Active Directory 設定之基準 DN 下的使用者 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。

5 按一下**儲存**。

檢閱使用者設定檔資訊

VMware Identity Manager 主控台中的 [使用者] 頁面會顯示能夠登入 Workspace ONE 的使用者。

選取使用者名稱可檢視詳細的使用者資訊。

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。

使用者設定檔頁面也包含群組、VMware Verify 和應用程式的連結。[群組] 頁面會顯示使用者所屬的群組。VMware Verify 會列出設定為使用 VMware Verify 進行驗證的裝置。[應用程式] 頁面會列出使用者有權使用的應用程式。

管理群組

在 VMware Identity Manager 服務中，群組可依群組名稱和網域精確識別出來。

從 VMware Identity Manager 3.1 開始，當新的群組從 Active Directory 新增至目錄時，群組名稱即會同步至目錄。在下列情況下，屬於群組成員的使用者可以同步至目錄。

- 群組有權使用 Workspace ONE 中的應用程式。
- 群組名稱已新增至存取原則。
- 群組中的使用者已從 [群組] > [使用者] 設定檔頁面手動同步。

在 3.1 之前，群組的成員會在群組新增時同步至目錄。

備註 如果在群組同步至目錄之前需要驗證某些使用者，您可以將個別使用者新增至目錄的 [同步設定] > [使用者] 頁面。

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，您可以在網域 eng.example.com 中有稱為 ALL_USERS 的群組，而在網域 sales.example.com 中有另一個稱為 ALL_USERS 的群組。

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 VMware Identity Manager 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。在此清單中，您可以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」。

將 Active Directory 群組同步至目錄

當群組辨別名稱從企業目錄對應至 VMware Identity Manager 目錄時，群組名稱會新增至該目錄。群組成員不會同步至目錄。

VMware Identity Manager 主控台中的 [群組] 頁面會顯示已同步的群組名稱。[群組中的使用者] 資料行會顯示已同步的成員數目。如果成員尚未同步，則 [群組中的使用者] 資料行會顯示**未同步**。

群組成員會在群組有權使用 [目錄] 中的應用程式或群組新增至 VMware Identity Manager 中的存取原則規則時同步至目錄。您也可以從 [群組] > [使用者] 頁面手動同步屬於群組成員的使用者。

升級至 VMware Identity Manager 3.1 之後群組同步的運作方式

VMware Identity Manager 升級至 3.1 版或更新版本之後，群組成員資格的同步行為會取決於群組 DN 何時設定於服務中。

- 當您升級至 VMware Identity Manager 3.1 和更新版本時，在升級後新增至服務的新群組會在該群組有權使用資源時，或在該群組新增至存取原則規則時進行成員的同步。此群組後續的同步會遵循較舊的行為。
- 在升級至 3.1 之前新增的群組，即便該群組無權使用資源或未用於存取原則規則中，仍會繼續在其成員新增至群組時同步群組成員。也就是說，針對現有的群組和使用者，系統會保留 3.1 之前的行為。
- 如果某個群組在升級前即已存在，則在 DN 組態經過修改後，群組同步設定檔將會變更為新的行為。群組名稱會同步至目錄。群組成員會在群組有權使用資源時或群組新增至存取原則規則時進行同步。
- 即便從群組中移除權利，群組中的使用者仍會在後續同步中繼續進行同步。
- 如果在 VMware Identity Manager 服務中建立包含 Active Directory 群組的本機群組，且該本機群組有權使用資源，則該本機群組中 Active Directory 群組所包含的使用者並不會作為權利的一部分而同步至目錄。若要同步 Active Directory 群組中的使用者，請直接賦予 Active Directory 群組使用資源的權利。

建立本機群組和設定群組規則

您可以建立群組、將成員新增至群組，以及建立群組規則。接著，您可以根據自己定義的規則來填入群組。

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。

您可以指定要套用至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 VMware Identity Manager 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 將使用者新增至群組。若要將使用者新增至群組，請輸入使用者名稱的若干字母。當您輸入文字時，系統會顯示相符的名稱。

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，以管理群組中哪些使用者屬於您建立的群組的成員。
屬性規則	下列規則是否可用，視您所選取的屬性而定。 ■ 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 sales_username@example.com。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 sales_」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 hr_username@example.com，那麼您可以設定類似「電子郵件開頭不是 hr_」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	(選用) 若要將「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。 ■ 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；群組是客戶服務」。針對「群組是客戶服務」，「下列所有項目：電子郵件開頭為 cs_；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 cs，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**。

後續步驟

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 VMware Identity Manager 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。所有群組成員皆可存取該群組有權使用的應用程式。

先決條件

應用程式會新增至 [目錄] 頁面。

程序

1 在 VMware Identity Manager 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**。

同步會在背景中執行。同步完成後，群組中的使用者會同步至目錄且有權使用應用程式。

將群組的成員手動同步至 VMware Identity Manager 目錄

您可以在群組有權使用應用程式或設定於原則規則中之前，將該群組的成員同步至 VMware Identity Manager 目錄。

程序

1 在 VMware Identity Manager 主控台的 [使用者和群組] 索引標籤中，選取**群組**。

2 按一下要同步的群組名稱。

3 開啟**使用者**索引標籤，然後按一下**同步使用者**。

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

程序

1 在 VMware Identity Manager 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。

後續步驟

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 VMware Identity Manager 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。

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 VMware Identity Manager 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 [帳戶設定] > [設定檔] 頁面中的下拉式功能表依名稱變更其密碼。

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 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。您也可以設定鎖定原則

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。

您可以設定帳戶鎖定原則，以防止未經授權的情況下存取帳戶。原則設定可決定在一段特定時間內登入嘗試失敗多少次時會啟動使用者帳戶鎖定。帳戶會依據原則中定義的分鐘數處於鎖定狀態。預設組態是在 15 分鐘內嘗試登入失敗五次。當使用者在 15 分鐘內第六次嘗試登入並失敗時，帳戶將會鎖定 15 分鐘。

程序

1 在 VMware Identity Manager 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。底數 10 的基本數字 (0-9)
特殊字元	非英數字元 (例如 & # % $!) 的數目下限
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。
允許先前密碼的字元數	強制執行可在新密碼中重複使用的字元數目下限。例如，如果設為 0，使用者無法使用任何與先前密碼相同的字元。如果此文字方塊保留為空白，則不會套用此規則。

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。若不要設定密碼存留期原則，請輸入 0。

4 在 [帳戶鎖定] 區段中定義帳戶鎖定原則。

選項	說明
密碼失敗的嘗試次數	可輸入錯誤密碼的次數。預設值為 5。如果您將預設值設為 0，則帳戶永遠不會因為密碼嘗試失敗而遭到鎖定。
驗證失敗嘗試次數的間格	計算登入失敗嘗試次數的分鐘數。預設值為 15 分鐘。
帳戶鎖定期間	達到失敗的驗證嘗試間隔後，帳戶即會依據此處設定的分鐘數處於鎖定狀態。在這段時間結束後，帳戶會自動解除鎖定。預設值為 15 分鐘。如果您將分鐘數設為 0，則使用者的帳戶不會遭到鎖定。使用者可以持續重新嘗試登入。

5 按一下**儲存**。

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 VMware Identity Manager 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。

管理目錄

9

目錄是您可授權給使用者之所有資源的存放庫。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。用來填入目錄的方法取決於資源類型。

您可以將下列類型的資源與 VMware Identity Manager 整合。

- Web 應用程式
- VMware Horizon Cloud Service 應用程式和桌面平台
- VMware Horizon® 7、Horizon 6 和 View 桌面平台與應用程式集區
- Citrix 發佈的資源
- VMware ThinApp® 封裝應用程式

這些資源分別位於適用於 Web 應用程式的 [Web 應用程式] 頁面，或適用於 Horizon、Citrix、Horizon Cloud 或 ThinApp 桌面平台和應用程式的 [虛擬應用程式] 頁面。Web 應用程式可直接從 [Web 應用程式] 頁面新增至您的目錄。

若要整合及啟用 Horizon Cloud Service、Horizon Client 桌面平台和應用程式集區、Citrix 發佈的資源或 ThinApp 封裝應用程式，您需要使用 [虛擬應用程式] 頁面上的 [虛擬應用程式集合] 功能。

如需設定資源的相關資訊，請參閱《在 VMware Identity Manager 中設定資源》指南。

本章包含以下主題：

將資源分組為類別

您可以將資源歸類為邏輯類別，以便使用者從瀏覽器在其 Workspace ONE 應用程式入口網站中尋找他們所需的資源，或是在裝置上從 VMware Workspace ONE® Intelligent Hub 應用程式中尋找資源。

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。例如，您可以建立稱為 HR 的類別，以及另一個稱為「福利」的類別。請將 HR 指派給目錄中的所有 HR 資源。同時請將「福利」指派給您想要讓使用者使用的特定 HR 福利資源。您也可以將多個類別指派給資源。例如，上述範例中的資源也可以屬於「銷售」類別。

目錄中會顯示名為**建議**的預先定義類別。您可以將常用的應用程式歸類為「建議」；這些應用程式將會在應用程式入口網站中和使用者裝置上的 Intelligent Hub 應用程式中顯示為「建議」。使用者可以檢視建議的應用程式清單，並將其新增至應用程式入口網站和裝置。

在應用程式入口網站中，歸類為「建議」的應用程式可設定為會自動推送至 [書籤] 頁面。在 [目錄] > [設定] > [使用者入口網站組態] 頁面中，選取**在 [書籤] 索引標籤中顯示建議的應用程式**選項。使用者會看到這些應用程式自動出現在其 [書籤] 頁面中。此功能可讓新的使用者更輕鬆接收您建議他們使用的應用程式。此方法可簡化新使用者接收應用程式的方式。當建議的應用程式自動出現在 [書籤] 中時，其行為就如同使用者已新增一般。這表示僅使用者可將其移除。管理員無法在建議的應用程式新增至 [書籤] 後加以移除。

在 Intelligent Hub 應用程式中，[建議] 區段會顯示您歸類為「建議」的常用應用程式。使用者可選取應用程式加以使用，並且可將其標記為我的最愛。這些應用程式會顯示在 Intelligent Hub 應用程式的 [我的最愛] 區段中。此外，在應用程式入口網站中顯示於 [書籤] 頁面中的應用程式，也會顯示在 Intelligent Hub 應用程式的 [我的最愛] 中。

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 VMware Identity Manager 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。

後續步驟

將類別套用至其他應用程式。請參閱套用類別至資源。

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 VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager 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。

管理目錄中的設定

目錄設定包括適用於目錄中所有資源的全域設定，以及 Web 應用程式或虛擬應用程式的專用設定。

下列全域目錄設定可從 [目錄] > [設定] 功能表中存取。

- 「全域設定」，可停用為虛擬應用程式下載協助程式應用程式的啟動器喜好設定提示。
- 「遠端應用程式存取」，用以建立要啟用遠端應用程式存取的用戶端。
- 「使用者入口網站品牌」，用以自訂 Workspace ONE 使用者入口網站的標誌和背景外觀。
- 「使用者入口網站組態」，用以自訂在 Workspace ONE 使用者入口網站頁面中顯示資源的方式。
- 「People Search」，用以在 Workspace ONE 中啟用此功能。

[Web 應用程式] 頁面上的 [目錄] > [Web 應用程式] > [設定] 功能表包含 [全域核准] 選項 (用來管理需要核准的應用程式存取) 和 [SaaS 應用程式] 頁面 (用來產生簽署憑證)。

[目錄] > [虛擬應用程式] > [虛擬應用程式設定] 頁面包含 [網路設定] (列出已設定的網路範圍)、[Citrix 發佈的應用程式] 頁面 (為個別 Citrix 發佈的應用程式和桌面平台編輯設定)，和 [ThinApp 應用程式警示] 連結 (用來檢視 ThinApp 警示)。

請參閱在 VMware Identity Manager 中設定資源

停用下載協助程式應用程式之提示的全域設定

Horizon 桌面平台、Citrix 發行的應用程式和 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。

- Horizon 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 [目錄] 索引標籤中，選取**設定 > 全域設定**。

2 選取不應要求啟動協助程式應用程式的作業系統。

3 按一下**儲存**。

建立適用於遠端應用程式存取的用戶端

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，以允許使用者存取 [目錄] > [設定] 頁面中啟用的特定應用程式。

您也可以建立範本，讓用戶端群組動態地對 VMware Identity Manager 服務進行登錄，進而允許存取指定的應用程式。

初始使用者驗證要求須遵循 OIDC 規格中定義的驗證流程。

管理存取權杖存留時間

存取權杖會提供對應用程式安全的暫時性存取。存取權杖具有有限的存留期。當您建立用戶端認證時，即會設定存取權杖的存留時間 (TTL)。設定的時間即為可在應用程式內使用有效存取權杖的時間上限。

如果使用者經常使用某個應用程式，例如 Workspace ONE，則可以將用戶端認證設定為不要求這些使用者在每次存取權杖到期時都必須登入。

啟用 [發出重新整理權杖] 即可在存取權杖到期時，讓應用程式使用重新整理權杖以要求新的存取權杖。重新整理權杖會使用 TTL 進行設定。在重新整理權杖到期之前皆可要求新的存取權杖。當重新整理權杖到期時，使用者必須登入應用程式。

您可以設定重新整理權杖在無法再次使用之前的閒置時間長度。如果重新整理權杖未使用的時間已達重新整理權杖閒置 TTL，則使用者必須重新登入應用程式。

範例：存取權杖存留時間的運作方式

用戶端認證中存取權杖存留時間 (TTL) 設定的設定方式如下所示。

- 存取權杖 TTL 設為九小時
- 重新整理權杖 TTL 設為三個月
- 重新整理權杖閒置 TTL 設為七天

如果使用者每天使用應用程式，則根據重新整理權杖 TTL 設定，使用者在三個月內皆不需再次登入。不過，如果使用者閒置且未使用應用程式達七天，則根據重新整理權杖閒置 TTL 設定，使用者將需要在七天之後登入。

設定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。

登錄應用程式的詳細資料，可將該應用程式識別為 OAuth 服務的受信任用戶端。

您可以將用戶端識別碼、用戶端密碼和重新導向 URI 登錄至 VMware Identity Manager 服務。

程序

1 在 VMware Identity Manager 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]。設為**服務用戶端權杖**。這表示應用程式會代表本身存取 API，而非代表使用者存取。
用戶端識別碼	輸入應用程式用來對 VMware Identity Manager 進行驗證的唯一用戶端識別碼。用戶端識別碼不得與您承租人中的任何用戶端識別碼相符。可使用的字元如下：英數字元 (A-Z、a-z、0-9)、句號 (.)、底線 (_)、連字號 (-) 和 @ 記號。
應用程式	選取 [Identity Manager]。
範圍	選取權杖包含的資訊。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	按一下**進階**。

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	若要使用重新整理權杖，請保持此選項的啟用狀態。
權杖類型	選取 [持有人]。此屬性會告訴應用程式它收到的存取權杖類型。VMware Identity Manager 的權杖是持有人權杖。
存取權杖 TTL	存取權杖的到期時間取決於**存取權杖存留時間**中所設定的秒數。如果啟用 [發出重新整理權杖]，則當存取權杖到期時，應用程式將會使用重新整理權杖以要求新的存取權杖。
重新整理權杖 TTL	設定「重新整理權杖」存留時間。在重新整理權杖到期之前皆可要求新的存取權杖。
閒置權杖 TTL	設定重新整理權杖在無法再次使用之前的閒置時間長度。
使用者授與	請勿選取**提示使用者進行存取**。

4 按一下**新增**。

用戶端組態會顯示在 [OAuth2 用戶端] 頁面上。

後續步驟

在資源應用程式中，設定用戶端識別碼和產生的共用密碼。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 VMware Identity Manager 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	輸入可識別此範本的唯一名稱。
應用程式	選取 [Identity Manager]
範圍	選取權杖包含的資訊。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	按一下**進階**。
權杖類型	選取 [持有人]。此屬性會告訴應用程式它收到的存取權杖類型。VMware Identity Manager 的權杖是持有人權杖。
權杖長度	保留預設設定：32 個位元組。

標籤	說明
發出重新整理權杖	若要使用重新整理權杖，請保持此選項的啟用狀態。
存取權杖 TTL	設定存取權杖的存留時間長度。存取權杖的到期時間取決於**存取權杖存留時間**中所設定的 TTL。如果啟用 [發出重新整理權杖]，則當存取權杖到期時，應用程式將會使用重新整理權杖以要求新的存取權杖。
重新整理權杖 TTL	設定「重新整理權杖」存留時間。在重新整理權杖到期之前皆可要求新的存取權杖。
閒置權杖存留時間 (TTL)	設定重新整理權杖在無法再次使用之前的閒置時間長度。
使用者授與	請勿選取 [提示使用者進行存取]。

5 按一下**新增**。

後續步驟

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。

設定 Workspace ONE 入口網站中的目錄和書籤索引標籤視圖

Workspace ONE 入口網站的預設視圖會顯示 [目錄] 頁面和 [書籤] 頁面。

您可以變更入口網站組態以僅顯示其中一個頁面。如果未隱藏 [書籤] 頁面，您可以選取**在 [書籤] 索引標籤中顯示建議的應用程式**，以在 [書籤] 頁面中預先填入標示為 [建議] 的應用程式。

程序

1 在 [目錄] > [設定] 頁面中，選取**使用者入口網站組態**。

2 針對您要隱藏的索引標籤選取方塊，例如 **[隱藏目錄] 索引標籤**或 **[隱藏書籤] 索引標籤**。

3 如果您選取 [隱藏目錄] 索引標籤，您可以啟用**在 [書籤] 索引標籤中顯示建議的應用程式**。

[書籤] 索引標籤會預先填入標示為 [建議] 的應用程式。

使用者入口網站視圖每 24 小時會重新整理一次，以顯示這些變更。若要在較短的時間內推送變更，請以管理員身分開啟新的索引標籤並輸入此 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`。

針對資源使用量啟用應用程式核准

您可以在 [目錄] > [Web 應用程式設定] 頁面中啟用 [核准]，並在應用程式中設定授權，以針對需要由您的組織核准的應用程式進行存取管理。

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。應用程式圖示會顯示「擱置」通知。

VMware Identity Manager 會將核准要求訊息傳送至組織已設定的核准 REST 端點 URL。伺服器工作流程程序會檢閱要求，然後將核准或拒絕訊息傳回至 VMware Identity Manager。應用程式經過核准後，「擱置」會變更為「已新增」，且應用程式會顯示在使用者的 Workspace ONE 啟動器頁面中。

您可以使用兩種核准引擎。

- REST API。REST API 核准引擎會使用透過您 Webserver REST API 進行路由的外部核准工具來執行要求和核准回應。您可以在 VMware Identity Manager 服務中輸入您的 REST API URL，然後使用 VMware Identity Manager OAuth 用戶端認證值以及圖說文字要求和回應動作來設定您的 REST API。
- 透過連接器的 REST API。透過連接器的 REST API 核准引擎會使用 Websocket 型通訊通道，並透過連接器進行回呼的路由。您可以使用圖說文字要求和回應動作設定您的 REST API 端點。

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 REST API 核准引擎

您可以登錄您的標註 REST URI 以整合應用程式管理系統與 VMware Identity Manager。

先決條件

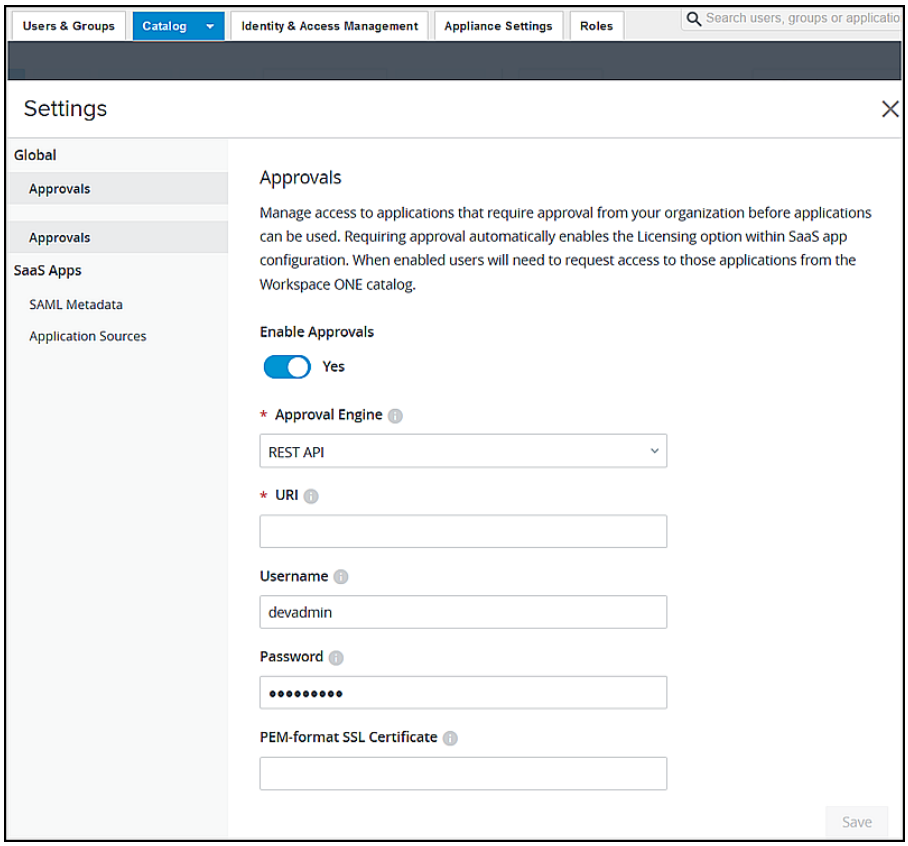
當您選取 REST API 核准引擎時，您必須已設定應用程式管理系統，並且可透過從 VMware Identity Manager 接收要求的標註 REST API 取得 URI。

程序

1. 在 VMware Identity Manager 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 **REST API**。
4. 設定下列文字方塊。

選項	說明
URI	輸入接聽標註要求之 REST 資源的回撥 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。

選項	說明
密碼	(選用) 輸入使用者的密碼。
PEM 格式 SSL 憑證	(選用) 如果您的 REST 資源執行所在的伺服器具有自我簽署憑證或不受公用憑證授權機構信任的憑證，且使用的是 HTTPS，請在此處新增 PEM 格式的 SSL 憑證。



後續步驟

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。

SAML 簽署憑證

SAML 簽署憑證可確保訊息會來自預期的身分識別和服務提供者。SAML 憑證會用來簽署從服務到信賴應用程式 (例如 WebEx 或 Google Apps) 的 SAML 要求、回應和判斷提示。

[SAML 中繼資料] 頁面會顯示於 [目錄] > [設定] 索引標籤中。隨即會顯示 SAML 簽署憑證。此頁面也會顯示 SAML 身分識別提供者和服務提供者中繼資料檔案的連結。中繼資料包含組態資訊和憑證。

系統會在 VMware Identity Manager 服務中自動建立 SAML 簽署所需的自我簽署憑證。如果您的組織需要來自憑證授權機構的憑證，您可以從 VMware Identity Manager 主控台產生憑證簽署要求 (CSR)，並使用該 CSR 來產生憑證。當您收到已簽署的憑證時，您可以將憑證上傳至 VMware Identity Manager 服務以取代自我簽署憑證。SAML 簽署憑證和 SAML 中繼資料檔案會使用新憑證進行更新。

下載 SAML 憑證以設定信賴應用程式

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 在 VMware Identity Manager 主控台的 [目錄] 索引標籤中，選取 **Web 應用程式設定 > SAML 中繼資料**。

   a 複製**簽署憑證**區段中的憑證資訊。

2 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 **SAML 中繼資料**區段中，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。

3 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。

後續步驟

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。

產生憑證簽署要求

若要將外部憑證用於 SAML 簽署，您必須從 VMware Identity Manager 主控台產生憑證簽署要求 (CSR)。CSR 會傳送至憑證授權機構以產生 SSL 憑證。

備註 不支援在未使用 CSR 的情況下從 VMware Identity Manager 主控台產生憑證。

程序

1 在 [目錄] 索引標籤中，選取 **Web 應用程式設定 > SAML 中繼資料**。

2 按一下**產生 CSR**

3 輸入要求的資訊。具有星號 (*) 的選項為必填。

選項	說明
一般名稱*	輸入完整網域名稱，例如 `www.example.com`。
組織*	輸入組織的合法登錄名稱。例如，`Mycompany, Inc.`
部門	輸入在憑證中新增的公司部門。例如，`IT Services`。
城市*	輸入您的組織合法登記的所在城市。
州/省*	輸入您的組織所在的州或區域。請勿使用縮寫。
國家/地區*	輸入國家/地區名稱的數個字母，即可從清單中選取正確的國家/地區。
金鑰產生演算法*	選取用來簽署 CSR 的安全雜湊演算法。
金鑰大小*	選取金鑰中使用的位元數。建議使用 RSA 2048。RSA 金鑰大小小於 2048 時會視為不安全。

4 按一下**產生**。

將 CSR 提供給憑證授權機構以建立憑證。

後續步驟

當您收到憑證時，請將憑證上傳至 VMware Identity Manager 服務。CA 會取代自我簽署憑證。

上傳 SAML 簽署憑證的新憑證授權機構

發行已簽署的憑證後，請從 [目錄] > [SAML 中繼資料] 頁面上傳檔案，並重新啟動服務以更新中繼資料。

先決條件

產生憑證簽署要求。

將您收到的已簽署憑證儲存至可從 VMware Identity Manager 主控台存取的檔案。

程序

1 在 [目錄] 索引標籤中，選取 **Web 應用程式設定 > SAML 中繼資料**。

2 按一下**產生 CSR**。

3 按一下**上傳憑證**，然後導覽至憑證。

4 按一下**開啟**。

SAML 簽署憑證和 SAML 中繼資料檔案會使用新憑證進行更新。

5 移至 [身分識別與存取管理] 索引標籤中的**設定 > 連接器**，然後按一下**重新啟動**。

連接器中的中繼資料即會進行更新。

後續步驟

重要　使用已更新的 SAML 中繼資料檔案，重新設定所有 SAML 服務提供者和身分識別提供者組態。此作業包括重新設定已設定的其他連接器。若未執行此動作，SAML 交易將會失敗，且單一登入將無法正常運作。

設定應用程式來源

您可以在 Workspace ONE 目錄中新增第三方身分識別提供者作為應用程式來源，以簡化從第三方身分識別提供者到 Workspace ONE 的大量應用程式部署程序。

使用 SAML 2.0 驗證設定檔的 Web 應用程式可以新增至目錄。應用程式組態以應用程式來源中所做的設定為基礎。您僅需設定應用程式名稱和目標 URL。

從第三方應用程式來源所設定的設定和原則，可套用至受應用程式來源管理的所有應用程式。

如需詳細資訊，請參閱《在 VMware Identity Manager 中設定資源》指南的〈提供在 Workspace ONE 中對第三方受管理應用程式的存取權〉一章。

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 內容文字方塊會是空的。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。

在 VMware Identity Manager 主控台儀表板中工作

10

管理主控台內的使用者參與儀表板可用來監控使用者和資源使用量。

本章包含以下主題：

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。

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。您可以查看整個 VMware Identity Manager 資料庫伺服器以及每個機器上各項可用服務的整體健全狀況。

您可以在 [系統診斷儀表板] 中選取您要監控的機器，並查看該機器上的服務狀態，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，您可以選取顯示為紅色的機器。

每個服務的資訊會個別載入。會顯示每個服務上次更新資料的時間與日期。您可以重新整理每個區段以取得更新的資訊。

服務受到監控	說明
磁碟空間	磁碟空間使用量資訊會依 /db、/var、/opt/vmware 和 /horizon 的磁碟分割顯示。
連接埠連線	會顯示叢集中每個節點的連接埠連線情形。
使用者密碼過期	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。
設定程式 - 應用程式部署狀態	[Web 伺服器狀態] 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。
整合式元件	會顯示 VMware Identity Manager 資料庫連線、稽核服務、分析連線資訊、Elasticsearch 健全狀況，以及 Elasticsearch 組態詳細資料。
憑證	顯示憑證簽發者、主體、開始日期和結束日期。若要管理憑證，請移至 [應用裝置設定] 頁面並選取 **VA 組態**。開啟**安裝 SSL 憑證**頁面。
ACS 健全狀況 - 應用程式部署狀態	
檔案權限檢查	會顯示為下列檔案授與的權限層級。 ■ /etc/krb5.conf 檔案擁有者 ■ /etc/krb5.conf 檔案群組 ■ /etc/krb5.conf 檔案權限 ■ /usr/local/horizon/conf/idm-cacerts 檔案擁有者 ■ /usr/local/horizon/conf/idm-cacerts 檔案群組 ■ /usr/local/horizon/conf/idm-cacerts 檔案權限
應用程式管理員 - 應用程式部署狀態	顯示 VMware Identity Manager Web 應用程式連線狀態。

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 10-1. 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。
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。
角色成員資格	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。
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的使用者相關的事件，例如，過去 30 天的使用者登入情形和登入失敗。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。請參閱產生稽核事件報告。

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。

程序

1 在 VMware Identity Manager 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	選取此文字方塊，可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	此下拉式功能表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。此下拉式功能表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	此下拉式功能表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] 下拉式功能表中選取了存取事件，由於這是非動作事件，因此請不要在 [動作] 下拉式功能表中指定動作。

稽核事件準則	說明
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**。

使用 SSL 憑證

11

安裝 VMware Identity Manager 應用裝置後，系統會自動產生預設的 SSL 伺服器憑證。您可以對您的實作的一般測試使用此自我簽署憑證。

CA 是一個受信任的實體，可保證憑證的身分及其建立者。當憑證是由受信任的 CA 簽署時，使用者不會再收到要求他們驗證憑證的訊息。

您可以從**應用裝置設定 > 管理組態 > 安裝 CA 憑證 > 伺服器憑證**頁面安裝已簽署的 CA 憑證。

如果您使用自我簽署 SSL 憑證部署 VMware Identity Manager，根 CA 憑證必須作為受信任的 CA 提供給存取 VMware Identity Manager 服務的任何用戶端使用。用戶端可包含使用者機器、負載平衡器和 Proxy 等。您可以從**安裝 SSL 憑證 > 伺服器憑證**頁面下載根 CA。

安裝 VMware Identity Manager Connector 後，系統會產生預設的自我簽署 SSL 憑證。在多數情況下，您可以繼續使用此自我簽署憑證。您可以從連接器管理頁面為連接器安裝已簽署的 SSL 憑證，網址為 **`https://connectorFQDN:8443/cfg/login`**。請參閱將 SSL 憑證用於 VMware Identity Manager Connector。

本章包含以下主題：

- 安裝適用於 VMware Identity Manager 服務的 SSL 憑證
- 安裝受信任的根憑證
- 安裝傳遞憑證
- 取代 VMware Identity Manager 服務中的 SSL 憑證
- 更新連接器的 SSL 憑證

安裝適用於 VMware Identity Manager 服務的 SSL 憑證

安裝 VMware Identity Manager 服務時，系統會產生預設 SSL 伺服器憑證。您可以使用此自我簽署憑證進行測試。不過，最佳做法是將公用憑證授權機構 (CA) 所簽署的 SSL 憑證用於生產環境。

備註 如果位於 VMware Identity Manager 前方的負載平衡器終止了 SSL，則 SSL 憑證會套用至負載平衡器。

先決條件

- 產生憑證簽署要求 (CSR)，並自 CA 取得有效且已簽署的 SSL 憑證。憑證可以是 PEM 或 PFX 檔案。

- 對於主體 DN 的一般名稱部分，請採用使用者用來存取 VMware Identity Manager 服務的完整網域名稱。如果 VMware Identity Manager 應用裝置位於負載平衡器後方，則此名稱將是負載平衡器的伺服器名稱。
- 如果 SSL 並未在負載平衡器上終止，則服務所使用的 SSL 憑證必須包含 VMware Identity Manager 叢集中每個完整網域名稱的主體別名 (SAN)。包含 SAN 可讓叢集中的節點互相進行要求。此外，因為某些瀏覽器的要求，除了用於一般名稱之外，也包含使用者用來存取 VMware Identity Manager 服務之 FQDN 主機名稱的 SAN。

程序

1. 在 VMware Identity Manager 主控台中，按一下**應用裝置設定**索引標籤。
2. 按一下**管理組態**，然後輸入管理員使用者密碼。
3. 選取**安裝 SSL 憑證 > 伺服器憑證**。
4. 在 [SSL 憑證] 索引標籤中，選取**自訂憑證**。
5. 若要匯入憑證檔案，請按一下**選擇檔案**，並導覽至要匯入的憑證檔案。

   如果匯入 PEM 檔案，請確定檔案中包含順序正確的完整憑證鏈結。必須包含 -----BEGIN CERTIFICATE----- 與 -----END CERTIFICATE---- 之間的所有內容 (包括這兩行)。
6. 如果匯入 PEM 檔案，請匯入私密金鑰。按一下**選擇檔案**，然後導覽至私密金鑰檔案。必須包含 ----BEGIN RSA PRIVATE KEY 與 ---END RSA PRIVATE KEY 之間的所有內容。

   如果匯入 PFX 檔案，請輸入 PFX 密碼。
7. 按一下**儲存**。

範例：PEM 憑證範例

憑證鏈結範例
-----BEGIN CERTIFICATE-----
jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+ ... W53+O05j5xsxzDJfWr1lqBlFF/OkIYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+ ... O05j5xsxzDJfWr1lqBlFF/OkIYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjlQvt9W5+C3HU17bUOwvhp/r0+ ... 5j5xsxzDJfWr1lqW53+O0BlFF/OkIYCPcyK1
-----END CERTIFICATE-----

私密金鑰範例
-----BEGIN RSA PRIVATE KEY-----
jlQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+ ... 1lqBlFFW53+O05j5xsxzDJfWr/OkIYCPcyK1
-----END RSA PRIVATE KEY-----

安裝受信任的根憑證

安裝 VMware Identity Manager 伺服器應信任的根憑證或中繼憑證。VMware Identity Manager 伺服器將能夠對憑證鏈結包含任何此類憑證的伺服器建立安全連線。

如果 VMware Identity Manager 伺服器設定於負載平衡器後方，且 SSL 已在負載平衡器上終止，請安裝負載平衡器的根憑證。

程序

1 在 VMware Identity Manager 主控台中，按一下**應用裝置設定**索引標籤。

2 按一下**管理組態**，然後輸入 Admin 使用者密碼。

3 按一下**安裝 SSL 憑證**，然後選取**受信任的 CA** 索引標籤。

4 在文字方塊中貼上根憑證或中繼憑證。

包含 -----BEGIN CERTIFICATE----- 與 -----END CERTIFICATE---- 之間的所有內容 (包括這兩行)。

5 按一下**新增**。

安裝傳遞憑證

若要啟用使用憑證驗證方法的登入，您必須在負載平衡器上為連接埠設定在 VMware Identity Manager 主控台中的 [安裝 SSL 憑證] > [傳遞憑證] 索引標籤上定義的 SSL 傳遞。

若要啟用 VMware Identity Manager 內部部署的憑證驗證，則必須在負載平衡器上設定 SSL 傳遞。將根憑證和中繼憑證以及私密金鑰上傳至 [傳遞憑證] 索引標籤。如需使用負載平衡器設定 SSL 傳遞的詳細資訊，請參閱部署 VMware Identity Manager 出版品。

您也可以上傳要用於 Android SSO 裝置驗證的憑證。請參閱 VMware Workspace ONE 的 Android 行動單一登入出版品。

取代 VMware Identity Manager 服務中的 SSL 憑證

服務的憑證到期後，您必須從 VMware Identity Manager 主控台更新憑證。

先決條件

在目前的有效憑證到期前，從 CA 取得更新過的伺服器和中繼憑證。

程序

1 在 VMware Identity Manager 主控台中，按一下**應用裝置設定**索引標籤。

2 按一下**管理組態**，然後輸入管理員使用者密碼。

3 選取**安裝 SSL 憑證 > 伺服器憑證**。

4 在 [SSL 憑證] 文字方塊中，選取**自訂憑證**。

5 若要匯入檔案，請按一下**選擇檔案**，並導覽至要匯入的憑證檔案。

若為 PEM 檔案，請確定檔案中包含順序正確的完整憑證鏈結。必須包含 -----BEGIN CERTIFICATE----- 與 -----END CERTIFICATE---- 之間的所有內容 (包括這兩行)。

6 如果匯入 PEM 檔案，請匯入私密金鑰 **Private Key**。必須包含 ----BEGIN RSA PRIVATE KEY 與 ---END RSA PRIVATE KEY 之間的所有內容。

如果匯入 PFX 檔案，請輸入 PFX 密碼。

7 按一下**儲存**。

服務會重新啟動，並更新憑證。

更新連接器的 SSL 憑證

VMware Identity Manager Connector 憑證到期後，您必須從 https://connetorFQDN:8443/cfg/ssl 上的連接器管理頁面更新憑證。

先決條件

在目前的有效憑證到期前，從 CA 取得更新過的伺服器和中繼憑證。

程序

1 以管理員使用者身分登入連接器管理組態頁面，然後輸入 **`https://connectorFGDN:8443/cf/login`**。

2 選取**安裝 SSL 憑證 > 伺服器憑證**。

3 在 [SSL 憑證] 文字方塊中，選取**自訂憑證**。

4 若要匯入檔案，請按一下**選擇檔案**，並導覽至要匯入的憑證檔案。

若為 PEM 檔案，請確定檔案中包含順序正確的完整憑證鏈結。必須包含 -----BEGIN CERTIFICATE----- 與 -----END CERTIFICATE---- 之間的所有內容 (包括這兩行)。

5 如果匯入 PEM 檔案，請匯入私密金鑰 **Private Key**。必須包含 ----BEGIN RSA PRIVATE KEY 與 ---END RSA PRIVATE KEY 之間的所有內容。

如果匯入 PFX 檔案，請輸入 PFX 密碼。

6 按一下**儲存**。

服務會重新啟動，並更新憑證。

VMware Identity Manager 服務的自訂品牌

12

您可以自訂在 VMware Identity Manager 主控台、使用者和管理員登入畫面，以及 Workspace ONE 應用程式入口網站的 Web 視圖中顯示的標誌、字型和背景。

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。

本章包含以下主題：

在 VMware Identity Manager 服務中自訂品牌

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。

程序

1 在 VMware Identity Manager 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。

表單欄位	說明
	名稱與標誌索引標籤
公司名稱	[公司名稱] 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] 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。
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。
	登入畫面索引標籤

表單欄位	說明
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**。

VMware Identity Manager 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。

後續步驟

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

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 VMware Identity Manager 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 VMware Identity Manager 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 [背景反白]，支援多重背景影像的瀏覽器將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。
圖示背景色彩	輸入六位數的十六進位色彩碼，以變更應用程式圖示周圍的背景色彩方塊。
圖示背景不透明度	若要設定透明度，請移動透明度列上的滑桿。
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。
背景反白	如果啟用，則會針對支援多重背景影像的瀏覽器，在書籤和目錄頁面中顯示背景重疊。
背景圖樣	如果啟用，則會針對支援多重背景影像的瀏覽器，在書籤和目錄頁面中顯示背景重疊。
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`。

後續步驟

檢閱各種介面中的品牌變更外觀。

適用於 Windows 10 自訂全新品牌的 Workspace ONE

當 VMware Workspace ONE UEM 提供的 Windows 10 佈建服務用來進行新的 Windows 10 裝置佈建時，您可以在 Workspace ONE 應用程式中設定自訂品牌和歡迎訊息。

當使用者開啟新電腦的電源並使用其認證首次登入時，Workspace ONE UEM 佈建代理程式可確保 Workspace ONE 應用程式可供使用。Workspace ONE 會在 Windows 準備就緒後啟動。在 Workspace ONE 應用程式目錄開啟之前，使用者會看見附有公司品牌的自訂歡迎訊息。在此期間，如果在 [目錄] > [設定] > [使用者入口網站組態] 頁面中啟用了 [在書籤索引標籤中顯示建議的應用程式]，Workspace ONE 即會下載建議的應用程式。

備註 如需 Workspace ONE UEM 所提供 Windows 10 佈建服務的相關資訊，請參閱《Windows 桌面平台指南》。

程序

1 在 VMware Identity Manager 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 在**桌面平台全新體驗**區段中編輯設定，以自訂 Workspace ONE 登錄頁面。

表單項目	說明
歡迎畫面標誌	新增要顯示於歡迎畫面頂端中央的標誌。 影像的大小上限為 250 x 250 像素。格式為 PNG。
歡迎畫面背景色彩	針對開始畫面和歡迎畫面背景顯示的色彩。 輸入六位數十六進位色彩碼來取代現有代碼，即可變更背景色彩。預覽畫面會更新為新的色彩。
歡迎畫面下一步按鈕的色彩	輸入六位數的十六進位色彩碼，即可變更歡迎畫面上所顯示 [下一步] 按鈕的背景色彩。
歡迎畫面字型色彩	輸入六位數的十六進位色彩碼，即可變更 [下一步] 按鈕的字型色彩。
歡迎訊息	建立顯示於歡迎頁面上關於使用 Workspace ONE 的歡迎訊息。

3 按一下**儲存**。

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**。