



配置聯合

NetApp Console setup and administration

NetApp

February 11, 2026

目錄

配置聯合	1
將NetApp Console與 Active Directory 聯合服務 (AD FS) 聯合起來	1
將NetApp Console與 Microsoft Entra ID 聯合起來	2
使用 PingFederate 聯合NetApp Console	4
與 SAML 身分提供者聯合	5

配置聯合

將NetApp Console與 Active Directory 聯合服務 (AD FS) 聯合起來

將您的 Active Directory 聯合驗證服務 (AD FS) 與NetApp Console聯合起來，以便為NetApp Console啟用單一登入 (SSO)。這允許用戶使用他們的公司憑證登入控制台。

必備角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。["了解有關訪問角色的更多資訊。"](#)



您可以與您的企業 IdP 或NetApp支援網站聯合。 NetApp建議選擇其中一個，但不要同時選擇兩者。

NetApp僅支援服務供應商發起的（SP發起的）SSO。首先，配置身分提供者以信任NetApp Console作為服務提供者。然後，使用您的身分提供者的配置在控制台中建立連線。

您可以與 AD FS 伺服器建立聯合，以啟用NetApp Console的單一登入 (SSO)。這個過程涉及配置您的 AD FS 以信任控制台作為服務提供者，然後在NetApp Console中建立連線。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“Federation”以查看“Federations”頁面。
3. 選擇*配置新聯合*。
4. 輸入您的網域詳細資料：
 - a. 選擇您是否要使用已驗證的網域或您的電子郵件網域。電子郵件網域是與您登入的帳戶關聯的網域。
 - b. 輸入您正在設定的聯盟的名稱。
 - c. 如果您選擇已驗證的網域，請從清單中選擇該網域。
5. 選擇“下一步”。
6. 對於您的連線方法，選擇*協定*，然後選擇*Active Directory 聯合驗證服務 (AD FS)*。
7. 選擇“下一步”。
8. 在您的 AD FS 伺服器中建立依賴方信任。您可以使用 PowerShell 或在 AD FS 伺服器上手動設定它。有關如何建立信賴方信任的詳細信息，請參閱 AD FS 文件。
 - a. 使用以下腳本透過 PowerShell 建立信任：

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]::UTF8}).DownloadString("https://raw.githubusercontent.com/auth0/AD-FS-auth0/master/AD-FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-cloud-account.auth0.com/login/callback"
```

- b. 或者，您可以在 AD FS 管理控制台中手動建立信任。建立信任時使用以下NetApp Console值：
- 建立依賴信任識別碼時，使用 **YOUR_TENANT** 值： netapp-cloud-account
 - 當您選擇 啟用對 **WS-Federation** 的支援 時，請使用 **YOUR_AUTH0_DOMAIN** 值： netapp-cloud-account.auth0.com
- c. 建立信任後，從 AD FS 伺服器複製元資料 URL 或下載聯合元資料檔。您需要此 URL 或檔案來完成控制台中的連線。

NetApp建議使用元資料 URL 讓NetApp Console自動擷取最新的 AD FS 設定。如果您下載聯合元資料文件，則每當 AD FS 配置發生變更時，都需要在NetApp Console中手動更新它。

9. 返回控制台，然後選擇「下一步」來建立連線。
10. 建立與 AD FS 的連線。
 - a. 輸入您在上一個步驟中從 AD FS 伺服器複製的 **AD FS URL** 或上傳您從 AD FS 伺服器下載的聯合元資料檔案。
11. 選擇*建立連線*。建立連線可能需要幾秒鐘。
12. 選擇“下一步”。
13. 選擇*測試連線*來測試您的連線。您將被引導至 IdP 伺服器的登入頁面。使用您的身分提供者憑證登入。登入後，返回控制台啟用連線。



在受限模式下使用控制台時，請將 URL 複製到隱身瀏覽器視窗或單獨的瀏覽器中，以登入您的身分提供者 (IdP)。

14. 在控制台中，選擇「下一步」以查看摘要頁面。
15. 設定通知。

您可以選擇七天或三十天。系統會透過電子郵件向具有以下角色的任何使用者發送到期通知，並在控制台中顯示這些通知：超級管理員、組織管理員、聯盟管理員和聯盟檢視者。

16. 查看聯盟詳細信息，然後選擇“啟用聯盟”。
17. 選擇“完成”以完成該過程。

啟用聯合身份驗證後，使用者可以使用其企業憑證登入NetApp Console。

將NetApp Console與 Microsoft Entra ID 聯合起來

與您的 Microsoft Entra ID IdP 提供者聯合，為NetApp Console啟用單一登入 (SSO)。這允許用戶使用他們的公司憑證登入。

必備角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。["了解有關訪問角色的更多資訊。"](#)



您可以與您的企業 IdP 或NetApp支援網站聯合。 NetApp建議選擇其中一個，但不要同時選擇兩者。

NetApp僅支援服務供應商發起的 (SP發起的) SSO。您需要先配置身分提供者以信任NetApp作為服務提供

者。然後，您可以在控制台中建立使用身分提供者配置的連線。

您可以與 Microsoft Entra ID 建立聯合連接，以啟用控制台的單一登入 (SSO)。這個過程涉及配置您的 Microsoft Entra ID 以信任控制台作為服務提供者，然後在控制台中建立連線。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”以查看**“Federations”**頁面。
3. 選擇*配置新聯合*。

域名詳細資訊

1. 輸入您的網域詳細資料：
 - a. 選擇您是否要使用已驗證的網域或您的電子郵件網域。電子郵件網域是與您登入的帳戶關聯的網域。
 - b. 輸入您正在設定的聯盟的名稱。
 - c. 如果您選擇已驗證的網域，請從清單中選擇該網域。
2. 選擇“下一步”。

連接方法

1. 對於您的連線方法，選擇*提供者*，然後選擇*Microsoft Entra ID*。
2. 選擇“下一步”。

配置說明

1. 配置您的 Microsoft Entra ID 以信任NetApp為服務提供者。您需要在 Microsoft Entra ID 伺服器上執行此步驟。
 - a. 註冊 Microsoft Entra ID 應用程式以信任控制台時，請使用下列值：
 - 對於 重定向 URL，使用 <https://services.cloud.netapp.com>
 - 對於 回覆 URL，使用 <https://netapp-cloud-account.auth0.com/login/callback>
 - b. 為您的 Microsoft Entra ID 應用程式建立客戶端機密。您需要提供客戶端 ID、客戶端金鑰和 Entra ID 網域來完成聯合。
2. 返回控制台，然後選擇「下一步」來建立連線。

建立連接

1. 使用 Microsoft Entra ID 建立連接
 - a. 輸入您在上一個步驟中建立的客戶端 ID 和客戶端金鑰。
 - b. 輸入 Microsoft Entra ID 網域。
2. 選擇*建立連線*。系統在幾秒鐘內建立連線。

測試並啟用連接

1. 選擇“下一步”。

2. 選擇*測試連線*來測試您的連線。您將被引導至 IdP 伺服器的登入頁面。使用您的身分提供者憑證登入。登入後，返回控制台啟用連線。



在受限模式下使用控制台時，請將 URL 複製到隱身瀏覽器視窗或單獨的瀏覽器中，以登入您的身分提供者 (IdP)。

3. 在控制台中，選擇「下一步」以查看摘要頁面。
4. 設定通知。

您可以選擇七天或三十天。系統會透過電子郵件向具有以下角色的任何使用者發送到期通知，並在控制台中顯示這些通知：超級管理員、組織管理員、聯盟管理員和聯盟檢視者。

5. 查看聯盟詳細信息，然後選擇“啟用聯盟”。
6. 選擇“完成”以完成該過程。

啟用聯合身份驗證後，使用者可以使用其企業憑證登入NetApp Console。

使用 PingFederate 聯合NetApp Console

與您的 PingFederate IdP 提供者聯合，為NetApp Console啟用單一登入 (SSO)。這允許用戶使用他們的公司憑證登入。

必備角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。["了解有關訪問角色的更多資訊。"](#)



您可以與您的企業 IdP 或NetApp支援網站聯合。 NetApp建議選擇其中一個，但不要同時選擇兩者。

NetApp僅支援服務供應商發起的（SP發起的）SSO。您需要先配置身分提供者以信任NetApp作為服務提供者。然後，您可以在控制台中建立使用身分提供者配置的連線。

您可以使用 PingFederate 設定聯合連接，以啟用控制台的單一登入 (SSO)。這個過程涉及配置您的 PingFederate 伺服器以信任控制台作為服務提供者，然後在控制台中建立連線。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”以查看“**Federations**”頁面。
3. 選擇*配置新聯合*。
4. 輸入您的網域詳細資料：
 - a. 選擇您是否要使用已驗證的網域或您的電子郵件網域。電子郵件網域是與您登入的帳戶關聯的網域。
 - b. 輸入您正在設定的聯盟的名稱。
 - c. 如果您選擇已驗證的網域，請從清單中選擇該網域。
5. 選擇“下一步”。
6. 對於您的連線方法，選擇*提供者*，然後選擇*PingFederate*。

7. 選擇“下一步”。
8. 設定您的 PingFederate 伺服器以信任NetApp為服務提供者。您需要在 PingFederate 伺服器上執行此步驟。
 - a. 設定 PingFederate 以信任NetApp Console時，請使用下列值：
 - 對於回覆 URL 或斷言消費者服務 (ACS) URL，使用 <https://netapp-cloud-account.auth0.com/login/callback>
 - 對於*登出 URL*，使用 <https://netapp-cloud-account.auth0.com/logout>
 - 對於*受眾/實體 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` 其中 `<fed-domain-name-pingfederate>` 是聯合的網域名稱。例如，如果您的網域是 `example.com`，受眾/實體 ID 將是 `urn:auth0:netappcloud-account:fed-example-com-pingfederate`。
 - b. 複製 PingFederate 伺服器 URL。在控制台中建立連線時，您將需要此 URL。
 - c. 從您的 PingFederate 伺服器下載 X.509 憑證。它需要採用 Base64 編碼的 PEM 格式 (.pem、.crt、.cer)。
9. 返回控制台，然後選擇「下一步」來建立連線。
10. 使用 PingFederate 建立連接
 - a. 輸入您在上一個步驟中複製的 PingFederate 伺服器 URL。
 - b. 上傳 X.509 簽署憑證。證書必須採用 PEM、CER 或 CRT 格式。
11. 選擇*建立連線*。系統在幾秒鐘內建立連線。
12. 選擇“下一步”。
13. 選擇*測試連線*來測試您的連線。您將被引導至 IdP 伺服器的登入頁面。使用您的身分提供者憑證登入。登入後，返回控制台啟用連線。



在受限模式下使用控制台時，請將 URL 複製到隱身瀏覽器視窗或單獨的瀏覽器中，以登入您的身分提供者 (IdP)。

14. 在控制台中，選擇「下一步」以查看摘要頁面。

15. 設定通知。

您可以選擇七天或三十天。系統會透過電子郵件向具有以下角色的任何使用者發送到期通知，並在控制台中顯示這些通知：超級管理員、組織管理員、聯盟管理員和聯盟檢視者。

16. 查看聯盟詳細信息，然後選擇“啟用聯盟”。

17. 選擇“完成”以完成該過程。

啟用聯合身份驗證後，使用者可以使用其企業憑證登入NetApp Console。

與 SAML 身分提供者聯合

與您的 SAML 2.0 IdP 提供者聯合，為 NetApp 控制台啟用單一登入 (SSO)。這允許用戶使用他們的公司憑證登入。

所需角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。["了解有關訪問角色的更多資訊。"](#)



您可以與您的企業 IdP 或 NetApp 支援網站聯合。你不能與兩者結盟。

NetApp 僅支援服務供應商發起的（SP 發起的）SSO。您需要先配置身分提供者以信任 NetApp 作為服務提供者。然後，您可以在控制台中建立使用身分提供者配置的連線。

您可以與 SAML 2.0 提供者建立聯合連接，以便為控制台啟用單一登入 (SSO)。該過程涉及配置您的提供者以信任 NetApp 作為服務提供者，然後在控制台中建立連接。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”以查看“**Federations**”頁面。
3. 選擇*配置新聯合*。
4. 輸入您的網域詳細資料：
 - a. 選擇您是否要使用已驗證的網域或您的電子郵件網域。電子郵件網域是與您登入的帳戶關聯的網域。
 - b. 輸入您正在設定的聯盟的名稱。
 - c. 如果您選擇已驗證的網域，請從清單中選擇該網域。
5. 選擇“下一步”。
6. 對於您的連線方法，選擇*協定*，然後選擇*SAML 身分提供者*。
7. 選擇“下一步”。
8. 配置您的 SAML 身分提供者以信任 NetApp 作為服務提供者。您需要在 SAML 提供者伺服器上執行此步驟。
 - a. 確保您的 IdP 具有屬性 `email` 設定為使用者的電子郵件地址。這是控制台正確識別使用者所必需的：

```
<saml:AttributeStatement
  xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <saml:Attribute Name="email"
    NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
    <saml:AttributeValue
      xsi:type="xs:string">email@domain.com</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

1. 在控制台中註冊 SAML 應用程式時，請使用下列值：

- 對於 **回覆 URL** 或 **斷言消費者服務 (ACS) URL**，使用 <https://netapp-cloud-account.auth0.com/login/callback>
- 對於***登出 URL***，使用 <https://netapp-cloud-account.auth0.com/logout>
- 對於***受眾/實體 ID***，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`、其

中 <fed-domain-name-saml> 是您想要用於聯合的網域名稱。例如，如果您的網域是 `example.com，受眾/實體 ID 將是 urn:auth0:netapp-cloud-account:fed-example-com-samlp。

2. 建立信任後，從 SAML 提供者伺服器複製以下值：

- 登入網址
- 退出 URL (可選)

3. 從您的 SAML 提供者伺服器下載 X.509 憑證。它需要採用 PEM、CER 或 CRT 格式。

- 返回控制台，然後選擇「下一步」來建立連線。
- 使用 SAML 建立連線。

4. 輸入您的 SAML 伺服器的 登入 URL。

5. 上傳從 SAML 提供者伺服器下載的 X.509 憑證。

6. 或者，輸入您的 SAML 伺服器的 退出 URL。

- 選擇*建立連線*。系統在幾秒鐘內建立連線。
- 選擇“下一步”。
- 選擇*測試連線*來測試您的連線。您將被引導至 IdP 伺服器的登入頁面。使用您的身分提供者憑證登入。登入後，返回控制台啟用連線。



在受限模式下使用控制台時，請將 URL 複製到隱身瀏覽器視窗或單獨的瀏覽器中，以登入您的身分提供者 (IdP)。

- 在控制台中，選擇「下一步」以查看摘要頁面。
- 設定通知。

您可以選擇七天或三十天。系統會透過電子郵件向具有以下角色的任何使用者發送到期通知，並在控制台中顯示這些通知：超級管理員、組織管理員、聯盟管理員和聯盟檢視者。

- 查看聯盟詳細信息，然後選擇“啟用聯盟”。
- 選擇“完成”以完成該過程。

啟用聯合身份驗證後，使用者可以使用其企業憑證登入NetApp Console。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP 「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。