身分聯合

NetApp Console setup and administration

NetApp
February 11, 2026

目錄

身分聯合

使用NetApp Console的身份聯合實作單一登入

單一登入（聯合）允許使用者使用其公司憑證登入NetApp Console，從而簡化了登入流程並增強了安全性。您可以使用身分識別提供者 (IdP) 或NetApp支援網站啟用單一登入 (SSO)。

所需角色

組織管理員、聯盟管理員、聯盟檢視器。"了解有關訪問角色的更多資訊。"

透過 NetApp Support Site 進行單一登入

與NetApp支援網站聯合允許使用者使用相同的憑證登入控制台、 Active IQ Digital Advisor和其他相關應用程式。

如果您與NetApp支援網站聯合，則您不能與您的企業身分管理提供者聯合。選擇最適合您組織的一種。

步驟

1. 下載並完成 "NetApp聯合申請表"。
2. 將表格提交至表格中指定的電子郵件地址。

   NetApp支援團隊將審核並處理您的請求。

使用身分提供者進行單一登入

您可以與身分識別提供者建立聯合連接，以便為控制台啟用單一登入 (SSO)。這個過程涉及配置您的身分提供者以信任NetApp作為服務提供者，然後在控制台中建立連線。

如果您之前使用NetApp Cloud Central（控制台的外部應用程式）配置了聯合，則需要使用聯合頁面匯入聯合以在控制台內進行管理。"了解如何導入您的聯盟。"

支援的身份提供者

NetApp支援以下聯合協定和身分提供者：

協定

- 安全性斷言標記語言 (SAML) 身分提供者
- Active Directory 聯合驗證服務 (AD FS)

身分提供者

- 微軟Entra ID
- Ping聯邦

與**NetApp Console**聯合工作流程

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。

您可以與您的電子郵件網域或您擁有的其他網域聯合。若要與不同於您的電子郵件網域的網域聯合，請先驗證您擁有該網域。


驗證您的網域名稱（如果不使用您的電子郵件網域）

若要與不同於您的電子郵件網域的網域聯合，請驗證您擁有該網域。您無需任何額外步驟即可聯合您的電子郵件網域。


配置您的 **IdP** 以信任**NetApp**作為服務提供者

透過建立新應用程式並提供 ACS URL、實體 ID 或其他憑證資訊等詳細信息，將您的身分提供者配置為信任NetApp 。服務提供者資訊因身分提供者而異，因此請參閱特定身分提供者的文件以了解詳細資訊。您需要與您的 IdP 管理員合作來完成此步驟。


在控制台中建立聯合連接

提供來自身分提供者的 SAML 元資料 URL 或檔案以建立連線。此資訊用於建立控制台和您的身分提供者之間的信任關係。您提供的資訊取決於您使用的 IdP。例如，如果您使用 Microsoft Entra ID，則需要提供用戶端 ID、金鑰和網域。


在控制台中測試您的聯盟

在啟用聯合連線之前對其進行測試。使用控制台中聯合頁面上的測試選項來驗證您的測試使用者是否可以成功進行身份驗證。如果測試成功，則可以啟用連線。


在控制台中啟用您的連接

啟用連線後，使用者可以使用其公司憑證登入控制台。

查看對應協議或 IdP 的主題以開始：

- "與 AD FS 設定聯合連接"
- "與 Microsoft Entra ID 建立聯合連接"
- "使用 PingFederate 設定聯合連接"
- "與 SAML 身分提供者建立聯合連接"

網域驗證

驗證聯合連線的電子郵件網域

如果您想要與不同於您的電子郵件網域的網域聯合，您必須先驗證您擁有該網域。您只能

使用已驗證的網域進行聯合。

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。"

驗證您的網域名稱涉及向您的網域的 DNS 設定新增 TXT 記錄。此記錄用於證明您擁有該網域並允許NetApp Console信任該網域進行聯合。您可能需要與您的 IT 或網路管理員協調來完成此步驟。

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. 選擇*驗證網域所有權*。
5. 輸入您要驗證的網域並選擇*繼續*。
6. 複製提供的 TXT 記錄。
7. 轉到您網域的 DNS 設定並配置作為您網域的 TXT 記錄提供的 TXT 值。如果需要，請與您的 IT 或網路管理員合作。
8. 新增TXT記錄後，返回控制台並選擇*驗證*。

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.github.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。
   a. 返回控制台，然後選擇「下一步」來建立連線。
   b. 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**。
   a. 選擇*建立連線*。系統在幾秒鐘內建立連線。
   b. 選擇“下一步”。
   c. 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)。

   d. 在控制台中，選擇「下一步」以查看摘要頁面。

e. 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。

f. 查看聯盟詳細信息，然後選擇“啟用聯盟”。

g. 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。

管理聯盟

在NetApp Console中管理聯合

您可以在NetApp Console中管理您的聯合。您可以停用它，更新過期的憑證，以及在不再需要它時停用它。

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。"

您也可以為現有聯盟新增額外的已驗證網域，從而允許您為聯盟連線使用多個網域。

- 如果您使用NetApp Cloud Central 設定了聯合，請透過 **Federation** 頁面匯入它以在控制台中進行管理。"了解如何匯入您的聯盟"
- 您可以在「審核」頁面上查看聯盟管理事件，例如啟用、停用和更新聯盟。 "了解有關在NetApp Console中監控操作的更多資訊。"

啟用聯盟

如果您已經建立了聯盟但尚未啟用，您可以透過*聯盟*頁面啟用它。啟用聯合允許與聯合關聯的使用者使用其公司憑證登入控制台。在啟用聯合之前，請先成功建立並測試聯合。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇操作選單 ••• 旁邊的您想要啟用的聯盟並選擇*啟用*。

將已驗證的網域新增至現有聯合

您可以在控制台中將已驗證的網域新增至現有聯合，以便使用具有相同身分提供者 (IdP) 的多個網域。

您必須先在控制台中驗證該網域，然後才能將其新增至聯合中。如果您尚未驗證域名，可以按照以下步驟進行驗證"在控制台中驗證您的網域"。

步驟

1. 選擇*管理>身分和存取*。

2. 選擇“**Federation**”選項卡。
3. 選擇操作選單⋮在您要新增已驗證網域的聯盟旁邊，然後選擇*更新網域*。 *更新網域*對話方塊顯示已與此聯合關聯的網域。
4. 從可用網域清單中選擇一個已驗證的網域。
5. 選擇*更新*。新網域使用者可以在 30 秒內獲得聯合控制台存取權限。

更新即將到期的聯合連接

您可以在控制台中更新聯合的詳細資訊。例如，如果憑證或用戶端機密等憑證過期，則需要更新聯合。在需要時，更新通知日期以提醒您在連線到期之前更新連線。

ⓘ 在更新 IdP 之前，請先更新控制台以避免登入問題。在此過程中保持登入控制台。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇要更新的聯合旁邊的操作選單（三個垂直點），然後選擇*更新聯合*。
4. 根據需要更新聯盟的詳細資訊。
5. 選擇*更新*。

測試現有的聯盟

測試現有聯合的連線以驗證其是否有效。這可以幫助您識別聯盟中的任何問題並進行故障排除。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇操作選單⋮旁邊的您想要新增已驗證網域的聯盟，然後選擇*測試連線*。
4. 選擇*測試*。系統提示您使用公司憑證登入。如果連線成功，您將被重新導向到NetApp Console。如果連線失敗，您會看到錯誤訊息，表示聯合存在問題。
5. 選擇“完成”返回“聯合”選項卡。

禁用聯合

如果您不再需要聯合，您可以停用它。這可以防止與聯盟關聯的使用者使用其公司憑證登入控制台。如果需要，您可以稍後重新啟用聯合。

在刪除聯合之前，請先停用它，例如在停用 IdP 或停止聯合時。如果需要的話，您可以稍後重新啟用它。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇操作選單⋮在您要新增已驗證網域的聯盟旁邊，然後選擇*停用*。

刪除聯盟

如果您不再需要聯盟，您可以將其刪除。這將刪除聯合併阻止與聯合關聯的任何使用者使用其公司憑證登入控制台。例如，如果 IdP 被停用或不再需要聯合。

刪除聯合後，您將無法恢復它。您必須創建一個新的聯盟。

您必須先停用聯合，然後才能刪除它。一旦刪除聯盟，就無法恢復刪除。

步驟

1. 選擇“管理”>“身份和存取”。
2. 選擇“**Federations**”以查看“**Federations**”頁面。
3. 選擇操作選單：在您要新增已驗證網域的聯盟旁邊，然後選擇*刪除*。

將您的聯合匯入**NetApp Console**

如果您先前已透過NetApp Cloud Central（ NetApp Console的外部應用程式）設定聯合，則聯合頁面會提示您將現有的聯合連接匯入控制台，以便您可以在新介面中對其進行管理。然後，您可以利用最新的增強功能，而無需重新建立聯合連接。

匯入現有聯盟後，您可以從「聯盟」頁面管理該聯盟。"了解有關管理聯盟的更多資訊。"

所需角色

組織管理員或聯盟管理員。"了解有關訪問角色的更多資訊。"

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇*導入聯合*。

版權資訊

商標資訊