# 使用單一登入 (SSO)

StorageGRID software

NetApp
July 23, 2026

# 目錄

# 使用單一登入 (SSO)

## 了解 StorageGRID 單一登入

啟用單一登入 （SSO） 後，使用者只有在透過貴組織實作的 SSO 登入流程驗證其憑證後，才能存取 Grid Manager、Tenant Manager、Grid Management API 或 Tenant Management API。本機使用者無法登入 StorageGRID。

${post_edited_translations.segment}

${post_edited_translations.segment}

### ${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 在網頁瀏覽器中輸入任何 StorageGRID 管理節點的完整網域名稱或 IP 位址。

   StorageGRID 登入頁面隨即出現。

   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

   > 當您輸入租戶帳戶的完整 URL （即完整網域或 IP 位址，後跟 `/?accountId=20-digit-account-id`）時，不會顯示 StorageGRID 登入頁面。相反地，您會立即被重新導向至您組織的 SSO 登入頁面，您可以在該頁面 使用您的 SSO 憑證登入。

2. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - 若要存取 Tenant Manager，請輸入 20 位數的租戶帳戶 ID，或如果租戶出現在最近的帳戶清單中，請按名稱選擇租戶。
3. 選擇 **Sign in**

   StorageGRID 會將您重新導向至您組織的 SSO 登入頁面。例如：

4. 使用您的 SSO 憑證登入。

   如果您的 SSO 憑證正確：

   a. ${post_edited_translations.segment}
   b. StorageGRID 驗證驗證回應。
   c. ${post_edited_translations.segment}

   > ${post_edited_translations.segment}

5. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

### 啟用 SSO 後登出

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. 選擇「登出」。

   StorageGRID 登入頁面隨即顯示。最近使用的帳戶 下拉式功能表已更新，包含 **Grid Manager** 或租戶名稱，以便您日後能更快速地存取這些使用者介面。

   此表摘要說明如果您使用的是單一瀏覽器工作階段，在登出時會發生什麼事。如果您在多個瀏覽器工作階段中登入 StorageGRID，則必須個別登出所有的瀏覽器工作階段。

| 如果您已登入..... | 然後您登出..... | 您已登出..... |
| --- | --- | --- |
| Grid Manager 位於一個或多個管理節點上 | 任何管理節點上的 Grid Manager | 所有管理節點上的 Grid Manager<br><br>*注意：*如果您使用 Entra ID 進行 SSO，則可能需要幾分鐘才能從所有管理節點登出。 |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | 所有管理節點上的租戶管理器 |
| ${post_edited_translations.segment} | Grid Manager | 僅限 Grid Manager。您也必須從 Tenant Manager 登出才能登出單一登入 （SSO）。 |

# StorageGRID 單一登入的要求和注意事項

在為 StorageGRID 系統啟用單一登入 （SSO） 之前，請審查相關要求和注意事項。

## ${post_edited_translations.segment}

StorageGRID 支援以下 SSO 身分供應商 (IdP)：

- Active Directory Federation Service （AD FS）
- ${post_edited_translations.segment}
- PingFederate

您必須先為您的 StorageGRID 系統設定身分識別同盟，然後才能設定 SSO 身分識別供應商。您用於身分識別同盟的 LDAP 服務類型會控制您可以實作的 SSO 類型。

| ${post_edited_translations.segment} | ${post_edited_translations.segment} |
| --- | --- |
| Active Directory | • Active Directory<br>• Entra ID<br>• PingFederate |
| Entra ID | Entra ID |

**${post_edited_translations.segment}**

您可以使用以下任何版本的 AD FS：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Windows Server 2016 應該使用 "KB3201845 更新"或更高版本。

其他要求

- 傳輸層安全協定 (TLS) 1.2 或 1.3
- Microsoft .NET Framework，版本 3.5.1 或更高版本

**Entra ID** 的相關注意事項

如果您使用 Entra ID 作為 SSO 類型，且使用者的使用者主體名稱未使用 sAMAccountName 作為前綴，則當 StorageGRID 與 LDAP 伺服器斷開連線時，可能會出現登入問題。若要允許使用者登入，您必須還原與 LDAP 伺服器的連線。

## 伺服器憑證要求

預設情況下，StorageGRID 會在每個管理節點上使用管理介面憑證來保護對 Grid Manager、Tenant Manager、Grid Management API 和 Tenant Management API 的存取。當您為 StorageGRID 設定信賴方信任（AD FS）、企業應用程式（Entra ID）或服務供應商連線（PingFederate）時，您將使用伺服器憑證作為 StorageGRID 請求的簽署憑證。

如果您尚未"已為管理介面設定自訂憑證"，請立即執行。安裝自訂伺服器憑證後，該憑證將用於所有管理節點，您可以將其用於所有 StorageGRID 信賴方信任、企業應用程式或 SP 連線。

不建議在信賴方信任、企業應用程式或 SP 連線中使用管理節點的預設伺服器憑證。如果節點發生故障並恢復後，系統會產生一個新的預設伺服器憑證。在登入已復原的節點之前，您必須使用新憑證更新信賴方信任、企業應用程式或 SP 連線。

您可以透過登入該節點的命令 shell 並前往 `/var/local/mgmt-api` 目錄，來存取 Admin Node 的伺服器憑證。自訂伺服器憑證的名稱為 `custom-server.crt`。該節點的預設伺服器憑證名稱為 `server.crt`。

### 連接埠需求

單一登入 (SSO) 在受限的 Grid Manager 或 Tenant Manager 連接埠上不可用。如果您希望使用者使用單一登入進行驗證，則必須使用預設的 HTTPS 連接埠 (443)。請參閱"${post_edited_translations.segment}"。

# 確認聯合使用者可以登入 StorageGRID

## ${post_edited_translations.segment}

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"特定存取權限"。
- ${post_edited_translations.segment}

步驟

1. 如果存在租戶帳戶，請確認沒有租戶使用自己的身分來源。

   啟用單一登入 （SSO） 後，租戶管理員中設定的身分來源將會被 Grid Manager 中設定的身分來源覆寫。除非擁有 Grid Manager 身分來源的帳戶，否則屬於租戶身分來源的使用者將無法再登入。

   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
   a. 從 Grid Manager 中，選擇 **Configuration** > **Access control** > **Admin groups**。
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. 確認您可以以聯合群組使用者的身分重新登入 Grid Manager。

3. ${post_edited_translations.segment}
   a. 從 Grid Manager 中選擇 租戶。
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

   e. ${post_edited_translations.segment}
   f. 從 Tenant Manager 中選擇 **Access Management** > **Groups**。
   g. ${post_edited_translations.segment}
   h. ${post_edited_translations.segment}

i. 請確認您可以以聯合群組中的使用者身分重新登入租戶。

相關資訊

- "單一登入的要求和注意事項"
- "${post_edited_translations.segment}"
- "使用租戶帳戶"

# 在 StorageGRID 中設定 SSO

您可以依照 「Configure SSO」 精靈的指示並進入沙箱模式，在為所有 StorageGRID 使用者啟用單一登入 （SSO） 之前進行設定與測試。啟用 SSO 之後，您可以在需要變更或重新測試組態時返回沙箱模式。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。
- 您已為 StorageGRID 系統設定身分識別聯盟。
- 對於身分識別聯合 **LDAP** 服務類型，您可以根據計畫使用的 SSO 身分識別供應商選擇 Active Directory 或 Entra ID。

| **${post_edited_translations.segment}** | **${post_edited_translations.segment}** |
|---|---|
| Active Directory Federation Service （AD FS） | • Active Directory<br>• Entra ID<br>• PingFederate |
| Entra ID | Entra ID |

關於此任務

啟用 SSO 後，當使用者嘗試登入管理節點時，StorageGRID 會向 SSO 身分供應商傳送驗證請求。SSO 身分供應商隨後會向 StorageGRID 傳送驗證回應，指示驗證要求是否成功。對於成功的請求：

- 來自 Active Directory 或 PingFederate 的回應包含使用者的通用唯一識別碼 (UUID)。
- Entra ID 的回應包含使用者主體名稱 (UPN)。

為了讓 StorageGRID （服務供應商）和 SSO 身分供應商能夠安全地就使用者身分驗證請求進行通訊，您需要完成以下任務：

1. 在 StorageGRID 中設定組態。
2. 使用 SSO 身分識別供應商的軟體，為每個管理節點建立信任憑證者關係（AD FS）、企業應用程式（Entra ID）或服務供應商（PingFederate）。
3. 返回 StorageGRID 以啟用 SSO。

沙盒模式便於進行此來回組態，並在啟用單一登入 (SSO) 之前測試所有設定。使用沙盒模式時，使用者無法使

用 SSO 登入。

## ${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Access control** > **Single sign-on**。「單一登入」頁面隨即出現。

   如果「設定 SSO 設定」按鈕處於停用狀態，請確認您已將身分識別供應商設定為聯合身分識別來源。請參閱 "單一登入的要求和注意事項"。

2. 選取 **Configure SSO settings**。「提供身分供應商詳細資料」頁面隨即出現。

### 提供身分識別供應商詳細資訊

步驟

1. 從下拉清單中選取 **SSO** 類型。
2. ${post_edited_translations.segment}

   若要尋找同盟服務名稱，請前往 Windows Server Manager。選取 **Tools** > **AD FS Management**。從 Action 功能表中，選取 **Edit Federation Service Properties**。同盟服務名稱會顯示在第二個欄位中。

3. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

   - ${post_edited_translations.segment}

     如果變更 CA 憑證，請立即 "${post_edited_translations.segment}" 並測試是否能成功單一登入 Grid Manager。

4. 選擇 繼續。隨即顯示「提供信任憑證者識別碼」頁面。

## ${post_edited_translations.segment}

1. 根據您選擇的 SSO 類型，填寫「提供信賴方識別碼」頁面上的欄位。

**Active Directory**

a. 為 StorageGRID 指定*信賴方識別碼*。此值控制您在 AD FS 中為每個信賴方信任所使用的名稱。

   - 例如，如果您的網格只有一個 Admin 節點，且您預計未來不會增加更多 Admin 節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示網格中每個管理節點的信賴方識別碼。

   > 您必須為 StorageGRID 系統中的每個管理節點建立信賴憑證者信任。為每個管理節點建立信賴憑證者信任，可確保使用者能夠安全地登入和登出任何管理節點。

b. ${post_edited_translations.segment}

**Entra ID**

a. 在「企業應用程式」區段中，指定 StorageGRID 的 企業應用程式名稱。此值控制您在 Entra ID 中為每個企業應用程式使用的名稱。

   - 例如，如果您的網格只有一個 Admin 節點，且您預計未來不會增加更多 Admin 節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示系統中每個管理節點對應的企業應用程式名稱。

   > 您必須為 StorageGRID 系統中的每個管理節點建立一個企業應用程式。為每個管理節點配備企業應用程式可確保使用者可以安全地登入和登出任何管理節點。

b. 請按照 "在 Entra ID 中建立企業應用程式" 中的步驟，為表格中列出的每個管理節點建立企業應用程式。

c. 從 Entra ID 複製每個企業應用程式的同盟中繼資料 URL。然後，將此 URL 貼到 StorageGRID 中對應的*同盟中繼資料 URL* 欄位中。

d. 複製並貼上所有管理節點的聯盟中繼資料 URL 後，選取 儲存並進入沙盒模式。

**PingFederate**

a. 在「服務供應商 （SP）」部分，為 StorageGRID 指定 **SP** 連線 **ID**。此值控制您在 PingFederate 中每個 SP 連線所使用的名稱。

   - 例如，如果您的網格只有一個 Admin 節點，且您預計未來不會增加更多 Admin 節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示系統中每個管理節點的 SP 連線 ID。

   > 您必須為 StorageGRID 系統中的每個管理節點建立一個 SP 連線。為每個管理節點建立 SP 連線可確保使用者可以安全地登入和登出任何管理節點。

b. ${post_edited_translations.segment}

${post_edited_translations.segment}

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

c. ${post_edited_translations.segment}

## 設定信賴方信任、企業應用程式或 **SP** 連線

儲存組態並進入沙盒模式後，您可以完成並測試所選 SSO 類型的組態。

StorageGRID 可依需求保持在沙盒模式下。但是，只有同盟使用者和本機使用者才能登入。

**Active Directory**

步驟

1. 前往 Active Directory Federation Services （AD FS）。
2. 使用「設定 SSO」頁面上表格中顯示的每個信賴方識別碼，為 StorageGRID 建立一個或多個信賴方信任。

   ${post_edited_translations.segment}

   如需說明，請前往 "${post_edited_translations.segment}"。

**Entra ID**

步驟

1. ${post_edited_translations.segment}
2. 然後，對網格中的任何其他管理節點重複這些步驟：
   a. 登入節點。
   b. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   c. 下載並儲存該節點的 SAML 中繼資料。
3. ${post_edited_translations.segment}
4. 請依照 "在 Entra ID 中建立企業應用程式" 中的步驟，將每個管理節點的 SAML 中繼資料檔案上傳至其對應的 Entra ID 企業應用程式。

**PingFederate**

步驟

1. ${post_edited_translations.segment}
2. 然後，對網格中的任何其他管理節點重複這些步驟：
   a. 登入節點。
   b. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   c. 下載並儲存該節點的 SAML 中繼資料。
3. 前往 PingFederate。
4. "為 StorageGRID 建立一個或多個服務供應商 （SP） 連線"。使用每個管理節點的 SP 連線 ID （顯示在「設定 SSO」頁面上的表格中）以及您為該管理節點下載的 SAML 中繼資料。

   您必須為表中所示的每個管理節點建立一個 SP 連線。

## 測試組態

在對整個 StorageGRID 系統強制使用單一登入之前，請確認每個管理節點的單一登入和單一登出都已正確設定。

**Active Directory**

步驟

1. 在「設定 SSO」頁面上，找到精靈的「測試組態」步驟中的連結。

   URL 源自於您在「聯合服務名稱」欄位中輸入的值。

2. 選擇連結，或將 URL 複製並貼上到瀏覽器中，即可存取您的身分提供者的登入頁面。
3. 若要確認您可以使用 SSO 登入 StorageGRID，請選取 * 登入下列其中一個網站 *，選取您主要管理節點的信賴方識別碼，然後選取 * 登入 *。
4. 請輸入您的聯合使用者名稱和密碼。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。
   - 如果 SSO 作業未成功，則會出現錯誤訊息。請修正此問題，清除瀏覽器的 Cookie，然後重試。
5. 重複這些步驟，以驗證網格中每個管理節點的 SSO 連線。

**Entra ID**

步驟

1. 前往 Azure 入口網站中的單一登入頁面。
2. 選擇 **Test this application**。
3. 請輸入聯合使用者的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。
   - 如果 SSO 作業未成功，則會出現錯誤訊息。請修正此問題，清除瀏覽器的 Cookie，然後重試。
4. 重複這些步驟，以驗證網格中每個管理節點的 SSO 連線。

**PingFederate**

步驟

1. 在「設定 SSO」頁面中，選取「沙盒模式」訊息中的第一個連結。

   一次選擇並測試一個連結。

2. 請輸入聯合使用者的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。
   - 如果 SSO 作業未成功，則會出現錯誤訊息。請修正此問題，清除瀏覽器的 Cookie，然後重試。
3. ${post_edited_translations.segment}

   如果看到「頁面已過期」訊息，請選擇瀏覽器中的「後退」按鈕，然後重新提交您的憑證。

## 啟用單一登入

${post_edited_translations.segment}

當啟用 SSO 時，所有使用者都必須使用 SSO 來存取 Grid Manager、Tenant Manager、Grid Management API 及 Tenant Management API。本機使用者無法再存取 StorageGRID。

步驟

1. 在設定 SSO 精靈的測試組態步驟中，選取 啟用 **SSO**。
2. 查看警告訊息，然後選擇 **Enable SSO**。

   現在已啟用單一登入。單一登入頁面隨即出現，且現在包含您剛才設定的 SSO 詳細資料。

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}

如果您正在使用 Azure Portal，且您從用於存取 Entra ID 的相同電腦存取 StorageGRID，請確保 Azure Portal 使用者也是授權的 StorageGRID 使用者（已匯入至 StorageGRID 的聯合群組中的使用者），或在嘗試登入 StorageGRID 之前登出 Azure Portal。

# 在 AD FS 中為 StorageGRID 建立信賴方信任

## 您必須使用 Active Directory Federation Services （AD FS） 為系統中的每個管理節點建立信賴方信任。您可以使用 PowerShell 命令建立信賴方信任、從 StorageGRID 匯入 SAML 中繼資料，或手動輸入資料。

開始之前

- 您已為 StorageGRID 設定單一登入，並選取 **AD FS** 作為 SSO 類型。
- 您在 Grid Manager 中有 "進入沙盒模式"。
- 您知道系統中每個 Admin 節點的完整網域名稱（或 IP 位址）和信任憑證者識別碼。您可以在 StorageGRID 設定單一登入頁面的 Admin 節點詳細資料表中找到這些值。

  您必須為 StorageGRID 系統中的每個管理節點建立信賴憑證者信任。為每個管理節點建立信賴憑證者信任，可確保使用者能夠安全地登入和登出任何管理節點。

- ${post_edited_translations.segment}
- 您正在使用 AD FS Management 嵌入式管理單元，且您屬於 Administrators 群組。
- ${post_edited_translations.segment}

關於此任務

這些說明適用於 Windows Server 2016 AD FS。如果您使用的是不同版本的 AD FS，您會注意到程序中的些微差異。如果您有任何疑問，請參閱 Microsoft AD FS 文件。

## 使用 **Windows PowerShell** 建立信賴憑證者信任

您可以使用 Windows PowerShell 快速建立一個或多個信賴方信任。

步驟

1. 從 Windows 開始功能表中，以滑鼠右鍵選取 PowerShell 圖示，然後選取*以系統管理員身分執行*。

2. 在 PowerShell 命令提示字元下，輸入以下命令：

   `Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL "https://Admin_Node_FQDN/api/saml-metadata"` United States (US) - Company name: NetApp - Source text: `Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL "https://Admin_Node_FQDN/api/saml-metadata"` - The source text only contains an image placeholder tag. - According to the instructions, I must keep all `` tags exactly as they appear in the source text and return only the correct translation.

Output: `Add-AdfsRelyingPartyTrust -Name "*Admin_Node_Identifer*" -MetadataURL "https://*Admin_Node_FQDN*/api/saml-metadata"`_

+ 對於 ***`Admin_Node_Identifier`***，請輸入管理節點的信賴方識別碼，其內容必須與單一登入頁面上顯示的內容完全一致。例如， **`SG-DC1-ADM1`**。 針對 *`Admin_Node_FQDN`*，請輸入相同 Admin Node 的完整網域。（如有需要，您也可以改用該節點的 IP 位址。然而，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴憑證者信任。）

1. ${post_edited_translations.segment}

   AD FS 管理工具出現。

2. ${post_edited_translations.segment}

   信賴方信任清單隨即出現。

3. 為新建立的信賴方信任新增存取控制原則：
   a. 找到您剛建立的信賴方信任。
   b. ${post_edited_translations.segment}
   c. 選擇存取控制原則。
   d. ${post_edited_translations.segment}
4. 為新建立的信賴方信任新增宣告發行原則：
   a. 找到您剛建立的信賴方信任。
   b. ${post_edited_translations.segment}
   c. 選擇 新增規則。
   d. ${post_edited_translations.segment}
   e. 在「設定規則」頁面上，輸入該規則的顯示名稱。

      ${post_edited_translations.segment}

   f. ${post_edited_translations.segment}
   g. 在映射表的 LDAP 屬性欄中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   h. 在對應表的「傳出宣告類型」欄位中，從下拉清單中選擇「名稱 ID」。
   i. 選擇 **Finish**，然後選擇 **OK**。
5. 確認中繼資料已成功匯入。
   a. 以滑鼠右鍵按一下信賴方信任，以開啟其屬性。

b. 確認「端點」、「識別碼」和「簽名」標籤上的欄位已填寫。

如果缺少中繼資料，請確認 Federation 中繼資料地址是否正確，或手動輸入值。

6. 重複這些步驟，為 StorageGRID 系統中的所有管理節點設定信賴方信任。
7. 完成後，返回 StorageGRID 並"測試所有信賴憑證者信任"確認其組態是否正確。

## ${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 在 Windows Server 管理員中，選取 工具，然後選取 **AD FS Management**。
2. 在「操作」下，選擇 **Add Relying Party Trust**。
3. 在歡迎頁面上，選擇 **Claims aware**，然後選擇 **Start**。
4. 選擇「匯入有關依賴方的線上或區域網路上發佈的資料」。
5. 在「聯合中繼資料位址（主機名稱或 URL）」中，輸入此管理節點的 SAML 中繼資料的位置：

`https://Admin_Node_FQDN/api/saml-metadata`

針對 *Admin_Node_FQDN*，請輸入相同 Admin Node 的完整網域。（如有需要，您也可以改用該節點的 IP 位址。然而，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴憑證者信任。）

6. ${post_edited_translations.segment}

輸入顯示名稱時，請使用管理節點的信賴方識別碼，該識別碼必須與 Grid Manager 單一登入頁面上顯示的識別碼完全一致。例如， `SG-DC1-ADM1`。

7. 新增聲明規則：
   a. ${post_edited_translations.segment}
   b. 選擇 新增規則：
   c. ${post_edited_translations.segment}
   d. 在「設定規則」頁面上，輸入該規則的顯示名稱。

      ${post_edited_translations.segment}

   e. ${post_edited_translations.segment}
   f. 在映射表的 LDAP 屬性欄中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   g. 在對應表的「傳出宣告類型」欄位中，從下拉清單中選擇「名稱 ID」。
   h. 選擇 **Finish**，然後選擇 **OK**。
8. 確認中繼資料已成功匯入。
   a. 以滑鼠右鍵按一下信賴方信任，以開啟其屬性。
   b. 確認「端點」、「識別碼」和「簽名」標籤上的欄位已填寫。

如果缺少中繼資料，請確認 Federation 中繼資料地址是否正確，或手動輸入值。

9. 重複這些步驟，為 StorageGRID 系統中的所有管理節點設定信賴方信任。
10. 完成後，請返回 StorageGRID 並"測試所有信賴憑證者信任"以確認其已正確設定。

## 手動建立信賴方信任

如果您選擇不匯入依賴方信託的資料，您可以手動輸入這些值。

步驟

1. 在 Windows Server 管理員中，選取 工具，然後選取 **AD FS Management**。
2. 在「操作」下，選擇 **Add Relying Party Trust**。
3. 在歡迎頁面上，選擇 **Claims aware**，然後選擇 **Start**。
4. 選擇 **Enter data about the relying party manually**，然後選擇 **Next**。
5. 完成信賴方信任嚮導：

   a. ${post_edited_translations.segment}

      為保持一致性，請使用管理節點的信賴方識別碼，該識別碼應與 Grid Manager 單一登入頁面上顯示的識別碼完全一致。例如， `SG-DC1-ADM1`。

   b. ${post_edited_translations.segment}

   c. ${post_edited_translations.segment}

   d. 輸入管理節點的 SAML 服務端點 URL：

      `https://Admin_Node_FQDN/api/saml-response`

      針對 *`Admin_Node_FQDN`*，請輸入 Admin Node 的完整網域。（如有需要，您也可以改用該節點的 IP 位址。然而，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴憑證者信任。）

   e. ${post_edited_translations.segment}

      `*Admin_Node_Identifier*`_

      對於 *`Admin_Node_Identifier`*，請輸入管理節點的信賴方識別碼，其內容必須與單一登入頁面上顯示的內容完全一致。例如， `SG-DC1-ADM1`。

   f. 檢查設定，儲存信賴方信任，然後結束精靈。

      「編輯宣告簽發原則」對話方塊隨即出現。

      ${post_edited_translations.segment}

6. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

   b. 在「設定規則」頁面上，輸入該規則的顯示名稱。

${post_edited_translations.segment}

c. ${post_edited_translations.segment}

d. 在映射表的 LDAP 屬性欄中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。

e. 在對應表的「傳出宣告類型」欄位中，從下拉清單中選擇「名稱 ID」。

f. 選擇 **Finish**，然後選擇 **OK**。

7. 以滑鼠右鍵按一下信賴方信任，以開啟其屬性。

8. ${post_edited_translations.segment}

a. 選擇 新增 **SAML**。

b. ${post_edited_translations.segment}

c. ${post_edited_translations.segment}

d. ${post_edited_translations.segment}

```
https://Admin_Node_FQDN/api/saml-logout
```

對於 *Admin_Node_FQDN*，請輸入管理節點的完整網域名稱。（如有必要，您也可以使用節點的 IP 位址。但是，如果您在此輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴方信任。）

a. 選擇 **OK** 。

9. 在「簽署」標籤上，指定此信賴方信任的簽署憑證：

a. 新增自訂憑證：

- 如果您有已上傳至 StorageGRID 的自訂管理憑證，請選擇該憑證。
- 如果沒有自訂憑證，請登入管理節點，前往管理節點的 `/var/local/mgmt-api`目錄，然後新增 `custom-server.crt`憑證檔案。

> 不建議使用管理節點的預設憑證 (`server.crt`。如果管理節點發生故障，恢復節點後將重新產生預設憑證，屆時您需要更新信賴方信任關係。

b. ${post_edited_translations.segment}

${post_edited_translations.segment}

10. 重複這些步驟，為 StorageGRID 系統中的所有管理節點設定信賴方信任。

11. 完成後，請返回 StorageGRID 並"測試所有信賴憑證者信任"以確認其已正確設定。

# 在 Entra ID 中為 StorageGRID 建立企業應用程式

您可以使用 Entra ID 為系統中的每個管理節點建立一個企業應用程式。

開始之前

- 您已開始為 StorageGRID 設定單一登入，並選擇了 **Entra ID** 作為 SSO 類型。
- 您在 Grid Manager 中有 "進入沙盒模式"。

- 您擁有系統中每個管理節點的 企業應用程式名稱。您可以從「設定 SSO」頁面上的管理節點詳細資料表格中複製這些值。

> 您必須為 StorageGRID 系統中的每個管理節點建立一個企業應用程式。為每個管理節點配備企業應用程式可確保使用者可以安全地登入和登出任何管理節點。

- 您擁有使用 Entra ID 建立企業應用程式的經驗。
- ${post_edited_translations.segment}
- 您在 Entra ID 帳戶中擁有以下角色之一：Global Administrator、Cloud Application Administrator、Application Administrator 或服務主體的擁有者。

## 存取 **Entra ID**

步驟

1. 登入 "${post_edited_translations.segment}"。
2. 導航至 "Entra ID"。
3. 選擇 "企業應用程式"。

## ${post_edited_translations.segment}

若要在 StorageGRID 中儲存 Entra ID 的單一登入組態，您必須使用 Entra ID 為每個管理節點建立一個企業應用程式。您將從 Entra ID 複製同盟中繼資料 URL，並將其貼到「設定單一登入」頁面上對應的 同盟中繼資料 **URL** 欄位中。

步驟

1. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. 選擇 **Create your own application**。
   c. 對於名稱，請輸入您從「設定 SSO」頁面上的「管理節點詳細資料」表中複製的*企業應用程式名稱*。
   d. 保持選取「整合您在資源庫中找不到的任何其他應用程式（非資源庫）」選項按鈕。
   e. 選擇 **Create** 。
   f. 在「2. 設定單一登入」方塊中選擇「開始使用」連結，或在左側邊欄中選擇「單一登入」連結。
   g. 選取 **SAML** 核取方塊。
   h. 複製 **App Federation Metadata Url**，您可以在 **Step 3 SAML Signing Certificate** 下找到它。
   i. 前往「設定 SSO」頁面，並將 URL 貼到與您使用的「企業應用程式名稱」對應的「同盟中繼資料 URL」欄位中。
2. 為每個管理節點貼上同盟中繼資料 URL 並對 SSO 組態進行所有其他必要的變更後，在「設定 SSO」頁面上選擇「儲存」。

## ${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
   a. 從管理節點登入 StorageGRID。
   b. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   c. 選擇按鈕以下載該管理節點的 SAML 中繼資料。
   d. 儲存檔案，然後將其上傳到 Entra ID。

### 將 SAML 中繼資料上傳到每個企業應用程式

為每個 StorageGRID 管理節點下載 SAML 中繼資料檔案後，在 Entra ID 中執行下列步驟：

步驟

1. ${post_edited_translations.segment}
2. 對每個企業應用程式重複這些步驟：

   ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}
   b. 將 **Assignment required** 設為 **No** （除非您想單獨設定指派）。
   c. 前往單一登入頁面。
   d. ${post_edited_translations.segment}
   e. 選擇「上傳中繼資料檔案」按鈕，然後選擇您為對應的管理節點下載的 SAML 中繼資料檔案。
   f. 檔案載入完成後，選擇 **Save**，然後選擇 **X** 以關閉窗格。您將返回「使用 SAML 設定單一登入」頁面。
3. "${post_edited_translations.segment}"。

# 在 PingFederate 中為 StorageGRID 建立服務提供者連線

您需要使用 PingFederate 為系統中的每個管理節點建立一個服務供應商 （SP） 連線。為了加快此過程，您將從 StorageGRID 匯入 SAML 中繼資料。

開始之前

- ${post_edited_translations.segment}
- 您在 Grid Manager 中有 "進入沙盒模式"。
- 您擁有系統中每個管理節點的 **SP** 連線 **ID**。您可以在「設定 SSO」頁面的管理節點詳細資料表中找到這些值。
- 您已下載系統中每個管理節點的 **SAML** 中繼資料。
- 您有在 PingFederate Server 中建立 SP 連線的經驗。
- 您已取得 "管理員參考指南" PingFederate 伺服器端所需的檔案。PingFederate 文件中提供了詳細的逐步說明和解釋。
- 您已取得 "管理員權限" PingFederate 伺服器端所需的檔案。

關於此任務

這些說明摘要介紹如何將 PingFederate Server 10.3 版設定為 StorageGRID 的 SSO 供應商。如果您使用的是其他版本的 PingFederate，您可能需要調整這些說明。有關您版本的詳細說明，請參閱 PingFederate Server 文件。

## 完成 PingFederate 中的先決條件

在您可以建立將用於 StorageGRID 的 SP 連線之前，您必須先在 PingFederate 中完成先決條件工作。當您設定 SP 連線時，將會使用來自這些先決條件的資訊。

### 建立資料儲存區

如果您尚未執行此操作，請建立資料儲存區以將 PingFederate 連線至 AD FS LDAP 伺服器。請使用您在 StorageGRID 中 "${post_edited_translations.segment}" 時所使用的值。

- 類型：目錄（LDAP）
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

### 建立密碼認證資料驗證器

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 搜尋篩選條件：sAMAccountName=${username}
- ${post_edited_translations.segment}

### 建立 IdP 介面卡執行個體

如果還沒有建立 IdP 介面卡執行個體，請建立一個。

步驟

1. 前往 **Authentication** > **Integration** > **IdP Adapters**。
2. 選擇 **Create New Instance**。
3. 在「類型」標籤上，選擇「HTML Form IdP Adapter」。
4. 在 IdP Adapter 標籤上，選擇「在『Credential Validators』新增一行」。
5. 選取您建立的 ${post_edited_translations.segment}。
6. 在「介面卡屬性」標籤上，為「**Pseudonym**」選擇「**username**」屬性。
7. 選取 **Save** 。

#### ${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 前往 **Security** > **Signing & Decryption Keys & Certificates**。
2. 建立或匯入簽署憑證。

## 在 PingFederate 中建立 SP 連線

在 PingFederate 中建立 SP 連線時，您需要匯入從 StorageGRID 下載的管理節點 SAML 中繼資料。該中繼資料檔案包含您需要的許多特定值。

> 您必須為 StorageGRID 系統中的每個管理節點建立一個 SP 連線，以便使用者可以安全地登入和登出任何節點。請依照以下說明建立第一個 SP 連線。然後，前往 <<${post_edited_translations.segment}>> 建立您所需的任何其他連線。

選擇 **SP** 連線類型

步驟

1. 前往 **Applications** > **Integration** > **SP Connections**。
2. 選擇 **Create Connection**。
3. 選擇 **Do not use a template for this connection**。
4. ${post_edited_translations.segment}

匯入 **SP** 中繼資料

步驟

1. 在「匯入中繼資料」索引標籤上，選取 檔案。
2. 選擇您從管理節點的「設定 SSO」頁面下載的 SAML 中繼資料檔案。
3. ${post_edited_translations.segment}

   合作夥伴實體 ID 和連線名稱設定為 StorageGRID SP 連線 ID。（例如，10.96.105.200-DC1-ADM1-105-200）。基本 URL 是 StorageGRID 管理節點的 IP 位址。

4. 選擇 **Next** 。

**${post_edited_translations.segment}**

步驟

1. 在「瀏覽器 SSO」標籤中，選擇「設定瀏覽器 SSO」。
2. ${post_edited_translations.segment}
3. 選擇 **Next** 。
4. ${post_edited_translations.segment}
5. 在「斷言建立」標籤上，選取「設定斷言建立」。
   a. 在「身分映射」標籤上，選取 **Standard**。
   b. ${post_edited_translations.segment}
6. 如需延長合約，請選擇 **Delete** 以移除 `urn:oid`（未使用）。

對應介面卡執行個體

步驟

1. 在「驗證來源對應」標籤上，選擇 **Map New Adapter Instance**。
2. 在「介面卡執行個體」標籤上，選擇您建立的介面卡執行個體。
3. 在「映射方法」標籤上，選取*從資料儲存區擷取其他屬性*。
4. 在「屬性來源和使用者尋找」標籤上，選擇 **Add Attribute Source**。
5. 在「資料儲存區」標籤上，提供執行摘要並選擇您新增的 資料儲存區 。
6. 在 LDAP 目錄搜尋標籤上：
   - 輸入 **Base DN**，該值應與您在 StorageGRID 中為 LDAP 伺服器輸入的值完全相符。
   - 在搜尋範圍中，選擇 **Subtree**。
   - 對於根物件類別，搜尋並新增下列屬性之一：**objectGUID** 或 **userPrincipalName**。
7. 在 LDAP 二進位屬性編碼類型標籤上，為 **objectGUID** 屬性選擇 **Base64**。
8. 在 LDAP 篩選器標籤上，輸入 **sAMAccountName=${username}**。
9. 在「屬性合約履行」標籤上，從「來源」下拉清單中選擇 **LDAP** （屬性），然後從「值」下拉清單中選擇 **objectGUID** 或 **userPrincipalName**。
10. 審查並儲存屬性來源。
11. 在「Failsave 屬性來源」標籤上，選取 中止 **SSO** 交易。
12. 審查摘要並選擇 **Done**。
13. 選擇 **Done**。

設定通訊協定設定

步驟

1. 在「**SP Connection**」>「**Browser SSO**」>「**Protocol Settings**」標籤上，選擇「**Configure Protocol Settings**」。
2. 在「Assertion Consumer Service URL」索引標籤上，接受預設值，這些預設值是從 StorageGRID SAML 中繼資料匯入的（Binding 為 **POST**，Endpoint URL 為 `/api/saml-response`）。
3. 在 SLO 服務 URL 索引標籤上，接受預設值，這些預設值是從 StorageGRID SAML 中繼資料匯入的（Binding 為 **REDIRECT**， `/api/saml-logout`為端點 URL）。
4. 在「允許的 SAML 綁定」標籤中，清除 **ARTIFACT** 和 **SOAP**。只需 **POST** 和 **REDIRECT**。
5. 在「簽署原則」標籤上，保持選取「要求對驗證要求進行簽署」和「始終簽署判斷提示」核取方塊。
6. 在「加密原則」索引標籤上，選取 **None**。
7. 審查摘要並選取 **Done** 以儲存通訊協定設定。
8. 審查摘要並選擇「完成」以儲存瀏覽器 SSO 設定。

設定認證資料

步驟

1. 在 SP Connection 標籤中，選擇「憑證」。

2. ${post_edited_translations.segment}
3. 選擇您建立或匯入的 簽署憑證 。
4. ${post_edited_translations.segment}
    a. 在「信任模型」標籤上，選擇 **Unanchored** 。
    b. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

**${post_edited_translations.segment}**

您可以複製第一個 SP 連線，為網格中的每個管理節點建立所需的 SP 連線。每個複本都需要上傳新的中繼資料。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
    a. ${post_edited_translations.segment}
    b. 選擇 **Choose File** 並上傳中繼資料。
    c. 選擇 **Next** 。
    d. 選取 **Save** 。
4. ${post_edited_translations.segment}
    a. ${post_edited_translations.segment}
    b. ${post_edited_translations.segment}
    c. ${post_edited_translations.segment}
    d. 選取 **Save** 。

# 停用 StorageGRID 中的 SSO

如果您不再需要此功能，可以停用單一登入 （SSO） 。您必須先停用單一登入，然後才能停用身分識別聯盟。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"特定存取權限"。

步驟

1. 選擇 **Configuration** > **Access control** > **Single sign-on** 。

    單一登入頁面隨即出現。

2. 選擇 停用單一登入。
3. ${post_edited_translations.segment}

   螢幕上出現警告訊息，指出本機使用者現在可以登入。

${post_edited_translations.segment}

# 暫時停用並重新啟用 StorageGRID 管理節點的 SSO

如果單一登入 （SSO） 系統故障，您可能無法登入 Grid Manager。在這種情況下，您可以暫時停用並重新啟用一個 Admin Node 的 SSO。若要停用並重新啟用 SSO，您必須存取該節點的命令 shell。

開始之前

- 您有"特定存取權限"。
- 您擁有 `Passwords.txt` 檔案。
- 您知道本機 root 使用者的密碼。

關於此任務

在您停用一個管理節點的 SSO 之後，您可以本機 root 使用者身分登入 Grid Manager。為了確保您的 StorageGRID 系統是安全的，您必須在登出後立即使用該節點的命令 shell 重新啟用管理節點上的 SSO。

> 停用單一 Admin Node 的 SSO 並不會影響網格中任何其他 Admin Node 的 SSO 設定。Grid Manager 中「單一登入」頁面上的「啟用 **SSO**」核取方塊仍會保持選取狀態，且所有現有的 SSO 設定都會保留，除非您對其進行更新。

步驟

1. ${post_edited_translations.segment}
   a. 輸入以下命令： `ssh admin@Admin_Node_IP`
   b. 請輸入 `Passwords.txt`檔案中列出的密碼。
   c. 輸入以下命令以切換至根目錄： `su -`
   d. 請輸入 `Passwords.txt`檔案中列出的密碼。

      當您以根目錄身分登入時，提示符號會從 `$`變為 `#`。

2. 執行下列命令：`disable-saml`

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

4. 透過網頁瀏覽器，存取同一管理節點上的 Grid Manager。

   由於 SSO 已停用，現在將顯示 Grid Manager 登入頁面。

5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}
   a. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   b. ${post_edited_translations.segment}
   c. 選取 **Save** 。

      ${post_edited_translations.segment}
7. 如果您因為需要存取 Grid Manager 而暫時停用了 SSO：
   a. 執行您需要執行的任何工作。
   b. ${post_edited_translations.segment}
   c. 在 Admin 節點上重新啟用 SSO。您可以執行下列任一步驟：
      - 執行下列命令： `enable-saml`

        ${post_edited_translations.segment}

      ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   - 重啟網格節點： `reboot`
8. 透過網頁瀏覽器，從同一個管理節點存取 Grid Manager。
9. 確認 StorageGRID 登入頁面出現，且您必須輸入 SSO 憑證才能存取 Grid Manager。