フェデレーションを構成する

NetApp Console setup and administration

NetApp
February 11, 2026

目次

フェデレーションを構成する

NetApp ConsoleをActive Directory フェデレーション サービス (AD FS) と連携する

Active Directory フェデレーション サービス (AD FS) をNetApp Consoleと連携させて、NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してコンソールにログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp Consoleをサービス プロバイダーとして信頼するように ID プロバイダーを構成します。次に、ID プロバイダーの構成を使用してコンソールで接続を作成します。

AD FS サーバーとのフェデレーションを設定して、 NetApp Consoleのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように AD FS を構成し、 NetApp Consoleで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
    a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
    b. 構成するフェデレーションの名前を入力します。
    c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、[プロトコル] を選択し、[**Active Directory** フェデレーション サービス **(AD FS)**] を選択します。
7. *次へ*を選択します。
8. AD FS サーバーに証明書利用者信頼を作成します。 PowerShell を使用することも、AD FS サーバー上で手動で構成することもできます。証明書利用者信頼を作成する方法の詳細については、AD FS のドキュメントを参照してください。
    a. 次のスクリプトを使用して PowerShell を使用して信頼を作成します。

```
(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. または、AD FS 管理コンソールで信頼を手動で作成することもできます。信頼を作成するときは、次のNetApp Consoleの値を使用します。

- 信頼信頼識別子を作成するときは、**YOUR_TENANT** 値を使用します。 `netapp-cloud-account`
- **WS-Federation** のサポートを有効にする を選択した場合は、**YOUR_AUTH0_DOMAIN** 値を使用します。 `netapp-cloud-account.auth0.com`

c. 信頼を作成した後、AD FS サーバーからメタデータ URL をコピーするか、フェデレーション メタデータ ファイルをダウンロードします。コンソールで接続を完了するには、この URL またはファイルが必要になります。

NetApp、メタデータ URL を使用してNetApp Consoleが最新の AD FS 構成を自動的に取得できるようにすることをお勧めします。フェデレーション メタデータ ファイルをダウンロードした場合は、AD FS 構成に変更があるたびに、 NetApp Consoleで手動で更新する必要があります。

9. コンソールに戻り、[次へ] を選択して接続を作成します。
10. AD FS との接続を作成します。
    a. 前の手順で AD FS サーバーからコピーした **AD FS URL** を入力するか、AD FS サーバーからダウンロードしたフェデレーション メタデータ ファイルをアップロードします。
11. *接続を作成*を選択します。接続の作成には数秒かかる場合があります。
12. *次へ*を選択します。
13. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdP のクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

    コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

14. コンソールで、[次へ] を選択して概要ページを確認します。
15. 通知を設定します。

    7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

16. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。
17. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

NetApp ConsoleをMicrosoft Entra ID と連携する

Microsoft Entra ID IdP プロバイダーと連携して、 NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

Microsoft Entra ID とのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように Microsoft Entra ID を構成し、コンソールで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。

ドメインの詳細

1. ドメインの詳細を入力してください:
    a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
    b. 構成するフェデレーションの名前を入力します。
    c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
2. *次へ*を選択します。

接続方法

1. 接続方法として、*プロバイダー*を選択し、*Microsoft Entra ID*を選択します。
2. *次へ*を選択します。

設定手順

1. NetApp をサービス プロバイダーとして信頼するように Microsoft Entra ID を構成します。この手順は Microsoft Entra ID サーバーで実行する必要があります。
    a. コンソールを信頼するには、Microsoft Entra ID アプリを登録するときに次の値を使用します。

- *リダイレクトURL*には、 https://services.cloud.netapp.com
- *返信URL*には、 https://netapp-cloud-account.auth0.com/login/callback

b. Microsoft Entra ID アプリのクライアント シークレットを作成します。フェデレーションを完了するには、クライアント ID、クライアント シークレット、Entra ID ドメイン名を提供する必要があります。

2. コンソールに戻り、[次へ] を選択して接続を作成します。

接続を作成

1. Microsoft Entra IDで接続を作成する
   a. 前の手順で作成したクライアント ID とクライアント シークレットを入力します。
   b. Microsoft Entra ID ドメイン名を入力します。
2. *接続を作成*を選択します。システムは数秒で接続を作成します。

接続をテストして有効にする

1. *次へ*を選択します。
2. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdP のクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

   コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

3. コンソールで、[次へ] を選択して概要ページを確認します。
4. 通知を設定します。

   7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

5. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。
6. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

PingFederateでNetApp Consoleを連携

PingFederate IdP プロバイダーと連携して、 NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

PingFederate とのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように PingFederate サーバーを構成し、コンソールで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、*プロバイダー*を選択し、次に*PingFederate*を選択します。
7. *次へ*を選択します。
8. PingFederate サーバーを、サービス プロバイダーとしてNetApp を信頼するように構成します。この手順は PingFederate サーバーで実行する必要があります。
   a. PingFederate を構成してNetApp Consoleを信頼する場合は、次の値を使用します。
      - *返信URL*または*アサーションコンシューマーサービス（ACS）URL*の場合は、`https://netapp-cloud-account.auth0.com/login/callback`
      - *ログアウトURL*には、`https://netapp-cloud-account.auth0.com/logout`
      - *オーディエンス/エンティティID*には、`urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`ここで、`<fed-domain-name-pingfederate>` はフェデレーションのドメイン名です。たとえば、ドメインが `example.com`オーディエンス/エンティティIDは次のようになります。 `urn:auth0:netappcloud-account:fed-example-com-pingfederate`。
   b. PingFederate サーバーの URL をコピーします。コンソールで接続を作成するときに、この URL が必要になります。
   c. PingFederate サーバーから X.509 証明書をダウンロードします。 Base64 でエンコードされた PEM 形式 (.pem、.crt、.cer) である必要があります。
9. コンソールに戻り、[次へ] を選択して接続を作成します。
10. PingFederateで接続を作成する
    a. 前の手順でコピーした PingFederate サーバーの URL を入力します。

b. X.509 署名証明書をアップロードします。証明書は PEM、CER、または CRT 形式である必要があります。

11. *接続を作成*を選択します。システムは数秒で接続を作成します。
12. *次へ*を選択します。
13. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdP のクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

> コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

14. コンソールで、[次へ] を選択して概要ページを確認します。
15. 通知を設定します。

    7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

16. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。
17. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

SAML ID プロバイダとの連携

SAML 2.0 IdP プロバイダーと連携して、NEtApp コンソールのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

> 企業の IdP またはNetAppサポート サイトと連携できます。両方と連携することはできません。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

SAML 2.0 プロバイダーとのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、プロバイダーがNetApp をサービス プロバイダーとして信頼するように構成し、コンソールで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。

3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、*プロトコル*を選択し、*SAML ID プロバイダー*を選択します。
7. *次へ*を選択します。
8. SAML ID プロバイダーを構成して、 NetApp をサービス プロバイダーとして信頼します。この手順は SAML プロバイダー サーバーで実行する必要があります。
   a. IdPに属性があることを確認する `email`ユーザーのメールアドレスに設定されます。これは、コンソールがユーザーを正しく識別するために必要です。

```
<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. SAML アプリケーションをコンソールに登録するときは、次の値を使用します。
   - *返信URL*または*アサーションコンシューマーサービス（ACS）URL*の場合は、 https://netapp-cloud-account.auth0.com/login/callback
   - *ログアウトURL*には、 https://netapp-cloud-account.auth0.com/logout
   - *オーディエンス/エンティティID*には、 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`ここで、<fed-domain-name-saml> はフェデレーションに使用するドメイン名です。たとえば、ドメインが `example.com`オーディエンス/エンティティIDは次のようになります。 `urn:auth0:netapp-cloud-account:fed-example-com-samlp`。
2. 信頼を作成したら、SAML プロバイダー サーバーから次の値をコピーします。
   - サインインURL
   - サインアウトURL（オプション）
3. SAML プロバイダー サーバーから X.509 証明書をダウンロードします。 PEM、CER、または CRT 形式である必要があります。
   a. コンソールに戻り、[次へ] を選択して接続を作成します。
   b. SAML を使用して接続を作成します。

4. SAML サーバーの サインイン **URL** を入力します。
5. SAML プロバイダー サーバーからダウンロードした X.509 証明書をアップロードします。
6. 必要に応じて、SAML サーバーの サインアウト **URL** を入力します。
   a. *接続を作成*を選択します。システムは数秒で接続を作成します。
   b. *次へ*を選択します。
   c. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdPのクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

      コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

   d. コンソールで、[次へ] を選択して概要ページを確認します。
   e. 通知を設定します。

      7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

   f. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。
   g. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

著作権に関する情報

商標に関する情報