



# 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 .....	1
NetApp ConsoleをActive Directory フェデレーション サービス (AD FS) と連携する .....	1
NetApp ConsoleをMicrosoft Entra ID と連携する .....	3
PingFederateでNetApp Consoleを連携 .....	4
SAML ID プロバイダとの連携 .....	6

# 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.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. 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

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。