# フェデレーションを構成する

BlueXP setup and administration

NetApp
August 18, 2025

# 目次

# フェデレーションを構成する

## BlueXP をActive Directory フェデレーション サービス (AD FS) と連携させる

Active Directory フェデレーションサービス（AD FS）をBlueXPと連携させることで、BlueXPのシングルサインオン（SSO）を有効にできます。これにより、ユーザーは企業の認証情報を使用してBlueXP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、組織管理者またはフェデレーション管理者が必要です。フェデレーション閲覧者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。"

社内のIdPまたはNetAppサポートサイトと連携できます。NetAppNetApp、どちらか一方を選択することを推奨しており、両方を選択することは推奨していません。

NetAppは、サービスプロバイダ主導（SP主導）のSSOのみをサポートしています。まず、 BlueXPをサービスプロバイダとして信頼するようにアイデンティティプロバイダを設定します。次に、アイデンティティプロバイダの設定を使用して、 BlueXP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することで、 BlueXP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、AD FS でBlueXP をサービスプロバイダーとして信頼するように設定し、 BlueXPで接続を作成します。

作業を開始する前に

- 管理者権限を持つIdPアカウントが必要です。IdP管理者と調整して手順を完了してください。
- 連携に使用するドメインを特定します。ご自身のメールドメイン、またはご自身で所有している別のドメインを使用できます。メールドメイン以外のドメインを使用する場合は、まずBlueXPでドメインを検証する必要があります。これは、以下の手順に従って行うことができます。 "BlueXPでドメインを認証する"トピック。

手順

1. BlueXP コンソールの右上で、>* IDおよびアクセス管理*を選択します。
2. *Federation*タブを選択します。
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。メールドメインとは、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を使用するか、AD FS サーバー上で手動で構成できます。証明書利用者信頼の作成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 管理コンソールで手動で信頼関係を作成することもできます。信頼関係を作成する際は、以下のBlueXP値を使用してください。

      - 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. 信頼関係を作成したら、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てください。BlueXP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BlueXP 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BlueXPで手動で更新する必要があります。

9. BlueXP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」を選択してください。IdPサーバーのログインページに移動します。IdPの認証情報でログインしてテストを完了し、 BlueXPに戻って接続を有効にしてください。
14. 「 * 次へ * 」を選択します。
15. *フェデレーションの有効化*ページでフェデレーションの詳細を確認し、*フェデレーションの有効化*を選択します。
16. 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BlueXPにログインできるようになります。

# BlueXPと Microsoft Entra ID を連携させる

Microsoft Entra ID IdPプロバイダーと連携して、 BlueXPのシングルサインオン（SSO）を有効にします。これにより、ユーザーは企業の認証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、組織管理者またはフェデレーション管理者が必要です。フェデレーション閲覧者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。"

社内のIdPまたはNetAppサポートサイトと連携できます。NetAppNetApp、どちらか一方を選択することを推奨しており、両方を選択することは推奨していません。

NetAppは、サービスプロバイダ主導（SP主導）のSSOのみをサポートしています。まず、 NetAppをサービスプロバイダとして信頼するようにアイデンティティプロバイダを設定する必要があります。その後、BlueXPでアイデンティティプロバイダの設定を使用して接続を作成できます。

BlueXPのシングルサインオン（SSO）を有効にするには、Microsoft Entra ID とのフェデレーション接続を設定します。このプロセスでは、Microsoft Entra ID を設定してBlueXP をサービスプロバイダーとして信頼し、BlueXPで接続を作成します。

作業を開始する前に

- 管理者権限を持つIdPアカウントが必要です。IdP管理者と調整して手順を完了してください。
- 連携に使用するドメインを特定します。ご自身のメールドメイン、またはご自身で所有している別のドメインを使用できます。メールドメイン以外のドメインを使用する場合は、まずBlueXPでドメインを検証する必要があります。これは、以下の手順に従って行うことができます。 "BlueXPでドメインを認証する"トピック。

手順

1. BlueXP  コンソールの右上で、>* IDおよびアクセス管理*を選択します。
2. *Federation*タブを選択します。
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。メールドメインとは、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を設定してください。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. BlueXP を信頼するために Microsoft Entra ID アプリを登録するときは、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 ドメイン名を入力する必要があります。
2. BlueXP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。数秒で接続が作成されます。

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」を選択してください。IdPサーバーのログインページに移動します。IdPの認証情報でログインしてテストを完了し、 BlueXPに戻って接続を有効にしてください。
3. 「 * 次へ * 」を選択します。
4. *フェデレーションの有効化*ページでフェデレーションの詳細を確認し、*フェデレーションの有効化*を選択します。
5. 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BlueXPにログインできるようになります。

# BlueXPをPingFederateで連携

PingFederate IdPプロバイダーと連携して、 BlueXPのシングルサインオン（SSO）を有効にします。これにより、ユーザーは企業の認証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、組織管理者またはフェデレーション管理者が必要です。フェデレーション閲覧者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。"

社内のIdPまたはNetAppサポートサイトと連携できます。NetAppNetApp、どちらか一方を選択することを推奨しており、両方を選択することは推奨していません。

NetAppは、サービスプロバイダ主導（SP主導）のSSOのみをサポートしています。まず、 NetAppをサービスプロバイダとして信頼するようにアイデンティティプロバイダを設定する必要があります。その後、BlueXPでアイデンティティプロバイダの設定を使用して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することで、 BlueXP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、PingFederateサーバーをBlueXPをサービスプロバイダーとして信頼するように設定し、 BlueXPで接続を作成します。

作業を開始する前に

- 管理者権限を持つIdPアカウントが必要です。IdP管理者と調整して手順を完了してください。
- 連携に使用するドメインを特定します。ご自身のメールドメイン、またはご自身で所有している別のドメインを使用できます。メールドメイン以外のドメインを使用する場合は、まずBlueXPでドメインを検証する必要があります。これは、以下の手順に従って行うことができます。 "BlueXPでドメインを認証する"トピック。

手順

1. BlueXP コンソールの右上で、>* IDおよびアクセス管理*を選択します。
2. *Federation*タブを選択します。
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。メールドメインとは、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サーバーを設定して、 NetAppをサービスプロバイダーとして信頼するようにします。この手順はPingFederateサーバー上で実行する必要があります。
   a. PingFederate がBlueXP を信頼するように構成する場合は、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>` <fed-domain-name-pingfederate>はフェデレーションのドメイン名です。例えば、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をコピーしてください。BlueXP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てください。証明書はBase64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. BlueXP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てください。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。数秒で接続が作成されます。
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」を選択してください。IdPサーバーのログインページに移動します。IdPの認証情報でログインしてテストを完了し、 BlueXPに戻って接続を有効にしてください。
14. 「 * 次へ * 」を選択します。
15. *フェデレーションの有効化*ページでフェデレーションの詳細を確認し、*フェデレーションの有効化*を選択します。
16. 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BlueXPにログインできるようになります。

# 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、 BlueXPのシングルサインオン（SSO）を有効にします。これにより、ユーザーは企業の認証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

組織管理者。 "アクセス ロールの詳細について説明します。"

社内IdPまたはNetAppサポートサイトのいずれかと連携できます。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主導（SP主導）のSSOのみをサポートしています。まず、 NetAppをサービスプロバイダとして信頼するようにアイデンティティプロバイダを設定する必要があります。その後、BlueXPでアイデンティティプロバイダの設定を使用して接続を作成できます。

BlueXPのシングルサインオン（SSO）を有効にするには、SAML 2.0プロバイダとのフェデレーション接続を設定します。このプロセスでは、プロバイダがNetAppをサービスプロバイダとして信頼するように設定し、BlueXPで接続を作成します。

作業を開始する前に

- 管理者権限を持つIdPアカウントが必要です。IdP管理者と調整して手順を完了してください。
- 連携に使用するドメインを特定します。ご自身のメールドメイン、またはご自身で所有している別のドメインを使用できます。メールドメイン以外のドメインを使用する場合は、まずBlueXPでドメインを検証する必要があります。これは、以下の手順に従って行うことができます。 "BlueXPでドメインを認証する"ト

ピック。

手順

1. BlueXP コンソールの右上で、>* IDおよびアクセス管理*を選択します。
2. *Federation*タブを選択します。
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。メールドメインとは、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アイデンティティプロバイダを設定して、 NetAppをサービスプロバイダとして信頼するようにします。この手順はSAMLプロバイダ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を設定します。これはBlueXP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>
```

   b. SAML アプリケーションをBlueXP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>` <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。例えば、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` 。
   c. 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）

d. 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てください。証明書はPEM、CER、またはCRT形式である必要があります。

9. BlueXPに戻り、[次へ] を選択して接続を作成します。
10. SAML を使用して接続を作成します。
    a. SAML サーバーの サインイン **URL** を入力します。
    b. 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。
    c. 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。
11. *接続を作成*を選択します。数秒で接続が作成されます。
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」を選択してください。IdPサーバーのログインページに移動します。IdPの認証情報でログインしてテストを完了し、 BlueXPに戻って接続を有効にしてください。
14. 「 * 次へ * 」を選択します。
15. *フェデレーションの有効化*ページでフェデレーションの詳細を確認し、*フェデレーションの有効化*を選択します。
16. 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BlueXPにログインできるようになります。

## 著作権に関する情報



## 商標に関する情報