Configurar federações

NetApp Console setup and administration

NetApp
February 10, 2026

Índice

Configurar federações

Federar o NetApp Console com os Serviços de Federação do Active Directory (AD FS)

Federe seus Serviços de Federação do Active Directory (AD FS) com o NetApp Console para habilitar o logon único (SSO) para o NetApp Console. Isso permite que os usuários façam login no Console usando suas credenciais corporativas.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . A NetApp recomenda escolher um ou outro, mas não ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, configure o provedor de identidade para confiar no NetApp Console como um provedor de serviços. Em seguida, crie uma conexão no Console usando a configuração do seu provedor de identidade.

Você pode configurar a federação com seu servidor AD FS para habilitar o logon único (SSO) para o NetApp Console. O processo envolve configurar o AD FS para confiar no Console como um provedor de serviços e, em seguida, criar a conexão no NetApp Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
5. Selecione **Avançar**.
6. Para seu método de conexão, escolha **Protocolo** e depois selecione **Serviços de Federação do Active Directory (AD FS)**.
7. Selecione **Avançar**.
8. Crie uma Relying Party Trust no seu servidor AD FS. Você pode usar o PowerShell ou configurá-lo manualmente no seu servidor AD FS. Consulte a documentação do AD FS para obter detalhes sobre como criar uma confiança de terceira parte confiável.
   a. Crie a confiança usando o PowerShell usando o seguinte script:

```
(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. Como alternativa, você pode criar a confiança manualmente no console de gerenciamento do AD FS. Use os seguintes valores do NetApp Console ao criar a confiança:

   - Ao criar o Relying Trust Identifier, use o valor **YOUR_TENANT**: `netapp-cloud-account`
   - Ao selecionar **Habilitar suporte para WS-Federation**, use o valor **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`

c. Depois de criar a confiança, copie o URL de metadados do seu servidor AD FS ou baixe o arquivo de metadados da federação. Você precisará deste URL ou arquivo para concluir a conexão no Console.

A NetApp recomenda usar o URL de metadados para permitir que o NetApp Console recupere automaticamente a configuração mais recente do AD FS. Se você baixar o arquivo de metadados da federação, precisará atualizá-lo manualmente no NetApp Console sempre que houver alterações na configuração do AD FS.

9. Retorne ao Console e selecione **Avançar** para criar a conexão.
10. Crie a conexão com o AD FS.
    a. Insira o **URL do AD FS** que você copiou do seu servidor AD FS na etapa anterior ou carregue o arquivo de metadados da federação que você baixou do seu servidor AD FS.
11. Selecione **Criar conexão**. A criação da conexão pode levar alguns segundos.
12. Selecione **Avançar**.
13. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Faça login com suas credenciais do IdP. Após efetuar o login, volte ao Console para ativar a conexão.

    Ao usar o Console no modo restrito, copie o URL para uma janela anônima do navegador ou para um navegador separado para fazer login no seu IdP.

14. No Console, selecione **Avançar** para revisar a página de resumo.
15. Configure as notificações.

    Escolha entre sete dias ou 30 dias. O sistema envia notificações de expiração por e-mail e as exibe no Console para qualquer usuário com as seguintes funções: Superadministrador, Administrador da organização, Administrador da federação e Visualizador da federação.

16. Analise os detalhes da federação e selecione **Ativar federação**.
17. Selecione **Concluir** para finalizar o processo.

Após habilitar a federação, os usuários fazem login no NetApp Console usando suas credenciais corporativas.

Federar NetApp Console com Microsoft Entra ID

Federe com seu provedor de IdP do Microsoft Entra ID para habilitar o logon único (SSO) para o NetApp Console. Isso permite que os usuários façam login usando suas credenciais corporativas.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . A NetApp recomenda escolher um ou outro, mas não ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode configurar uma conexão federada com o Microsoft Entra ID para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu ID do Microsoft Entra para confiar no Console como um provedor de serviços e, em seguida, criar a conexão no Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.

Detalhes do domínio

1. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
2. Selecione **Avançar**.

Método de conexão

1. Para seu método de conexão, escolha **Provedor** e depois selecione **Microsoft Enterprise ID**.
2. Selecione **Avançar**.

Instruções de configuração

1. Configure seu ID Microsoft Entra para confiar na NetApp como provedora de serviços. Você precisa executar esta etapa no seu servidor Microsoft Entra ID.
   a. Use os seguintes valores ao registrar seu aplicativo Microsoft Entra ID para confiar no Console:
      - Para o **URL de redirecionamento**, use `https://services.cloud.netapp.com`
      - Para o **URL de resposta**, use `https://netapp-cloud-account.auth0.com/login/`

`callback`

b. Crie um segredo do cliente para seu aplicativo Microsoft Entra ID. Você precisará fornecer o ID do cliente, o segredo do cliente e o nome de domínio do Entra ID para concluir a federação.

2. Retorne ao Console e selecione **Avançar** para criar a conexão.

Criar conexão

1. Crie a conexão com o Microsoft Entra ID
   a. Insira o ID do cliente e o segredo do cliente que você criou na etapa anterior.
   b. Digite o nome de domínio do ID do Microsoft Entra.
2. Selecione **Criar conexão**. O sistema cria a conexão em poucos segundos.

Teste e habilite a conexão

1. Selecione **Avançar**.
2. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Faça login com suas credenciais do IdP. Após efetuar o login, volte ao Console para ativar a conexão.

   Ao usar o Console no modo restrito, copie o URL para uma janela anônima do navegador ou para um navegador separado para fazer login no seu IdP.

3. No Console, selecione **Avançar** para revisar a página de resumo.
4. Configure as notificações.

   Escolha entre sete dias ou 30 dias. O sistema envia notificações de expiração por e-mail e as exibe no Console para qualquer usuário com as seguintes funções: Superadministrador, Administrador da organização, Administrador da federação e Visualizador da federação.

5. Analise os detalhes da federação e selecione **Ativar federação**.
6. Selecione **Concluir** para finalizar o processo.

Após habilitar a federação, os usuários fazem login no NetApp Console usando suas credenciais corporativas.

Federar o NetApp Console com o PingFederate

Federe com seu provedor PingFederate IdP para habilitar o logon único (SSO) para o NetApp Console. Isso permite que os usuários façam login usando suas credenciais corporativas.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . A NetApp recomenda escolher um ou outro, mas não ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro,

você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode configurar uma conexão federada com o PingFederate para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu servidor PingFederate para confiar no Console como um provedor de serviços e, em seguida, criar a conexão no Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
5. Selecione **Avançar**.
6. Para seu método de conexão, escolha **Provedor** e depois selecione **PingFederate**.
7. Selecione **Avançar**.
8. Configure seu servidor PingFederate para confiar na NetApp como provedora de serviços. Você precisa executar esta etapa no seu servidor PingFederate.
   a. Use os seguintes valores ao configurar o PingFederate para confiar no NetApp Console:
      - Para o **URL de resposta** ou **URL do serviço de consumidor de declaração (ACS)**, use `https://netapp-cloud-account.auth0.com/login/callback`
      - Para o **URL de logout**, use `https://netapp-cloud-account.auth0.com/logout`
      - Para **ID do público/entidade**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` onde <fed-domain-name-pingfederate> é o nome de domínio da federação. Por exemplo, se o seu domínio for `example.com` , o ID do público/entidade seria `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Copie a URL do servidor PingFederate. Você precisará deste URL ao criar a conexão no Console.
   c. Baixe o certificado X.509 do seu servidor PingFederate. Ele precisa estar no formato PEM codificado em Base64 (.pem, .crt, .cer).
9. Retorne ao Console e selecione **Avançar** para criar a conexão.
10. Crie a conexão com PingFederate
    a. Digite a URL do servidor PingFederate que você copiou na etapa anterior.
    b. Carregue o certificado de assinatura X.509. O certificado deve estar no formato PEM, CER ou CRT.
11. Selecione **Criar conexão**. O sistema cria a conexão em poucos segundos.
12. Selecione **Avançar**.
13. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Faça login com suas credenciais do IdP. Após efetuar o login, volte ao Console para ativar a conexão.

Ao usar o Console no modo restrito, copie o URL para uma janela anônima do navegador ou para um navegador separado para fazer login no seu IdP.

14. No Console, selecione **Avançar** para revisar a página de resumo.
15. Configure as notificações.

    Escolha entre sete dias ou 30 dias. O sistema envia notificações de expiração por e-mail e as exibe no Console para qualquer usuário com as seguintes funções: Superadministrador, Administrador da organização, Administrador da federação e Visualizador da federação.

16. Analise os detalhes da federação e selecione **Ativar federação**.
17. Selecione **Concluir** para finalizar o processo.

Após habilitar a federação, os usuários fazem login no NetApp Console usando suas credenciais corporativas.

Federe com um provedor de identidade SAML

Federe com seu provedor SAML 2.0 IdP para habilitar o logon único (SSO) para o NEtApp Console. Isso permite que os usuários façam login usando suas credenciais corporativas.

Função necessária

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . Você não pode federar com ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode configurar uma conexão federada com seu provedor SAML 2.0 para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu provedor para confiar na NetApp como provedora de serviços e, em seguida, criar a conexão no Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
5. Selecione **Avançar**.
6. Para seu método de conexão, escolha **Protocolo** e depois selecione **Provedor de identidade SAML**.

7. Selecione **Avançar**.
8. Configure seu provedor de identidade SAML para confiar na NetApp como provedora de serviços. Você precisa executar esta etapa no servidor do seu provedor SAML.
   a. Certifique-se de que seu IdP tenha o atributo `email` definido como o endereço de e-mail do usuário. Isso é necessário para que o Console identifique os usuários corretamente:

```
<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. Use os seguintes valores ao registrar seu aplicativo SAML no Console:
   - Para o **URL de resposta** ou **URL do serviço de consumidor de declaração (ACS)**, use `https://netapp-cloud-account.auth0.com/login/callback`
   - Para o **URL de logout**, use `https://netapp-cloud-account.auth0.com/logout`
   - Para **ID do público/entidade**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` onde <fed-domain-name-saml> é o nome de domínio que você deseja usar para federação. Por exemplo, se o seu domínio for `example.com` , o ID do público/entidade seria `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
2. Depois de criar a confiança, copie os seguintes valores do servidor do seu provedor SAML:
   - URL de login
   - URL de saída (opcional)
3. Baixe o certificado X.509 do servidor do seu provedor SAML. Precisa estar no formato PEM, CER ou CRT.
   a. Retorne ao Console e selecione **Avançar** para criar a conexão.
   b. Crie a conexão com SAML.
4. Digite o **URL de login** do seu servidor SAML.
5. Faça upload do certificado X.509 que você baixou do servidor do seu provedor SAML.
6. Opcionalmente, insira o **URL de saída** do seu servidor SAML.
   a. Selecione **Criar conexão**. O sistema cria a conexão em poucos segundos.
   b. Selecione **Avançar**.
   c. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Faça login com suas credenciais do IdP. Após efetuar o login, volte ao Console para ativar a conexão.

Ao usar o Console no modo restrito, copie o URL para uma janela anônima do navegador ou para um navegador separado para fazer login no seu IdP.

d. No Console, selecione **Avançar** para revisar a página de resumo.

e. Configure as notificações.

   Escolha entre sete dias ou 30 dias. O sistema envia notificações de expiração por e-mail e as exibe no Console para qualquer usuário com as seguintes funções: Superadministrador, Administrador da organização, Administrador da federação e Visualizador da federação.

f. Analise os detalhes da federação e selecione **Ativar federação**.

g. Selecione **Concluir** para finalizar o processo.

Após habilitar a federação, os usuários fazem login no NetApp Console usando suas credenciais corporativas.

Informações sobre direitos autorais

Informações sobre marcas comerciais