



Segurança e conformidade

NetApp Console setup and administration

NetApp
January 23, 2026

Índice

Segurança e conformidade	1
Federação de identidade	1
Habilitar logon único usando federação de identidade com o NetApp Console	1
Verificação de domínio	3
Configurar federações	3
Gerenciar federações	10
Aplicar permissões ONTAP para o ONTAP Advanced View (ONTAP System Manager)	13
Ativar o modo somente leitura para uma organização do NetApp Console	14
Ative o modo somente leitura para sua organização do Console	14
Cadastre-se no NetApp Console como administrador inicial da organização	14
Cadastre-se ou faça login no NetApp Console se já existir uma organização	15

Segurança e conformidade

Federação de identidade

Habilitar logon único usando federação de identidade com o NetApp Console

O logon único (federação) simplifica o processo de login e aumenta a segurança, permitindo que os usuários façam login no NetApp Console usando suas credenciais corporativas. Você pode habilitar o logon único (SSO) com seu provedor de identidade (IdP) ou com o site de suporte da NetApp .

Função necessária

Administrador da organização, administrador da federação, visualizador da federação."Saiba mais sobre funções de acesso."

Federação de identidade com o site de suporte da NetApp

A federação com o site de suporte da NetApp permite que os usuários façam login no Console, no Active IQ Digital Advisor e em outros aplicativos associados usando as mesmas credenciais.



Se você se federar com o Site de Suporte da NetApp , não poderá se federar também com seu provedor de gerenciamento de identidade corporativa. Escolha o que funciona melhor para sua organização.

Passos

1. Baixe e complete o "[Formulário de solicitação de federação da NetApp](#)" .
2. Envie o formulário para o endereço de e-mail especificado no formulário.

A equipe de suporte da NetApp analisa e processa sua solicitação.

Configure uma conexão federada com seu provedor de identidade

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



Se você configurou a federação anteriormente usando o NetApp Cloud Central (um aplicativo externo ao Console), será necessário importar sua federação usando a página Federação para gerenciá-la no Console."[Aprenda como importar sua federação.](#)"

Provedores de identidade suportados

A NetApp oferece suporte aos seguintes protocolos e provedores de identidade para federação:

Protocolos

- Provedores de identidade de Linguagem de Marcação de Asserção de Segurança (SAML)
- Serviços de Federação do Active Directory (AD FS)

Provedores de identidade

- ID de entrada da Microsoft
- PingFederate

Federação com fluxo de trabalho do NetApp Console

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 federar com seu domínio de e-mail ou com um domínio diferente que você possui. Para federar com um domínio diferente do seu domínio de e-mail, primeiro verifique se você é o proprietário do domínio.

1

Verifique seu domínio (se não estiver usando seu domínio de e-mail)

Para federar com um domínio diferente do seu domínio de e-mail, verifique se você é o proprietário dele. Você pode federar seu domínio de e-mail sem nenhuma etapa extra.

2

Configure seu IdP para confiar na NetApp como um provedor de serviços

Configure seu provedor de identidade para confiar no NetApp criando um novo aplicativo e fornecendo detalhes como URL do ACS, ID da entidade ou outras informações de credencial. As informações do provedor de serviços variam de acordo com o provedor de identidade, portanto, consulte a documentação do seu provedor de identidade específico para obter detalhes. Você precisará trabalhar com o administrador do seu IdP para concluir esta etapa.

3

Crie a conexão federada no Console

Forneça o URL ou arquivo de metadados SAML do seu provedor de identidade para criar a conexão. Essas informações são usadas para estabelecer a relação de confiança entre o Console e seu provedor de identidade. As informações fornecidas dependem do IdP que você está usando. Por exemplo, se estiver usando o Microsoft Entra ID, você precisará fornecer o ID do cliente, o segredo e o domínio.

4

Teste sua federação no Console

Teste sua conexão federada antes de habilitá-la. Use a opção de teste na página Federação no Console para verificar se o usuário de teste pode ser autenticado com sucesso. Se o teste for bem-sucedido, você poderá habilitar a conexão.

5

Habilite sua conexão no Console

Depois de habilitar a conexão, os usuários podem efetuar login no Console usando suas credenciais corporativas.

Revise o tópico do seu respectivo protocolo ou IdP para começar:

- "[Configurar uma conexão federada com o AD FS](#)"
- "[Configurar uma conexão federada com o Microsoft Entra ID](#)"
- "[Configurar uma conexão federada com PingFederate](#)"

- "Configurar uma conexão federada com um provedor de identidade SAML"

Verificação de domínio

Verifique o domínio de e-mail para sua conexão federada

Se você quiser federar com um domínio diferente do seu domínio de e-mail, primeiro você deve verificar se é o proprietário do domínio. Você só pode usar domínios verificados para federação.

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."

Verificar seu domínio envolve adicionar um registro TXT às configurações de DNS do seu domínio. Este registro é usado para provar que você é o proprietário do domínio e permite que o NetApp Console confie no domínio para federação. Talvez seja necessário coordenar com seu administrador de TI ou de rede para concluir esta etapa.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Selecione **Verificar propriedade do domínio**.
5. Digite o domínio que você deseja verificar e selecione **Continuar**.
6. Copie o registro TXT fornecido.
7. Acesse as configurações de DNS do seu domínio e configure o valor TXT que foi fornecido como um registro TXT para seu domínio. Trabalhe com seu administrador de TI ou de rede, se necessário.
8. Após o registro TXT ser adicionado, retorne ao Console e selecione **Verificar**.

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.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. 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.

Gerenciar federações

Gerenciar federações no NetApp Console

Você pode gerenciar sua federação no NetApp Console. Você pode desativá-lo, atualizar credenciais expiradas e também desativá-lo caso não precise mais dele.

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 também pode adicionar um domínio verificado adicional a uma federação existente, o que permite usar vários domínios para sua conexão federada.

-
- Se você configurou a federação usando o NetApp Cloud Central, importe-a por meio da página **Federação** para gerenciá-la no Console. ["Aprenda como importar sua federação"](#)
 - Na página de Auditoria, você pode visualizar eventos de gerenciamento de federação, como ativação, desativação e atualização de federações. ["Saiba mais sobre o monitoramento de operações no NetApp Console."](#)

Habilitar uma federação

Se você criou uma federação, mas ela não está habilitada, você pode habilitá-la na página **Federação**. Habilitar uma federação permite que usuários associados à federação façam login no Console usando suas credenciais corporativas. Crie e teste a federação com sucesso antes de habilitá-la.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações **•••** ao lado da federação que você deseja habilitar e selecione **Habilitar**.

Adicionar um domínio verificado a uma federação existente

Você pode adicionar um domínio verificado a uma federação existente no Console para usar vários domínios com o mesmo provedor de identidade (IdP).

Você já deve ter verificado o domínio no Console antes de poder adicioná-lo a uma federação. Se você ainda não verificou o domínio, pode fazê-lo seguindo as etapas em "["Verifique seu domínio no Console"](#)" .

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações **⋮** ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Atualizar domínios**. A caixa de diálogo **Atualizar domínios** exibe o domínio já associado a esta federação.
4. Selecione um domínio verificado na lista de domínios disponíveis.
5. Selecione **Atualizar**. Novos usuários de domínio podem obter acesso ao Console federado em 30 segundos.

Atualizando uma conexão federada que está expirando

Você pode atualizar os detalhes de uma federação no Console. Por exemplo, você precisará atualizar a federação se as credenciais, como um certificado ou segredo do cliente, expirarem. Quando necessário, atualize a data de notificação para lembrá-lo de atualizar a conexão antes que ela expire.



Atualize o Console antes de atualizar seu IdP para evitar problemas de login. Permaneça conectado ao Console durante o processo.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações (três pontos verticais) ao lado da federação que você deseja atualizar e selecione **Atualizar federação**.
4. Atualize os detalhes da federação conforme necessário.
5. Selecione **Atualizar**.

Testar uma federação existente

Teste a conexão de uma federação existente para verificar se ela funciona. Isso pode ajudar você a identificar

quaisquer problemas com a federação e solucioná-los.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações: ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Testar conexão**.
4. Selecione **Testar**. O sistema solicita que você faça login com suas credenciais corporativas. Se a conexão for bem-sucedida, você será redirecionado para o NetApp Console. Se a conexão falhar, você verá uma mensagem de erro indicando o problema com a federação.
5. Selecione **Concluído** para retornar à aba **Federação**.

Desabilitar uma federação

Se você não precisar mais de uma federação, poderá desativá-la. Isso impede que usuários associados à federação façam login no Console usando suas credenciais corporativas. Você pode reativar a federação mais tarde, se necessário.

Desabilite uma federação antes de excluí-la, como ao desativar o IdP ou descontinuar a federação. Isso permite que você o reactive mais tarde, se necessário.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações: ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Desativar**.

Excluir uma federação

Se você não precisar mais de uma federação, poderá excluí-la. Isso remove a federação e impede que qualquer usuário associado a ela faça login no Console usando suas credenciais corporativas. Por exemplo, se o IdP estiver sendo desativado ou se a federação não for mais necessária.

Não é possível recuperar uma federação após excluí-la. Você deve criar uma nova federação.



Você deve desabilitar uma federação antes de poder excluí-la. Não é possível recuperar uma federação após excluí-la.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federações** para visualizar a página **Federações**.
3. Selecione o menu de ações: ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Excluir**.

Importe sua federação para o NetApp Console

Se você tiver configurado anteriormente a federação por meio do NetApp Cloud Central (um aplicativo externo ao NetApp Console), a página Federação solicitará que você importe sua conexão federada existente para o Console para que você possa gerenciá-la

na nova interface. Você pode então aproveitar os aprimoramentos mais recentes sem precisar recriar sua conexão federada.



Depois de importar sua federação existente, você pode gerenciá-la na página **Federações**. ["Saiba mais sobre como gerenciar federações."](#)

Função necessária

Administrador da organização ou administrador da federação. ["Saiba mais sobre funções de acesso."](#)

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione **Importar Federação**.

Aplicar permissões ONTAP para o ONTAP Advanced View (ONTAP System Manager)

Por padrão, as credenciais do agente do Console permitem que os usuários acessem o Advanced View (ONTAP System Manager). Em vez disso, você pode solicitar aos usuários suas credenciais ONTAP . Isso garante que as permissões ONTAP de um usuário sejam aplicadas quando ele trabalha com clusters ONTAP nos clusters Cloud Volumes ONTAP e ONTAP locais.



Você deve ter a função de administrador da organização para editar as configurações do agente do console.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Editar agente**.

O agente do Console deve estar ativo para editá-lo.

3. Expanda a opção **Forçar credenciais**.
4. Marque a caixa de seleção para habilitar a opção **Forçar credenciais** e selecione **Salvar**.
5. Verifique se a opção **Forçar credenciais** está habilitada.



Ativar o modo somente leitura para uma organização do NetApp Console

Como medida de segurança, você pode ativar o modo somente leitura para sua organização do NetApp Console . No modo somente leitura, os usuários podem visualizar recursos e configurações, mas não podem fazer alterações.

No modo somente leitura, os usuários com funções de administrador precisam elevar manualmente suas permissões para fazer alterações, o que garante que as alterações sejam intencionais.

Funções de acesso necessárias

Superadministrador ou administrador da organização.

Ative o modo somente leitura para sua organização do Console.

Ative o modo somente leitura para restringir as alterações na sua organização do Console. Todos os usuários ainda podem visualizar os recursos. Usuários com funções de administrador não podem executar nenhuma ação no Console sem elevar manualmente suas permissões.

Quando o modo somente leitura está ativado, os usuários veem um banner que os notifica de que a organização está em modo somente leitura. Os usuários devem acessar as Configurações do usuário para elevar seu nível de privilégio.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Na guia **Organizações**, selecione **Editar configurações da organização** para a organização que você deseja definir como somente leitura.
3. Na seção **Modo somente leitura**, ative o modo somente leitura movendo a chave para a posição **Ligado** e, em seguida, selecione **Salvar**.



Save

Cadastre-se no NetApp Console como administrador inicial da organização.

Se sua empresa não possui uma organização NetApp Console , inscreva-se para criar uma. O primeiro usuário é o administrador e gerencia as contas e permissões. Você poderá atualizar as funções e adicionar administradores posteriormente.

Passos

1. Abra um navegador da web e vá para o "[NetApp Console](#)"
2. Se você possui uma conta no site de suporte da NetApp , insira o endereço de e-mail associado à sua conta diretamente na página de **Login**.

O Console realiza o seu cadastro como parte deste login inicial, utilizando as suas credenciais do Site de

3. Se você quiser se inscrever criando um login no Console, selecione **Inscrir-se**.
 - a. Na página **Inscrica-se**, insira as informações necessárias e selecione **Avançar**.
-  Somente caracteres em inglês são permitidos no formulário de inscrição.
- b. Verifique sua caixa de entrada para ver se recebeu um e-mail da NetApp com instruções para verificar seu endereço de e-mail.
- Verifique seu endereço de e-mail para concluir o cadastro.
4. Após efetuar o login, revise e aceite o Contrato de Licença do Usuário Final.
5. Na página **Boas-vindas**, crie uma organização.
6. Selecione **Vamos começar**.

+ Se você for um administrador iniciante, siga o processo guiado para adicionar armazenamento, criar um agente do Console e muito mais. "[Aprenda a usar o Assistente do Console](#)."

Próximos passos

Como administrador, após concluir as etapas incluídas no Assistente do Console, você deve planejar sua estratégia de identidade e acesso, adicionar usuários à sua organização e atribuir funções. "[Saiba mais sobre gerenciamento de identidade e acesso para o NetApp Console](#)."

Cadastre-se ou faça login no NetApp Console se já existir uma organização.

Se sua empresa já possui uma organização NetApp Console , inscreva-se ou faça login para acessá-la. O método de cadastro ou login depende se sua empresa utiliza federação de identidades ou possui credenciais do site de suporte da NetApp . Caso contrário, crie um login no NetApp Console .

Passos

1. Abra um navegador da web e vá para o "[NetApp Console](#)"
2. Se você possui uma conta no site de suporte da NetApp ou se sua empresa configurou o login único (SSO), insira seu endereço de e-mail associado ou suas credenciais de SSO na página **Entrar**. Siga as instruções para concluir o login.

Em ambos os casos, você se inscreve no Console como parte desse login inicial.

3. Se você quiser se inscrever criando um login no Console, selecione **Inscrir-se**.
 - a. Na página **Inscrica-se**, insira as informações necessárias e selecione **Avançar**.
-  Somente caracteres em inglês são permitidos no formulário de inscrição.
- b. Verifique sua caixa de entrada para ver se recebeu um e-mail da NetApp com instruções para verificar seu endereço de e-mail.
- Verifique seu endereço de e-mail para concluir o cadastro.
4. Após efetuar o login, revise e aceite o Contrato de Licença do Usuário Final.
5. Se o sistema solicitar que você crie uma organização, feche a caixa de diálogo e informe um administrador do Console para que ele possa adicioná-lo à sua organização do Console e conceder-lhe

acesso. ["Aprenda como entrar em contato com um administrador da organização."](#)

Próximos passos

Após receber acesso à sua organização, você poderá começar a gerenciar o armazenamento e usar os serviços de dados que lhe forem atribuídos.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.