Gerenciar configurações de autenticação SAML

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-918/config/concept_manage_saml_authentication_settings_um.html on November 13, 2026. Always check docs.netapp.com for the latest.

Índice

Gerenciar configurações de autenticação SAML . . . 1
- Ative a autenticação SAML no Active IQ Unified Manager . . . 1
- Utilize um provedor de identidade no Active IQ Unified Manager . . . 1
  - Padrões de criptografia suportados . . . 1
  - Provedores de identidade validados . . . 1
  - Requisitos de configuração do ADFS . . . 1
  - Outros requisitos de configuração . . . 2
- Ative a autenticação SAML no Active IQ Unified Manager . . . 2
- Altere o provedor de identidade de autenticação SAML no Active IQ Unified Manager . . . 3
- Atualize as configurações de autenticação SAML após uma alteração no certificado de segurança do Active IQ Unified Manager . . . 4
- Desative a autenticação SAML no Active IQ Unified Manager . . . 5
- Desative a autenticação SAML no console de manutenção do Active IQ Unified Manager . . . 6
- Utilize a página de autenticação SAML no Active IQ Unified Manager . . . 6

Gerenciar configurações de autenticação SAML

Ative a autenticação SAML no Active IQ Unified Manager

Após configurar as definições de autenticação remota, você pode ativar a autenticação Security Assertion Markup Language (SAML) para que os usuários remotos sejam autenticados por um provedor de identidade (IdP) seguro antes de poderem acessar a interface de usuário da web do Unified Manager.

Observe que somente os usuários remotos terão acesso à interface gráfica de usuário do Unified Manager após a autenticação SAML ter sido ativada. Os usuários locais e os usuários de manutenção não poderão acessar a interface. Essa configuração não afeta os usuários que acessam o console de manutenção.

Utilize um provedor de identidade no Active IQ Unified Manager

Ao configurar o Unified Manager para usar um provedor de identidade (IdP) para realizar autenticação SAML para todos os usuários remotos, você precisa estar ciente de algumas configurações obrigatórias para que a conexão com Unified Manager seja bem-sucedida.

Você deve inserir o URI e os metadados do Unified Manager no servidor IdP. Você pode copiar essas informações da página SAML Authentication do Unified Manager. O Unified Manager é considerado o provedor de serviços (SP) no padrão Security Assertion Markup Language (SAML).

Padrões de criptografia suportados

- Padrão de Criptografia Avançado (AES): AES-128 e AES-256
- Algoritmo de Hash Seguro (SHA): SHA-1 e SHA-256

Provedores de identidade validados

- O Shibboleth
- O Active Directory Federation Services (ADFS)

Requisitos de configuração do ADFS

- Você deve definir três regras de declaração na seguinte ordem, que são necessárias para que o Unified Manager analise as respostas SAML do ADFS para esta entrada de confiança da parte confiável.

Regra de reivindicação	Valor
SAM-account-name	ID do nome
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Grupos de tokens — nome não qualificado	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Você deve definir o método de autenticação como “Forms Authentication” ou os usuários poderão receber um erro ao sair do Unified Manager . Siga estas etapas:

a. Abra o ADFS Management Console.

b. Clique na pasta Políticas de Autenticação na exibição em árvore à esquerda.

c. Em Ações, à direita, clique em Editar política de autenticação primária global.

d. Defina o método de autenticação da intranet como “Forms Authentication” em vez do padrão “Windows Authentication”.

- Em alguns casos, o login pelo IdP é rejeitado quando o certificado de segurança do Unified Manager é assinado por uma CA. Existem duas soluções alternativas para resolver esse problema:
  - Siga as instruções indicadas no link para desativar a verificação de revogação no servidor ADFS da parte confiável associada ao certificado de AC encadeada:

    "Desativar a verificação de revogação por confiança de parte confiável"

  - Faça com que o servidor CA resida no servidor ADFS para assinar a solicitação de certificado do servidor do Unified Manager.

Outros requisitos de configuração

- O desvio de relógio do Unified Manager está configurado para 5 minutos, portanto a diferença de horário entre o servidor IdP e o servidor Unified Manager não pode ser superior a 5 minutos, caso contrário, a autenticação falhará.

Ative a autenticação SAML no Active IQ Unified Manager

Você pode habilitar a autenticação Security Assertion Markup Language (SAML) para que os usuários remotos sejam autenticados por um provedor de identidade (IdP) seguro antes de acessarem a interface de usuário da web do Unified Manager.

Antes de começar

- Você deve ter configurado a autenticação remota e verificado se ela foi bem-sucedida.
- Você deve ter criado pelo menos um Usuário Remoto, ou um Grupo Remoto, com a função de Administrador do Aplicativo.
- O provedor de identidade (IdP) deve ser compatível com o Unified Manager e deve estar configurado.
- Você precisa ter a URL do IdP e os metadados.
- Você precisa ter acesso ao servidor IdP.

Após habilitar a autenticação SAML no Unified Manager, os usuários não poderão acessar a interface gráfica de usuário até que o IdP seja configurado com as informações de host do servidor do Unified Manager. Portanto, você deve estar preparado para concluir ambas as partes da conexão antes de iniciar o processo de configuração. O IdP pode ser configurado antes ou depois de configurar o Unified Manager.

Somente usuários remotos terão acesso à interface gráfica de usuário do Unified Manager após a autenticação SAML ser ativada. Usuários locais e usuários de manutenção não poderão acessar a interface do usuário. Essa configuração não afeta usuários que acessam o console de manutenção, os comandos do Unified Manager ou as ZAPIs.



O Unified Manager é reiniciado automaticamente após você concluir a configuração SAML nesta página.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação SAML**.
2. Selecione a caixa de seleção **Enable SAML authentication**.

   São exibidos os campos necessários para configurar a conexão IdP.

3. Insira o URI do IdP e os metadados necessários para conectar o servidor do Unified Manager ao servidor IdP.

   Se o servidor IdP estiver acessível diretamente a partir do servidor do Unified Manager, você pode clicar no botão **Obter metadados do IdP** após inserir o URI do IdP para preencher automaticamente o campo de metadados do IdP.

4. Copie o URI de metadados do host do Unified Manager ou salve os metadados do host em um arquivo de texto XML.

   Você pode configurar o servidor IdP com essas informações agora.

5. Clique em **Salvar**.

   Uma caixa de mensagem será exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

6. Clique em **Confirmar e Sair** e o Unified Manager será reiniciado.

Na próxima vez que usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do IdP em vez da página de login do Unified Manager.

Caso ainda não tenha feito isso, acesse seu IdP e insira a URI e os metadados do servidor do Unified Manager para concluir a configuração.

Ao usar o ADFS como seu provedor de identidade, a GUI do Unified Manager não respeita o tempo limite do ADFS e continuará funcionando até que o tempo limite da sessão do Unified Manager seja atingido. Você pode alterar o tempo limite da sessão da GUI clicando em **Geral** > **Configurações de recursos** > **Tempo limite de inatividade**.

Altere o provedor de identidade de autenticação SAML no Active IQ Unified Manager

Você pode alterar o provedor de identidade (IdP) que o Unified Manager usa para autenticar usuários remotos.

Antes de começar

- Você precisa ter a URL do IdP e os metadados.
- Você precisa ter acesso ao IdP.

O novo IdP pode ser configurado antes ou depois de configurar o Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação SAML**.
2. Insira o novo URI do IdP e os metadados do IdP necessários para conectar o servidor do Unified Manager

ao IdP.

Se o IdP estiver acessível diretamente do servidor do Unified Manager, você poderá clicar no botão **Fetch IdP Metadata** após inserir a URL do IdP para preencher automaticamente o campo IdP Metadata.

3. Copie o URI de metadados do Unified Manager ou salve os metadados em um arquivo de texto XML.
4. Clique em **Salvar configuração**.

   Uma caixa de mensagem é exibida para confirmar que você deseja alterar a configuração.

5. Clique em **OK**.

Acesse o novo IdP e insira a URI do servidor do Unified Manager e os metadados para concluir a configuração.

Na próxima vez que usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles deverão inserir suas credenciais na nova página de login do IdP em vez da antiga página de login do IdP.

Atualize as configurações de autenticação SAML após uma alteração no certificado de segurança do Active IQ Unified Manager

Qualquer alteração no certificado de segurança HTTPS instalado no servidor do Unified Manager exige que você atualize as configurações de autenticação SAML. O certificado é atualizado se você renomear o sistema host, atribuir um novo endereço IP ao sistema host ou alterar manualmente o certificado de segurança do sistema.

Após a alteração do certificado de segurança e a reinicialização do servidor do Unified Manager, a autenticação SAML deixará de funcionar, e os usuários não poderão acessar a interface gráfica do Unified Manager. Você deve atualizar as configurações de autenticação SAML tanto no servidor IdP quanto no servidor do Unified Manager para reativar o acesso à interface de usuário.

Passos

1. Faça login no console de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

   Uma mensagem será exibida para confirmar que você deseja desativar a autenticação SAML e reiniciar o Unified Manager.

3. Inicie a interface de usuário do Unified Manager usando o FQDN ou endereço IP atualizado, aceite no seu navegador o certificado de servidor atualizado e faça login usando as credenciais do usuário de manutenção.
4. Na página **Configuração/Autenticação**, selecione a aba **Autenticação SAML** e configure a conexão com o IdP.
5. Copie o URI de metadados do host do Unified Manager ou salve os metadados do host em um arquivo de texto XML.
6. Clique em **Salvar**.

   Uma caixa de mensagem será exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

7. Clique em **Confirmar e Sair** e o Unified Manager será reiniciado.
8. Acesse o servidor IdP e insira o URI do servidor do Unified Manager e os metadados para concluir a configuração.

Provedor de identidade	Etapas de configuração
ADFS	a. Exclua a entrada de confiança da parte confiável existente na interface gráfica de gerenciamento do ADFS. b. Adicione uma nova entrada de confiança de terceira parte confiável usando o `saml_sp_metadata.xml`do servidor Unified Manager atualizado. c. Defina as três regras de declaração necessárias para que o Unified Manager analise as respostas SAML do ADFS para esta entrada de confiança da parte confiável. d. Reinicie o serviço ADFS do Windows.
O Shibboleth	a. Atualize o novo FQDN do servidor do Unified Manager nos arquivos `attribute-filter.xml` e `relying-party.xml`. b. Reinicie o servidor web Apache Tomcat e aguarde até que a porta 8005 fique online.

9. Faça login no Unified Manager e verifique se a autenticação SAML está funcionando conforme o esperado por meio do seu IdP.

Desative a autenticação SAML no Active IQ Unified Manager

Você pode desativar a autenticação SAML quando desejar interromper a autenticação de usuários remotos por meio de um provedor de identidade (IdP) seguro antes que eles possam fazer login na interface web do Unified Manager. Quando a autenticação SAML está desativada, os provedores de serviço de diretório configurados, como o Active Directory ou o LDAP, realizam a autenticação de login.

Após desativar a autenticação SAML, os usuários locais e os usuários de manutenção poderão acessar a interface gráfica do usuário, além dos usuários remotos configurados.

Você também pode desativar a autenticação SAML usando o console de manutenção do Unified Manager, caso não tenha acesso à interface gráfica de usuário.

O Unified Manager é reiniciado automaticamente após a desativação da autenticação SAML.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação SAML**.
2. Desmarque a caixa de seleção **Ativar autenticação SAML**.
3. Clique em **Salvar**.

Uma caixa de mensagem será exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

4. Clique em **Confirmar e Sair** e o Unified Manager será reiniciado.

Na próxima vez que os usuários remotos tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do Unified Manager em vez da página de login do IdP.

Acesse seu IdP e exclua o URI do servidor do Unified Manager e os metadados.

Desative a autenticação SAML no console de manutenção do Active IQ Unified Manager

Pode ser necessário desativar a autenticação SAML no console de manutenção quando não houver acesso à interface gráfica do Unified Manager. Isso pode ocorrer em casos de configuração incorreta ou se o IdP estiver inacessível.

Antes de começar

Você precisa ter acesso ao console de manutenção como o usuário de manutenção.

Quando a autenticação SAML está desativada, os provedores de serviço de diretório configurados, como Active Directory ou LDAP, realizam a autenticação de login. Os usuários locais e os usuários de manutenção poderão acessar a interface gráfica do usuário, além dos usuários remotos configurados.

Você também pode desativar a autenticação SAML na página Setup/Authentication da interface de usuário.

O Unified Manager é reiniciado automaticamente após a desativação da autenticação SAML.

Passos

1. Faça login no console de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

   Uma mensagem será exibida para confirmar que você deseja desativar a autenticação SAML e reiniciar o Unified Manager.

3. Digite **y** e pressione Enter para reiniciar o Unified Manager.

Na próxima vez que os usuários remotos tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do Unified Manager em vez da página de login do IdP.

Caso necessário, acesse seu IdP e exclua a URL do servidor do Unified Manager e os metadados.

Utilize a página de autenticação SAML no Active IQ Unified Manager

Você pode usar a página de autenticação SAML para configurar o Unified Manager para autenticar usuários remotos usando SAML por meio de um provedor de identidade (IdP) seguro antes que eles possam fazer login na interface web do Unified Manager.

- Você precisa ter a função Application Administrator para criar ou modificar a configuração do SAML.

- Você precisa ter configurado a autenticação remota.
- Você deve ter configurado pelo menos um usuário remoto ou um grupo remoto.

Após configurar a autenticação remota e os usuários remotos, você pode selecionar a caixa de seleção "Ativar autenticação SAML" para habilitar a autenticação usando um provedor de identidade seguro.

- **URI do IdP**

  O URI para acessar o IdP a partir do servidor Unified Manager. Veja abaixo alguns exemplos de URIs.

  Exemplo de URI do ADFS:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Exemplo de URI do Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Metadados do IdP**

  Os metadados do IdP em formato XML.

  Se o URL do IdP estiver acessível a partir do servidor do Unified Manager, você pode clicar no botão **Obter metadados do IdP** para preencher este campo.

- **Sistema host (FQDN)**

  O FQDN do sistema host do Unified Manager, conforme definido durante a instalação. Você pode alterar esse valor, se necessário.

- **URI do host**

  O URI para acessar o sistema host do Unified Manager a partir do IdP.

- **Metadados do host**

  Os metadados do sistema host em formato XML.

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.