



# **Gerenciando configurações de autenticação SAML**

**Active IQ Unified Manager 9.7**

NetApp  
October 22, 2024

# Índice

- Gerenciando configurações de autenticação SAML ..... 1
  - Requisitos do provedor de identidade ..... 1
  - Habilitando a autenticação SAML ..... 2
  - Alterar o provedor de identidade usado para autenticação SAML ..... 3
  - Atualizando as configurações de autenticação SAML após a alteração do certificado de segurança do Unified Manager ..... 4
  - Desativando a autenticação SAML ..... 6
  - Desativar a autenticação SAML a partir do console de manutenção ..... 6

# Gerenciando configurações de autenticação SAML

Depois de configurar as configurações de autenticação remota, é possível ativar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IDP) antes que eles possam acessar a IU da Web do Unified Manager.

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

## Requisitos do provedor de identidade

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

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

## Padrões de criptografia suportados

- AES (Advanced Encryption Standard): AES-128 e AES-256
- Algoritmo Hash seguro (SHA): SHA-1 e SHA-256

## Provedores de identidade validados

- Shibboleth
- Serviços de Federação do ative Directory (ADFS)

## Requisitos de configuração ADFS

- Você deve definir três regras de reivindicação na ordem a seguir, necessárias para que o Unified Manager analise respostas ADFS SAML para essa entrada confiável de parte confiável.

Regra de reclamação	Valor
Nome da conta SAM	ID do nome
Nome da conta SAM	urna:oid:0.9.2342.19200300.100.1.1
Grupos de token — Nome não qualificado	urna:oid:1.3.6.1.4.1.5923.1.5.1.1

- Você deve definir o método de autenticação como ""Autenticação de formulários"" ou os usuários podem

receber um erro ao fazer logout do Unified Manager . Siga estes passos:

- a. Abra o Console de Gerenciamento ADFS.
  - b. Clique na pasta Authentication Policies (políticas de autenticação) no modo de exibição de 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 ""Autenticação de formulários"" em vez da "Autenticação do Windows" padrão.
- Em alguns casos, o login pelo IDP é rejeitado quando o certificado de segurança do Unified Manager é assinado pela CA. Existem duas soluções alternativas para resolver este problema:
    - Siga as instruções identificadas no link para desativar a verificação de revogação no servidor ADFS para a entidade dependente associada a cert AC encadeada:  
<http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/>
    - Peça que o servidor da CA resida no servidor ADFS para assinar a solicitação de cert do servidor do Unified Manager.

## Outros requisitos de configuração

- O desvio do relógio do Unified Manager é definido para 5 minutos, portanto, a diferença de tempo entre o servidor IDP e o servidor do Unified Manager não pode ser superior a 5 minutos ou a autenticação falhará.

## Habilitando a autenticação SAML

Você pode ativar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IDP) antes que eles possam acessar a IU 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 Administrador do aplicativo.
- O provedor de identidade (IDP) deve ser suportado pelo Unified Manager e deve ser configurado.
- Você deve ter o URL e os metadados do IDP.
- Você deve ter acesso ao servidor IDP.

### Sobre esta tarefa

Depois de ativar a autenticação SAML do Unified Manager, os usuários não poderão acessar a interface gráfica do usuário até que o IDP tenha sido configurado com as informações do host do servidor 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 da configuração do Unified Manager.

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



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

## Passos

1. No painel de navegação à esquerda, clique em **Geral > Autenticação SAML**.
2. Marque a caixa de seleção **Enable SAML Authentication** (Ativar autenticação SAML\*).

São apresentados os campos necessários para configurar a ligação IDP.

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

Se o servidor IDP estiver acessível diretamente a partir do servidor do Unified Manager, você poderá clicar no botão **obter metadados IDP** depois de inserir o URI IDP para preencher o campo metadados IDP automaticamente.

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

Neste momento, você pode configurar o servidor IDP com essas informações.

5. Clique em **Salvar**.

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

6. Clique em **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.

## Resultados

Da próxima vez que os 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.

## Depois de terminar

Se ainda não estiver concluído, acesse seu IDP e insira o URI e os metadados do servidor do Unified Manager para concluir a configuração.



Ao usar o ADFS como provedor de identidade, a GUI do Unified Manager não honra o tempo limite do ADFS e continuará funcionando até que o tempo limite da sessão do Unified Manager seja atingido. Quando o Unified Manager é implantado no Windows, Red Hat ou CentOS, é possível alterar o tempo limite da sessão da GUI usando o seguinte comando da CLI do Unified Manager: `option set absolute.session.timeout=00:15:00` Este comando define o tempo limite da sessão da GUI do Unified Manager para 15 minutos.

## Alterar o provedor de identidade usado para autenticação SAML

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

## Antes de começar

- Você deve ter o URL e os metadados do IDP.
- Você deve ter acesso ao IDP.

## Sobre esta tarefa

O novo IDP pode ser configurado antes ou depois da configuração do Unified Manager.

## Passos

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

Se o IDP estiver acessível diretamente a partir do servidor do Unified Manager, você poderá clicar no botão **obter metadados IDP** depois de inserir o URL IDP para preencher o campo metadados IDP automaticamente.

3. Copie o URI de metadados do Unified Manager ou salve os metadados em um arquivo de texto XML.
4. Clique em **Save Configuration** (Guardar configuração).

É apresentada uma caixa de mensagem para confirmar que pretende alterar a configuração.

5. Clique em **OK**.

## Depois de terminar

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

Da próxima vez que os usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na nova página de login do IDP em vez da antiga página de login do IDP.

## Atualizando as configurações de autenticação SAML após a alteração do certificado de segurança do Unified Manager

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

## Sobre esta tarefa

Depois que o certificado de segurança for alterado e o servidor do Unified Manager for reiniciado, a autenticação SAML não funcionará e os usuários não poderão acessar a interface gráfica do Unified Manager. Você deve atualizar as configurações de autenticação SAML no servidor IDP e no servidor Unified Manager para reativar o acesso à interface do usuário.

## Passos

1. Inicie sessão na consola de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

Uma mensagem é 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 o endereço IP atualizado, aceite o certificado de servidor atualizado no navegador e faça login usando as credenciais de usuário de manutenção.
4. Na página **Configuração/Autenticação**, selecione a guia **Autenticação SAML** e configure a conexão 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 é exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

7. Clique em **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.
8. Acesse seu servidor IDP e insira o URI e os metadados do servidor Unified Manager para concluir a configuração.

Provedor de identidade	Etapas de configuração
ADFS	<ol style="list-style-type: none"><li>a. Exclua a entrada confiável de parte confiável existente na GUI de gerenciamento ADFS.</li><li>b. Adicione uma nova entrada confiável de parte confiável usando o <code>saml_sp_metadata.xml</code> do servidor Unified Manager atualizado.</li><li>c. Defina as três regras de reivindicação necessárias para que o Unified Manager analise respostas ADFS SAML para essa entrada confiável de parte confiável.</li><li>d. Reinicie o serviço ADFS Windows.</li></ol>
Shibboleth	<ol style="list-style-type: none"><li>a. Atualize o novo FQDN do servidor do Unified Manager para <code>attribute-filter.xml</code> os arquivos e <code>relying-party.xml</code></li><li>b. Reinicie o servidor web Apache Tomcat e aguarde até que a porta 8005 fique online.</li></ol>

9. Faça login no Unified Manager e verifique se a autenticação SAML funciona como esperado por meio do IDP.

# Desativando a autenticação SAML

Você pode desativar a autenticação SAML quando quiser parar de autenticar usuários remotos por meio de um provedor de identidade seguro (IDP) antes que eles possam fazer login na IU da Web do Unified Manager. Quando a autenticação SAML está desativada, os provedores de serviços de diretório configurados, como o ativo Directory ou LDAP, executam a autenticação de logon.

## Sobre esta tarefa

Depois de desativar a autenticação SAML, os utilizadores locais e os utilizadores de manutenção poderão aceder à interface gráfica do utilizador, além dos utilizadores remotos configurados.

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



O Unified Manager é reiniciado automaticamente após a autenticação SAML ser desativada.

## Passos

1. No painel de navegação à esquerda, clique em **Geral > Autenticação SAML**.
2. Desmarque a caixa de seleção **Enable SAML Authentication** (Ativar autenticação SAML\*).
3. Clique em **Salvar**.

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

4. Clique em **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.

## Resultados

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.

## Depois de terminar

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

## Desativar a autenticação SAML a partir do console de manutenção

Talvez seja necessário desativar a autenticação SAML do console de manutenção quando não houver acesso à GUI do Unified Manager. Isso pode acontecer em casos de má configuração ou se o IDP não estiver acessível.

## Antes de começar

Você deve ter acesso ao console de manutenção como usuário de manutenção.

## Sobre esta tarefa

Quando a autenticação SAML está desativada, os provedores de serviços de diretório configurados, como o ative Directory ou LDAP, executam a autenticação de logon. Usuários locais e usuários de manutenção poderão acessar a interface gráfica do usuário além de usuários remotos configurados.

Você também pode desativar a autenticação SAML na página Configuração/Autenticação na IU.



O Unified Manager é reiniciado automaticamente após a autenticação SAML ser desativada.

## Passos

1. Inicie sessão na consola de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

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

3. Digite **y** e pressione Enter e o Unified Manager será reiniciado.

## Resultados

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.

## Depois de terminar

Se necessário, acesse seu IDP e exclua o URL e os metadados do servidor do Unified Manager.

## **Informações sobre direitos autorais**

Copyright © 2024 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 DESTES DOCUMENTOS. 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 SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO 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 DESTES SOFTWARES, 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.