Usar SAML

SANtricity software

NetApp
March 17, 2026

Índice

Usar SAML

Configurar SAML no SANtricity Unified Manager

Para configurar autenticação para o Gerenciamento de Acesso, você pode usar os recursos da Security Assertion Markup Language (SAML) incorporados no array de storage. Essa configuração estabelece uma conexão entre um Identity Provider e o Storage Provider.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- Você deve saber o endereço IP ou nome de domínio do controlador no array de storage.
- Um administrador de IdP configurou um sistema IdP.
- Um administrador do IdP garantiu que o IdP suporta a capacidade de retornar um Name ID na autenticação.
- Um administrador assegurou que o servidor IdP e o relógio do controlador estão sincronizados (seja por meio de um servidor NTP ou ajustando as configurações do relógio do controlador).
- Um arquivo de metadados do IdP é baixado do sistema IdP e fica disponível no sistema local usado para acessar Unified Manager.

Sobre esta tarefa

Um Provedor de Identidade (IdP) é um sistema externo usado para solicitar credenciais de um usuário e determinar se esse usuário foi autenticado com sucesso. O IdP pode ser configurado para fornecer autenticação multifator e usar qualquer banco de dados de usuários, como Active Directory. Sua equipe de segurança é responsável por manter o IdP. Um Provedor de Serviços (SP) é um sistema que controla a autenticação e o acesso do usuário. Quando o Access Management é configurado com SAML, o array de storage atua como o Service Provider para solicitar autenticação do Identity Provider. Para estabelecer uma conexão entre o IdP e o array de storage, você compartilha arquivos de metadados entre essas duas entidades. Em seguida, você mapeia as entidades de usuário do IdP para as funções do array de storage. E, finalmente, você testa a conexão e os logins SSO antes de habilitar o SAML.

SAML e Serviços de Diretório. Se você habilitar SAML quando Serviços de Diretório estiver configurado como o método de autenticação, SAML substituirá Serviços de Diretório no Unified Manager. Se você desabilitar SAML depois, a configuração de Serviços de Diretório retornará à configuração anterior.

Edição e Desativação. Depois de ativar o SAML, você *não* pode desativá-lo pela interface de usuário, nem editar as configurações do IdP. Se precisar desativar ou editar a configuração do SAML, entre em contato com o Suporte Técnico para obter assistência.

Configurar a autenticação SAML é um procedimento que envolve várias etapas.

Etapa 1: Carregar o arquivo de metadados do IdP

Para fornecer ao array de storage as informações de conexão do IdP, você importa os metadados do IdP no Unified Manager. O sistema IdP precisa desses metadados para redirecionar as solicitações de autenticação para o URL correto e para validar as respostas recebidas.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **SAML**.

   A página exibe uma visão geral das etapas de configuração.

3. Clique no link **Import Identity Provider (IdP) file**.

   A caixa de diálogo Import Identity Provider File é aberta.

4. Clique em **Procurar** para selecionar e carregar o arquivo de metadados do IdP que você copiou para o seu sistema local.

   Após selecionar o arquivo, o IdP Entity ID é exibido.

5. Clique em **Importar**.

Etapa 2: exportar arquivos do provedor de serviços

Para estabelecer uma relação de confiança entre o IdP e o array de storage, você importa os metadados do Service Provider para o IdP. O IdP precisa desses metadados para estabelecer uma relação de confiança com o controlador e para processar solicitações de autorização. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP, para que o IdP possa se comunicar com os Service Providers.

Passos

1. Clique no link **Export Service Provider files**.

   A caixa de diálogo Export Service Provider Files é aberta.

2. Insira o endereço IP do controlador ou o nome DNS no campo **Controlador A** e clique em **Exportar** para salvar o arquivo de metadados em seu sistema local.

   Após clicar em **Export**, os metadados do Service Provider são baixados para o seu sistema local. Anote onde o arquivo foi armazenado.

3. No sistema local, localize o arquivo de metadados do provedor de serviços formatado em XML que você exportou.
4. A partir do servidor IdP, importe o arquivo de metadados do Service Provider para estabelecer a relação de confiança. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador a partir do arquivo.

Etapa 3: mapear funções

Para conceder autorização e acesso ao Unified Manager, você deve mapear os atributos de usuário e as associações de grupo do IdP para as funções predefinidas do array de storage.

Antes de começar

- Um administrador do IdP configurou os atributos do usuário e a associação a grupos no sistema IdP.
- O arquivo de metadados do IdP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado no sistema IdP para a relação de confiança.

Passos

1. Clique no link para **mapeamento de funções do Unified Manager**.

   A caixa de diálogo Mapeamento de Funções é aberta.

2. Atribua atributos de usuário e grupos do IdP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Atributo do usuário
Especifique o atributo (por exemplo, "member of") para o grupo SAML a ser mapeado.	Valor do atributo
Especifique o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular: \.[]{}()<>*+-=!?^$	
Funções	Clique no campo e selecione uma das funções do array de storage a ser mapeada para o atributo. Você deve selecionar individualmente cada função que deseja incluir. A função Monitor é necessária em combinação com as outras funções para fazer login no Unified Manager. A função Security Admin também é necessária para pelo menos um grupo. As funções mapeadas incluem as seguintes permissões: • **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e conjuntos de discos), mas sem acesso à configuração de segurança. • **Administrador de segurança** — Acesso à configuração de segurança no Gerenciamento de Acesso, gerenciamento de certificados, gerenciamento do log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (SYMbol). • **Administrador de suporte** — Acesso a todos os recursos de hardware no array de storage, dados de falhas, eventos MEL e atualizações de firmware do controlador. Sem acesso a objetos de armazenamento ou à configuração de segurança. • **Monitor** — Acesso somente leitura a todos os objetos de storage, mas sem acesso à configuração de segurança.

A função de Monitor é obrigatória para todos os usuários, incluindo o administrador. Unified Manager não funcionará corretamente para nenhum usuário sem a função de Monitor presente.

3. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.

Os mapeamentos de funções podem ser modificados após o SAML ser ativado.

4. Quando terminar com os mapeamentos, clique em **Salvar**.

Etapa 4: teste o login SSO

Para garantir que o sistema IdP e o array de storage possam se comunicar, você pode, opcionalmente, testar um login SSO. Esse teste também é realizado durante a etapa final para habilitar o SAML.

Antes de começar

- O arquivo de metadados do IdP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado no sistema IdP para a relação de confiança.

Passos

1. Selecione o link **Test SSO Login**.

   Uma caixa de diálogo é aberta para inserir as credenciais de SSO.

2. Insira as credenciais de login de um usuário com permissões de Security Admin e de Monitor.

   Uma caixa de diálogo é aberta enquanto o sistema testa o login.

3. Procure uma mensagem de Teste bem-sucedido. Se o teste for concluído com sucesso, vá para a próxima etapa para habilitar o SAML.

   Se o teste não for concluído com êxito, uma mensagem de erro será exibida com mais informações. Certifique-se de que:

   - O usuário pertence a um grupo com permissões de Security Admin e Monitor.
   - Os metadados que você carregou para o servidor IdP estão corretos.
   - O endereço do controlador nos arquivos de metadados do SP está correto.

Etapa 5: habilitar SAML

O último passo é concluir a configuração SAML para autenticação de usuário. Durante esse processo, o sistema também solicita que você teste um login SSO. O processo de teste de login SSO é descrito na etapa anterior.

Antes de começar

- O arquivo de metadados do IdP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado no sistema IdP para a relação de confiança.

- Pelo menos um mapeamento de função de Monitor e um de Security Admin está configurado.

> **Edição e Desativação.** Depois de ativar o SAML, você *não* pode desativá-lo pela interface de usuário, nem editar as configurações do IdP. Se precisar desativar ou editar a configuração do SAML, entre em contato com o Suporte Técnico para obter assistência.

Passos

1. Na aba **SAML**, selecione o link **Enable SAML**.

   A caixa de diálogo Confirm Enable SAML é aberta.

2. Digite `enable`, e clique em **Ativar**.
3. Insira as credenciais do usuário para um teste de login SSO.

Resultados

Após o sistema habilitar SAML, ele encerra todas as sessões ativas e começa a autenticar os usuários por meio de SAML.

Alterar mapeamentos de funções SAML no SANtricity Unified Manager

Se você já configurou o SAML para gerenciamento de acesso, pode alterar os mapeamentos de funções entre os grupos do IdP e as funções predefinidas do array de storage.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- Um administrador do IdP configurou os atributos do usuário e a associação a grupos no sistema IdP.
- SAML está configurado e ativado.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **SAML**.
3. Selecione **Role Mapping**.

   A caixa de diálogo Mapeamento de Funções é aberta.

4. Atribua atributos de usuário e grupos do IdP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

> Tenha cuidado para não remover suas permissões enquanto o SAML estiver ativado, ou você perderá o acesso ao Unified Manager.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Atributo do usuário
Especifique o atributo (por exemplo, "member of") para o grupo SAML a ser mapeado.	Valor do atributo
Especifique o valor do atributo para o grupo a ser mapeado.	Funções

A função de Monitor é obrigatória para todos os usuários, incluindo o administrador. Unified Manager não funcionará corretamente para nenhum usuário sem a função de Monitor presente.

5. Opcionalmente, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
6. Clique em **Salvar**.

Resultados

Após concluir esta tarefa, todas as sessões de usuário ativas são encerradas. Apenas a sua sessão de usuário atual é mantida.

Exportar arquivos do Service Provider SAML no SANtricity Unified Manager

Caso necessário, você pode exportar os metadados do Service Provider para o array de storage e reimportar o arquivo no sistema do Identity Provider (IdP).

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- SAML está configurado e ativado.

Sobre esta tarefa

Nesta tarefa, você exporta metadados do controlador. O IdP precisa desses metadados para estabelecer uma relação de confiança com o controlador e para processar solicitações de autenticação. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP que o IdP pode usar para enviar solicitações.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **SAML**.

3. Selecione **Export**.

   A caixa de diálogo Export Service Provider Files é aberta.

4. Clique em **Exportar** para salvar o arquivo de metadados em seu sistema local.

   O campo de nome de domínio é somente leitura.

   Anote onde o arquivo está armazenado.

5. No sistema local, localize o arquivo de metadados do provedor de serviços formatado em XML que você exportou.
6. No servidor IdP, importe o arquivo de metadados do Service Provider. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador.
7. Clique em **Close**.

Informações sobre direitos autorais

Informações sobre marcas comerciais