Configurar a Autenticação Externa do SSO da ID do Microsoft Entra para DMP

Contents

Introdução

Este documento descreve como configurar o logon único do Microsoft Entra ID para autenticação no portal do Cisco Domain Protection.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

- Proteção de domínio da Cisco
- ID do Microsoft Entra
- Certificados SSL X.509 com assinatura automática ou CA (opcional) no formato PEM

Componentes Utilizados

- Acesso de administrador do Cisco Domain Protection
- Acesso do administrador do centro de administração do Microsoft Entra ID

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

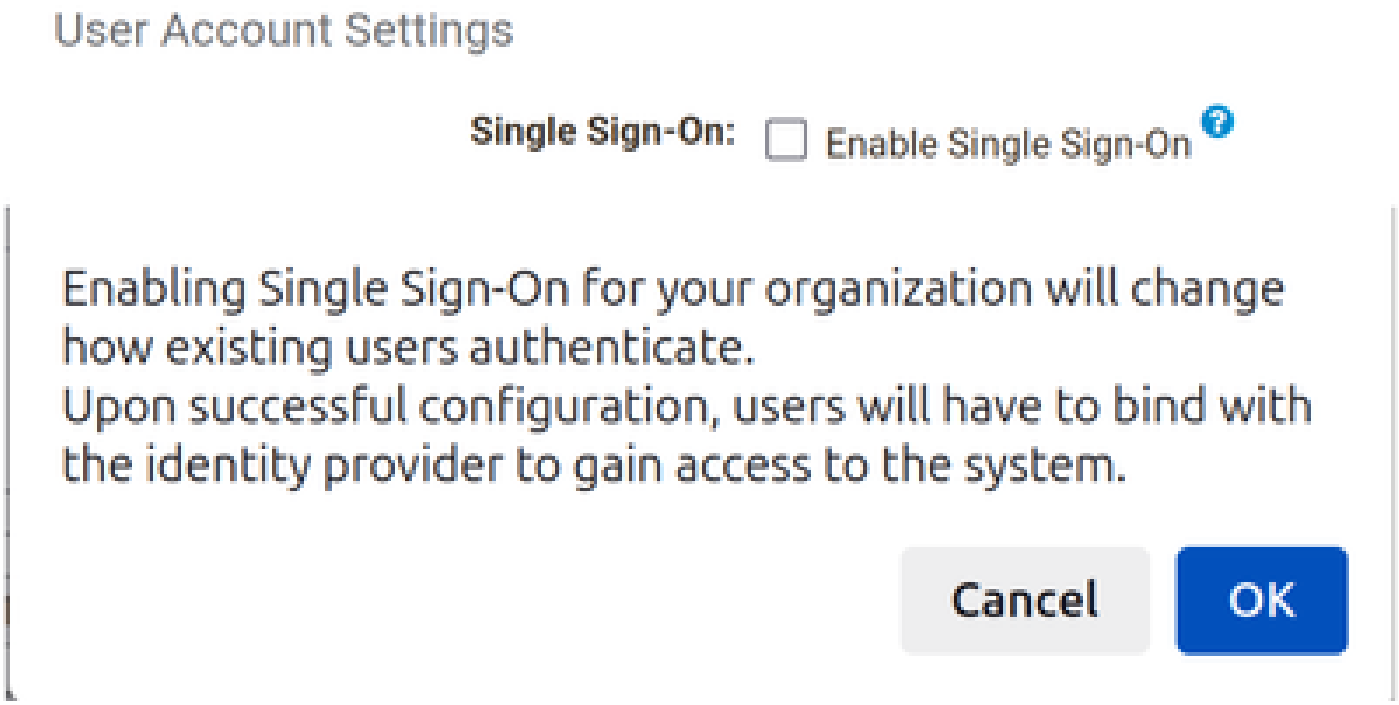
- O Cisco Domain Protection permite o login do SSO para usuários finais através do protocolo SAML 2.0.
- O Microsoft Entra SSO permite e controla o acesso a aplicativos de software como serviço (SaaS), aplicativos em nuvem ou aplicativos locais de qualquer lugar com logon único.
- O Cisco Domain Protection pode ser definido como um aplicativo de identidade gerenciada conectado ao Microsoft Entra com métodos de autenticação que incluem autenticação multifator, pois a autenticação somente por senha não é segura nem recomendada.
- O SAML é um formato de dados padrão aberto baseado em XML que permite que os administradores acessem um conjunto definido de aplicativos perfeitamente após o login em um desses aplicativos.
- Para saber mais sobre SAML, consulte: O que é SAML?

Configurar

Proteção de domínio da Cisco (Parte 1)

1. Faça login no portal de administração do Cisco Domain Protection e navegue até Admin > Organização. Clique no botão Editar detalhes da organização, como mostrado na imagem:

2. Navegue até a seção Configurações de Conta de Usuário e clique na caixa de seleção Ativar Signon Único. Uma mensagem é exibida conforme mostrado na imagem:

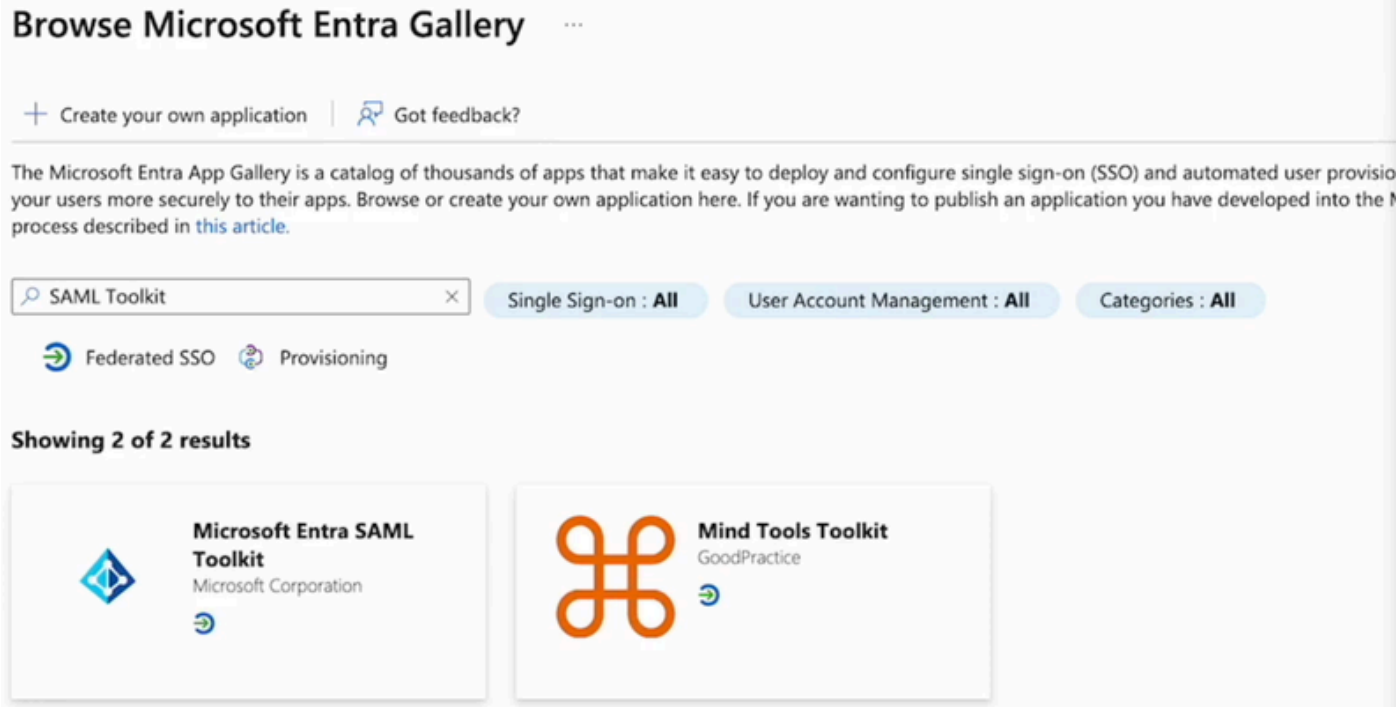


3. Clique no botão OK e copie os parâmetros do ID da entidade e do URL do Serviço de Consumidor de Asserção (ACS). Esses parâmetros devem ser usados na autenticação SAML básica do Microsoft Entra ID. Retorne mais tarde para configurar os parâmetros Name Identifier Format, SAML 2.0 Endpoint e Public Certificate.

- ID da entidade: dmp.cisco.com
- URL do Serviço de Consumidor de Asserção:https://<dmp_id>.dmp.cisco.com/auth/saml/callback

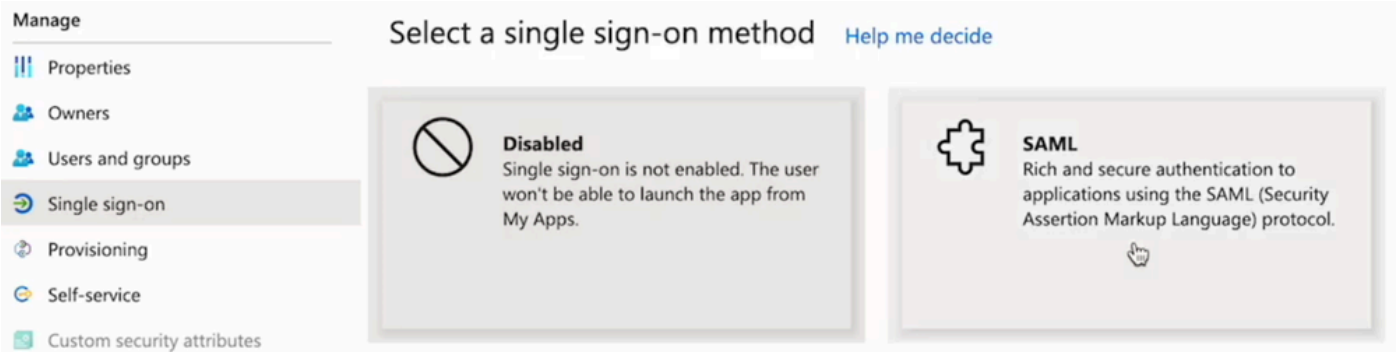
ID do Microsoft Entra

1. Navegue até o centro de administração do Microsoft Entra ID e clique no Botão Adicionar. Selecione Aplicativo Empresarial e procure por Microsoft Entra SAML Toolkit, como mostrado na imagem:



2. Nomeie-o com um valor significativo e clique em Criar. Por exemplo, Domain Protection Sign On.

3. Navegue até o painel do lado esquerdo, na seção Gerenciar. Clique em Single sign-on e selecione SAML.



4. No painel Configuração SAML básica, clique em Editar e preencha os parâmetros:

- Identificador (ID da entidade): dmp.cisco.com
- URL de Resposta (URL do Serviço de Consumidor de Asserção): https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- URL de entrada: https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- Click Save.

5. No painel Atributos e reivindicações, clique em Editar.

Em Required claim, clique na declaração Unique User Identifier (Name ID) para editá-la.

- Defina o campo Atributo de origem como user.userprincipalname. Isso pressupõe que o

valor de user.userprincipalname representa um endereço de email válido. Caso contrário, defina Source como user.primaryauthoritativeemail.

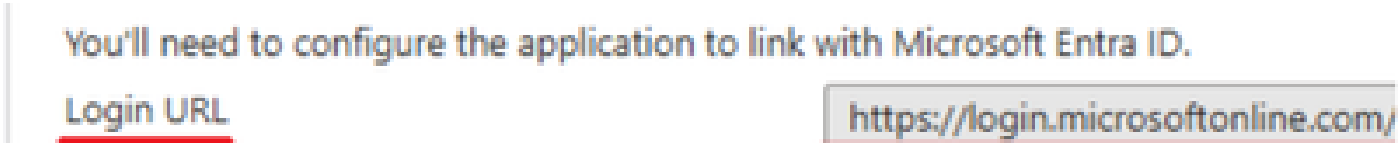
- No painel Declarações adicionais, clique em Editar e crie os mapeamentos entre as propriedades do usuário do Microsoft Entra ID e os atributos SAML.

Nome	Espaço de nomes	Atributo de Origem
endereço de e-mail	Nenhum valor	user.userprincipalname
firstName	Nenhum valor	user.givenname
sobrenome	Nenhum valor	user.surname

Certifique-se de limpar o campo Namespace para cada reivindicação, como mostrado abaixo:

6. Depois que as seções Atributos e Reivindicações forem preenchidas, a última seção Certificado de Autenticação SAML será preenchida.

- Salve o URL de login.

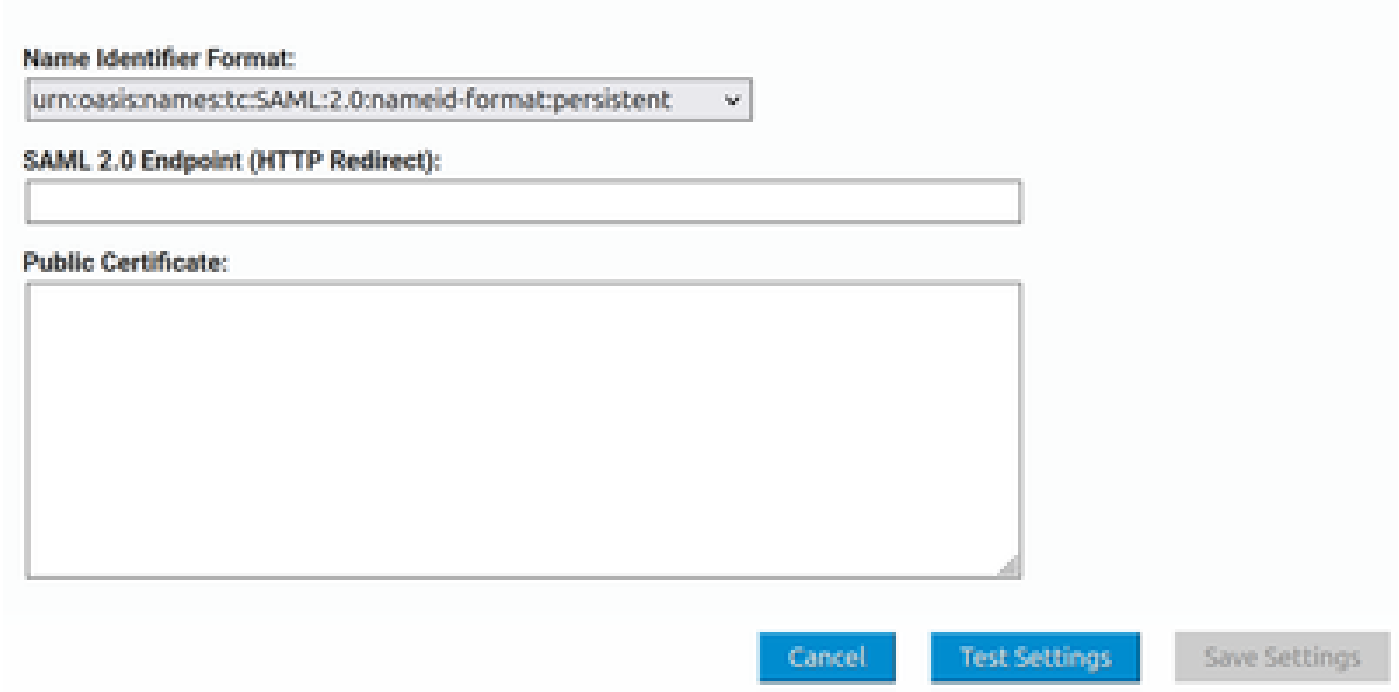


- Salve o Certificado (Base64).

Proteção de domínio da Cisco (Parte 2)

Retorne à seção Cisco Domain Protection > Enable Single Sign-On.

- Formato do Identificador de Nome: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- Ponto de Extremidade SAML 2.0 (Redirecionamento HTTP): URL de Logon fornecida pela ID do Microsoft Entra
- Certificado público: Certificado (Base64) fornecido pela ID do Microsoft Entra



Verificar

Clique em Testar Definições. Ele o redireciona para a página de login do seu Provedor de Identidade. Faça login usando suas credenciais de SSO.

Após um login bem-sucedido, você pode fechar a janela. Clique em Save Settings.

Troubleshooting

```
Error - Error parsing X509 certificate
```

- Verifique se o certificado está na Base64.

```
Error - Please enter a valid URL
```

- Verifique se a URL de Logon fornecida pela ID do Microsoft Entra está correta.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.