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

Contents

Introdução

Este documento descreve como configurar o Logon Único do Microsoft Entra ID para autenticação no Cisco Secure Email Encryption Service.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Serviço de criptografia de e-mail seguro (Envelope registrado)
- ID do Microsoft Entra
- Certificados SSL X.509 com assinatura automática ou CA (opcional) no formato PEM

Componentes Utilizados

- Acesso do administrador do Secure Email Encryption Service (Registered Envelope)
- 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.

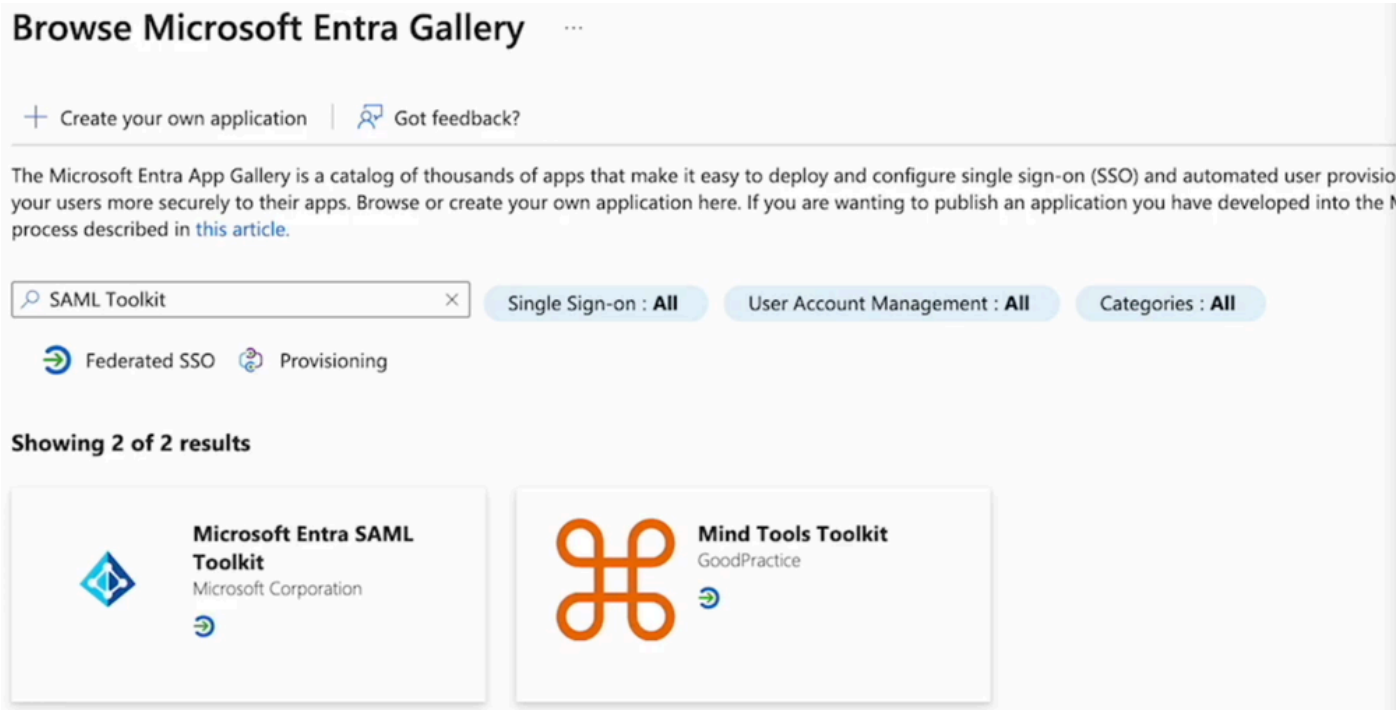
Informações de Apoio

- O Envelope registrado habilita o login de SSO para usuários finais que usam SAML.
- 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 Envelope registrado pode ser definido como um aplicativo de identidade gerenciado 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

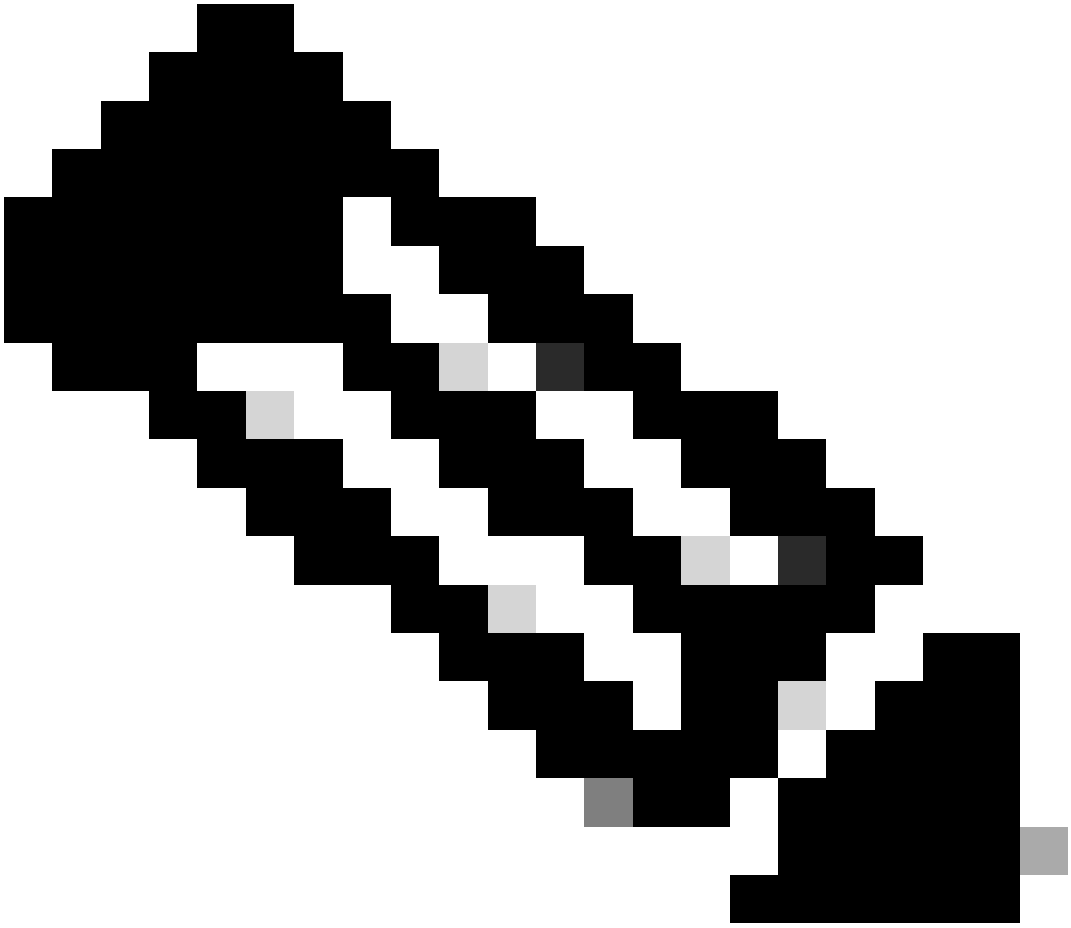
ID do Microsoft Entra

1. Navegue até o centro de administração do Microsoft Entra ID e clique no botão Adicionar. Selecione Enterprise Application e procure Microsoft Entra SAML Toolkit, como mostrado na imagem:



Navegar pela Galeria do Microsoft Entra

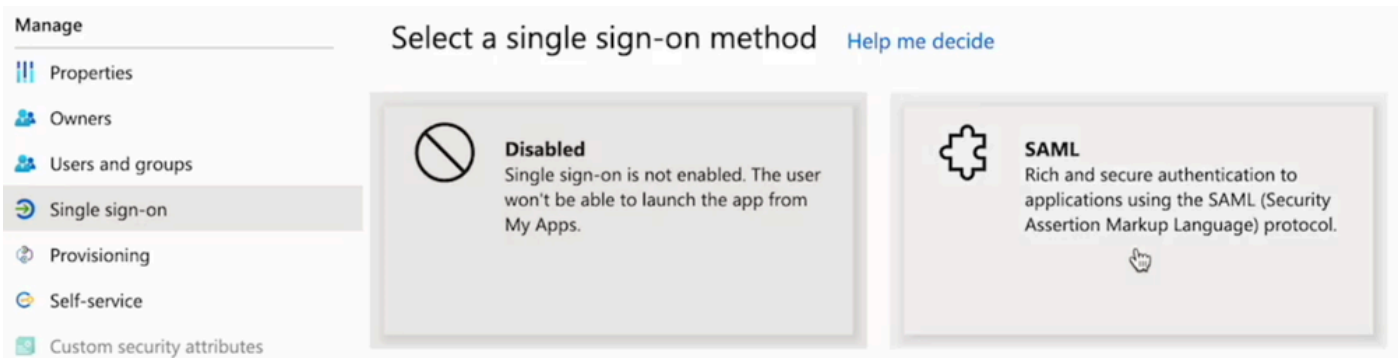
2. Nomeie-o com um valor significativo e clique em Criar. Por exemplo, CRES Single Sign On.



Note: Para permitir que todos os usuários se conectem ao portal do CRES, você precisa desativar manualmente a Atribuição obrigatória em Propriedades do logon do CRES (kit de ferramentas SAML) e, para Atribuição obrigatória, selecione Não.

---

3. Navegue até o painel do lado esquerdo, na seção Gerenciar, clique em Logon único e selecione SAML.



4. No painel Configuração SAML básica, clique em Editar e preencha os atributos da seguinte

maneira:

- Identificador (ID da entidade): https://res.cisco.com/
- URL de resposta (URL de serviço do consumidor de asserção): https://res.cisco.com/websafe/ssourl
- URL de entrada: https://res.cisco.com/websafe/ssourl
- 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.

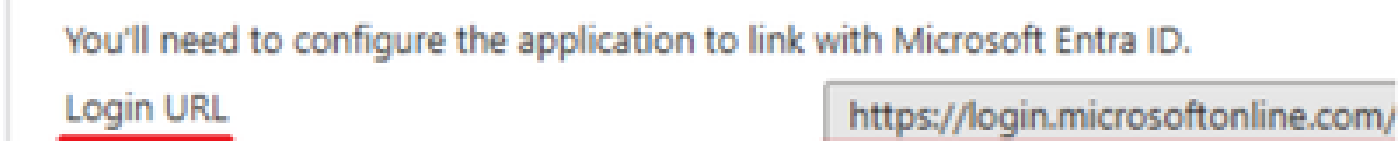
- Defina o campo Source attribute como user.userprincipalname. Isso pressupõe que o valor de user.userprincipalname representa um endereço de email válido. Caso contrário, defina Source como user.primaryauthoritativeemail.
- No painel Declarações adicionais, clique em Editar e crie os mapeamentos entre 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 os próximos valores conforme necessário no portal do CRES:

- Salve o URL de login.



- Selecione o link Download do certificado (Base64).

Serviço de criptografia de e-mail da Cisco

1. Faça login no portal da organização do Serviço de Criptografia Segura de E-mail como administrador.

2. Na guia Contas, selecione a guia Gerenciar Contas e clique em seu Número da Conta.

3. Na guia Detalhes, role até Método de autenticação e selecione SAML 2.0.

4.- Preencha os atributos da seguinte maneira:

- Nome do Atributo de Email Alternativo SSO: endereço de e-mail
- ID da entidade do provedor de serviços SSO*: https://res.cisco.com/
- URL do SSO para atendimento ao cliente*: Este link é fornecido pela Entra ID, em
- URL de Logoff do SSO: deixe em branco

5.- Clique em Ativar SAML.

Verificar

Uma nova janela é exibida confirmando que, após um login bem-sucedido, a autenticação SAML foi ativada. Clique em Próximo. Você será redirecionado para a página de login do seu Provedor de Identidade. Efetue login usando suas credenciais de SSO. Após um login bem-sucedido, você pode fechar a janela. Click Save.

Troubleshooting

Se a janela não o redirecionou para a página de logon do seu Provedor de identidade, um rastreamento de retorno será retornado, fornecendo o erro. Examine os Atributos e Declarações, verifique se ele está configurado com o mesmo nome da seção Método de Autenticação CRES. O endereço de email do usuário usado no logon SAML deve corresponder ao endereço de email no CRES. Não use aliases.

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.