Configurar a autenticação externa de SSO SAML para administração de ESA e SMA

Contents

Introdução

Este documento descreve como configurar a autenticação externa SSO SAML 2.0 para a administração do sistema ESA e SMA.

Ambiente

- Produtos: Dispositivo de segurança de e-mail (ESA), Dispositivo de gerenciamento de segurança (SMA)
- Aplicável a: Administração de sistema ESA e SMA
- Comportamento do cluster: Os perfis do provedor de serviços (SP) e do IdP são configurados no nível da máquina; o mapeamento de autenticação externa é configurado no nível do cluster.

Pré-requisitos

- Acesso administrativo à interface da Web do ESA/SMA
- Certificado X.509 e chave privada disponíveis no formato PKCS #12 (PFX) ou PEM (autoassinado ou CA-assinado)
- Acesso a um aplicativo de terceiros do Identity Provider (IdP) e seus metadados SAML/URL do SSO

Lista de verificação de pré-configuração

- Verificar o nome de host/FQDN da interface de gerenciamento que os administradores usam para acessar o dispositivo; confirme se a URL do Serviço de Consumidor de Asserção (ACS) corresponde a esse nome de host.
- Se o equipamento estiver em um cluster, planeje configurar o SAML no nível do computador para cada membro antes de habilitar a autenticação externa SAML.
- Determine se o IdP requer um aplicativo ou território separado por dispositivo.
- Confirme se os certificados e as chaves necessários estão disponíveis.
- Confirme se o IdP envia o atributo de grupo ou função necessário para o mapeamento de funções ESA/SMA.

Caution: Este documento não se aplica a EUQ (End User Quarantine, quarentena de usuário final) SAML SSO.

Informações de Apoio

- O Cisco TAC não oferece suporte técnico para a configuração de IdP de terceiros. Exemplos de referências de configuração são fornecidos para IdPs comuns.

IdPs SSO SAML

- O Gateway de Acesso Duo (DAG) adiciona autenticação de dois fatores, completa com serviços de nuvem populares usando a federação SAML 2.0.
- Serviços de Federação do Ative Diretory (ADFS) - testados com ADFS 2,3,4, Azure Ative Diretory (Azure AD), SecureAUTH e PingFederate
- Autenticação adicional de dois fatores pode ser usada se o IdP oferecer suporte a ela dentro da estrutura SAML 2.0 Single Sign-On.
- O Okta suporta a autenticação com um IdP que suporta o serviço.

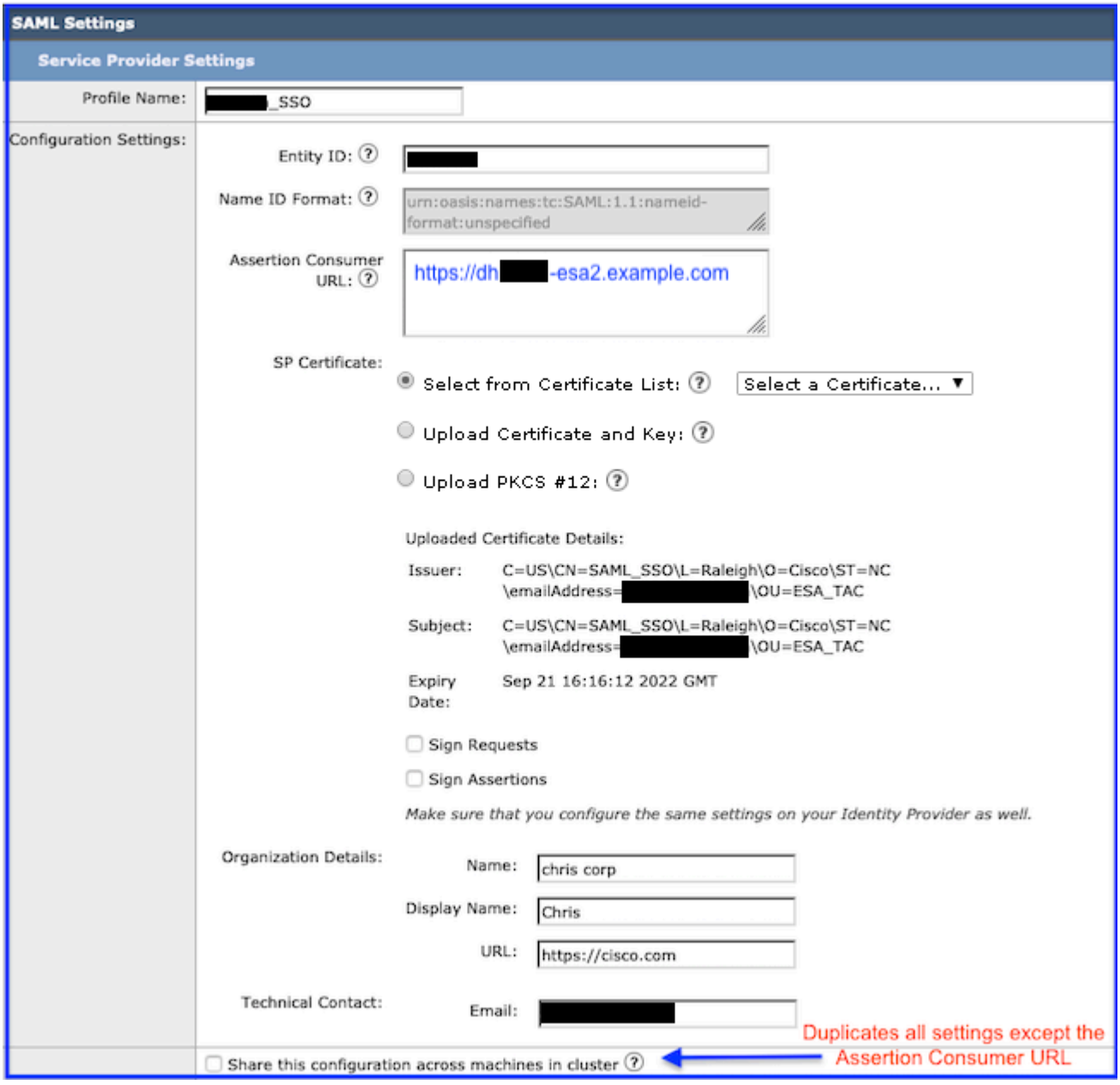
Configurar o ESA/SMA como um provedor de serviços

Navegue até Administração do sistema > SAML > (Nível da máquina) > Adicionar provedor de serviços.

Note: Os ESAs em um cluster exigem configuração em nível de máquina para todos os membros do cluster antes que o SAML possa ser habilitado.

- Se a opção na parte inferior da página, Compartilhar esta configuração entre máquinas no cluster, estiver selecionada, estas condições se aplicam:
    - Todos os campos são replicados para os membros do cluster, exceto o URL do Consumidor de Asserção.
    - A URL do consumidor de asserção preenche automaticamente o nome de host da interface de gerenciamento como o ACS.
    - Os ambientes que usam um nome de host alternativo para acessar o host exigem configuração manual para cada host, por exemplo, aplicativos hospedados no CES.
    - Nome do perfil: Nome usado para rotular a instância SP na interface ESA ou SMA.
    - ID da entidade: Nome usado para a instância do SP como o IdP a vê. Esse nome é o rótulo usado pelo IdP para representar o SP. Pode ser qualquer nome, por exemplo, ESA_SP ou ESA_SSO.
    - Formato de ID do Nome: Campo não configurável.
    - URL do Consumidor de Asserção ou Serviço do Consumidor de Asserção (ACS): URL usada pelo IdP para se comunicar com este host ESA/SMA.
    - Certificado SP:
        - Formato: Certificados públicos/privados X.509 em formato PFX/PKCS12 ou PEM.
        - Opção 1: Selecionar na Lista de Certificados: Selecione entre os certificados já criados no ESA em Rede > Certificados.
        - Opção 2: Carregar certificado e chave: Carregue um certificado e uma chave formatados em PEM.
        - Opção 3: Carregar PKCS 12: Carregue um arquivo PKCS #12.
        - Opcional: Crie um certificado autoassinado no ESA/SMA para Logon Único do SAML.
        - Se necessário, proteja a chave privada com senha.

Note: Se os certificados formatados em PEM forem usados, preserve cada certificado e chave privada em arquivos separados.



Página Configuração do provedor de serviços

Página Configuração do provedor de serviços

- Assinar solicitações: Opção para assinar a comunicação SAML ESA/SMA enviada ao IdP.
- Assinar Asserções: Opção para exigir que o IdP assine asserções enviadas ao ESA/SMA.
- Detalhes da Organização: Pode ser preenchido com os dados apropriados da empresa.
- Enviar e confirmar alterações para preservar as configurações.
- Faça download dos metadados SP da página SAML Configuration.

Configurar o provedor de identidade (IdP) para trabalhar com os dispositivos ESA/SMA

Note: Alguns IdPs exigem aplicativos ou territórios separados para cada ESA. (exemplo:

DUO)

Esses links fornecem configurações de exemplo para vários IdPs no momento da publicação. O Cisco TAC não oferece suporte técnico para produtos de terceiros. Esses exemplos são fornecidos como referências.

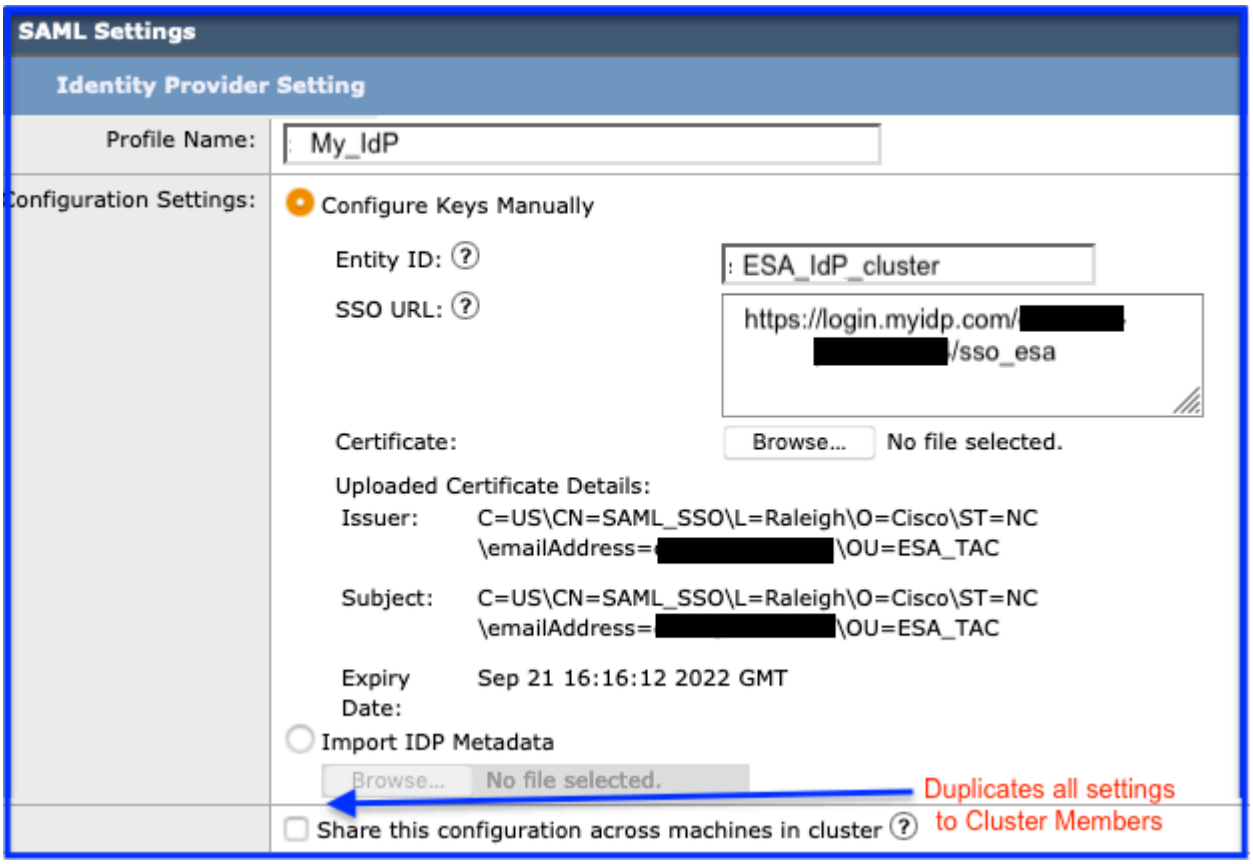
Definir configurações de IDP no ESA/SMA

1. Navegue até Administração do Sistema > SAML.

2. Selecione Adicionar Provedor de Identidade.

- Duas opções estão disponíveis:
- Importar Metadados IdP
- Configurar chaves manualmente:
    - ID da entidade: Pode ser qualquer valor usado para identificar o IdP
    - URL SSO: URL para a qual o SP envia solicitações de autenticação SAML
    - Carregar a chave privada e o certificado público em arquivos separados

3. Compartilhe essa configuração entre máquinas no cluster para replicar a configuração em todos os ESAs no cluster:

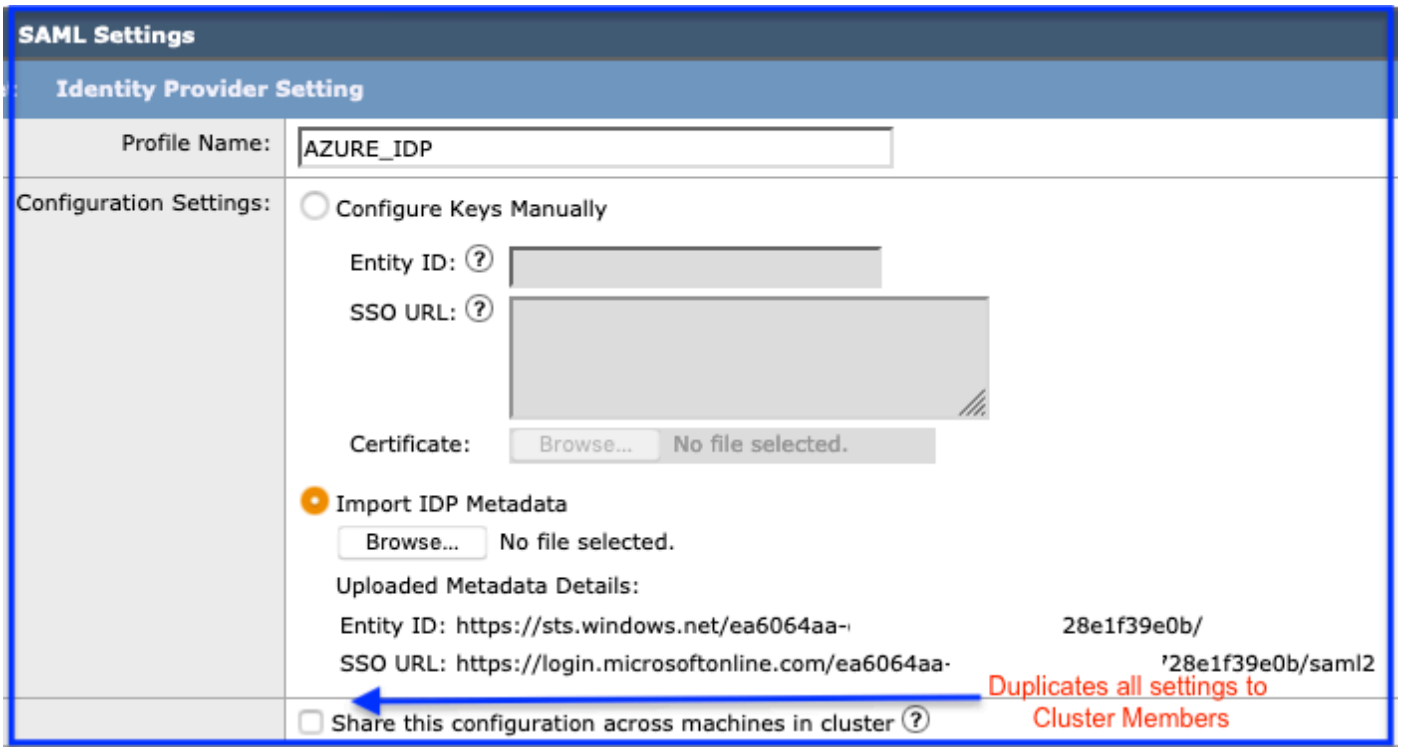


Inserir manualmente o conteúdo do IdP

Inserir manualmente o conteúdo do IdP

4. Carregar Metadados do IdP

- Selecione Importar Metadados IdP.
- Navegue até o arquivo de metadados salvo no IdP e salve a configuração.
- A opção para Compartilhar essa configuração entre máquinas em um cluster estará disponível se for aplicável à implantação.



Carregar Metadados de Idp

Carregar Metadados de Idp

Habilitar autenticação externa usando SAML no ESA/SMA

Semelhante à autenticação externa LDAP, o Logon único SAML requer mapeamento para atribuir grupos a funções administrativas.

1. Navegue até Administração do Sistema > Usuários (Nível de Cluster) > Autenticação Externa > Ativar.

2. Selecione o Tipo de Autenticação: SAML.

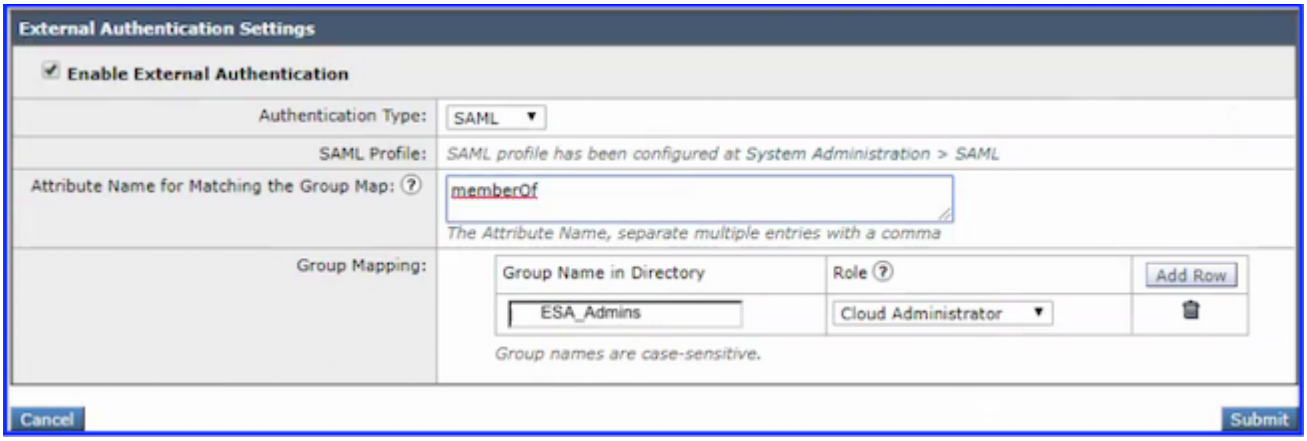
3. Nome do Atributo para Corresponder ao Mapa de Nomes (Opcional): Insira o nome do atributo a ser pesquisado no mapeamento do grupo.

Note: O nome do atributo depende dos atributos configurados para que o Provedor de Identidade retransmita na resposta SAML. O equipamento procura entradas correspondentes do nome de atributo especificado na resposta SAML em relação aos atributos configurados no campo Mapeamento de grupo. Se esse campo não estiver configurado, o equipamento pesquisará todos os atributos presentes na resposta SAML em relação ao campo Mapeamento de grupo configurado.

---

4. Informe o atributo de nome do grupo conforme definido no diretório SAML com base na função de usuário predefinida ou personalizada.

- O campo Mapeamento de grupo deve conter um atributo de grupo. O atributo Grupos Não Especificados pode ser adicionado para autenticar asserções ou respostas SAML.



Configurações de autenticação externa

Configurações de autenticação externa

5. Submeter e Confirmar Alterações.

Após a configuração bem-sucedida, um novo link será exibido na parte inferior da página de logon. A página de logon ESA/SMA exibe um link Usar logon único que redireciona os administradores para o Provedor de identidade (IdP) corporativo.

Quando selecionada, o administrador é redirecionado para a página de logon SAML corporativa.

Usar Link de Logon Único redirecionará para SAML

Troubleshooting

Use esses indicadores para identificar se o problema está relacionado à configuração do equipamento ou à configuração do IdP.

O link de redirecionamento de SSO não é exibido na página de login ("Usar login único")

Confirme se System Administration > Users > External Authentication > SAML está configurado.

Redirecionar retorna à página de login ESA/SMA com a mensagem "Single Sign-On Authentication Failed! Entre em contato com o administrador."

Erro: "Falha na Autenticação de Logon Único! Entre em contato com o administrador."

- Falha de autenticação no IdP.
    - Isso indica que a configuração está funcionando a ponto de acessar a página de autenticação de Signon Único e enviar credenciais.
    - Essa falha geralmente ocorre devido à configuração do IdP e requer verificação adicional das configurações do IdP.

Redirecionar retorna à página de login ESA/SMA com "Authorization Failure! (Falha de autorização!) Entre em contato com o administrador."

Erro: "Falha na autorização! Entre em contato com o administrador."

- A autenticação foi aprovada, mas a autorização falhou no ESA/SMA.
    - Concentre-se nas configurações em Users > External Authentication > SAML.
        - Nome do atributo, Nome do grupo e Mapeamento do grupo.

Informações Relacionadas

- Cisco Email Security Appliance - Guias do usuário
- Cisco Content Security Management Appliance - Guias do usuário
- Cisco Web Security - Guias do usuário

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.