Utilizar URL de metadados fixos do Umbrella para autenticação SAML do SWG

Contents

Introdução

Este documento descreve como utilizar a URL de metadados fixos do Umbrella para autenticação SAML do Secure Web Gateway (SWG).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Umbrella SWG.

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.

URL de Metadados Fixos

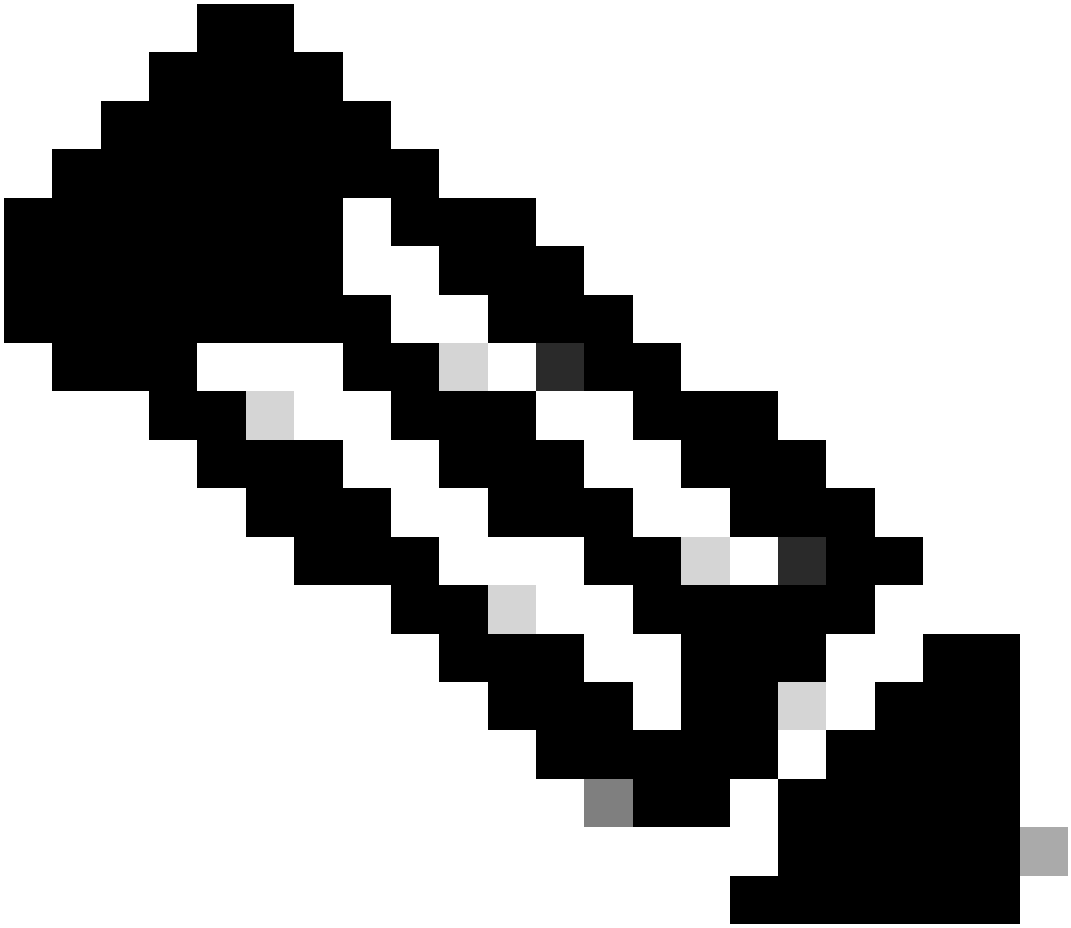
Ao utilizar a autenticação SAML para o Umbrella SWG, fornecemos duas opções para importar nossas informações de certificado para o seu Provedor de Identidade (IdP). Isso é necessário para os IdPs que verificam nosso certificado de assinatura de solicitação.

1. Configuração automática via URL de metadados fixos:

https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml

2. Importação manual do novo certificado de autenticação. Isso precisa ser feito a cada ano, à medida que o certificado é substituído.

A primeira opção agora é o método de configuração preferencial para provedores de identidade (IdP) que suportam atualizações automáticas de metadados baseadas em URL. Isso inclui IdPs populares, como Microsoft ADFS e Identidade de ping. O benefício é que o IdP importa automaticamente nosso novo certificado a cada ano sem intervenção manual.



Note: Muitos IDPs não executam validação de assinaturas de solicitação SAML e, portanto, essas etapas não são necessárias. Em caso de dúvida, entre em contato com o fornecedor do provedor de identidade para obter confirmação.

Requisitos

Requisitos para acessar o URL de metadados

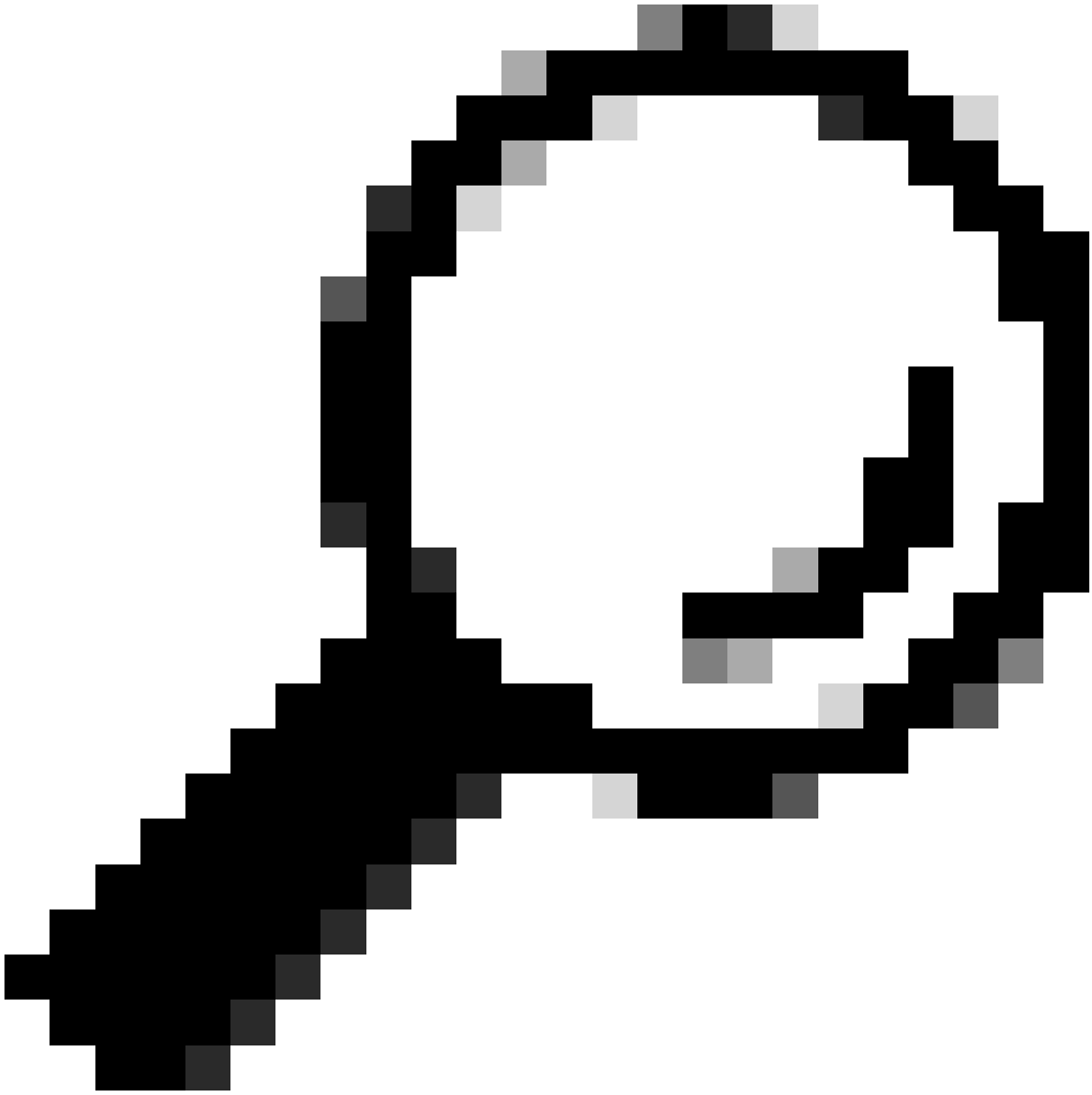
- Um IdP que oferece suporte a atualizações automáticas de metadados do provedor de

serviços da URL (como ADFS, Ping)
- Sua plataforma IdP deve ser capaz de acessar nosso URL de metadados, bem como os URLs de Autoridade de Certificação associados
- Sua plataforma IdP também deve ser capaz de acessar os URLs da Autoridade de Certificação para o próprio certificado
- Sua plataforma IdP deve suportar TLS 1.2 para se conectar ao URL de metadados com segurança. Se o aplicativo IDP utilizar o .NET framework 4.6.1 ou anterior, isso pode exigir alguma configuração adicional de acordo com a documentação da Microsoft.

Exemplo: Microsoft ADFS

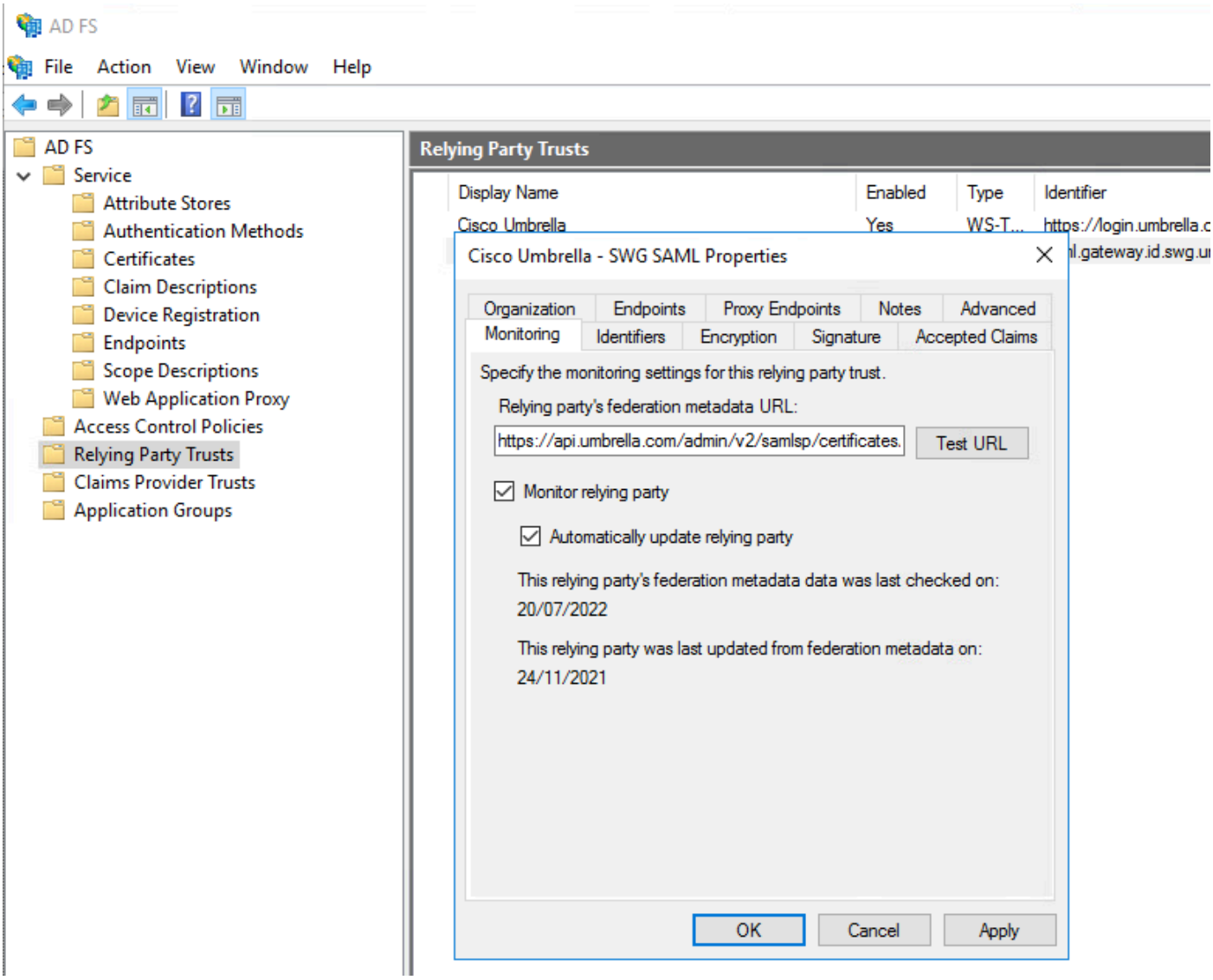
A URL de metadados fixa pode ser configurada editando a configuração da Confiança da Terceira Parte Confiável para o Umbrella:

1. Navegue até a guia Monitoramento e insira o URL de metadados.
2. Selecione Monitorar Terceira Parte Confiável e Atualizar a Terceira Parte Confiável Automaticamente.



Tip: Selecione o botão Testar URL para verificar se o ADFS entra em contato com o URL com êxito.

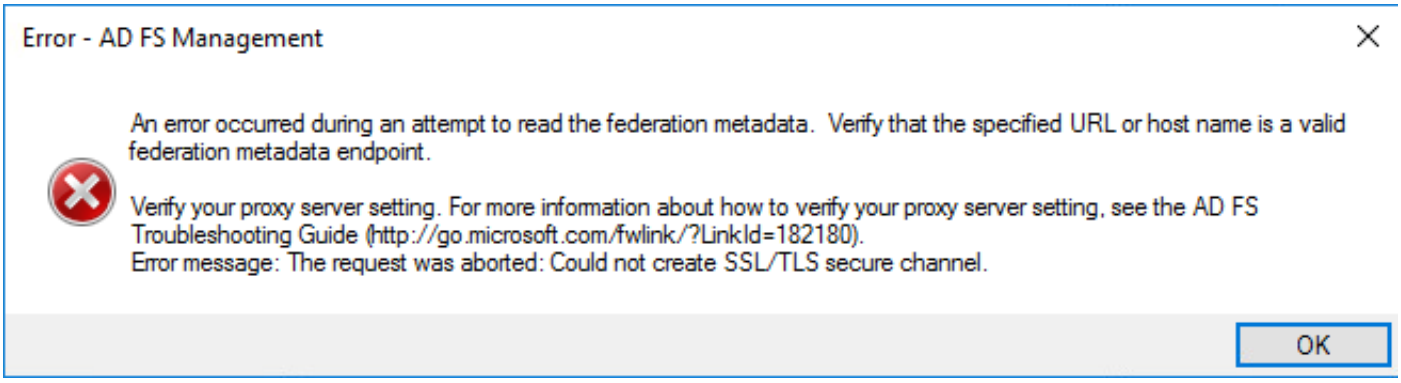
3. Selecione Aplicar.



ADFS_RelyingPartyTrust.png

Troubleshooting de Erros

Se você receber o erro, "Ocorreu um erro durante uma tentativa de ler os metadados de federação. Verifique se a URL ou o nome do host especificado é um ponto de extremidade de metadados de federação válido" ao testar a URL, isso geralmente indica que uma alteração no registro é necessária para definir sua versão do .NET Framework para usar criptografia forte e oferecer suporte ao TLS 1.2.



ADFSmetadata_TLS_error.png

Detalhes completos sobre essas alterações são publicados pela Microsoft na seção .Net Framework da documentação da Microsoft.

Geralmente, porém, isso requer a criação dessa chave e, em seguida, fechar e reabrir o console de Gerenciamento ADFS:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto" = dword:00000001
```

Limitação: Recurso EntityID Específico da Organização

Se estiver usando o recurso EntityID Específico da Org. do Umbrella SAML, você deve não usar o mecanismo de atualização de metadados baseado em URL. A ID de entidade específica da organização só se aplica se você tiver várias organizações Umbrella vinculadas ao mesmo provedor de identidade. Neste cenário, você deve adicionar manualmente o certificado a cada configuração de IDP.

Importação Manual de Certificados (Alternativa)

Se o seu IdP não suporta atualizações baseadas em URL, você deve importar manualmente o novo certificado de assinatura de solicitação Umbrella a cada ano para o seu provedor de identidade.

- O certificado é fornecido em nosso portal de Anúncios todos os anos pouco antes da data de expiração. Inscrever-se no portal para receber notificações
- Adicione o novo certificado à lista de certificados de Provedor de Serviços/Terceira Parte Confiável em seu IdP.
    - NÃO exclua nenhum certificado atual. A Umbrella continua assinando com o certificado antigo até o momento da expiração.
- Se o seu IdP não tiver a capacidade de importar um certificado de provedor de serviços/terceira parte confiável, isso é uma forte indicação de que ele não valida solicitações SAML, e nenhuma ação adicional é necessária. Entre em contato com o fornecedor do IdP para confirmar.

Se você encontrar um erro "UPN não configurado" após importar o novo certificado, isso indica que um erro foi feito. Consulte este artigo para solução de problemas: SWG SAML - erro de UPN não configurado

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.