Solucionar problemas de logon único do CCE com gerenciamento de certificado do Identity Service (IdS)

Contents

Introdução

Este documento descreve as etapas detalhadas para regenerar e trocar certificados SAML em UCCE/PCCE, garantindo processos seguros e claros.

Contribuição de Nagarajan Paramasivam, Engenheiro do TAC da Cisco.

Pré-requisitos

Requisitos

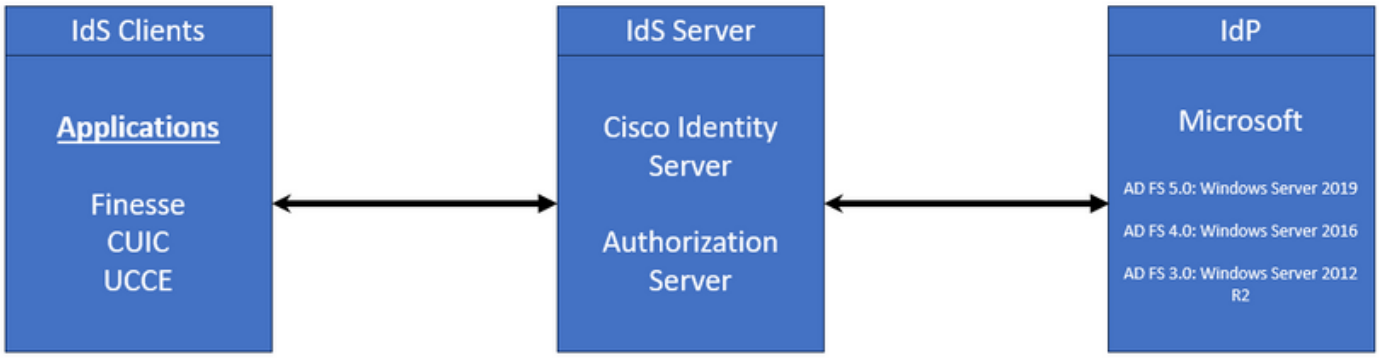
A Cisco recomenda que você conheça estes tópicos:

- Empacotamento/Unified Contact Center Enterprise (PCCE/UCCE)
- Plataforma de sistema operacional de voz (VOS)
- Gerenciamento de Certificados
- SAML (Security Assertion Markup Language, Linguagem de marcação de asserção de segurança)
- Secure Socket Layer (SSL)
- Serviços de Federação do Ative Diretory (AD FS)
- Logon Único (SSO)

Componentes Utilizados

As informações neste documento são baseadas nestes componentes:

- Cisco Identity Service (IdS da Cisco)
- Provedor de Identidade (IdP) - Microsoft Windows ADFS



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

No UCCE/PCCE, o Cisco Identity Service (Cisco IdS) fornece autorização entre o Identity Provider (IdP) e os aplicativos.

Ao configurar o Cisco IdS, você configura uma troca de metadados entre o Cisco IdS e o IdP.

Essa troca estabelece uma relação de confiança que permite que os aplicativos usem o Cisco IdS para SSO. Estabeleça a relação de confiança fazendo o download de um arquivo de metadados do Cisco IdS e carregando-o no IdP.

O certificado SAML é semelhante a um certificado SSL e, como ele, precisa ser atualizado ou alterado quando surgem certas situações. Quando você regenera ou troca o certificado SAML no servidor Cisco Identity Services (IdS), ele pode causar uma interrupção na conexão confiável com o Identity Provider (IdP). Essa interrupção pode levar a problemas em que os clientes ou usuários que dependem do Logon Único não podem obter a autorização necessária para acessar o sistema.

Este documento tem como objetivo cobrir uma ampla gama de situações comuns em que você precisa criar um novo certificado SAML no servidor Cisco IdS. Ele também explica como dar esse novo certificado ao Provedor de Identidade (IdP) para que a confiança possa ser reconstruída. Ao fazer isso, os clientes e usuários podem continuar a usar o Logon Único sem problemas. O objetivo é garantir que você tenha todas as informações necessárias para lidar com o processo de atualização de certificado sem problemas e sem confusão.

Pontos principais para lembrar:

1. O certificado SAML é gerado por padrão durante a instalação do servidor Cisco IdS com validade de 3 anos

2. O certificado SAML é um certificado autoassinado

3. O certificado SAML é um certificado SSL que reside no editor e no assinante do Cisco IDS

4. A regeneração do certificado SAML só pôde ser executada no nó do Cisco IDS Publisher

5. Os tipos disponíveis do algoritmo de hash seguro para o certificado SAML são SHA-1 e SHA-256

6. O algoritmo SHA-1 é usado no IdS 11.6 e nas versões anteriores, o algoritmo SHA-256 é usado no IdS 12.0 e em versões posteriores

7. O Provedor de Identidade (IdP) e o Serviço de Identidade (IdS) devem usar o mesmo tipo de algoritmo.

8. Só foi possível fazer download do certificado SAML do Cisco IdS a partir do nó Cisco IdS Publisher (sp-<Cisco IdS_FQDN>.xml)

9. Acesse este link para entender a configuração de logon único UCCE/PCCE. Guia de recursos do UCCE 12.6.1

Certificado SAML Expirado

O certificado SAML é gerado com 3 anos (1095 dias) de validade e é necessário renovar o

certificado SAML antes da expiração. O certificado SSL expirado é considerado inválido e quebra a cadeia de certificados entre o Cisco Identity Service (IdS) e o Identity Provider (IdP).

Solução

1. Verifique a data de expiração do certificado SAML

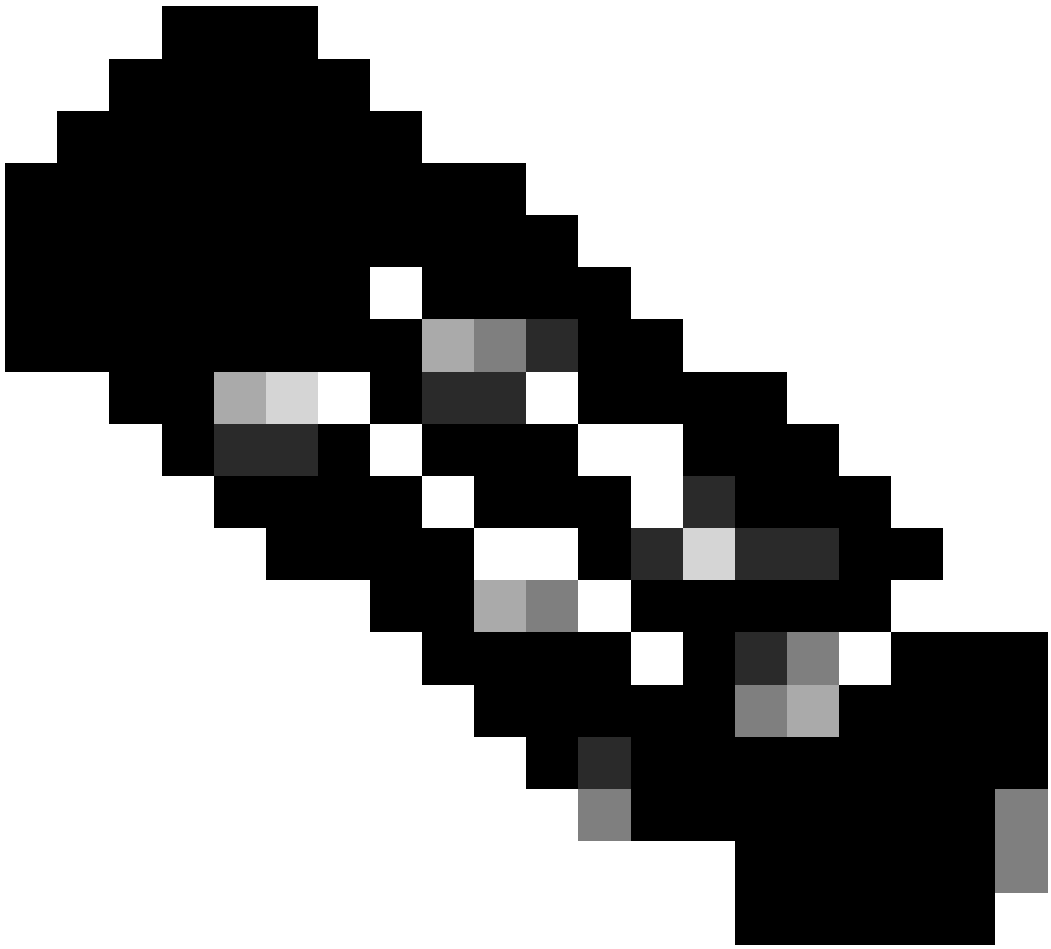
2. Regenerar o certificado SAML

3. Faça download do arquivo sp.xml

4. Recupere o certificado SAML do arquivo sp.xml

5. Substitua o certificado SAML antigo pelo novo certificado SAML no IdP

6. Consulte a seção Referência para obter etapas detalhadas



(Observação: {Como somente o certificado SAML foi alterado, a troca de metadados de

---

IdS para IdP não é necessária})

Alteração do Algoritmo de Hash Seguro no Provedor de Identidade (IdP)

Considere em um ambiente PCCE/UCCE existente com Logon único. O servidor IdP e Cisco IdS foi configurado com o algoritmo de hash seguro SHA-1. Considerando o ponto fraco no SHA-1 necessário para alterar o algoritmo hash seguro para SHA-256.

Solução

1. Altere o algoritmo de hash seguro na Terceira Parte Confiável Confiável do AD FS (SHA-1 para SHA-256)

2. Altere o algoritmo de hash seguro no editor de IdS em Chaves e Certificado (SHA-1 para SHA-256)

3. Gerar novamente o certificado SAML no Editor de IdS

4. Faça download do arquivo sp.xml

5. Recupere o certificado SAML do arquivo sp.xml

6. Substitua o certificado SAML antigo pelo novo certificado SAML no IdP

7. Consulte a seção Referência para obter etapas detalhadas

Alteração de nome de host ou endereço IP do servidor Cisco IdS - Editor co-residente de CUIC/LiveData/IdS ou Editor independente de IdS reconstruído - Assinante co-residente de CUIC/LiveData/IdS ou Assinante de IdS independente reconstruído

Essas situações ocorrem com pouca frequência e é altamente recomendável começar novamente com a configuração do SSO (Single Sign-On, login único) para garantir que a funcionalidade do SSO no ambiente de produção seja restaurada de forma rápida e eficiente. É essencial priorizar essa reconfiguração para minimizar qualquer interrupção nos serviços SSO dos quais os usuários dependem.

Solução

1. Excluir a Terceira Parte Confiável Confiável existente do AD FS
2. Carregue o certificado SSL do AD FS no servidor Cisco IdS para o qual o cliente confia
3. Faça download do arquivo sp.xml
4. Consulte a seção Referência e o Guia de Recursos para obter etapas detalhadas
5. Configure a Terceira Parte Confiável Confiável no AD FS
6. Adicionar as Regras de Reivindicação
7. Habilitar asserção SAML assinada
8. Baixar Metadados de Federação do AD FS
9. Carregue os Metadados de Federação para o servidor Cisco IdS
10. Executar SSO de Teste

Referência

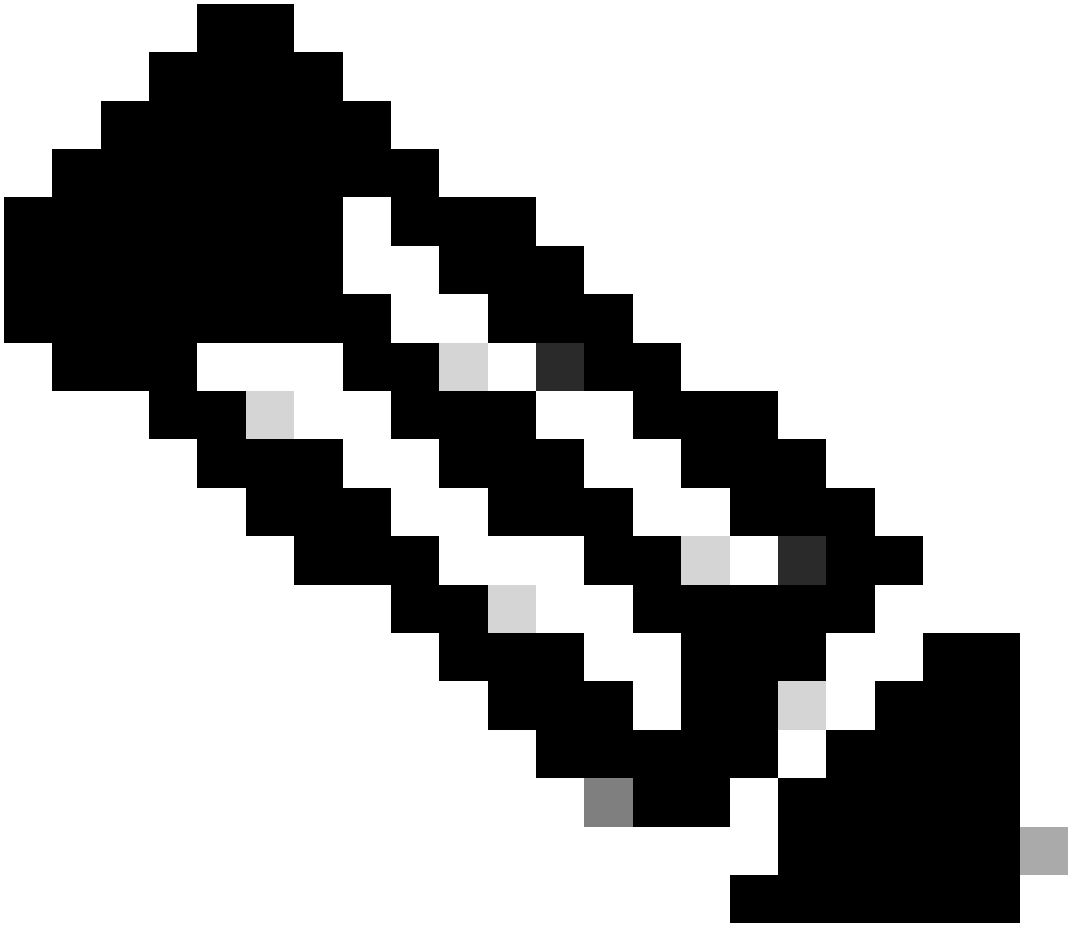
Como adicionar uma Terceira Parte Confiável Confiável no ADFS ou

Como habilitar a asserção SAML assinada

Consulte este documento para obter as etapas detalhadas: Guia de recursos do UCCE 12.6.1

Como carregar o certificado SSL do AD FS para o Cisco IdS tomcat trust

1. Baixar ou recuperar o certificado SSL do AD FS
2. Acessar a página de Administração do SO do Cisco IdS Publisher
3. Efetue login com a credencial do Administrador do SO
4. Navegue até Segurança > Gerenciamento de Certificado
5. Clique em Carregar Certificado/Cadeia de Certificados e uma janela pop-up será aberta
6. Clique no menu suspenso e selecione tomcat-trust em Certificate Purpose
7. Clique em Procurar e selecione o certificado SSL do AD FS
8. Clique em Carregar



(Observação: {Os certificados confiáveis são replicados nos nós do Assinante. Não é necessário carregar no nó Assinante.})

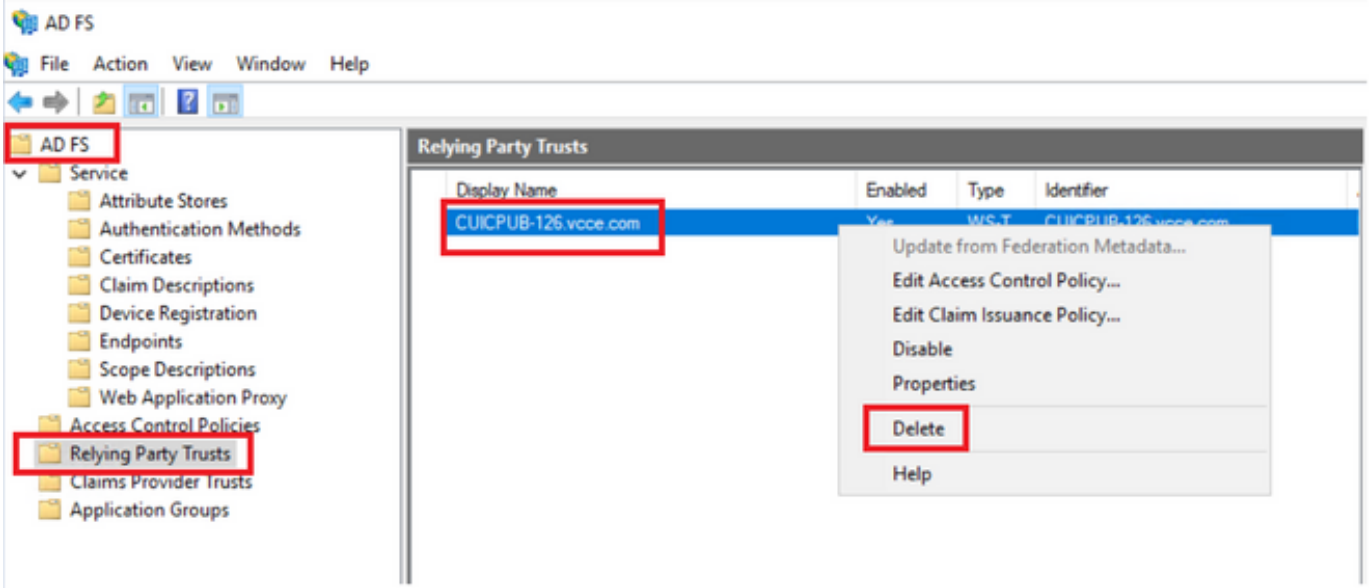
Como excluir a Terceira Parte Confiável Confiável no AD FS

1. Faça login no servidor do Provedor de Identidade (IdP) com a credencial privilegiada do administrador

2. Abra o Gerenciador de Servidores e Escolha AD FS >Ferramentas > Gerenciamento do AD FS

3. Na árvore do lado esquerdo, selecione os objetos de confiança da terceira parte confiável no AD FS

4. Clique com o botão direito no servidor Cisco IdS e selecione Excluir



Como verificar ou alterar o algoritmo de hash seguro configurado no Identity Provider (IdP)

1. Faça login no servidor do Provedor de Identidade (IdP) com a credencial privilegiada do administrador

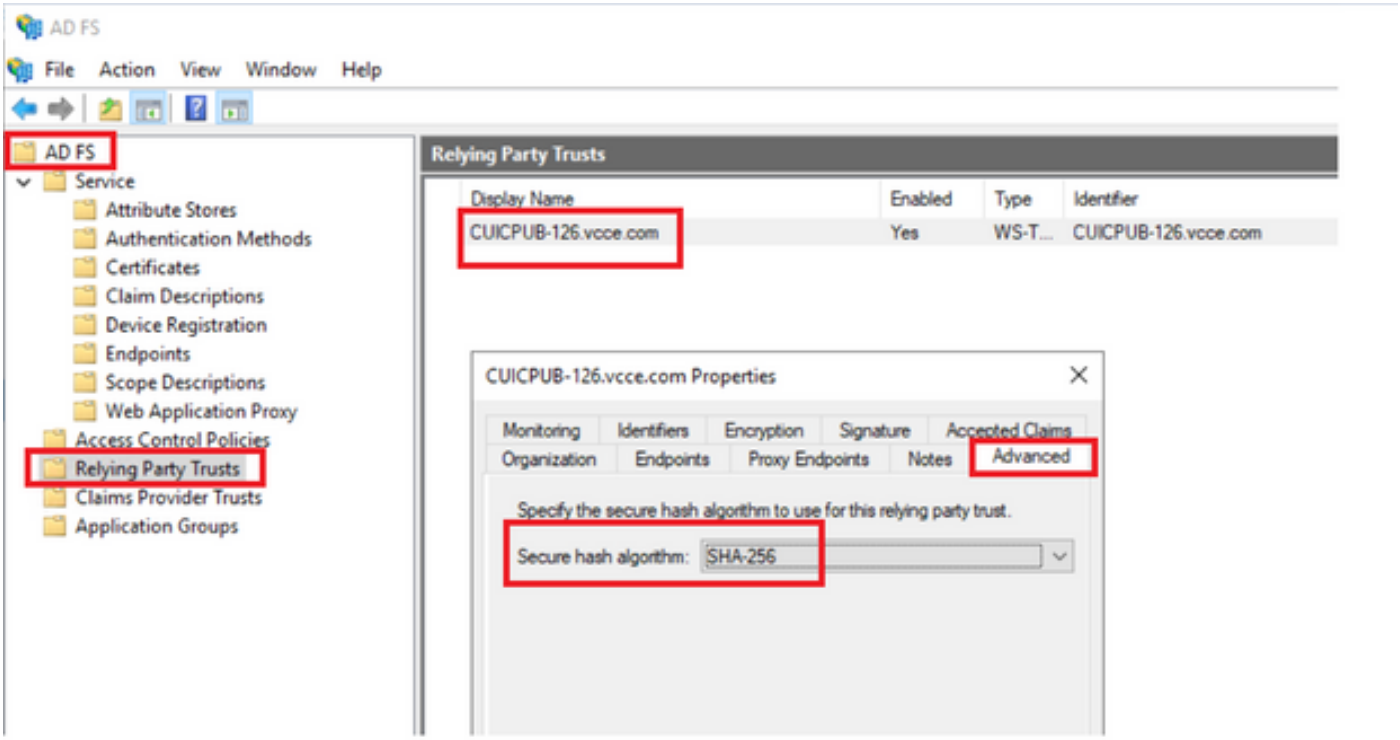
2. Abra o Gerenciador de Servidores e Escolha AD FS >Ferramentas > Gerenciamento do AD FS

3. Na árvore do lado esquerdo, selecione os objetos de confiança da terceira parte confiável no AD FS

4. Clique com o botão direito do mouse no servidor Cisco IdS e selecione Propriedades

5. Navegue até a guia Avançado

6. A opção Algoritmo Hash Seguro exibe o algoritmo hash seguro configurado no servidor AD FS.



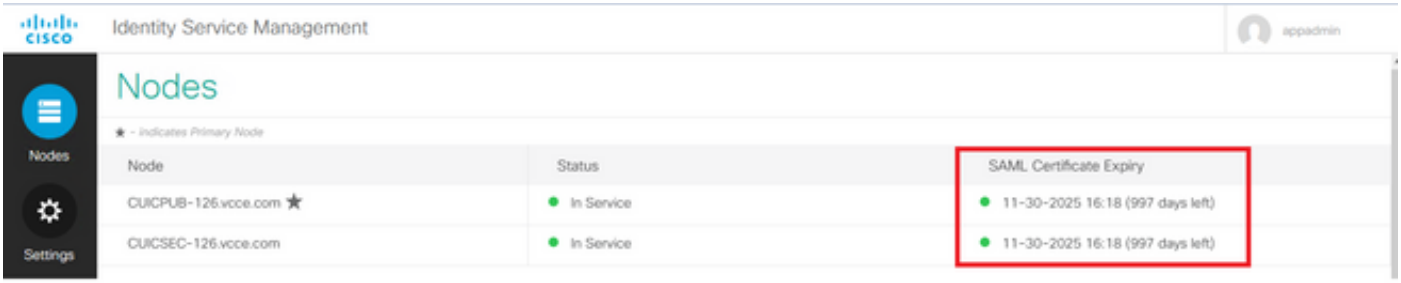
7. Clique no menu suspenso e selecione o algoritmo de hash seguro desejado.

Como verificar a data de expiração do certificado SAML do servidor Cisco IdS

1. Faça logon no nó do Publicador ou Assinante do servidor Cisco IdS com a credencial do usuário do aplicativo

2. Após o login bem-sucedido, a página chega ao Identity Service Management > Nós

3. Exibe o nó do Editor e do Assinante do Cisco IdS, o status e a Expiração do Certificado SAML



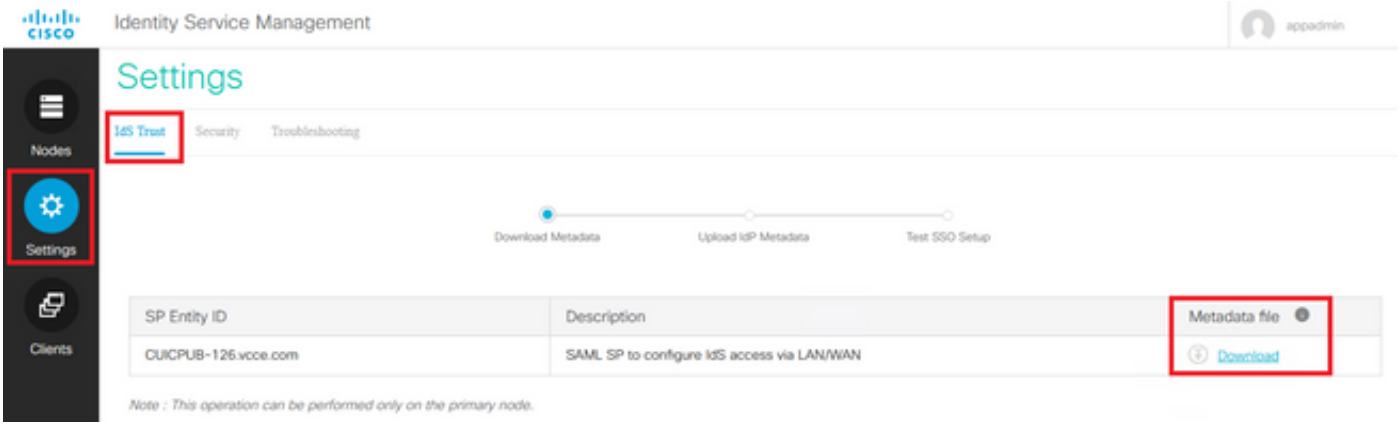
Como fazer download dos metadados do servidor Cisco IdS

1. Faça login no nó do Cisco IdS Publisher com a credencial do usuário do aplicativo

2. Clique no ícone Configurações

3. Navegue até a guia IDS Trust

4. Clique no link Download para baixar os metadados do cluster do Cisco IdS



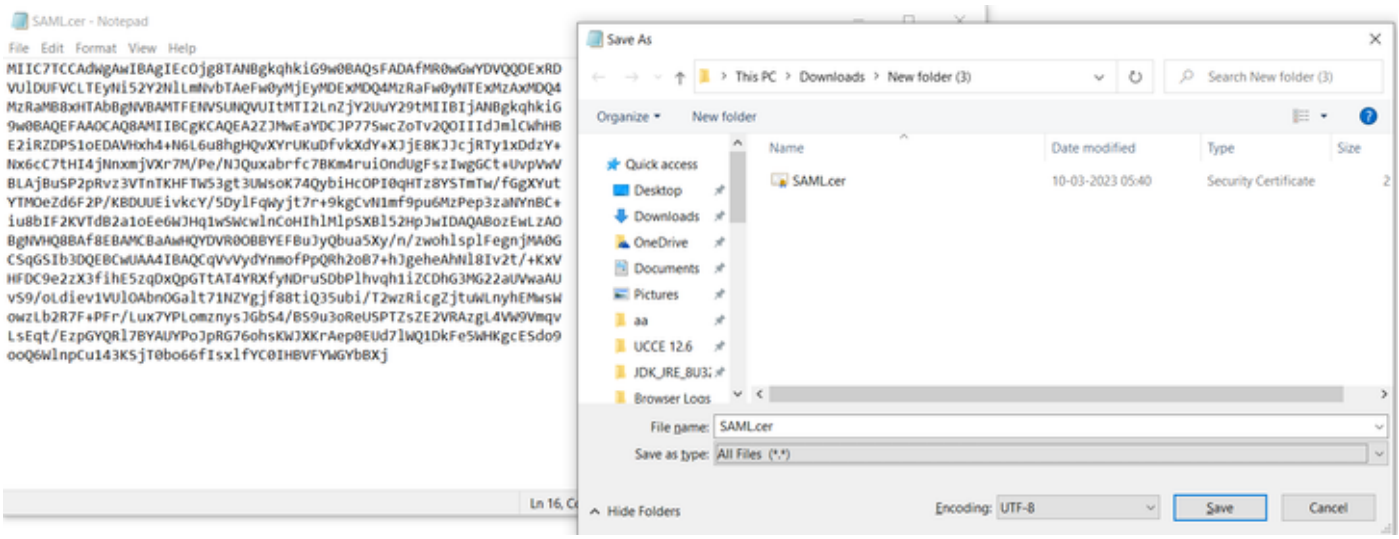
Como recuperar o certificado SAML do arquivo sp.xml

1. Abra o arquivo sp.xml com um editor de texto

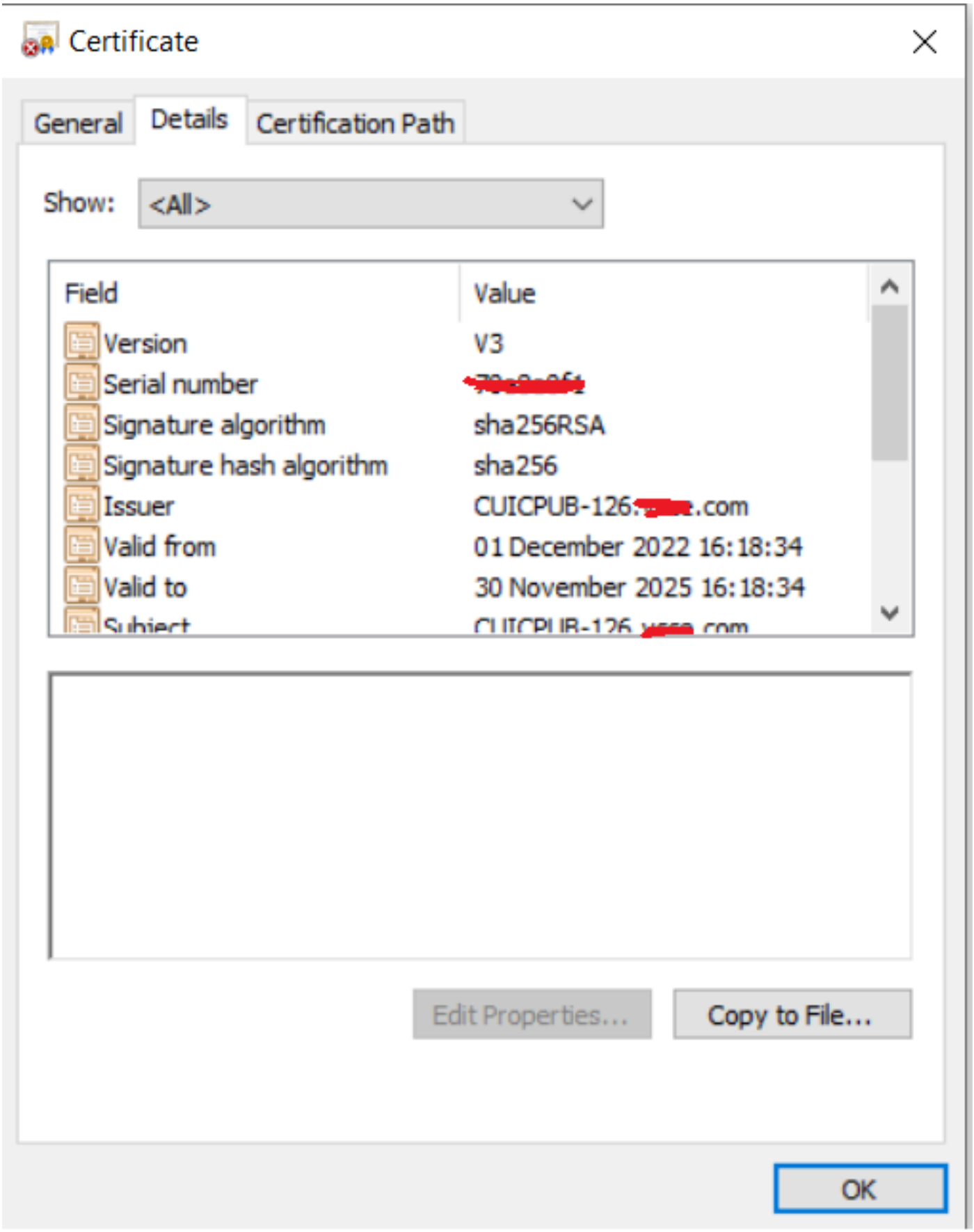
2. Copie os Dados Brutos entre o cabeçalho <ds:X509Certificate></ds:X509Certificate>

3. Abra outro editor de texto e cole os dados copiados

4. salve o arquivo no formato .CER



5. Abra o certificado para revisar as informações do certificado



Como substituir o certificado SAML no AD FS

1. Copie o arquivo de certificado SAML para o servidor AD FS que é recuperado de sp.xml

2. Abra o Gerenciador de Servidores e Escolha AD FS >Ferramentas > Gerenciamento do AD FS

3. Na árvore do lado esquerdo, selecione os objetos de confiança da terceira parte confiável no AD FS

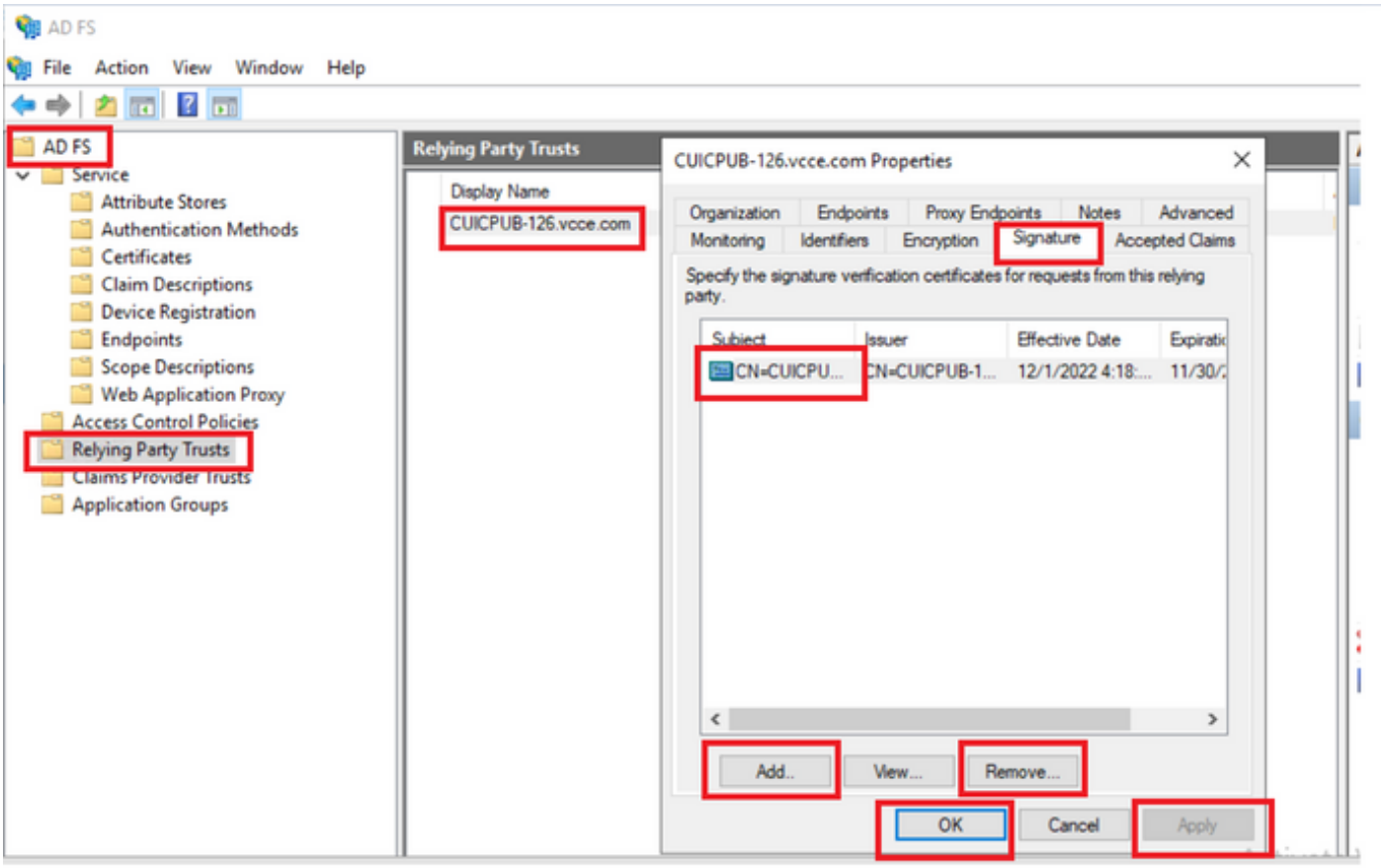
4. Clique com o botão direito do mouse no servidor Cisco IdS e selecione Propriedades

5. Navegue até a guia Assinatura

6. Clique em Adicionar e escolha o certificado SAML recém-gerado

7. Selecione o certificado SAML antigo e clique em Remover

8. Aplicar e Salvar



Como gerar novamente o certificado SAML no servidor Cisco IdS

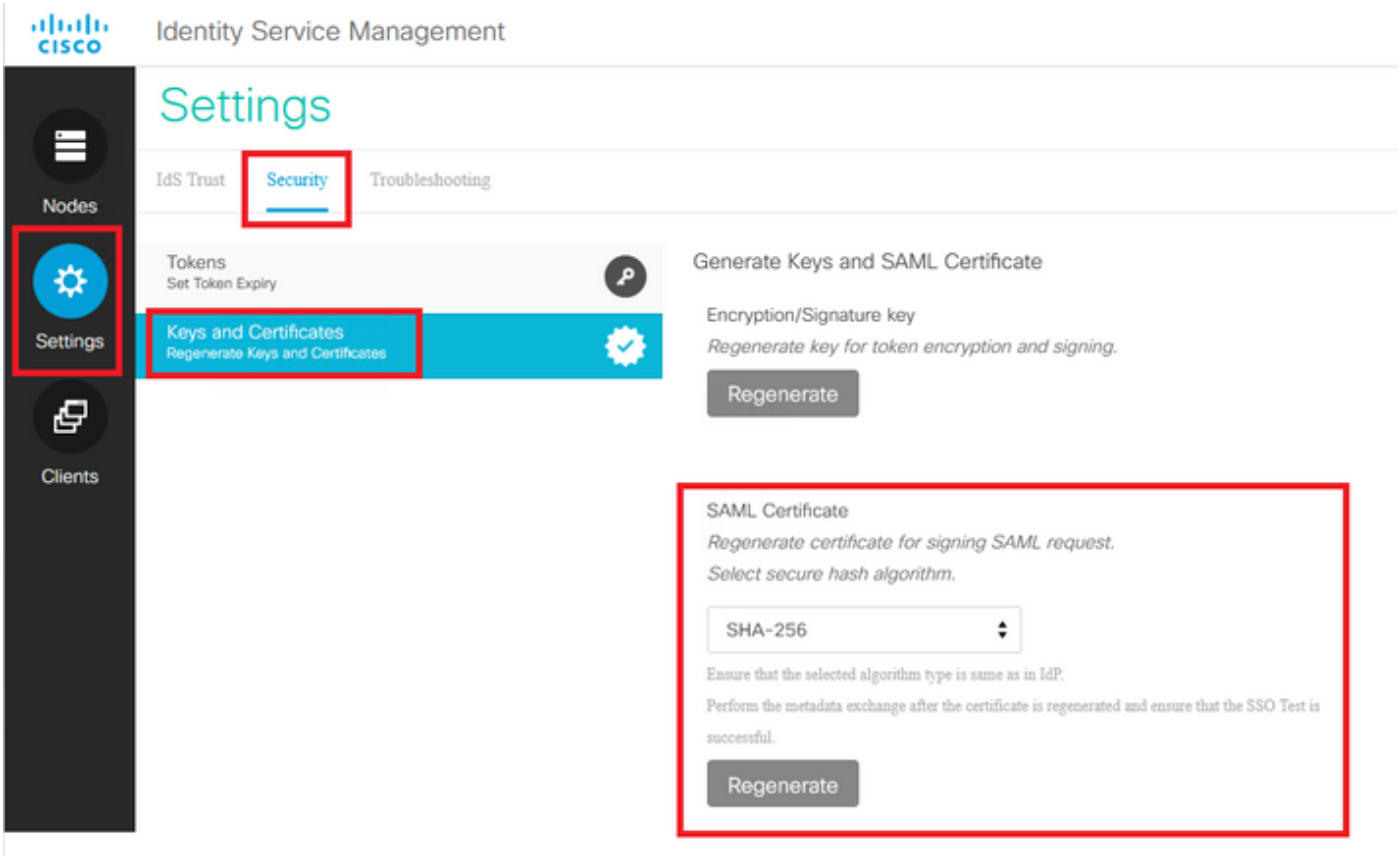
1. Faça login no nó do Cisco IdS Publisher com a credencial do usuário do aplicativo

2. Clique no ícone Configurações

3. Navegue até a guia Segurança

4. Selecione a opção Chaves e Certificados

5. clique no botão Regenerar na seção do certificado SAML (realçado)



Testar SSO

Sempre que houver uma alteração no certificado SAML, certifique-se de que o TEST SSO seja bem-sucedido no servidor Cisco IdS e registre novamente todos os aplicativos na página CCEAdmin.

1. Acesse a página CCEAdmin a partir do servidor AW Principal

2. Faça login no portal CCEAdmin com os privilégios de nível de administrador

3. Navegue até Visão Geral > Recursos > Signon Único

4. Clique no botão Register (Registrar) no Cisco Identity Service

5. Executar SSO de Teste

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.