Problemen oplossen met CCE Single Sign-On met Identity Service (IdS) - Certificaatbeheer

Inhoud

Inleiding

In dit document worden gedetailleerde stappen beschreven voor het regenereren en uitwisselen van SAML-certificaten in UCCE/PCCE, waarbij veilige, duidelijke processen worden gewaarborgd.

Bijgedragen door Nagarajan Paramasivam, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

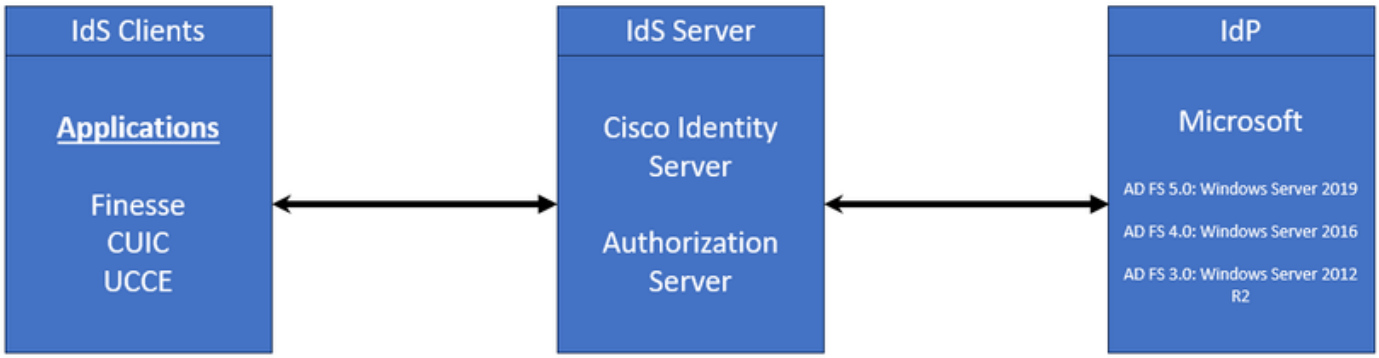
- Verpakt/Unified Contact Center Enterprise (PCCE/UCCE)
- VOS-platform (Voice Operating System)
- certificaatbeheer

- Security Assertion Markup Language (SAML)
- Secure Socket Layer (SSL)
- Active Directory Federation Services (AD FS)
- Eenmalige aanmelding (SSO)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze onderdelen:

- Cisco Identity Service (Cisco IDs)
- Identity Provider (IdP) - Microsoft Windows ADFS



De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

In UCCE/PCCE verleent de Cisco Identity Service (Cisco IdS) autorisatie tussen de Identity Provider (IdP) en applicaties.

Wanneer u de Cisco IdS configureert, stelt u een metagegevensuitwisseling in tussen de Cisco IdS en de IdP. Met deze uitwisseling wordt een vertrouwensrelatie tot stand gebracht waarmee toepassingen de Cisco IdS voor SSO kunnen gebruiken. U stelt de vertrouwensrelatie vast door een metagegevensbestand van de Cisco IdS te downloaden en naar de IdP te uploaden.

Het SAML-certificaat is vergelijkbaar met een SSL-certificaat en moet, net als het, worden bijgewerkt of gewijzigd wanneer bepaalde situaties zich voordoen. Wanneer u het SAML-certificaat op de Cisco Identity Services (IdS)-server opnieuw genereert of uitwisselt, kan dit leiden tot een breuk in de vertrouwde verbinding met de Identity Provider (IdP). Deze onderbreking kan leiden tot problemen waarbij klanten of gebruikers die vertrouwen op Single Sign-On niet de autorisatie kunnen krijgen die ze nodig hebben om toegang te krijgen tot het systeem.

Dit document is bedoeld voor een breed scala aan veelvoorkomende situaties waarin u een nieuw SAML-certificaat op de Cisco IdS-server moet maken. Ook wordt uitgelegd hoe je dit nieuwe

certificaat aan de Identity Provider (IdP) kunt geven zodat het vertrouwen weer opgebouwd kan worden. Hierdoor kunnen klanten en gebruikers zonder problemen Single Sign-On blijven gebruiken. Het doel is om ervoor te zorgen dat u over alle informatie beschikt die u nodig hebt om het proces voor het bijwerken van certificaten soepel en zonder verwarring af te handelen.

Belangrijkste punten om te onthouden:

1. Het SAML-certificaat wordt standaard gegenereerd tijdens de installatie van de Cisco IdS-server met een geldigheidsduur van 3 jaar

2. Het SAML-certificaat is een zelf ondertekend certificaat

3. SAML-certificaat is een SSL-certificaat dat zich bevindt op de Cisco IDS-uitgever en -abonnee

4. SAML-certificaatregeneratie kon alleen worden uitgevoerd in de Cisco IDS Publisher-node

5. De beschikbare typen van het beveiligde hash-algoritme voor het SAML-certificaat zijn SHA-1 en SHA-256

6. SHA-1 algoritme wordt gebruikt op IdS 11.6 en in eerdere versies, de SHA-256 algoritme wordt gebruikt op IdS 12.0 en in latere versies

7. Zowel Identity Provider (IdP) als Identity Service (IdS) moeten hetzelfde type algoritme gebruiken.

8. Het Cisco IdS SAML-certificaat kan alleen worden gedownload van de Cisco IdS Publisher-node (sp-<Cisco IdS_FQDN>.xml)

9. Zie deze link voor meer informatie over de eenmalige aanmeldingsconfiguratie UCCE/PCCE. UCCE 12.6.1 Kenmerkengids

SAML-certificaat verlopen

Het SAML-certificaat wordt gegenereerd met een geldigheid van 3 jaar (1095 dagen) en het is vereist om het SAML-certificaat vóór het verstrijken te verlengen. Het verlopen SSL-certificaat wordt als ongeldig beschouwd en verbreekt de certificaatketen tussen de Cisco Identity Service (IdS) en Identity Provider (IdP).

Oplossing

1. Controleer de vervaldatum van het SAML-certificaat

2. Regenereer het SAML-certificaat

3. Download het sp.xml-bestand

4. Het SAML-certificaat ophalen uit het sp.xml-bestand

5. Vervang het oude SAML-certificaat door het nieuwe SAML-certificaat in de IdP

6. Zie het gedeelte Referentie voor gedetailleerde stappen

(Opmerking: {Aangezien alleen het SAML-certificaat is gewijzigd, is de uitwisseling van IdS-metagegevens naar IdP niet vereist})

Wijziging van het Secure Hash Algorithm in de Identity Provider (IdP)

Ga uit van een bestaande PCCE/UCCE-omgeving met Single-Sign-On. Zowel de IdP- als de Cisco IdS-server is geconfigureerd met het SHA-1 secure hash-algoritme. Gezien de zwakte in de SHA-1 die nodig is om het beveiligde hash-algoritme te veranderen in SHA-256.

Oplossing

1. Wijzig het beveiligde hash-algoritme in de vertrouwenspartij van AD FS (SHA-1 in SHA-256)

2. Wijzig het beveiligde hash-algoritme in de IdS-uitgever onder Sleutels en certificaat (SHA-1 naar SHA-256)

3. Het SAML-certificaat opnieuw genereren in de IdS-uitgever

4. Download het sp.xml-bestand

5. Het SAML-certificaat ophalen uit het sp.xml-bestand

6. Vervang het oude SAML-certificaat door het nieuwe SAML-certificaat in de IdP

7. Zie het gedeelte Referentie voor gedetailleerde stappen

Cisco IdS-server IP-adres of wijziging van hostnaam - Co-resident CUIC/LiveData/IdS Publisher of standalone IdS Publisher opnieuw opgebouwd - Co-resident CUIC/LiveData/IdS-abonnee of standalone IdS-abonnee opnieuw opgebouwd

Deze situaties komen niet vaak voor en het wordt sterk aangeraden om opnieuw te beginnen met de Single Sign-On (SSO)-opstelling om ervoor te zorgen dat de SSO-functionaliteit in de productieomgeving snel en efficiënt wordt hersteld. Het is van essentieel belang om deze herconfiguratie te prioriteren om eventuele onderbrekingen van de SSO-services waarvan

gebruikers afhankelijk zijn, tot een minimum te beperken.

Oplossing

1. Verwijder de bestaande vertrouwenspersoon uit de AD FS

2. Upload het AD FS SSL-certificaat in de Cisco IdS-server naar cat trust

3. Download het sp.xml-bestand

4. Raadpleeg het gedeelte Referentie en de handleiding met kenmerken voor gedetailleerde stappen

5. Configureer de vertrouwenspersoon in de AD FS

6. Voeg de claimregels toe

7. Ondertekende SAML-bevestiging inschakelen

8. Metagegevens van de AD FS Federation downloaden

9. Upload de metagegevens van de Federatie naar de Cisco IdS-server

10. Test SSO uitvoeren

referentie

Hoe u een vertrouwenspersoon toevoegt aan de ADFS of

Hoe ondertekende SAML-bevestiging in te schakelen

Zie dit document voor gedetailleerde stappen: UCCE 12.6.1 Features Guide

Het AD FS SSL-certificaat uploaden naar de Cisco IdS tomcat trust

1. Het AD FS SSL-certificaat downloaden of ophalen

2. Toegang tot de beheerpagina van Cisco IdS Publisher OS

3. Aanmelden met de beheerdersreferenties voor het besturingssysteem

4. Navigeer naar Beveiliging > Certificaatbeheer

5. Klik op Certificaat/certificaatketen uploaden en er verschijnt een pop-upvenster

6. Klik op het Dropdown-menu en selecteer tomcat-trust voor het doel van het certificaat

7. Klik op Bladeren en selecteer het AD FS SSL-certificaat

8. Klik op Uploaden

(Opmerking: {De vertrouwenscertificaten worden gerepliceerd naar de abonneeknooppunten. U hoeft niet te uploaden op de abonnee node.})

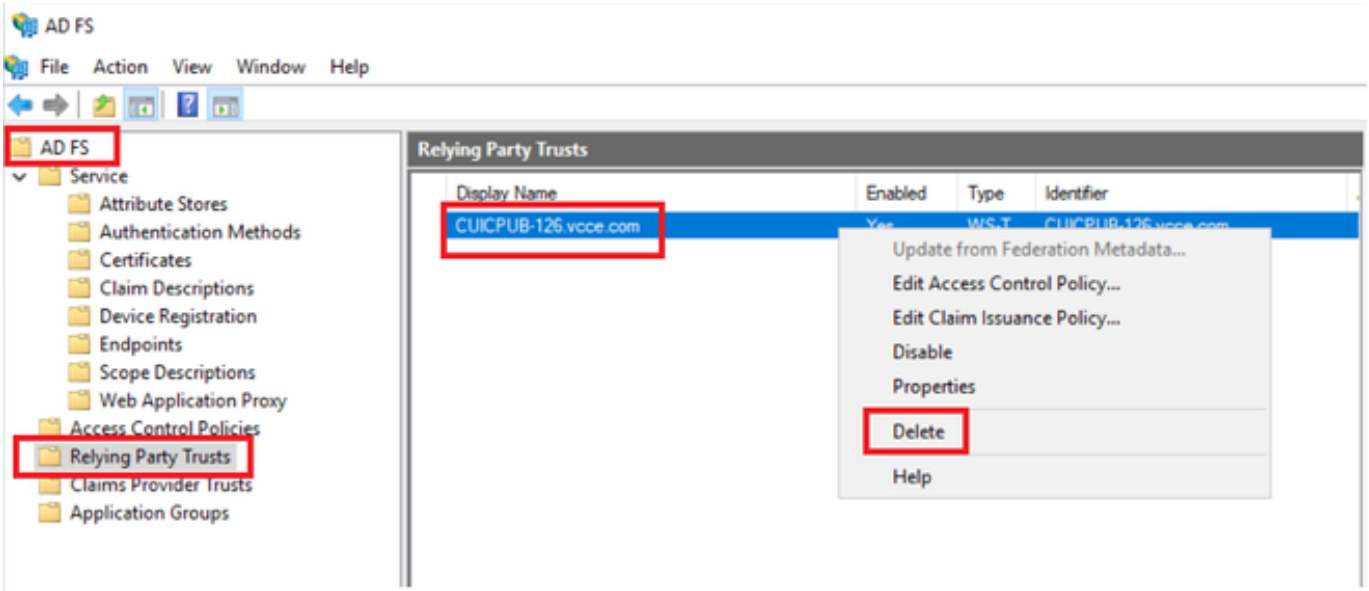
Hoe te verwijderen van de Relying Trust Party in de AD FS

1. Meld u aan bij de Identity Provider (IdP)-server met de aanmeldingsgegevens voor de beheerder

2. Open Serverbeheer en kies AD FS >Extra > AD FS-beheer

3. Selecteer in de linkerzijboom de vertrouwensrelatie met de vertrouwenspersoon onder de AD FS

4. Klik met de rechtermuisknop op de Cisco IdS-server en selecteer Verwijderen



Het beveiligde hash-algoritme controleren of wijzigen dat is geconfigureerd in de Identity Provider (IdP)

1. Meld u aan bij de Identity Provider (IdP)-server met de aanmeldingsgegevens voor de beheerder

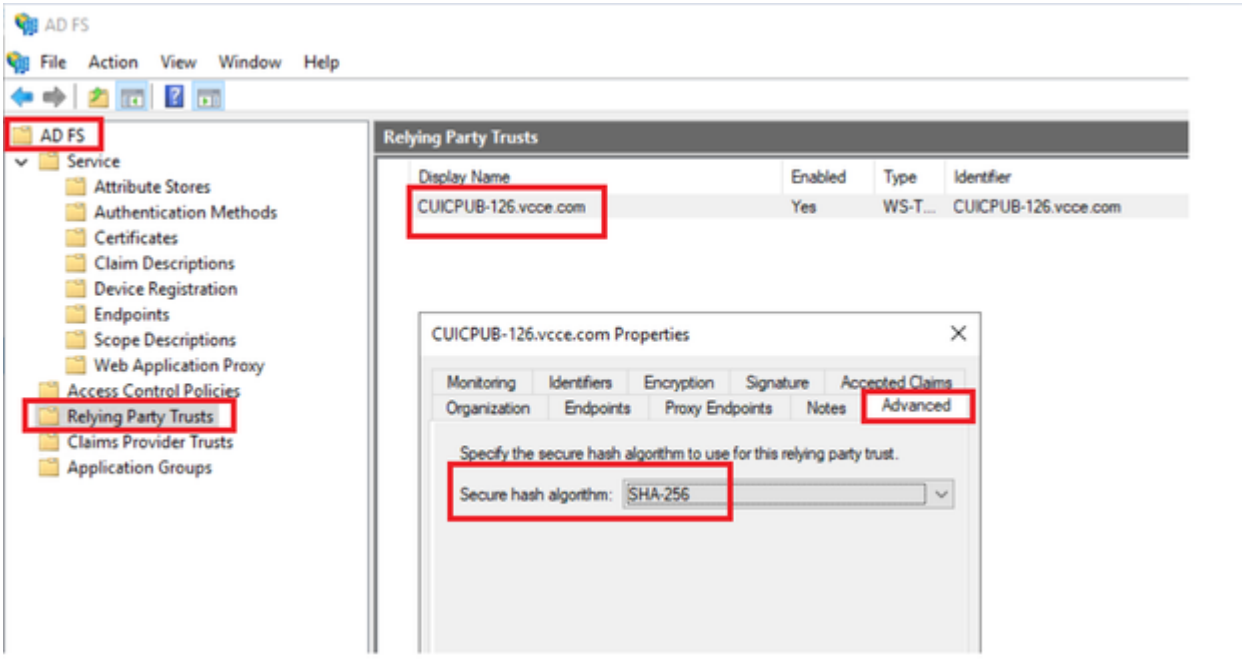
2. Open Serverbeheer en kies AD FS >Extra > AD FS-beheer

3. Selecteer in de linkerzijboom de vertrouwensrelatie met de vertrouwenspersoon onder de AD FS

4. Klik met de rechtermuisknop op de Cisco IdS-server en selecteer Eigenschappen

5. Navigeer naar het tabblad Geavanceerd

6. De optie Secure Hash Algorithm (Beveiligd hashalgoritme) geeft het beveiligde hashalgoritme weer dat is geconfigureerd in de AD FS-server.



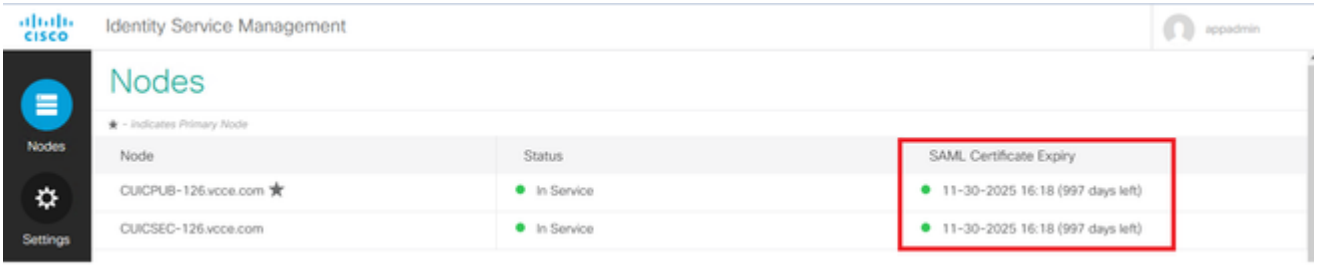
7. Klik op het vervolgkeuzemenu en selecteer het gewenste beveiligde hash-algoritme.

De vervaldatum van het SAML-certificaat voor de Cisco IdS-server controleren

1. Meld u aan bij Cisco IdS Server Publisher of Subscriber node met de gebruikersreferenties van de toepassing

2. Na het succesvol aanmelden op de pagina landt op Identity Service Management > Nodes

3. Geeft de Cisco IdS Publisher en Subscriber node, status en SAML Certificate Expiry weer



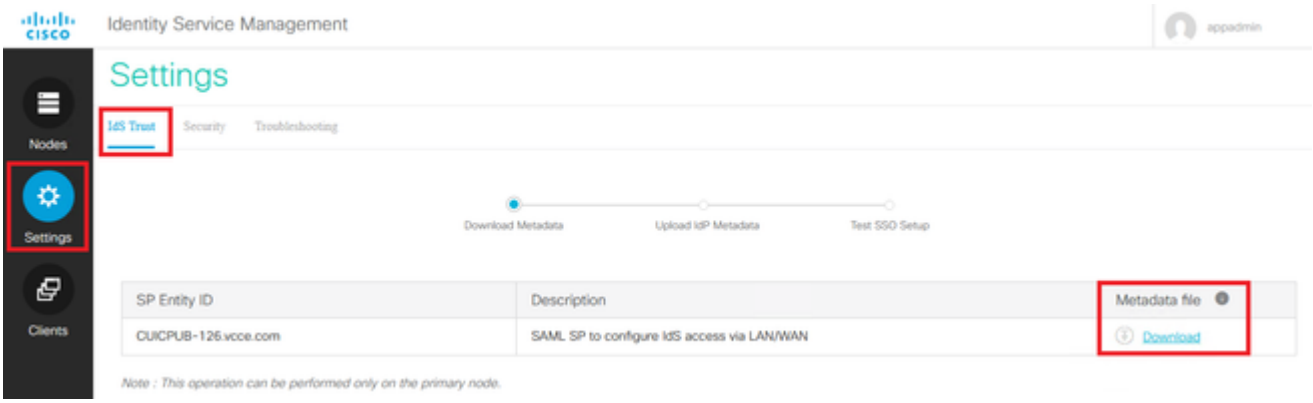
Hoe de metagegevens van de Cisco IdS-server te downloaden

1. Meld u aan bij de Cisco IdS Publisher-node met de gebruikersreferenties van de toepassing

2. Klik op het pictogram Instellingen

3. Navigeer naar het tabblad IDS-vertrouwen

4. Klik op de koppeling Download om de metagegevens van het Cisco IdS-cluster te downloaden



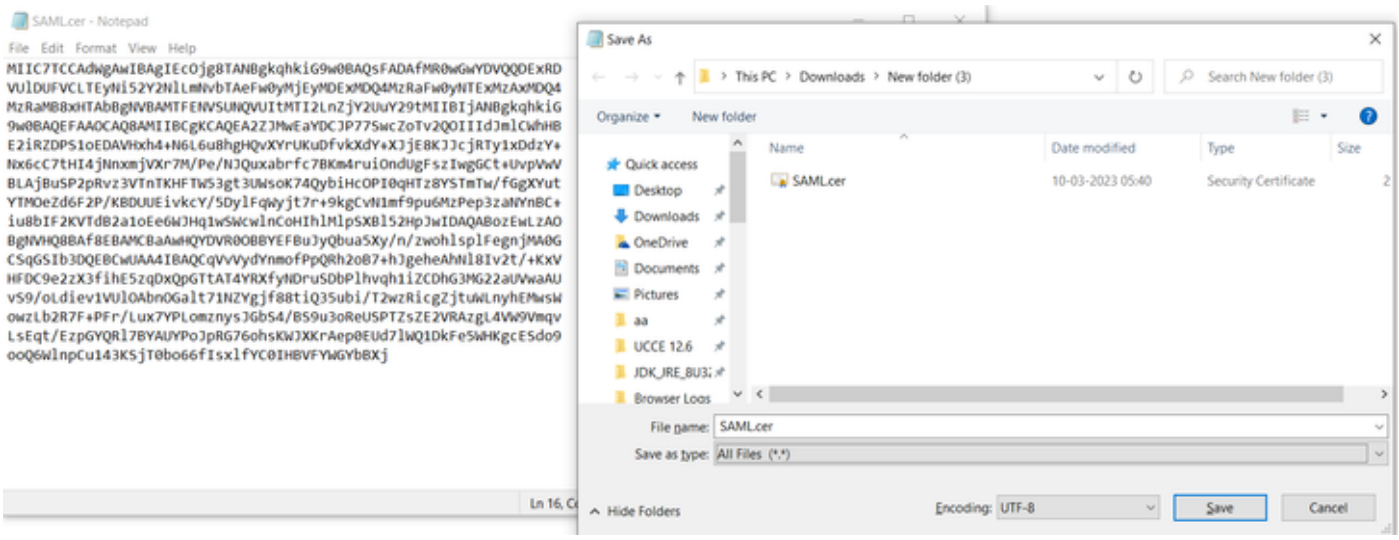
Het SAML-certificaat ophalen uit het sp.xml-bestand

1. Open het sp.xml bestand met een teksteditor

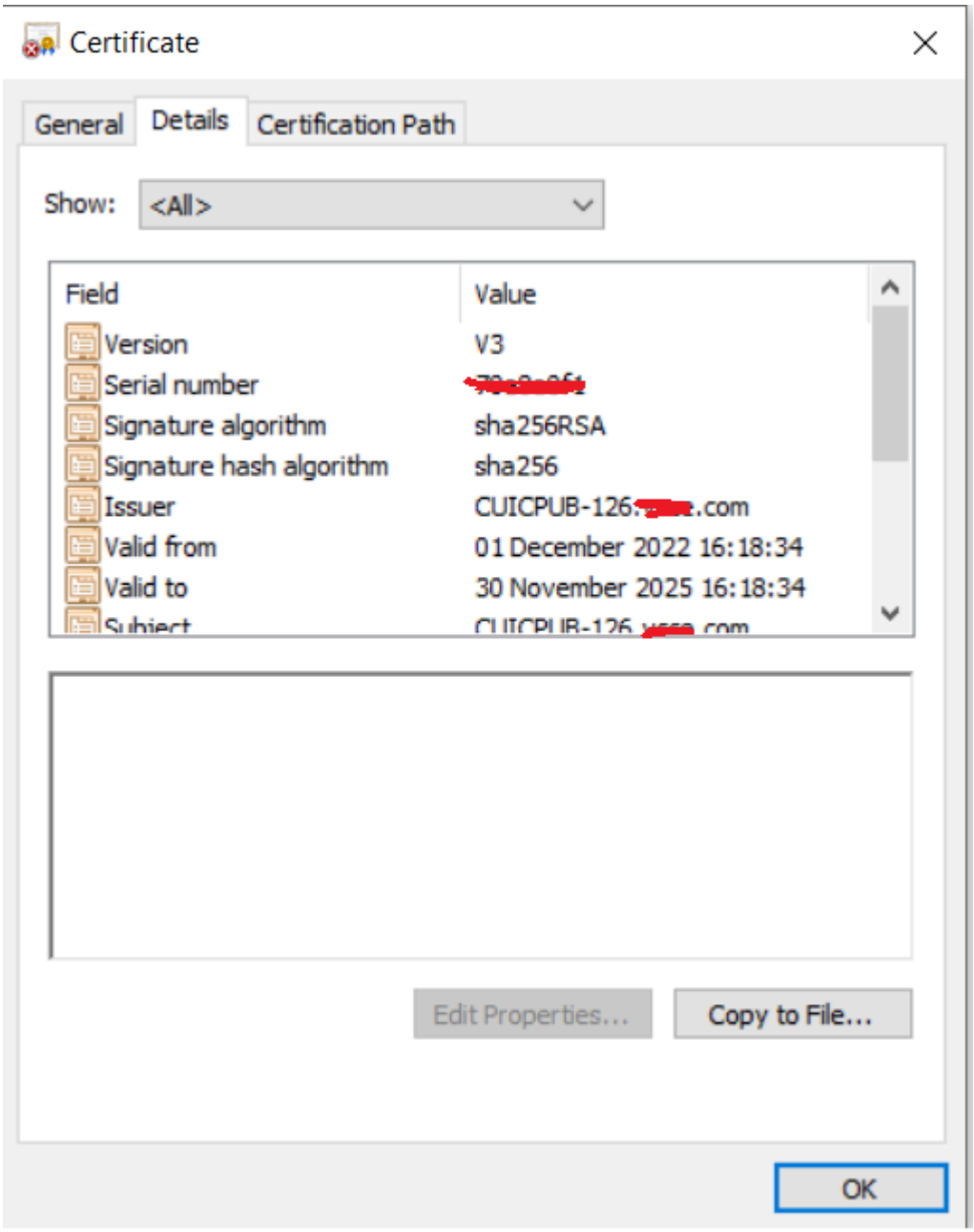
2. Kopieer de onbewerkte gegevens tussen de koptekst <ds:X509Certificate></ds:X509Certificate>

3. Open een andere teksteditor en plak de gekopieerde gegevens

4. Sla het bestand .CER-formaat op



5. Open het certificaat om de certificaatinformatie te bekijken



Het SAML-certificaat vervangen in de AD FS

1. Kopieer het SAML-certificaatbestand naar de AD FS-server die wordt opgehaald van sp.xml

2. Open Serverbeheer en kies AD FS >Extra > AD FS-beheer

3. Selecteer in de linkerzijboom de vertrouwensrelatie met de vertrouwenspersoon onder de AD FS

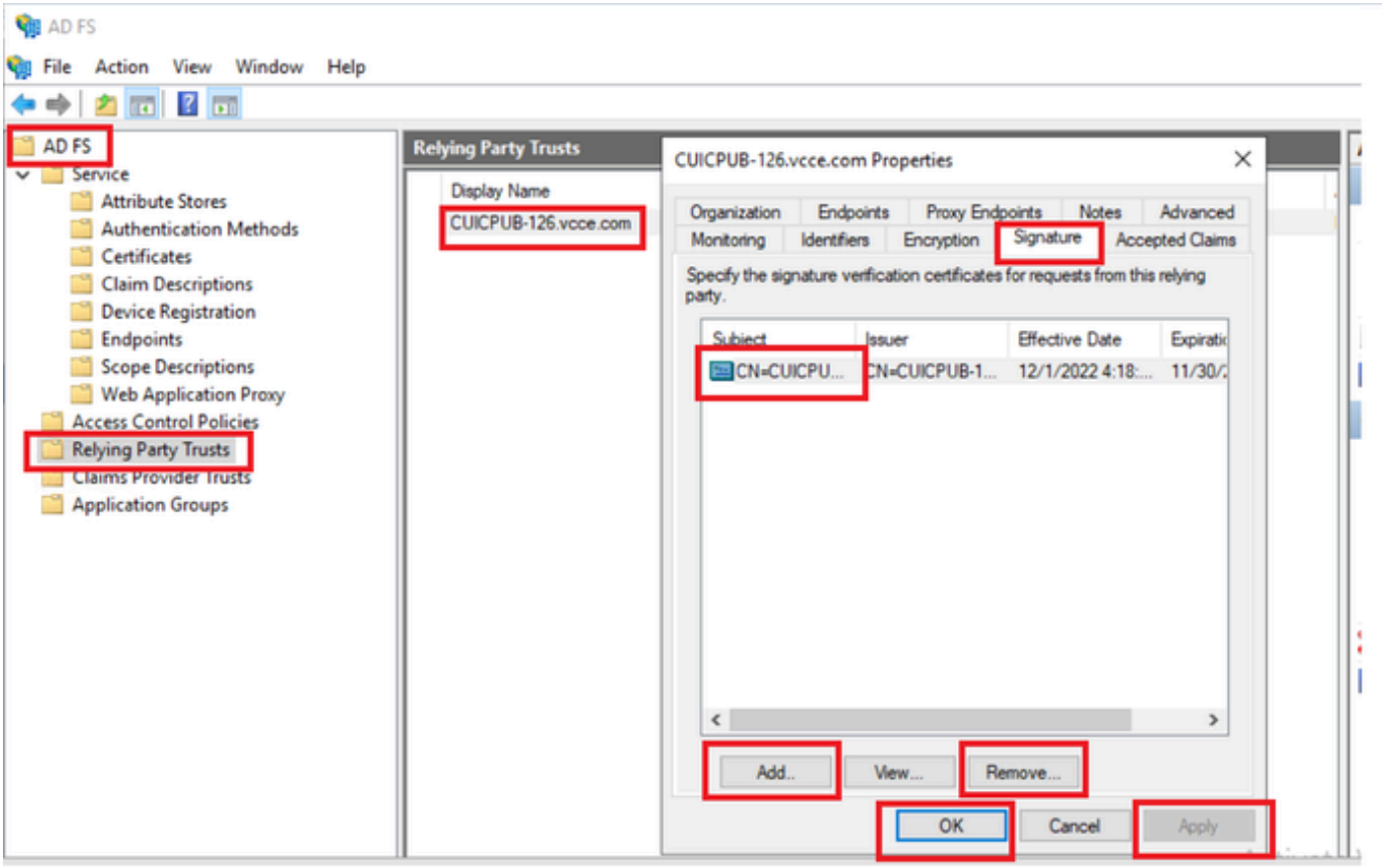
4. Klik met de rechtermuisknop op de Cisco IdS-server en selecteer Eigenschappen

5. Navigeer naar het tabblad Handtekening

6. Klik op Toevoegen en kies het nieuwe SAML-certificaat

7. Selecteer het oude SAML-certificaat en klik op Verwijderen

8. Toepassen en opslaan



Het SAML-certificaat opnieuw genereren in de Cisco IdS-server

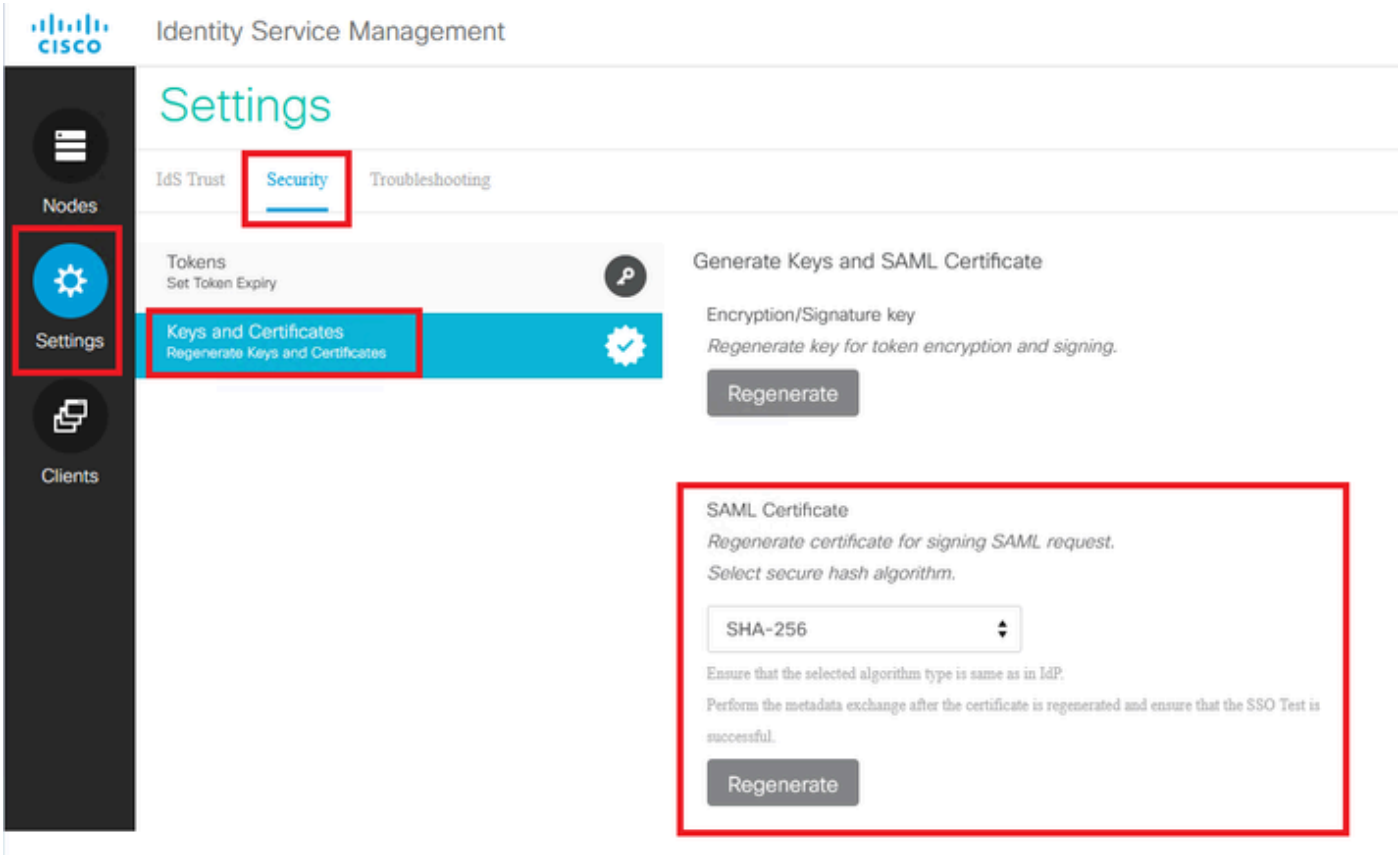
1. Meld u aan bij de Cisco IdS Publisher-node met de gebruikersreferenties van de toepassing

2. Klik op het pictogram Instellingen

3. Navigeer naar het tabblad Beveiliging

4. Selecteer de optie Sleutels en certificaten

5. Klik op de knop Regenereren onder het gedeelte SAML-certificaat (gemarkeerd)



SSO testen

Wanneer het SAML-certificaat wordt gewijzigd, moet u ervoor zorgen dat de TEST-SSO succesvol is in de Cisco IdS-server en alle toepassingen opnieuw registreren vanaf de CCEAdmin-pagina.

1. Toegang tot de CCEAdmin-pagina vanaf de hoofdserver voor AW

2. Meld u aan bij het CCEAdmin-portaal met de beheerdersrechten

3. Navigeer naar Overzicht > Functies > Eenmalige aanmelding

4. Klik op de knop Registreren onder Registreren bij Cisco Identity Service

5. Test SSO uitvoeren

Azure Certificate Regeneration

1. Regenereer certificaat van IDS, alleen in Publisher, dit zal het automatisch genereren voor zowel Publisher als Abonnee
2. Metagegevens downloaden van IDS en uploaden naar IDP/Azure
3. Certificaat vernieuwen van IDP / Azure, dit zal de metadata van Azure volledig veranderen en zal het ondertekenen van Microsoft Azure, het oplossen van de behoeften van de .pfx
4. Upload de metagegevens van IDP/Azure naar Cisco IDS, alleen in de Publisher
5. SSO-test van IDS

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.