Probleemoplossing CCE single aanmelding met Identity Service (ID's)-certificaatbeheer

Inhoud

Inleiding

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

Bijgedragen door Nagarajan Paramasivam, Cisco TAC Engineer.

Voorwaarden

Vereisten

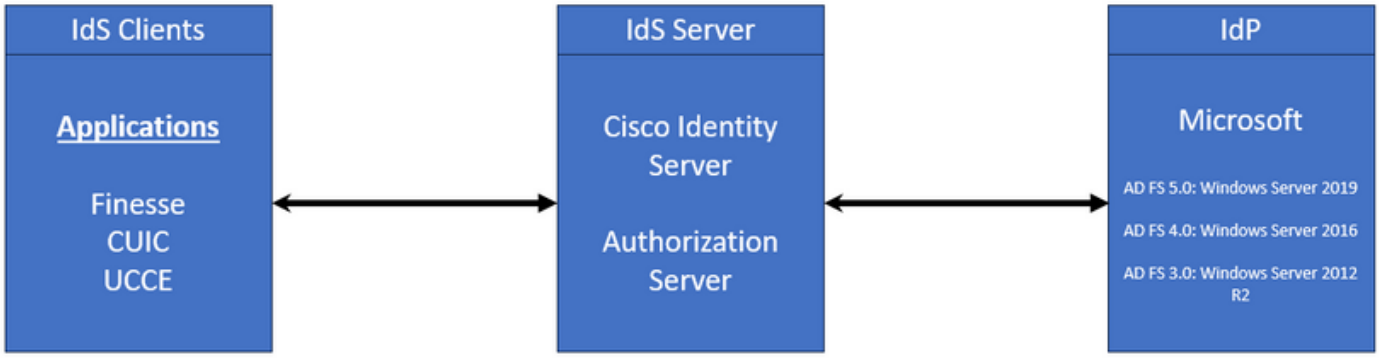
Cisco raadt u aan deze onderwerpen te kennen:

- Packaging/Unified contactcenters voor ondernemingen (PCE/UCCE)
- Voice Operating System (VOS) platform
- Certificaatbeheer
- Security Assertion Markup Language (SAML)
- Secure Socket Layer (SSL)
- Active Directory Federation Services (AD FS)
- Single Sign-On (SSO)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze componenten:

- Cisco Identity Service (Cisco ID's)
- 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 UCS/PCE biedt de Cisco Identity Service (Cisco ID's) autorisatie tussen de Identity Provider (IDP) en toepassingen.

Wanneer u Cisco IDs configureert, stelt u een metagegevensuitwisseling in tussen de Cisco IDs en de IDp. Deze uitwisseling brengt een vertrouwensrelatie tot stand die toepassingen vervolgens toestaat om de Cisco IDs voor een SSO te gebruiken. U stelt de vertrouwensrelatie vast door een metagegevensbestand te downloaden van de Cisco-id's en het te uploaden naar de IdP.

Het SAML-certificaat is vergelijkbaar met een SSL-certificaat en moet, net zoals het, worden bijgewerkt of gewijzigd wanneer bepaalde situaties zich voordoen. Wanneer u het SAML-certificaat regenereert of uitruilt op de Cisco Identity Services (IDS)-server, kan dit een breuk veroorzaken 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 brede reeks veelvoorkomende situaties waarin u een nieuw SAML-certificaat moet maken op de Cisco IDs-server. Het legt ook uit hoe dit nieuwe certificaat aan de Identity Provider (IDP) moet worden verstrekt, zodat het vertrouwen kan worden herbouwd. Op deze manier kunnen klanten en gebruikers Single Sign-On blijven gebruiken zonder problemen. Het doel is ervoor te zorgen dat u over alle informatie beschikt die u nodig hebt om het certificaat update proces soepel en zonder verwarring te behandelen.

Belangrijkste punten om te onthouden:

1. 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 zelfondertekend certificaat

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

4. SAML-certificaatregeneratie kan alleen worden uitgevoerd in het knooppunt Cisco IDS Publisher

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

6. Het algoritme SHA-1 wordt gebruikt op IDs 11.6 en in vorige versies, wordt het algoritme SHA-256 gebruikt op IDs 12.0 en in recentere versies

7. Zowel Identity Provider (IDP) als Identity Service (IDS) moeten hetzelfde algoritmetype gebruiken.

8. Cisco IDs SAML-certificaat kan alleen worden gedownload van de knooppunt Cisco IDs Publisher (sp-<Cisco IDS_FQDN>.xml)

9. Raadpleeg deze link om de configuratie van de UCCE/PCE single-Sign-On te begrijpen. UCS 12.6.1 Functiegids

SAML-certificaat verlopen

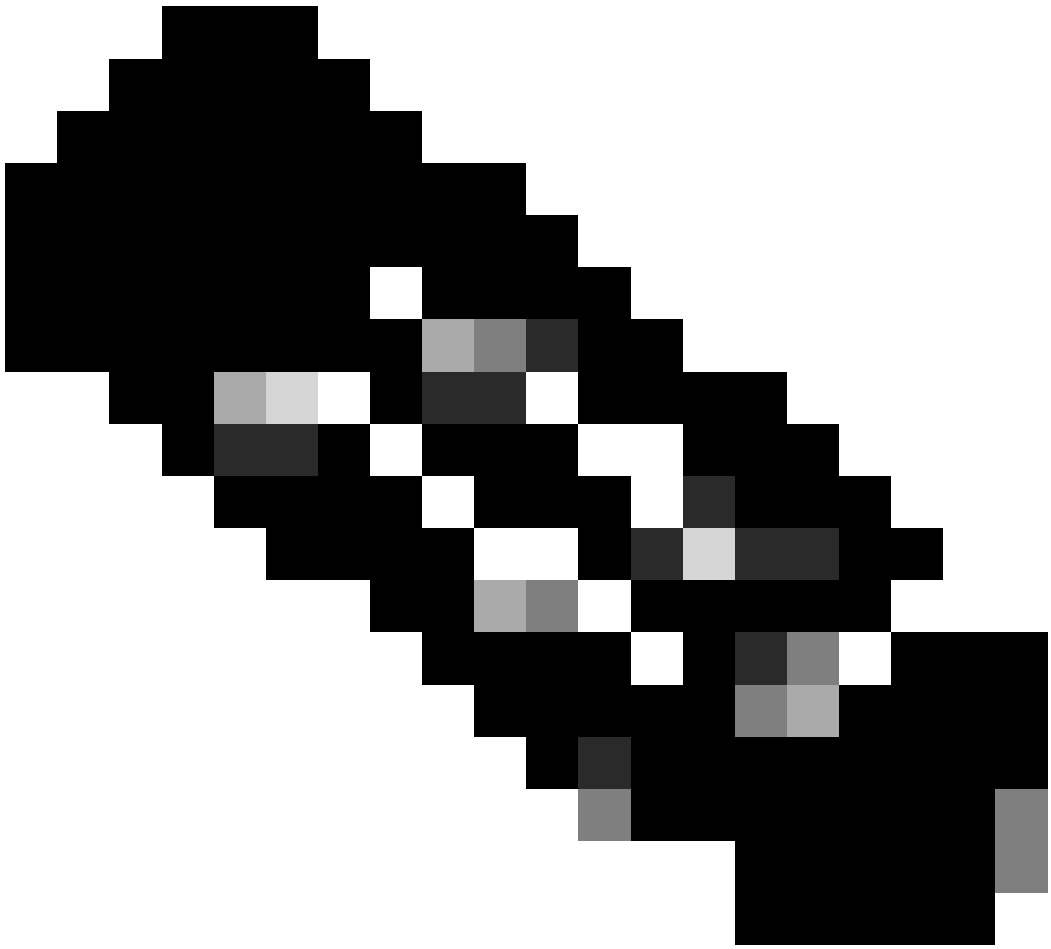
Het SAML-certificaat wordt gegenereerd met een geldigheidsduur van 3 jaar (1095 dagen) en het moet het SAML-certificaat vernieuwen voor de vervaldatum. Het verlopen SSL-certificaat wordt als ongeldig beschouwd en breekt de certificaatketen tussen de Cisco Identity Service (IDs) en

Identity Provider (IDP).

Oplossing

1. Controleer de vervaldatum van het SAML-certificaat
2. Het SAML-certificaat regenereren
3. Download het sp.xml bestand
4. Haal het SAML-certificaat uit het sp.xml-bestand.
5. Vervang het oude SAML-certificaat door het nieuwe SAML-certificaat in de IDp
6. Raadpleeg het referentiegedeelte voor gedetailleerde stappen

---



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

Secure Hash Algorithm Change in the Identity Provider (IDP)

Veronderstel in een bestaande omgeving PCE/UCCE met Single-Sign-On. Zowel IdP als Cisco IDs server is geconfigureerd met SHA-1 beveiligd hashalgoritme. Gezien de zwakte in de SHA-1 die nodig is om het beveiligde hashalgoritme in SHA-256 te veranderen.

Oplossing

1. Verander het beveiligde hashalgoritme in de AD FS Relying Trust Party (SHA-1 naar SHA-256)

2. Verander het beveiligde hashalgoritme in de IDs-uitgever onder Toetsen en Certificaat (SHA-1 naar SHA-256)

3. Het SAML-certificaat regenereren in de ID's-uitgever

4. Download het sp.xml bestand

5. Haal het SAML-certificaat uit het sp.xml-bestand.

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

7. Raadpleeg het referentiegedeelte voor gedetailleerde stappen

Cisco IDs server IP-adres of wijziging van hostnaam - Co-Resident CUIC/LiveData/IDs Publisher of Standalone IDs Publisher herbouwd - Co-Resident CUIC/LiveData/IDs Subscriber of Standalone IDs Subscriber herbouwd

Deze situaties doen zich zelden voor en het is sterk aan te raden om opnieuw te beginnen met de Single Sign-On (SSO)-instelling om ervoor te zorgen dat SSO-functionaliteit in de productieomgeving snel en efficiënt wordt hersteld. Het is essentieel om aan deze herconfiguratie prioriteit te geven om elke verstoring van de SSO-services waarvan gebruikers afhankelijk zijn tot een minimum te beperken.

Oplossing

1. Verwijder de bestaande Relying Trust Party uit de AD FS

2. Upload het AD FS SSL-certificaat in de Cisco IDS-server naar vertrouwen.

3. Download het sp.xml bestand

4. Raadpleeg het referentiegedeelte en de handleiding met functies voor uitgebreide stappen

5. De Relying Trust Party instellen in de AD FS

6. Voeg de vorderingsregels toe

7. Schakel ondertekende SAML-bevestiging in

8. Download metagegevens van AD FS Federation

9. Upload de Federatie Metadata naar de Cisco IDs server

10. Test SSO

Referentie

Relying Trust Party toevoegen in de ADFS of

Ondertekende SAML-bewering inschakelen

Raadpleeg dit document voor gedetailleerde stappen: UCCE 12.6.1 Functiehandleiding

Hoe het AD FS SSL-certificaat te uploaden naar het Cisco IDs-tomatvertrouwen

1. Het AD FS SSL-certificaat downloaden of ophalen

2. Open de beheerpagina van het besturingssysteem van Cisco Identity Publisher

3. Login met de OS Administrator credential

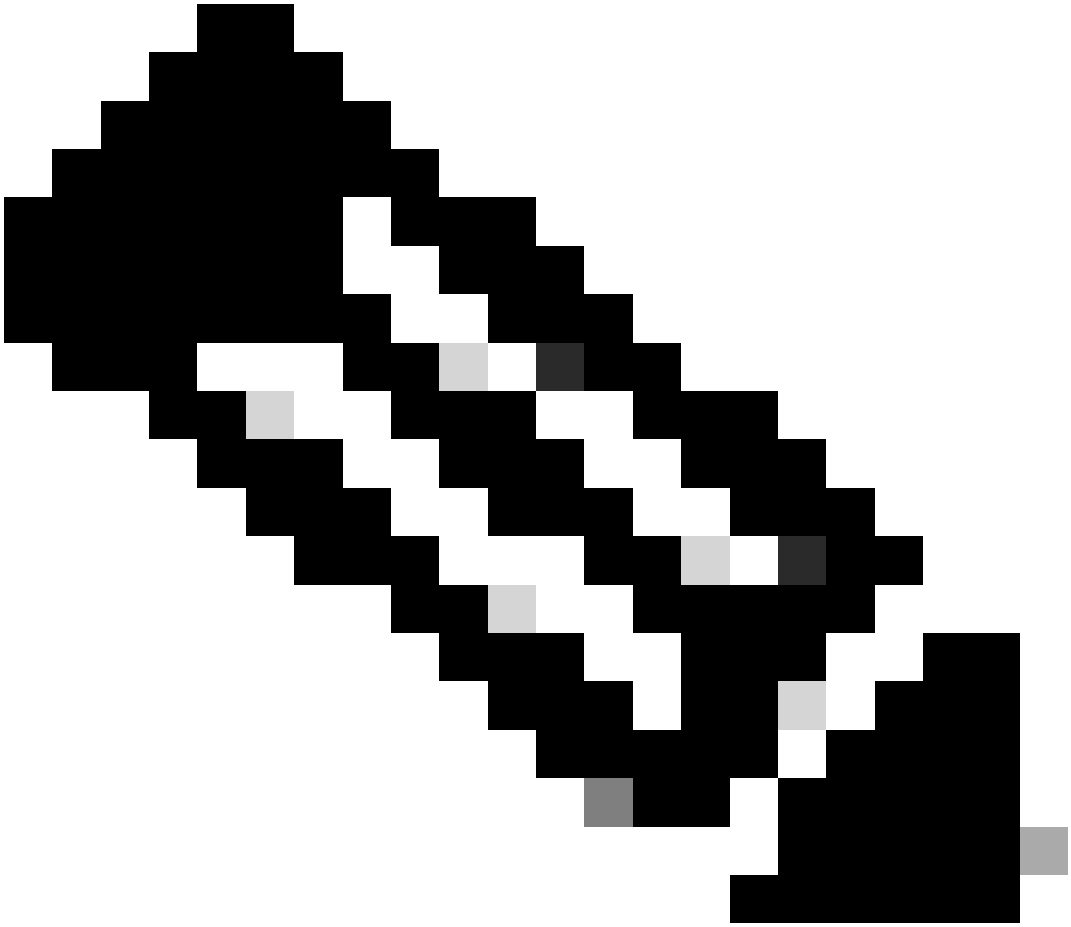
4. Navigeren naar Beveiliging > Certificaatbeheer

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

6. Klik op het vervolgkeuzemenu en selecteer tomcat-trust op Certificate Purpose

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

8. Klik op Upload



(Opmerking: {De vertrouwenscertificaten worden gerepliceerd naar de Subscriber-knooppunten. U hoeft niet te uploaden op de Subscriber-knooppunt.})

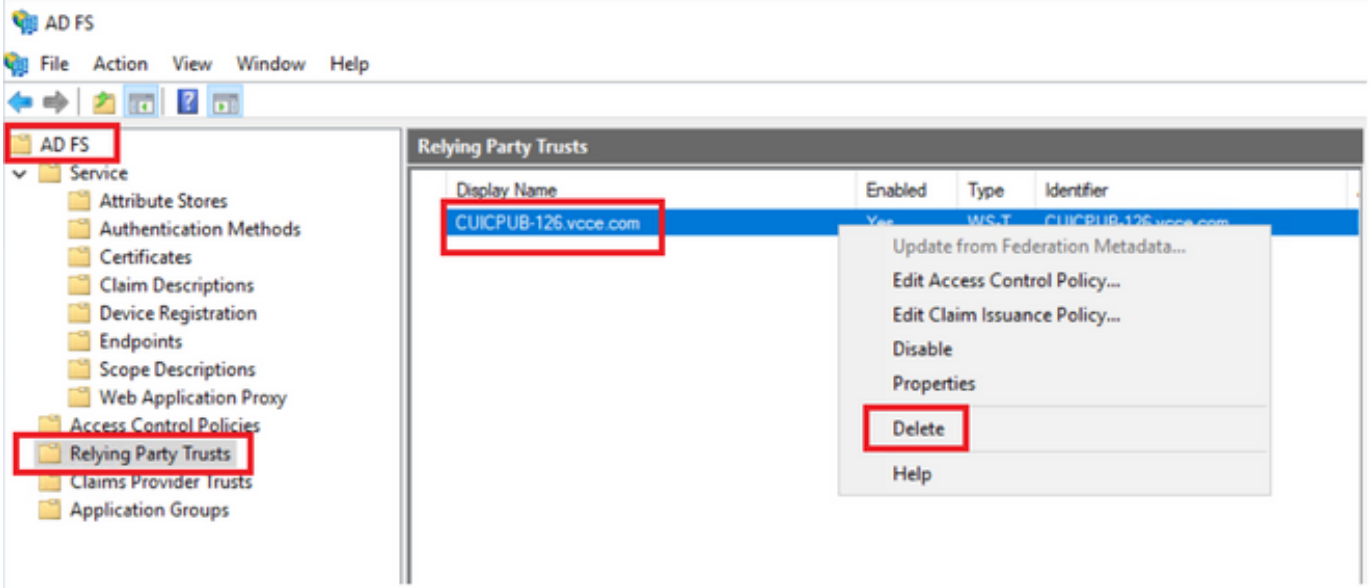
Hoe te verwijderen van de Relying Trust Party in de AD FS

1. Log in op de Identity Provider (IDP) server met de door de beheerder geprivilegieerde referenties

2. Open Server Manager en kies AD FS >Tools > AD FS Management

3. Selecteer in de linkerboom de Relying Party Trusts onder de AD FS

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



Hoe het beveiligde hash-algoritme te controleren of wijzigen dat is geconfigureerd in de Identity Provider (IDP)

1. Log in op de Identity Provider (IDP) server met de door de beheerder geprivilegieerde referenties

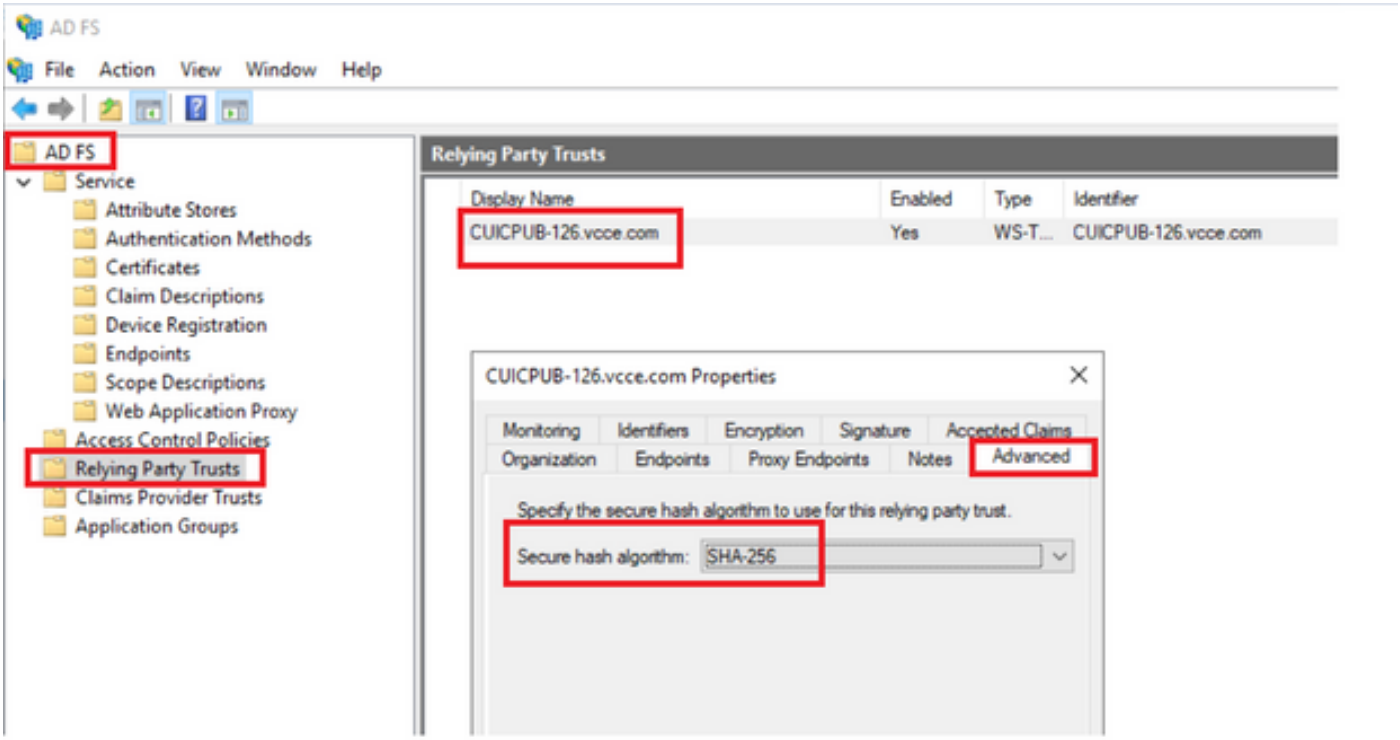
2. Open Server Manager en kies AD FS >Tools > AD FS Management

3. Selecteer in de linkerboom de Relying Party Trusts onder de AD FS

4. Klik met de rechtermuisknop op de Cisco IDs-server en selecteer eigenschappen

5. Navigeren naar het tabblad Geavanceerd

6. De optie Secure Hash Algorithm geeft het beveiligde hash-algoritme weer dat in de AD FS-server is geconfigureerd.



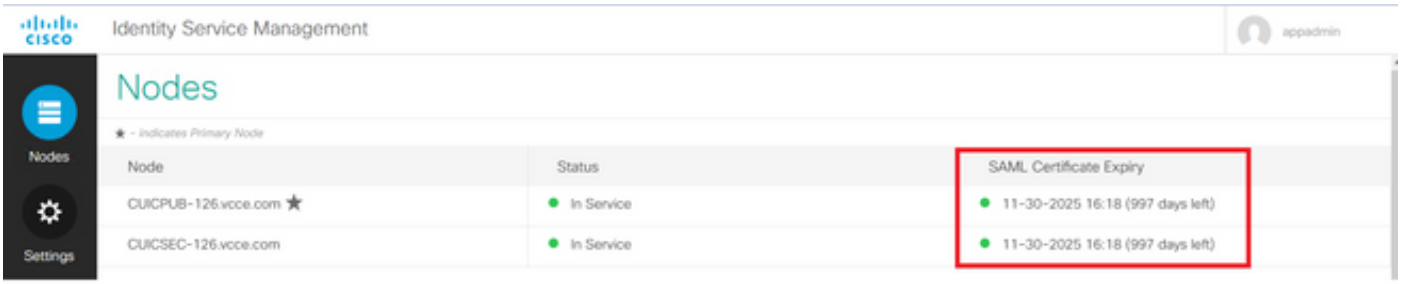
7. Klik op het uitrolmenu en selecteer het gewenste beveiligde hash-algoritme.

Hoe de vervaldatum van het SAML-certificaat voor de Cisco IDS-server te controleren

1. Log in op de Cisco IDs server Publisher of Subscriber knooppunt met de gebruikersreferenties van de toepassing

2. Nadat u de pagina hebt geopend, landt deze op Identity Service Management > Knooppunten

3. Hier worden de knooppunt, status en vervaldatum van het SAML-certificaat van Cisco IDs Publisher en Subscriber weergegeven



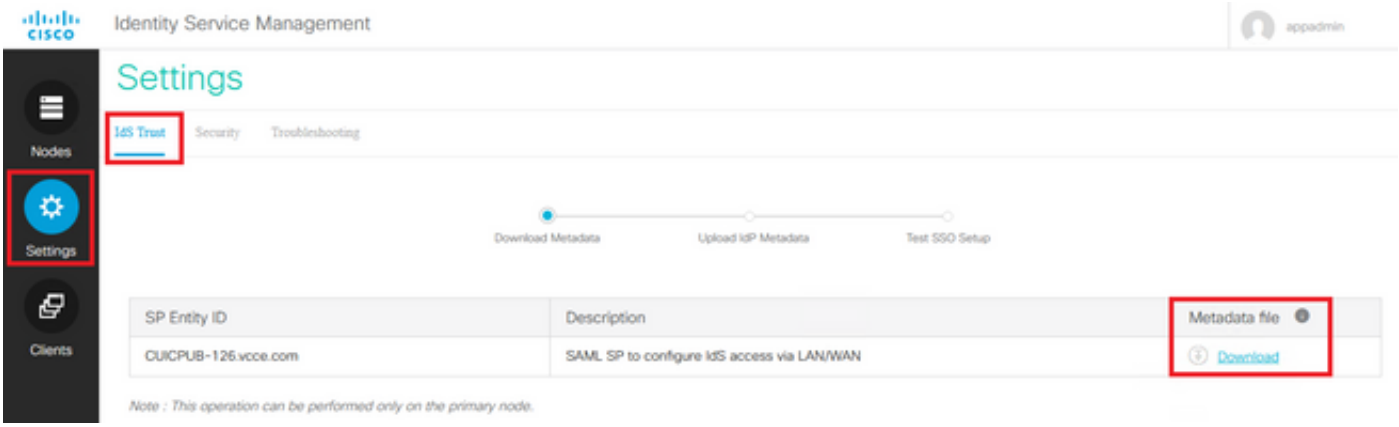
Hoe de metagegevens van de Cisco IDs-server te downloaden

1. Log in op het knooppunt Cisco IDS Publisher met de gebruikersreferenties van de toepassing

2. Klik op het pictogram Settings

3. Navigeer naar het tabblad IDS-vertrouwen

4. Klik op de koppeling Downloaden om de metagegevens van het Cisco IDs-cluster te downloaden



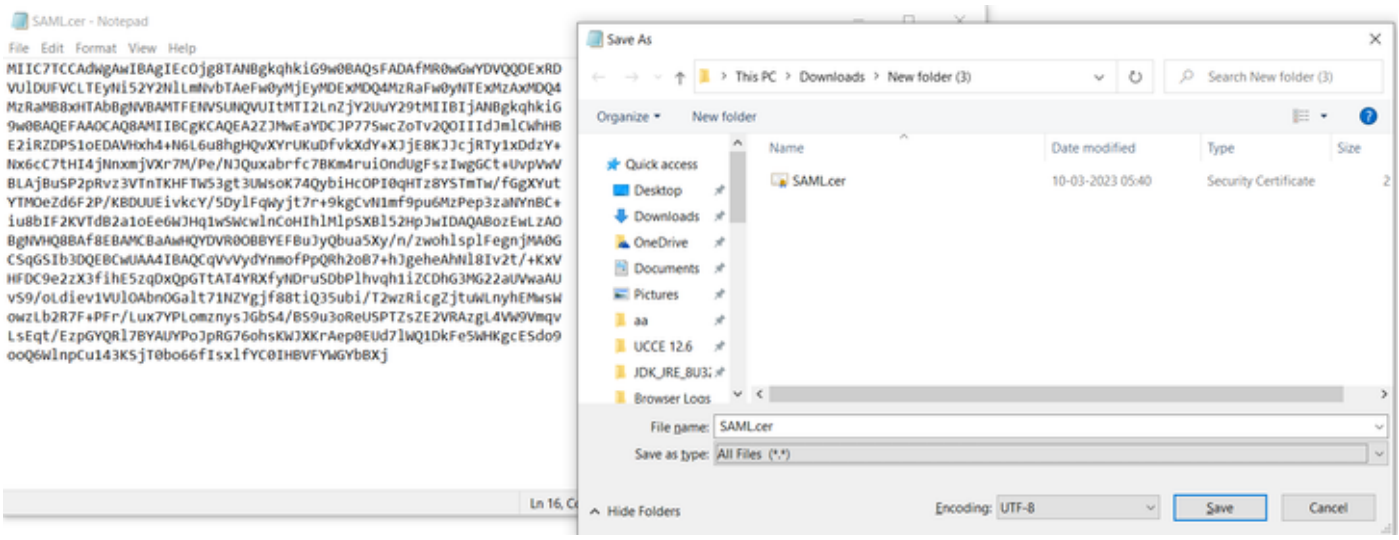
Hoe te om het certificaat van SAML van het sp.xml- dossier terug te winnen

1. Open het sp.xml-bestand met een teksteditor

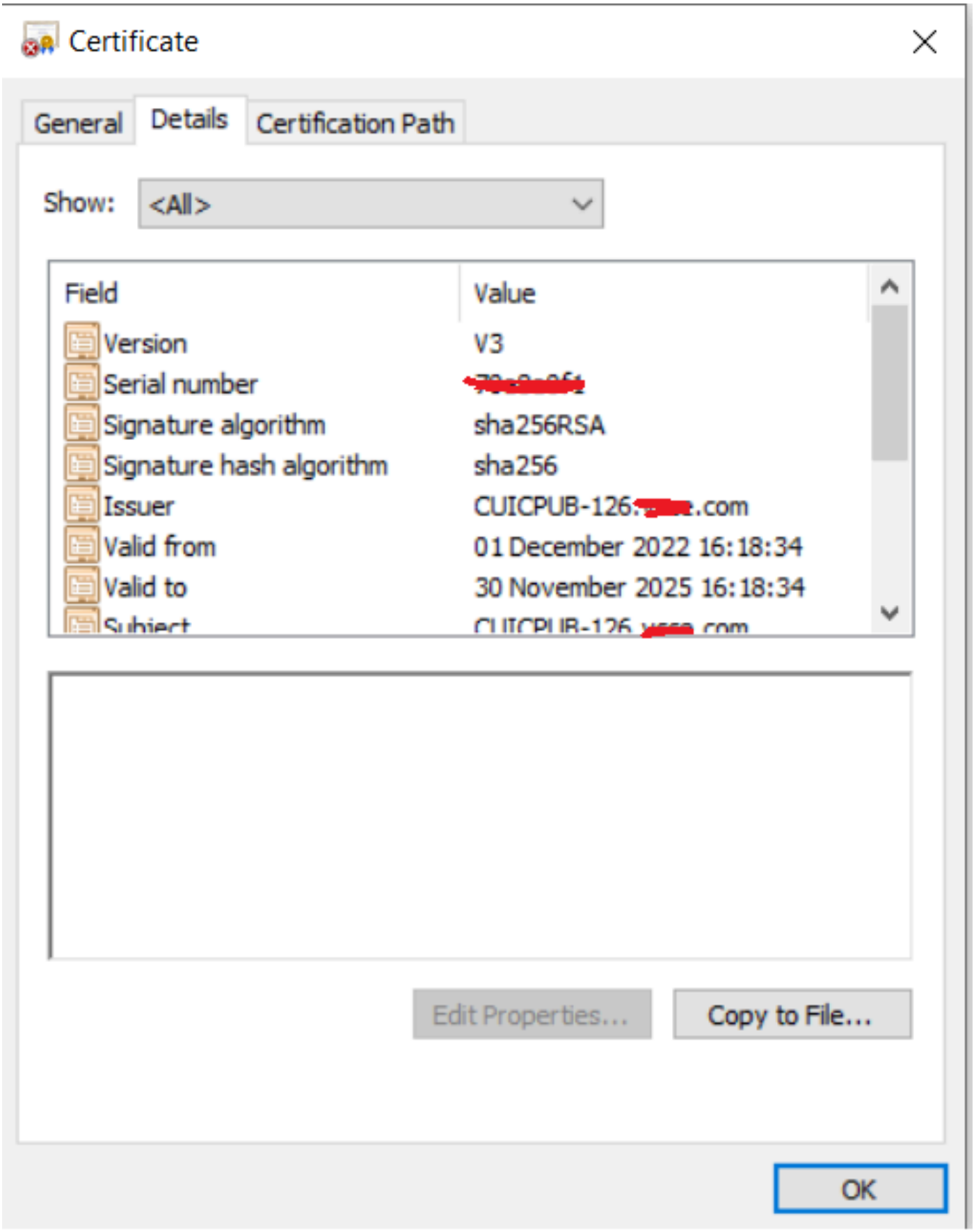
2. Kopieer de ruwe gegevens tussen de kop <ds:X509Certificate></ds:X509Certificate>

3. Open een andere teksteditor en plak de gekopieerde gegevens.

4. Sla het bestand op als .CER-formaat



5. Open het certificaat om de certificaatinformatie te bekijken



Hoe het SAML-certificaat in de AD FS te vervangen

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

2. Open Server Manager en kies AD FS >Tools > AD FS Management

3. Selecteer in de linkerboom de Relying Party Trusts onder de AD FS

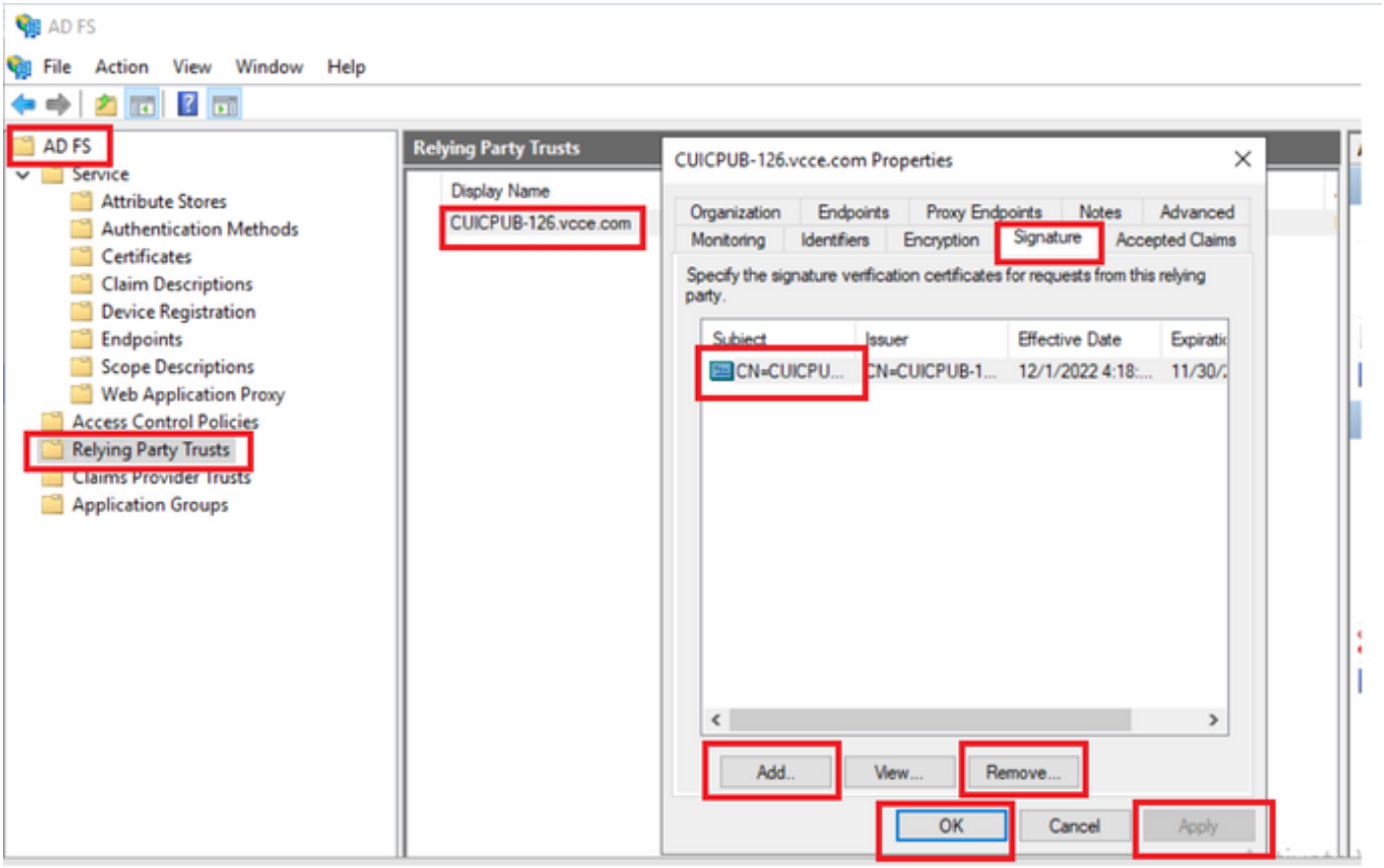
4. Klik met de rechtermuisknop op de Cisco IDs-server en selecteer eigenschappen

5. Navigeer naar het tabblad Handtekening

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

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

8. Toepassen en opslaan



Hoe het SAML-certificaat te regenereren in de Cisco IDs-server

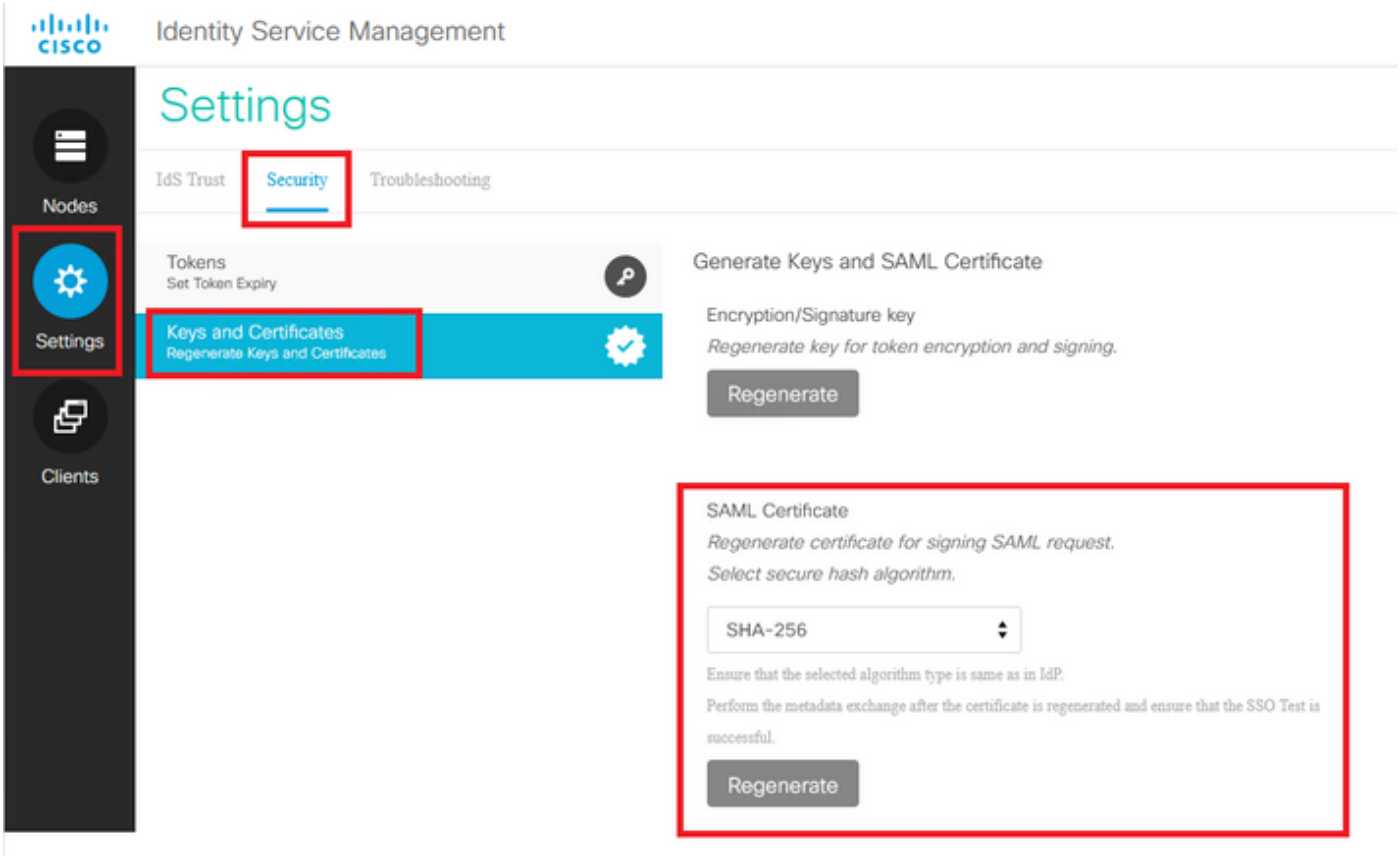
1. Log in op het knooppunt Cisco IDS Publisher met de gebruikersreferenties van de toepassing

2. Klik op het pictogram Settings

3. Navigeren naar het tabblad Beveiliging

4. Selecteer de optie Sleutels en certificaten

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



Test SSO

Wanneer er een wijziging in het SAML-certificaat optreedt, moet u ervoor zorgen dat de TEST-DSB is geslaagd in de Cisco IDs-server en alle toepassingen opnieuw registreren vanaf de CEAdmin-pagina.

1. Ga naar de CEAdmin-pagina vanaf de hoofdserver van AW

2. Log in op het CEAdmin-portal met de rechten op beheerdersniveau

3. Navigeer naar Overzicht > Functies > Single-Sign-On

4. Klik op de knop Registreren onder het kopje Registreer met Cisco Identity Service

5. Test SSO

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.