Id(Identity Service)로 CCE 단일 로그인 문제 해결 - 인증서 관리

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[배경 정보](#)

[SAML 인증서가 만료됨](#)

[솔루션](#)

[IdP(ID 공급자)의 보안 해시 알고리즘 변경](#)

[솔루션](#)

[Cisco IdS 서버 IP 주소 또는 호스트 이름 변경 - 공동 상주 CUIC/LiveData/Id 게시자 또는 독립형 Id 게시자 재구축 - 공동 상주 CUIC/LiveData/Id 가입자 또는 독립형 Id 가입자 재구축](#)

[솔루션](#)

[참조](#)

- [AD FS에 신뢰 신뢰 신뢰 당사자를 추가하는 방법 또는](#)
- [서명된 SAML 어설션을 활성화하는 방법](#)

소개

이 문서에서는 안전하고 명확한 프로세스를 보장하면서 UCCE/PCCE에서 SAML 인증서를 재생성하고 교환하는 세부 단계에 대해 설명합니다.

기고자: Nagarajan Paramasivam, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대해 알고 있으면 유용합니다.

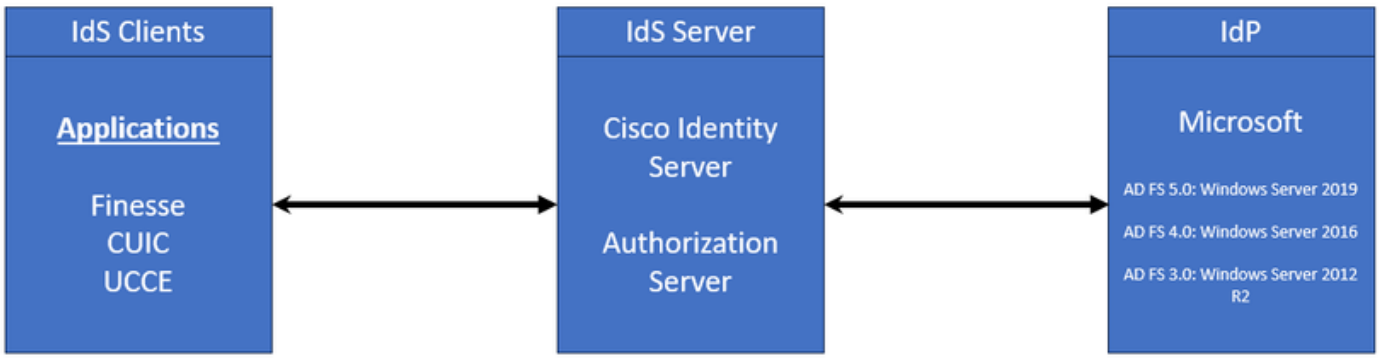
- Packaged/Unified Contact Center Enterprise(PCCE/UCCE)
- VOS(Voice Operating System) 플랫폼
- 인증서 관리
- SAML(Security Assertion Markup Language)

- SSL(Secure Socket Layer)
- AD FS(Active Directory Federation Services)
- 단일 로그인(SSO)

사용되는 구성 요소

이 문서의 정보는 다음 구성 요소를 기반으로 합니다.

- Cisco Identity Service(Cisco Id)
- IdP(ID 공급자) - Microsoft Windows AD FS



이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

UCCE/PCCE에서 Cisco Id(Cisco Identity Service)는 IdP(Identity Provider)와 애플리케이션 간의 권한 부여를 제공합니다.

Cisco Id를 구성할 때 Cisco Id와 IdP 간에 메타데이터 교환을 설정합니다. 이 교환은 신뢰 관계를 설정하며, 그러면 애플리케이션에서 SSO에 Cisco ID를 사용할 수 있습니다. Cisco Id에서 메타데이터 파일을 다운로드하고 IdP에 업로드하여 신뢰 관계를 설정합니다.

SAML 인증서는 SSL 인증서와 유사하며, 특정 상황이 발생하면 SAML 인증서와 마찬가지로 업데이트하거나 변경해야 합니다. Cisco Id(Identity Services) 서버에서 SAML 인증서를 다시 생성하거나 스왑하면 IdP(Identity Provider)와의 신뢰할 수 있는 연결이 끊어질 수 있습니다. 이 경우 Single Sign-On에 의존하는 클라이언트나 사용자가 시스템에 액세스하는 데 필요한 권한을 얻을 수 없는 문제가 발생할 수 있습니다.

이 문서에서는 Cisco IdS 서버에서 새 SAML 인증서를 생성해야 하는 광범위한 일반적인 상황을 다룹니다. 또한 이 새 인증서를 IdP(Identity Provider)에 제공하여 트러스트를 다시 작성하는 방법에 대해서도 설명합니다. 이렇게 하면 클라이언트와 사용자가 문제 없이 Single Sign-On을 계속 사용할 수 있습니다. 목표는 인증서 업데이트 프로세스를 원활하고 혼란 없이 처리하는 데 필요한 모든 정보가 있는지 확인하는 것입니다.

기억해야 할 핵심 사항:

1. SAML 인증서는 Cisco IdS 서버 설치 중에 기본적으로 생성되며 3년 유효합니다

2. SAML 인증서는 자체 서명 인증서임

3. SAML 인증서는 Cisco IDS 게시자 및 가입자에 있는 SSL 인증서입니다

4. SAML 인증서 재생성은 Cisco IDS 게시자 노드에서만 수행할 수 있습니다

5. SAML 인증서에 사용할 수 있는 보안 해시 알고리즘 유형은 SHA-1 및 SHA-256입니다

6. SHA-1 알고리즘은 IdS 11.6에서 사용되고 이전 버전에서는 SHA-256 알고리즘이 IdS 12.0 및 이후 버전에서 사용됩니다

7. IdP(Identity Provider)와 Id(Identity Service)는 모두 동일한 알고리즘 유형을 사용해야 합니다.

8. Cisco IdS SAML 인증서는 Cisco IdS 게시자 노드(sp-<Cisco IdS_FQDN>.xml)에서만 다운로드할 수 있습니다.

9. UCCE/PCCE Single-Sign-On 구성에 대한 내용은 이 링크를 참조하십시오. UCCE 12.6.1 기능 설명서

SAML 인증서가 만료됨

SAML 인증서는 유효기간이 3년(1095일)인 상태로 생성되며 만료 전에 SAML 인증서를 갱신해야 합니다. 만료된 SSL 인증서는 유효하지 않은 인증서로 간주되며 Cisco Id(Identity Service)와 IdP(Identity Provider) 간의 인증서 체인을 끊습니다.

솔루션

1. SAML 인증서 만료 날짜 확인

2. SAML 인증서를 다시 생성합니다.

3. sp.xml 파일 다운로드

4. sp.xml 파일에서 SAML 인증서를 검색합니다.

5. 기존 SAML 인증서를 IdP의 새 SAML 인증서로 교체합니다

6. 자세한 단계는 참조 섹션을 참조하십시오

(참고: {SAML 인증서만 변경되었으므로 IdS 메타데이터를 IdP로 교환할 필요가 없습니다.})

IdP(ID 공급자)의 보안 해시 알고리즘 변경

기존 PCCE/UCCE 환경에서 Single-Sign-On을 사용한다고 가정합니다. IdP 및 Cisco IdS 서버 모두 SHA-1 보안 해시 알고리즘으로 구성되었습니다. SHA-1의 취약점을 고려할 때 보안 해시 알고리즘을 SHA-256으로 변경해야 합니다.

솔루션

1. AD FS Relying Trust Party(SHA-1에서 SHA-256)에서 보안 해시 알고리즘을 변경합니다.

2. Keys and Certificate(키 및 인증서) 아래의 IdS 게시자에서 보안 해시 알고리즘을 변경합니다 (SHA-1에서 SHA-256)

3. IdS 게시자에서 SAML 인증서를 다시 생성합니다.

4. sp.xml 파일 다운로드

5. sp.xml 파일에서 SAML 인증서를 검색합니다.

6. 기존 SAML 인증서를 IdP의 새 SAML 인증서로 교체합니다

7. 자세한 단계는 참조 섹션을 참조하십시오

Cisco IdS 서버 IP 주소 또는 호스트 이름 변경 - 공동 상주 CUIC/LiveData/Id 게시자 또는 독립형 Id 게시자 재구축 - 공동 상주 CUIC/LiveData/Id 가입자 또는 독립형 Id 가입자 재구축

이러한 상황은 자주 발생하지 않으며, SSO(Single Sign-On) 설정으로 다시 시작하여 프로덕션 환경의 SSO 기능이 신속하고 효율적으로 복원되도록 하는 것이 좋습니다. 사용자가 의존하는 SSO 서비스의 중단을 최소화하려면 이러한 재구성에 우선 순위를 두어야 합니다.

솔루션

1. AD FS에서 기존 신뢰 신뢰 당사자 삭제

2. Cisco IdS 서버 tomcat 트러스트에 AD FS SSL 인증서를 업로드합니다

3. sp.xml 파일 다운로드

4. 자세한 단계는 참조 섹션 및 기능 가이드를 참조하십시오

5. AD FS에서 신뢰 신뢰 당사자 구성

6. 청구 규칙 추가

7. 서명된 SAML 어설션 활성화

8. AD FS 페더레이션 메타데이터 다운로드

9. Cisco IdS 서버에 페더레이션 메타데이터 업로드

10. 테스트 SSO 수행

참조

AD FS에 신뢰 신뢰 신뢰 당사자를 추가하는 방법 또는

서명된 SAML 어설션을 활성화하는 방법

자세한 단계는 이 문서를 참조하십시오. UCCE 12.6.1 기능 가이드

AD FS SSL 인증서를 Cisco IdS tomcat 트러스트에 업로드하는 방법

1. AD FS SSL 인증서 다운로드 또는 검색

2. Cisco IdS Publisher OS Administration 페이지에 액세스합니다.

3. OS 관리자 자격 증명으로 로그인합니다

4. 보안 > 인증서 관리로 이동합니다

5. 인증서/인증서 체인 업로드를 클릭하면 팝업 창이 열립니다

6. 드롭다운 메뉴를 클릭하고 인증서 용도의 tomcat-trust를 선택합니다

7. 찾아보기를 클릭하고 AD FS SSL 인증서를 선택합니다

8. 업로드를 클릭합니다

(참고: {신뢰 인증서가 가입자 노드에 복제됩니다. 구독자 노드에 업로드할 필요가 없습니다.})

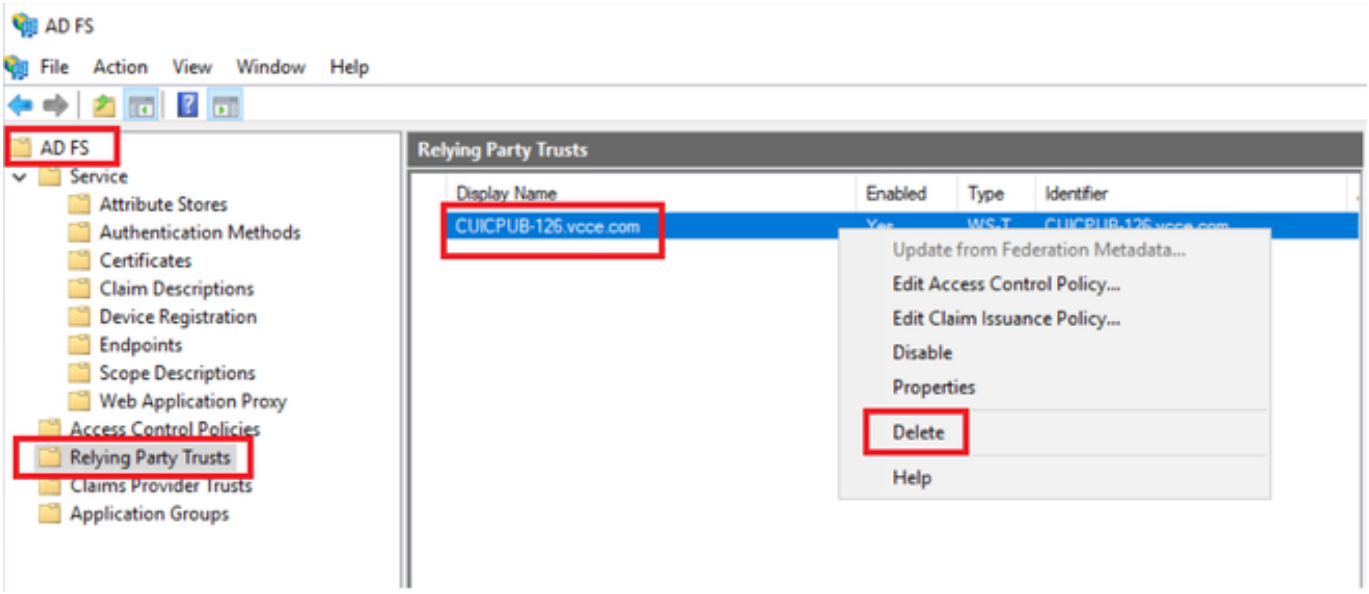
AD FS에서 신뢰 신뢰 신뢰 당사자를 삭제하는 방법

1. 관리자 권한 자격 증명을 사용하여 IdP(Identity Provider) 서버에 로그인합니다

2. 서버 관리자를 열고 AD FS > 도구 > AD FS 관리를 선택합니다

3. 왼쪽 트리에서 AD FS 아래의 당사자 Trust를 선택합니다

4. Cisco Id 서버를 마우스 오른쪽 버튼으로 클릭하고 Delete(삭제)를 선택합니다



IdP(ID 공급자)에 구성된 보안 해시 알고리즘을 확인하거나 변경하는 방법

1. 관리자 권한 자격 증명을 사용하여 IdP(Identity Provider) 서버에 로그인합니다

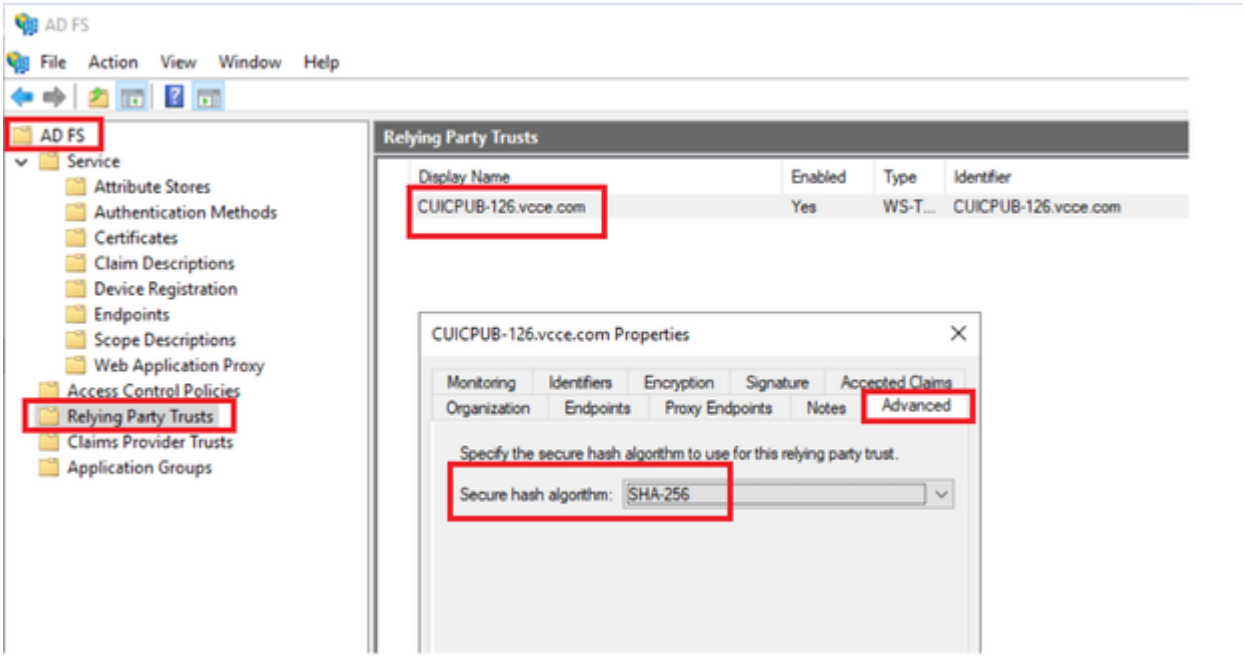
2. 서버 관리자를 열고 AD FS > 도구 > AD FS 관리를 선택합니다

3. 왼쪽 트리에서 AD FS 아래의 당사자 Trust를 선택합니다

4. Cisco IdS 서버를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다

5. 고급 탭으로 이동합니다

6. Secure Hash Algorithm(보안 해시 알고리즘) 옵션은 AD FS 서버에 구성된 보안 해시 알고리즘을 표시합니다.



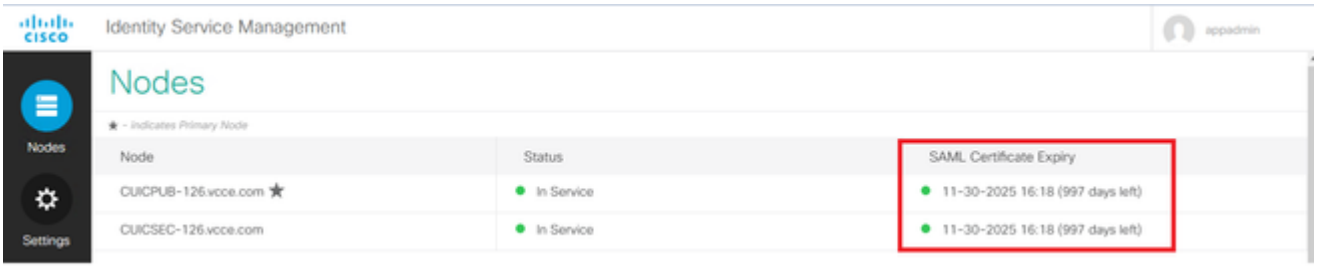
7. 드롭다운 메뉴를 클릭하고 원하는 보안 해시 알고리즘을 선택합니다.

Cisco IdS 서버 SAML 인증서 만료 날짜를 확인하는 방법

1. 애플리케이션 사용자 자격 증명을 사용하여 Cisco IdS 서버 게시자 또는 가입자 노드에 로그인합니다

2. 페이지에 성공적으로 로그인하면 Identity Service Management(ID 서비스 관리) > Nodes(노드)가 표시됩니다.

3. Cisco Id 게시자 및 가입자 노드, 상태 및 SAML 인증서 만료를 표시합니다



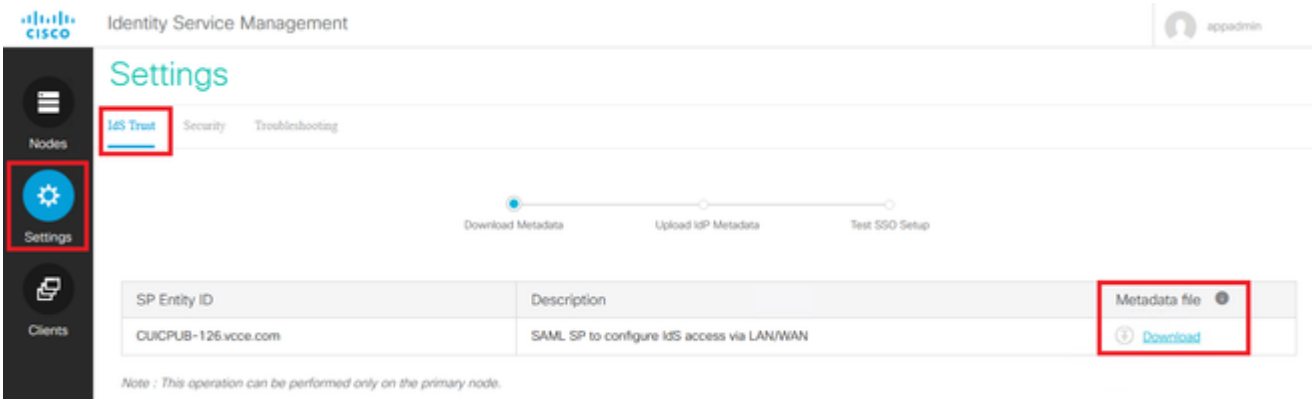
Cisco IdS 서버의 메타데이터를 다운로드하는 방법

1. 애플리케이션 사용자 자격 증명을 사용하여 Cisco Id 게시자 노드에 로그인합니다

2. 설정 아이콘을 클릭합니다

3. IDS Trust 탭으로 이동합니다

4. 다운로드 링크를 클릭하여 Cisco IdS 클러스터의 메타데이터를 다운로드합니다



sp.xml 파일에서 SAML 인증서를 검색하는 방법

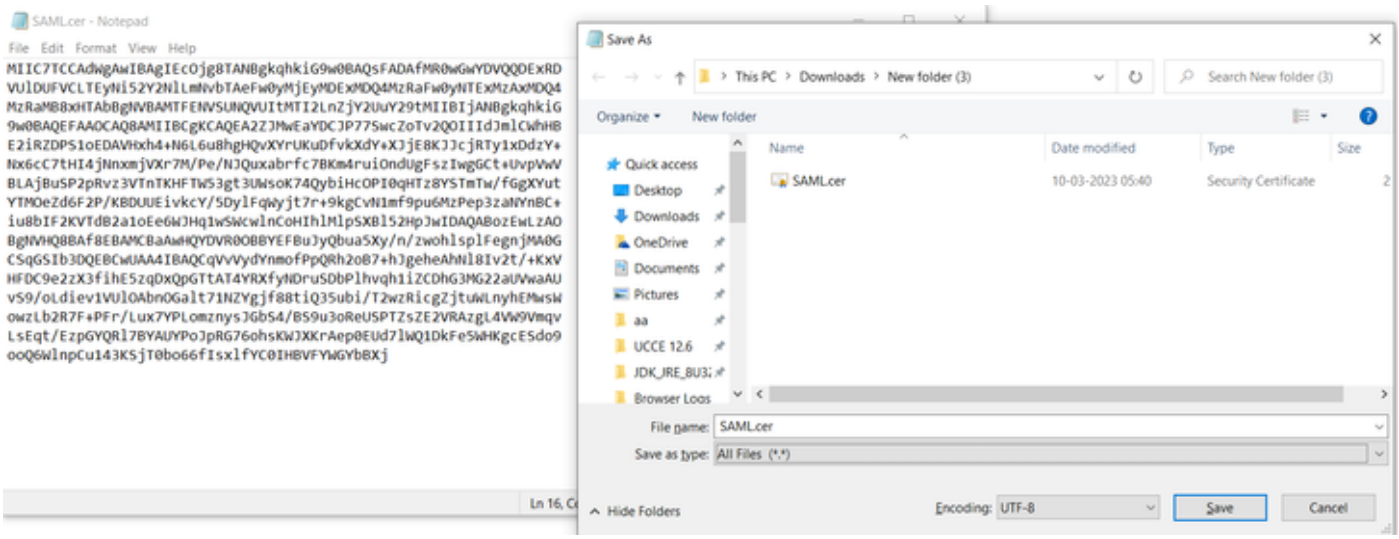
1. 텍스트 편집기를 사용하여 sp.xml 파일을 엽니다

2. 헤더 <ds:X509Certificate></ds:X509Certificate> 간에 원시 데이터를 복사합니다.

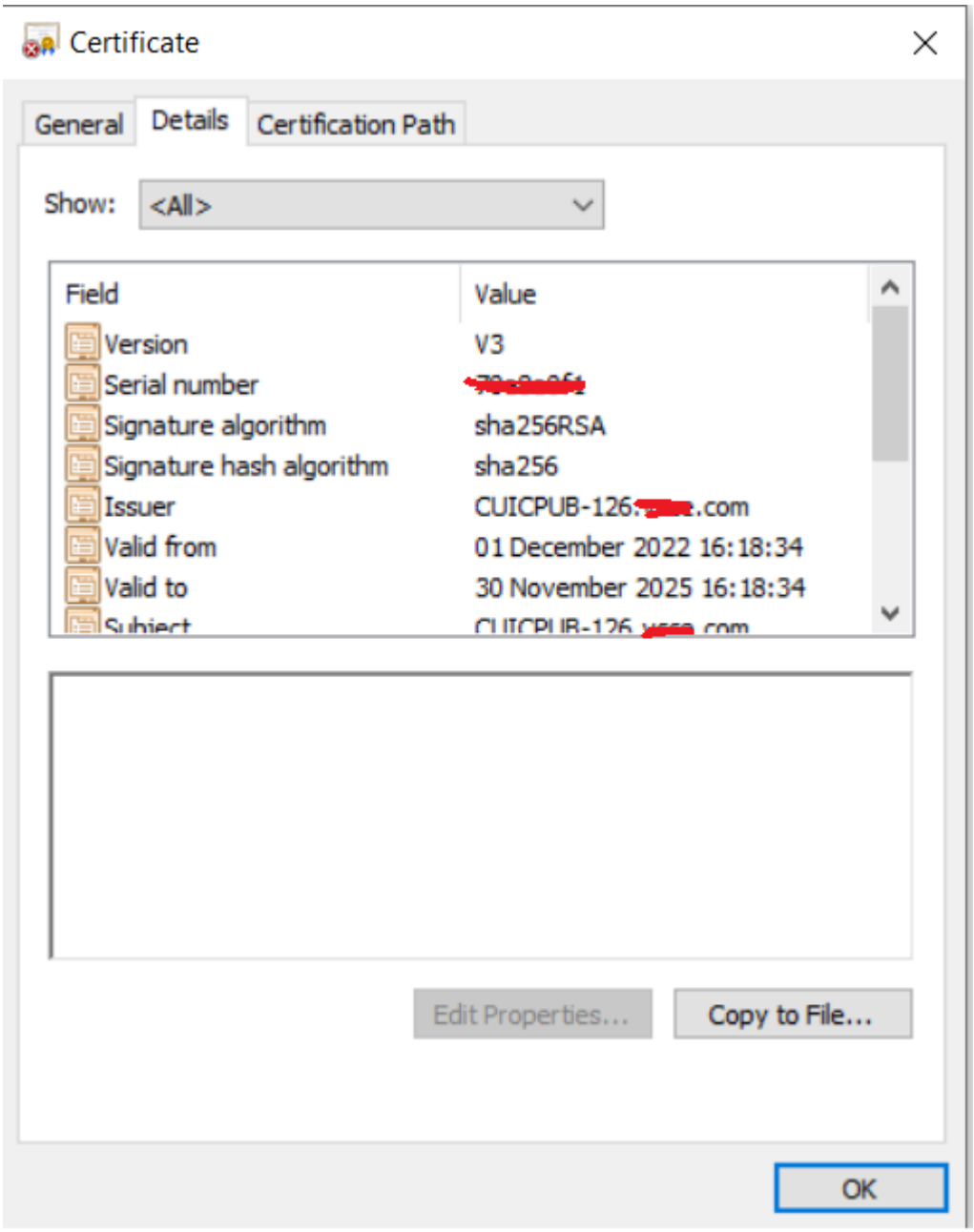
```
<ds:X509Certificate>MIIC7TCCAdWgAwIBAgIEcOjg8TANBgkqhkiG9w0BAQsFADAfMR0wGwYDVQQDExRD
VUlDUFVCLTEyNi52Y2NlLmNvbTAeFw0yMjEyMDExMDQ4MzRaFw0yNTExMzAxMDQ4
MzRaMB8xHTAbBgNVBAMTFENVSUNQVUItMTI2LnZjY2UuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ZJMwEaYDCJP77SwcZoTv2QOIIIdJmlCWhHB
E2iRZDPS1oEDAVHxh4+N6L6u8hgHQvXYrUKuDfvkXdY+XJjE8KJJcjRTy1xDdzY+
Nx6cC7tHI4jNnxmjVXr7M/Pe/NJQuxabrfc7BKm4ruiOndUgFszIwgGCt+UvpVwV
BLAjBuSP2pRvz3VTnTKHFTW53gt3UWsoK74QybiHcOPI0qHTz8YSTmTw/fGgXYut
YTMOeZd6F2P/KBDUUEivkcY/5DylFqWyjt7r+9kgCvN1mf9pu6MzPep3zaNYnBC+
iu8bIF2KVTdB2a1oEe6WJHq1wSWcwlnCoHIhlMlpSXBl52HpJwIDAQABozEwLzAO
BgNVHQ8BAf8EBAMCBaAwHQYDVR0OBBYEFBuJyQbua5Xy/n/zwohlsplFegnjMA0G
CSqGSIb3DQEBCwUAA4IBAQCqVvVydYnmofPpQRh2oB7+hJgeheAhNl8Iv2t/+KxV
HFDC9e2zX3fihE5zqDxQpGTtAT4YRXfyNDruSDbPlhvqh1iZCDhG3MG22aUVwaAU
vS9/oLdiev1VUlOAbnOGalt71NZYgjf88tiQ35ubi/T2wzRicgZjtuWLnyhEMwsW
owzLb2R7F+PFr/Lux7YPLomznysJGbS4/BS9u3oReUSPTZsZE2VRAzgL4VW9Vmqv
LsEqt/EzpGYQRl7BYAUYPoJpRG76ohsKWJXKrAep0EUd71WQ1DkFe5WHKgcESdo9
ooQ6WlnpCu143KSjT0bo66fIsxlfYC0IHBVFYWGYbBXj</ds:X509Certificate>
```

3. 다른 텍스트 편집기를 열고 복사한 데이터를 붙여넣습니다

4. 파일을 저장합니다.CER 형식



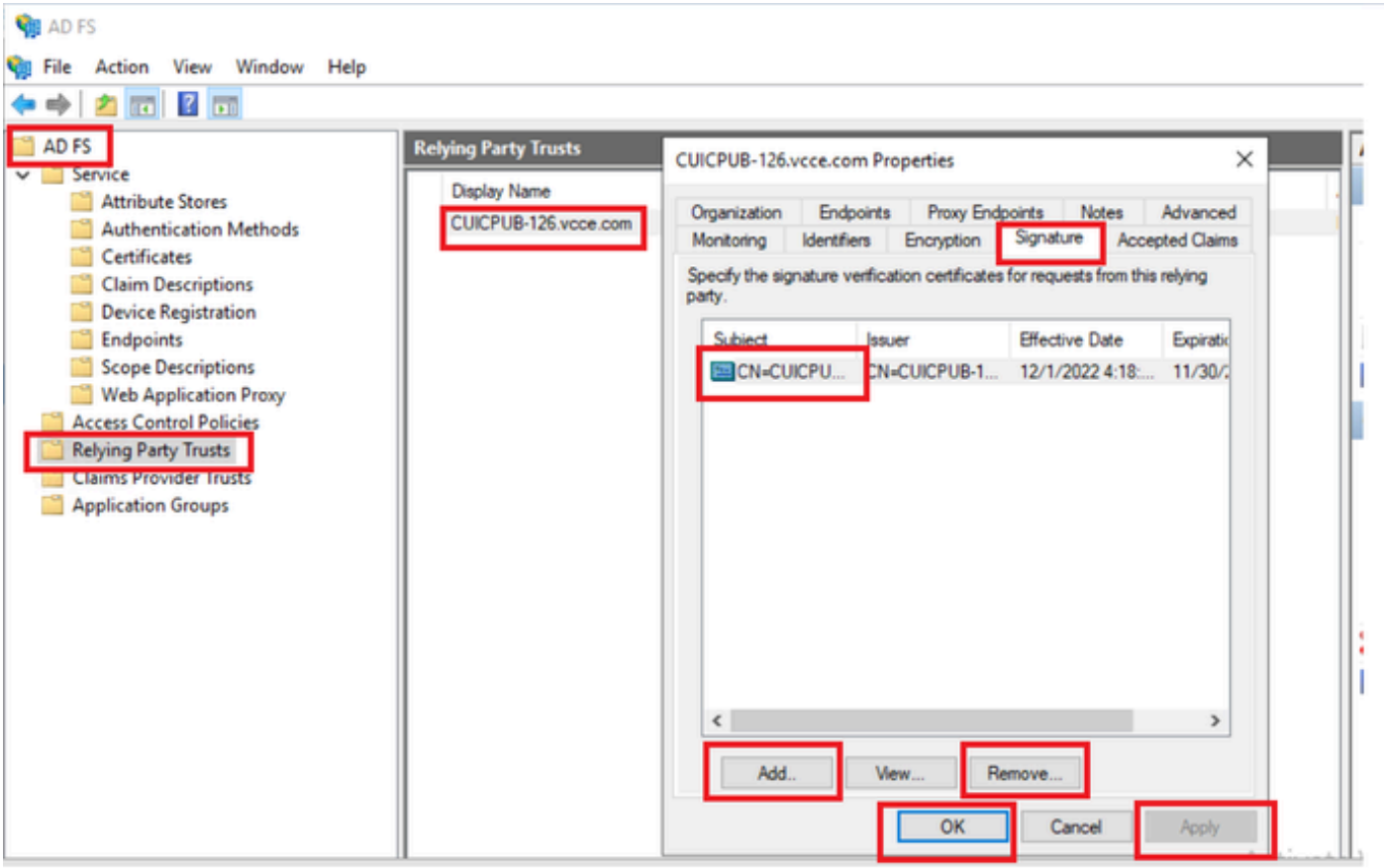
5. 인증서를 열어 인증서 정보를 검토합니다



AD FS에서 SAML 인증서를 교체하는 방법

1. sp.xml에서 검색된 AD FS 서버에 SAML 인증서 파일을 복사합니다
2. 서버 관리자를 열고 AD FS > 도구 > AD FS 관리를 선택합니다
3. 왼쪽 트리에서 AD FS 아래의 당사자 Trust를 선택합니다
4. Cisco IdS 서버를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다
5. 서명 탭으로 이동합니다
6. 추가를 클릭하고 새로 생성된 SAML 인증서를 선택합니다
7. 이전 SAML 인증서를 선택하고 제거를 클릭합니다

8. 적용 및 저장



Cisco IdS 서버에서 SAML 인증서를 재생성하는 방법

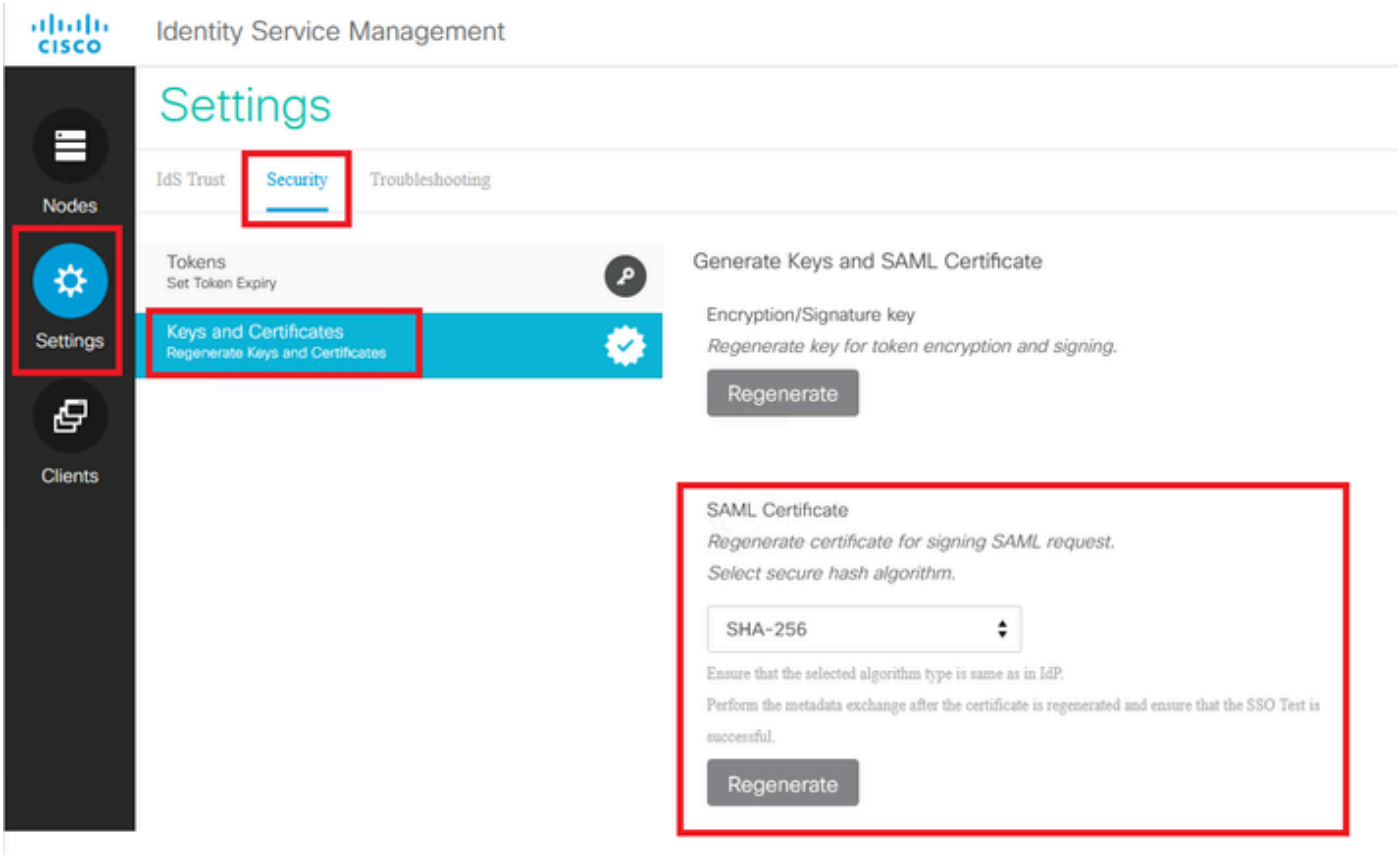
1. 애플리케이션 사용자 자격 증명을 사용하여 Cisco Id 게시자 노드에 로그인합니다

2. 설정 아이콘을 클릭합니다

3. 보안 탭으로 이동합니다

4. 키 및 인증서 옵션을 선택합니다

5. saml certificate 섹션(강조 표시) 아래의 Regenerate(재생성) 버튼을 클릭합니다.



SSO 테스트

SAML 인증서가 변경될 때마다 Cisco IdS 서버에서 테스트 SSO가 성공했는지 확인하고 CCEAdmin 페이지에서 모든 애플리케이션을 다시 등록합니다.

1. 주도자 AW 서버에서 CCEAdmin 페이지에 액세스

2. 관리자 레벨 권한을 사용하여 CCEAdmin 포털에 로그인합니다.

3. 개요 > 기능 > Single-Sign-On으로 이동합니다

4. Cisco Identity Service에 등록 아래에서 등록 버튼을 클릭합니다

5. 테스트 SSO 수행

Azure 인증서 재생성

1. Publisher에서만 IDS에서 인증서를 다시 생성하면 게시자와 구독자 모두에 대해 인증서가 자동으로 생성됩니다.
2. IDS에서 메타데이터를 다운로드하고 IDP/Azure에 업로드합니다.
3. IDP/Azure에서 인증서를 갱신합니다. 이렇게 하면 Azure의 메타데이터가 완전히 변경되고 Microsoft Azure에서 서명되어 .pfx의 요구 사항이 해결됩니다.
4. 게시자에서만 IDP/Azure에서 Cisco IDS로 메타데이터를 업로드합니다.
5. IDS에서 SSO 테스트

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.