UCCE(Unified Contact Center Enterprise) SSO(Single Sign On) 인증서 및 컨피그레이션

목차

소개

이 문서에서는 UCCE SSO에 필요한 인증서 컨피그레이션에 대해 설명합니다. 이 기능의 컨피그레이션에는 HTTPS, 디지털 서명 및 암호화용 여러 인증서가 포함됩니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- UCCE 릴리스 11.5
- Microsoft AD(Active Directory) - Windows Server에 설치된 AD
- ADFS(Active Directory Federation Service) 버전 2.0/3.0

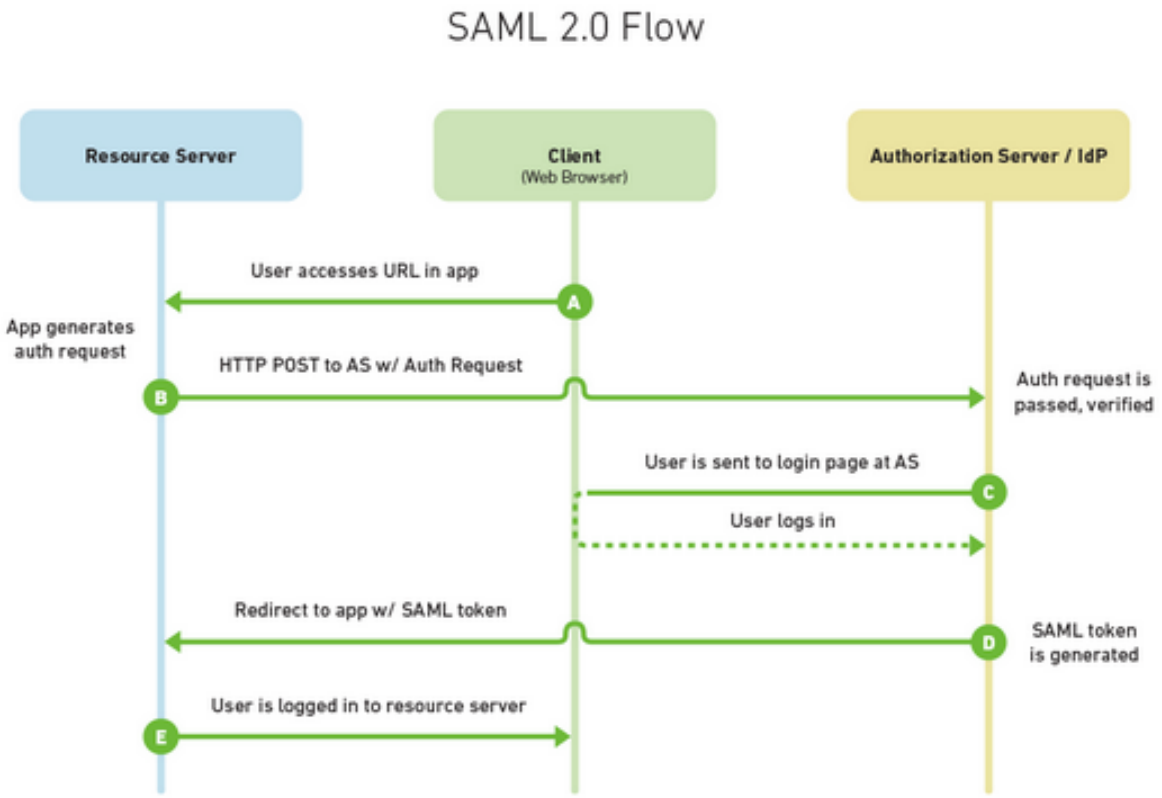
사용되는 구성 요소

UCCE 11.5

Windows 2012 R2

Part A. SSO 메시지 흐름

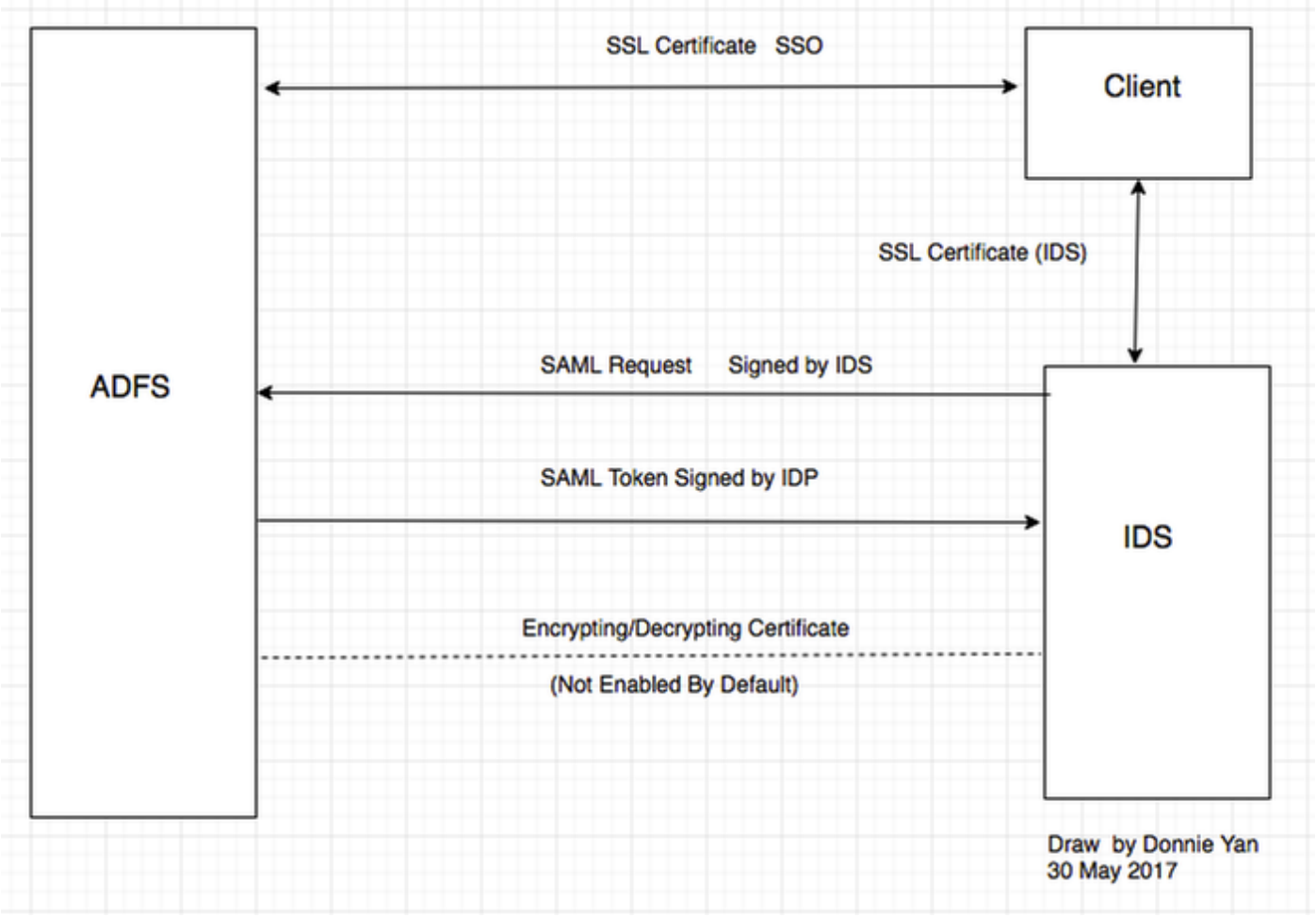
The most common SAML flow is shown below:



SSO가 활성화된 경우 에이전트가 Finesse 데스크톱에 로그인할 때:

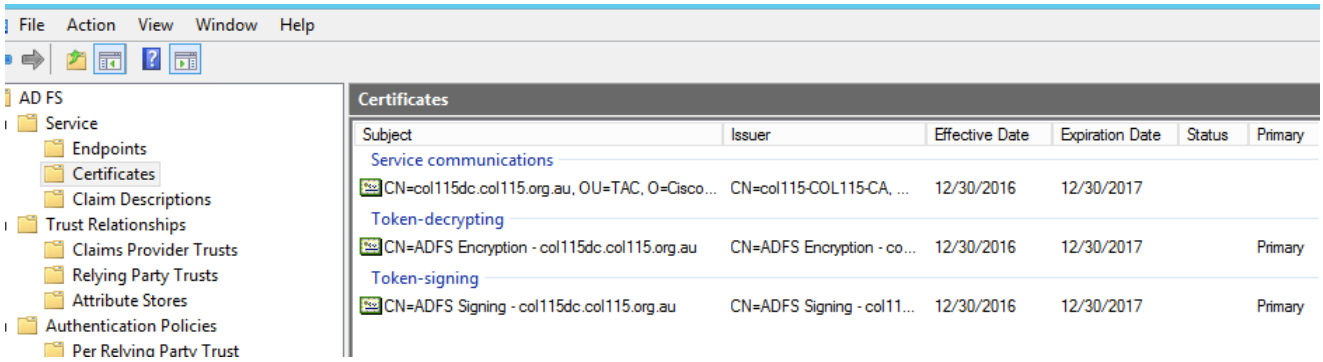
- Finesse 서버는 IDS(Identity Service)와 통신하도록 에이전트 브라우저를 리디렉션합니다.
- IDS는 에이전트 브라우저를 SAML 요청이 있는 IDP(Identity Provider)로 리디렉션합니다.
- IDP는 SAML 토큰을 생성하여 IDS 서버로 전달합니다.
- 토큰이 생성되면 에이전트가 애플리케이션을 탐색할 때마다 로그인에 이 유효한 토큰을 사용합니다

Part B. IDP 및 IDS에 사용되는 인증서



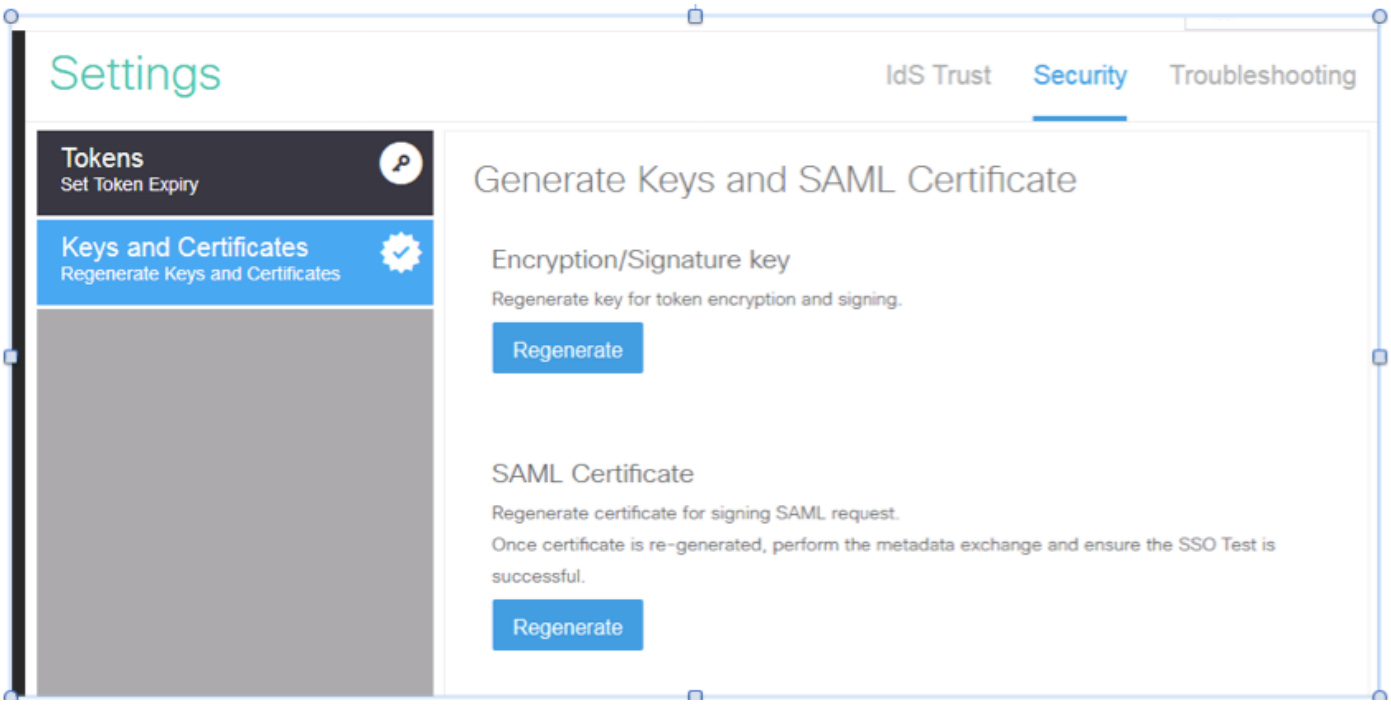
IDP 인증서

- SSL 인증서(SSO)
- 토큰 서명 인증서
- 토큰 - 암호 해독

1. 

IDS 인증서

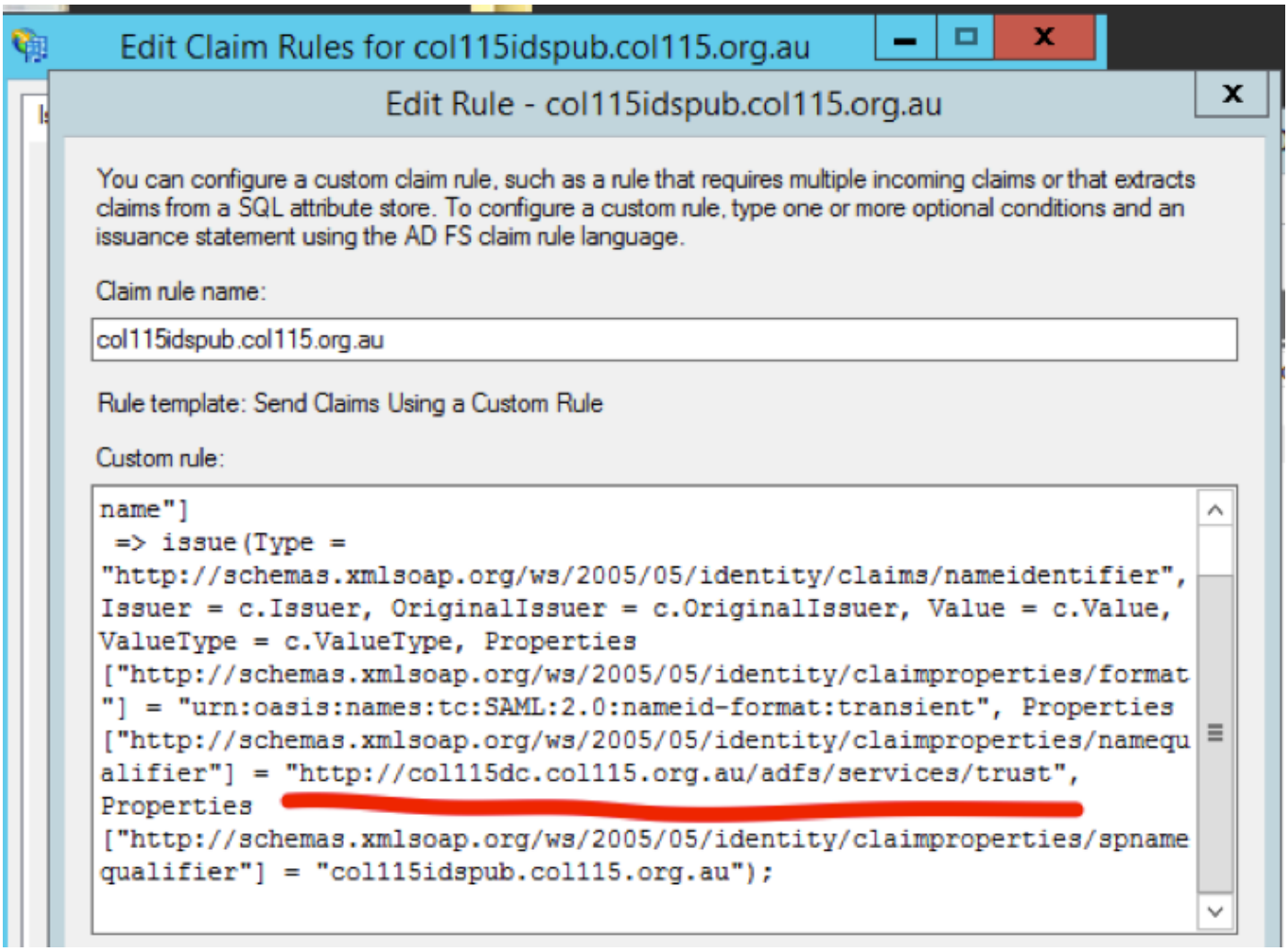
- SAML 인증서
- 서명 키
- 암호화 키



Part C. IDP 인증 세부 사항 및 구성

SSL 인증서(SSO)

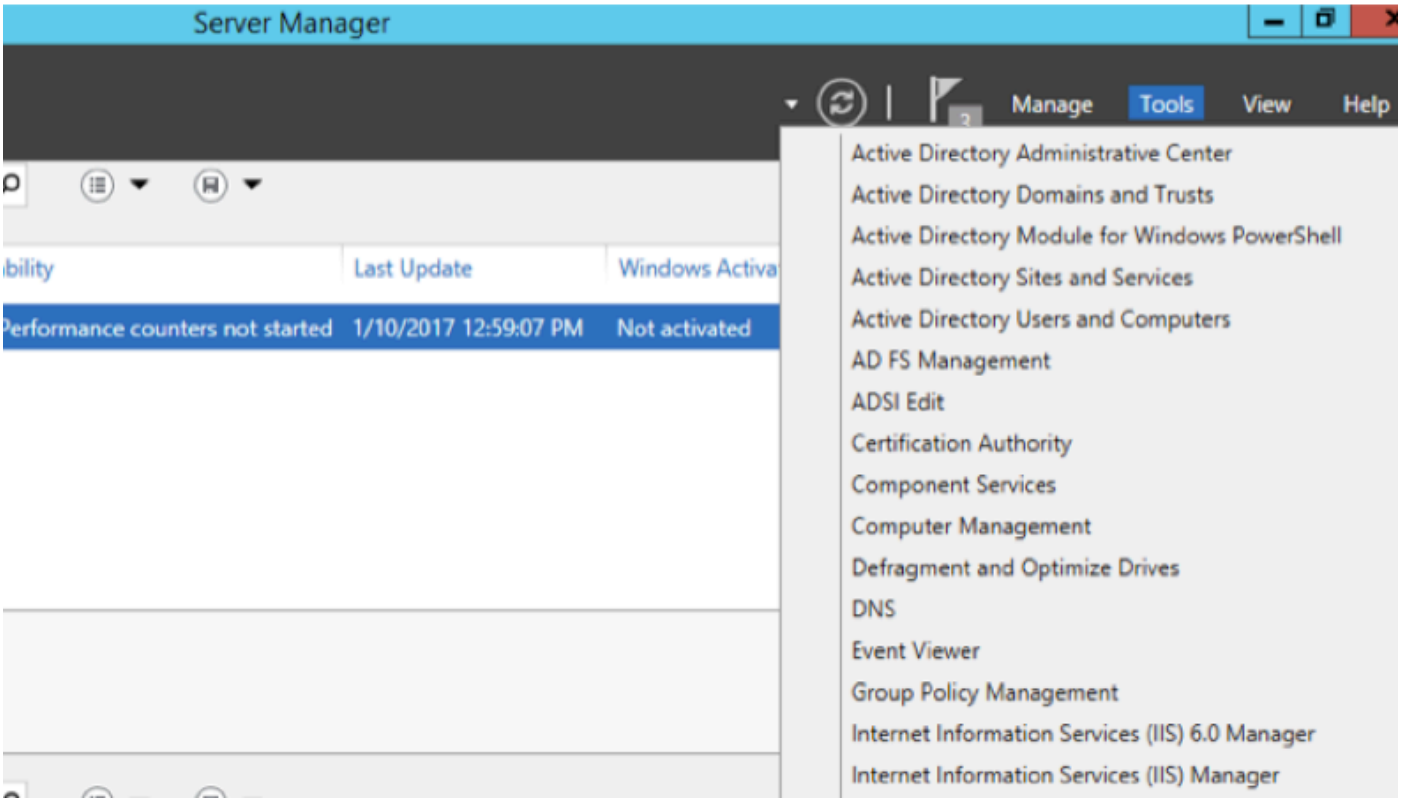
- 이 인증서는 IDP와 클라이언트 간에 사용됩니다. 클라이언트가 SSO 인증서를 신뢰해야 함
- SSL 인증서는 클라이언트와 IDP 서버 간의 세션을 암호화하기 위해 배치됩니다. 이 인증서는 AD FS에만 해당되지 않으며 IIS에만 해당됩니다.
- SSL 인증서의 주체는 AD FS 컨피그레이션에 사용된 이름과 일치해야 합니다

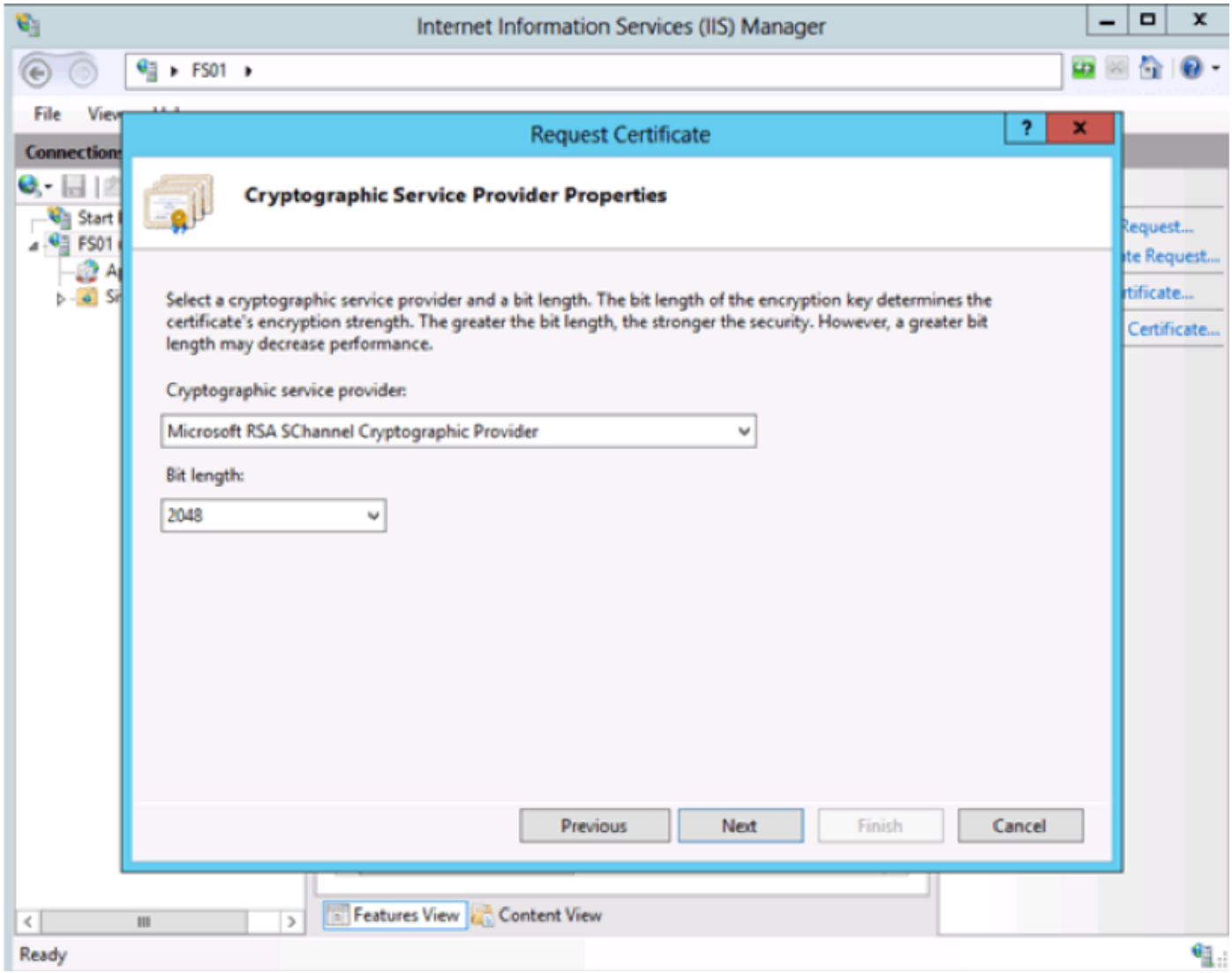


SSO용 SSL 인증서 구성 단계(내부 CA가 서명된 로컬 랩)

1단계. CSR(Certificate Signing Request)을 사용하여 SSL 인증서를 생성하고 내부 CA에서 AD FS에 대해 서명합니다.

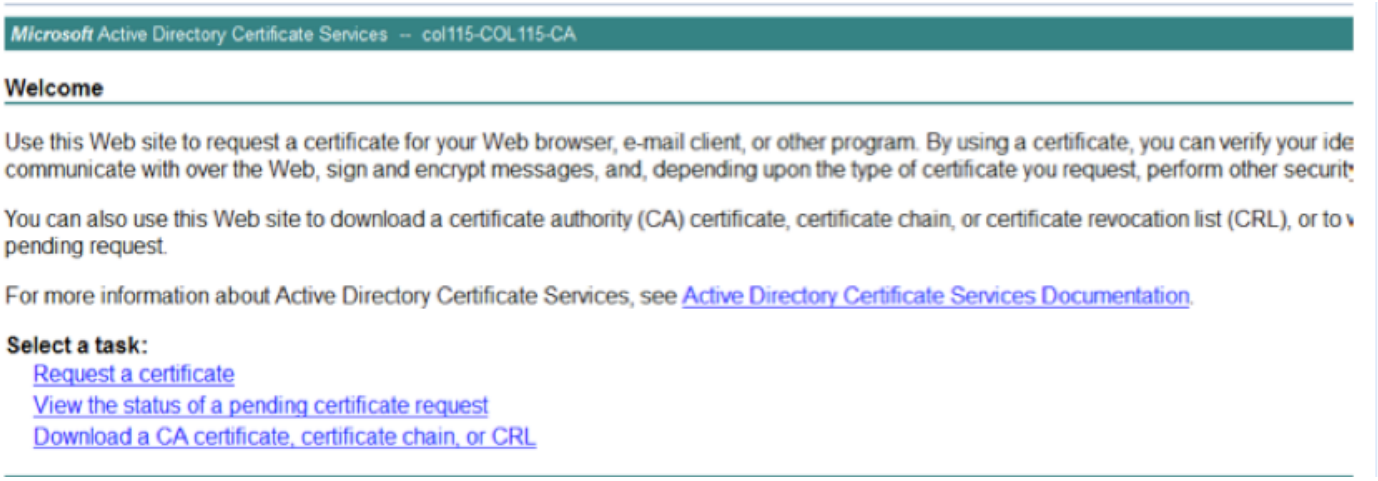
1. 서버 관리자를 엽니다.
2. Tools를 클릭합니다.
3. 인터넷 정보 서비스(IIS) 관리자를 클릭합니다.
4. 로컬 서버를 선택합니다.
5. Server Certificates를 선택합니다.
6. 피쳐 열기(Open Feature)(액션 패널)를 클릭합니다.
7. 인증서 요청 생성을 클릭합니다.
8. 암호화 서비스 공급자를 기본값으로 둡니다.
9. Bit Length(비트 길이)를 2048로 변경합니다.
10. Next(다음)를 클릭합니다.
11. 요청한 파일을 저장할 위치를 선택하십시오.
12. Finish(마침)를 클릭합니다.


Server Manager
Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) 6.0 Manager
Internet Information Services (IIS) Manager
Last Update
Windows Activa
Performance counters not started
1/10/2017 12:59:07 PM
Not activated


Internet Information Services (IIS) Manager
FS01
File
Connections
Request Certificate
Cryptographic Service Provider Properties
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.
Cryptographic service provider:
Microsoft RSA SChannel Cryptographic Provider
Bit length:
2048
Previous
Next
Finish
Cancel
Features View
Content View
Ready

2단계. CA는 1단계에서 생성된 CSR에 서명합니다.

1. 이 CSR http:<CA Server ip address>/certsrv/를 사용하려면 CA 서버를 엽니다.
2. Request a certificate를 클릭합니다.
3. Advanced certificate request를 클릭합니다.
4. CSR을 Based-64 인코딩 인증서 요청에 복사합니다.
5. 제출합니다.
6. 서명된 인증서를 다운로드합니다.



3단계. 서명된 인증서를 다시 ADFS 서버에 설치하고 ADFS 기능에 할당합니다.

1. 서명된 인증서를 다시 AD FS 서버에 설치합니다. 이 작업을 수행하려면 서버 관리자>도구>인터넷 정보 서비스(IIS) 관리자>를 엽니다.

Local Server(로컬 서버)>Server Certificate(서버 인증서)>Open Feature(Action Panel)(기능 열기)).

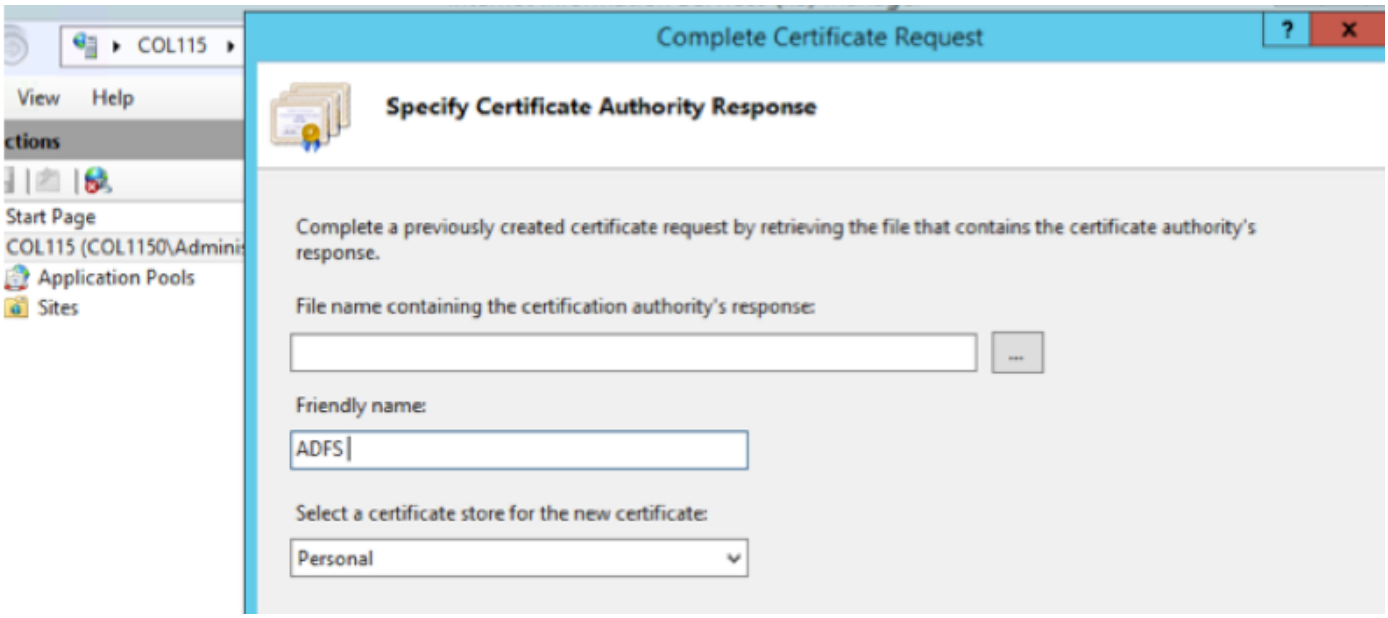
2. Complete Certificate Request를 클릭합니다.

3. 제3자 인증서 제공자에서 완료 및 다운로드한 전체 CSR 파일의 경로를 선택합니다.

4. 인증서의 이름을 입력합니다.

5. 인증서 저장소로 개인을 선택합니다.

6. 확인을 클릭합니다.



7. 이 단계에서는 모든 인증서가 추가되었습니다. 이제 SSL 인증서 할당이 필요합니다.

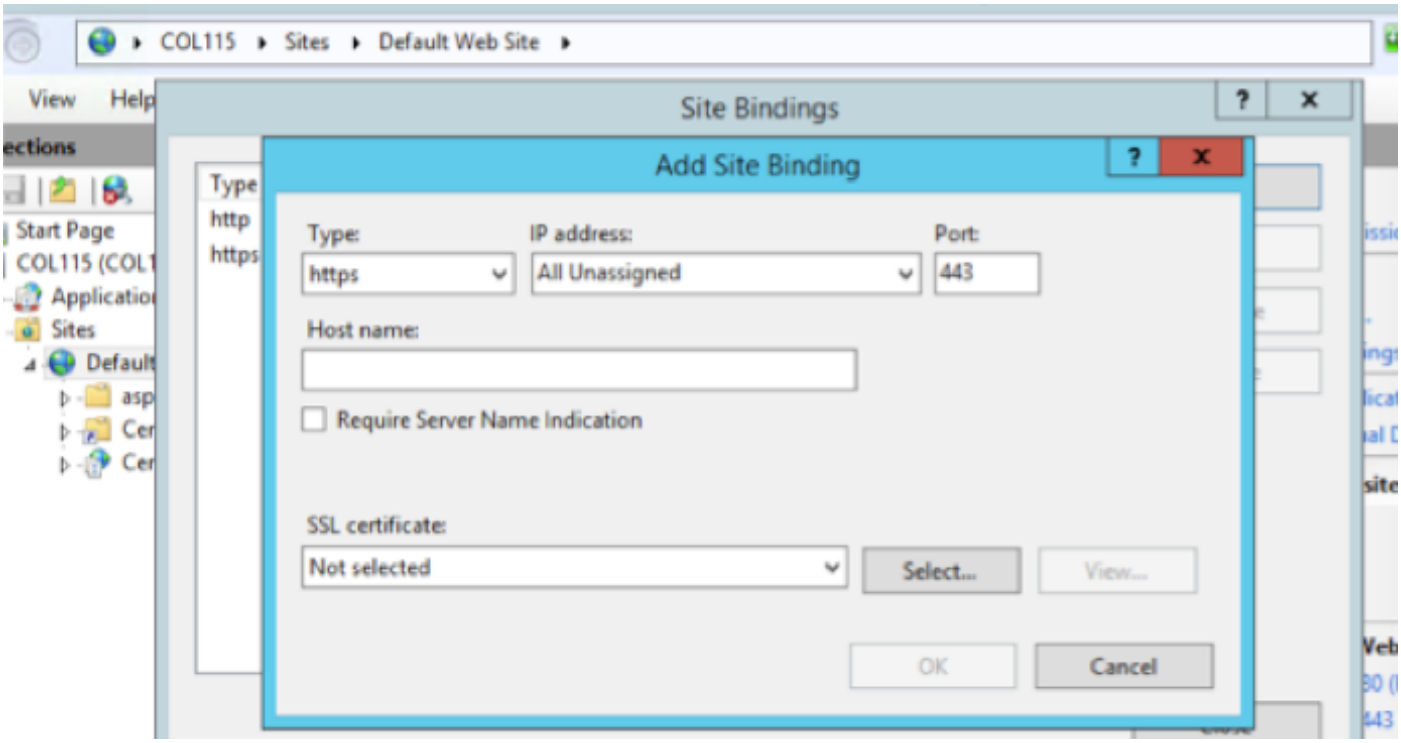
8. 로컬 서버를 >사이트 확장>기본 웹 사이트 선택 >바인딩 클릭(작업 창)을 확장합니다.

9. 추가를 클릭합니다.

10. 유형을 HTTPS로 변경합니다.

11. 드롭다운 메뉴에서 인증서를 선택합니다.

12. 확인을 클릭합니다.



이제 AD FS 서버에 대한 SSL 인증서가 할당되었습니다.

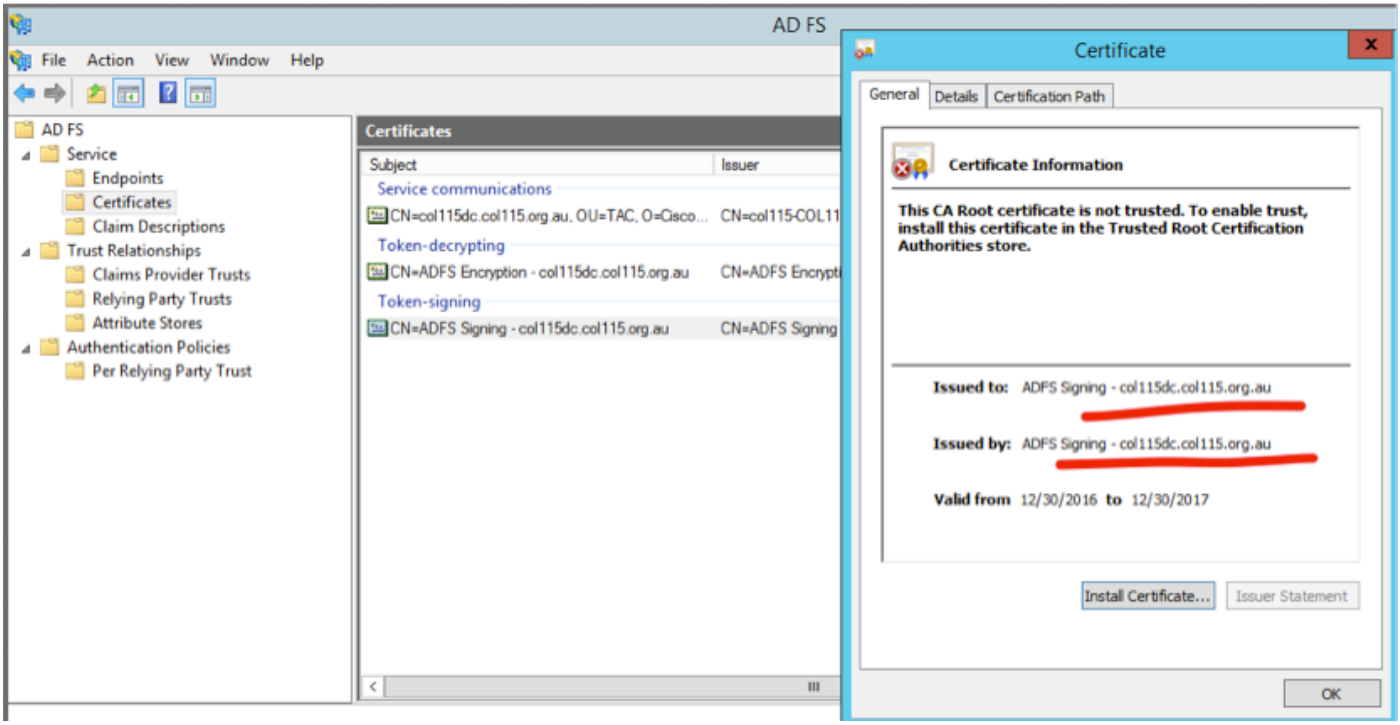
참고: ADFS 기능을 설치하는 동안 이전 SSL 인증서를 사용해야 합니다.

토큰 서명 인증서

AD FS는 토큰 서명 인증서에 대해 자체 서명 인증서를 생성합니다. 기본적으로 1년 동안 유효합니다.

IDP에서 생성된 SAML 토큰은 ADFS 개인 키(Token Signing Certificate Private Part)에 의해 서명됩니다. 그런 다음 IDS는 AD FS 공개 키를 사용하여 확인합니다. 서명된 토큰이 수정되지 않았음을 보장합니다.

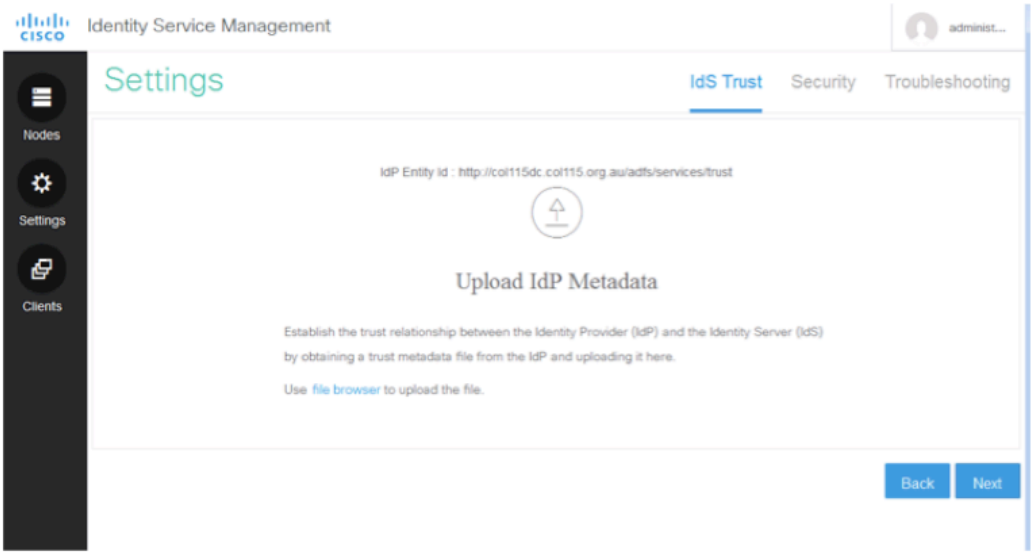
토큰 서명 인증서는 사용자가 신뢰 당사자 애플리케이션(Cisco IDS)에 액세스해야 할 때마다 사용됩니다.



Cisco IDS 서버는 Token Singing Certificate의 공개 키를 어떻게 받습니까?

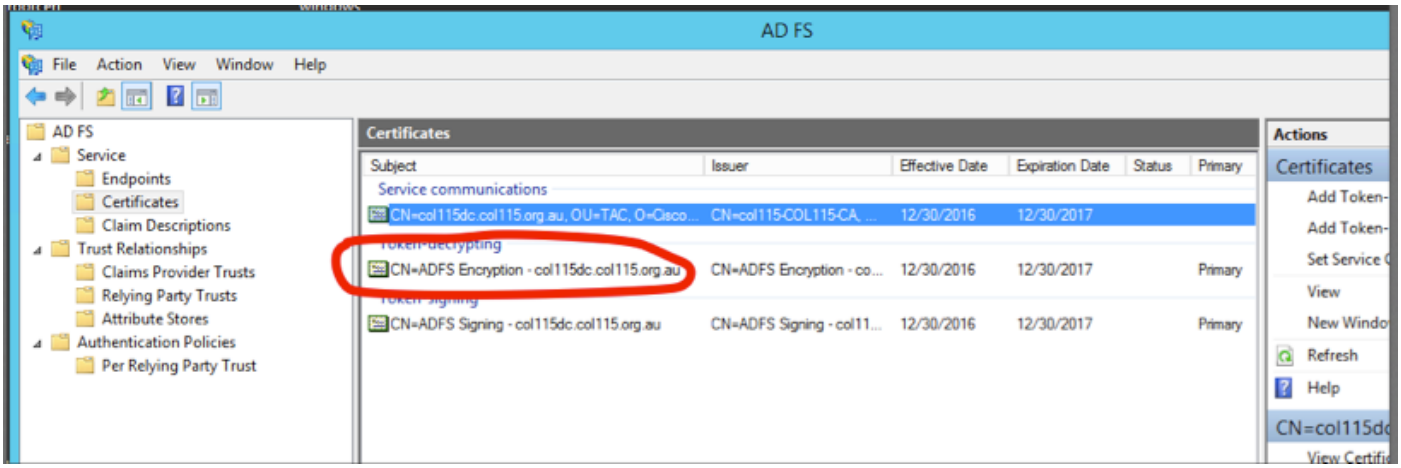
이는 AD FS 메타데이터를 IDS 서버에 업로드한 다음 AD FS의 공개 키를 IDS 서버에 전달하는 방식으로 수행됩니다. 이러한 방식으로 IDS는 AD FS 서버의 공개 키를 가져옵니다.

AD FS에서 IDP 메타데이터를 다운로드해야 합니다. IDP 메타데이터를 다운로드하려면 https://<FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml 링크를 참조하십시오.



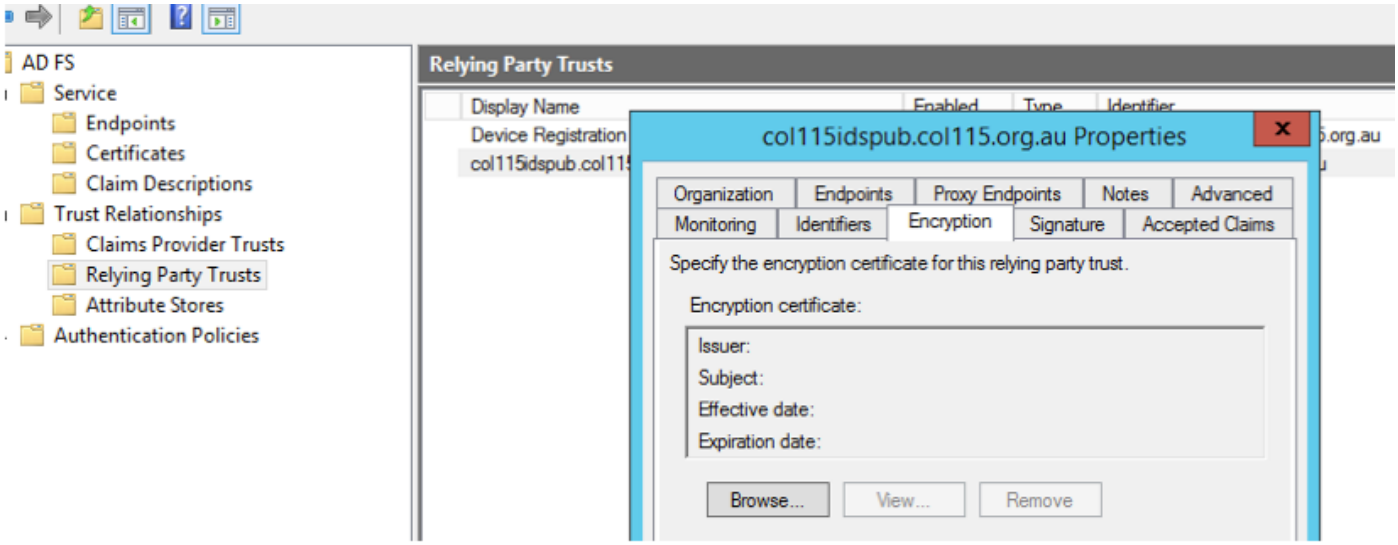
AD FS 메타데이터에서
AD FS 메타데이터를 IDS에 업로드
토큰 암호 해독

이 인증서는 AD FS 서버(자체 서명)에 의해 자동으로 생성됩니다. 토큰에 암호화가 필요한 경우 AD FS는 IDS 공개 키를 사용하여 해독합니다. 그러나 AD FS 토큰 암호 해독을 볼 때 토큰이 암호화됨을 의미하지는 않습니다.



토큰 암호화가 특정 신뢰 당사자 애플리케이션에 대해 활성화되었는지 확인하려면 특정 신뢰 당사자 애플리케이션의 암호화 탭을 확인해야 합니다.

이 그림에서는 토큰 암호화가 활성화되지 않았음을 보여 줍니다.



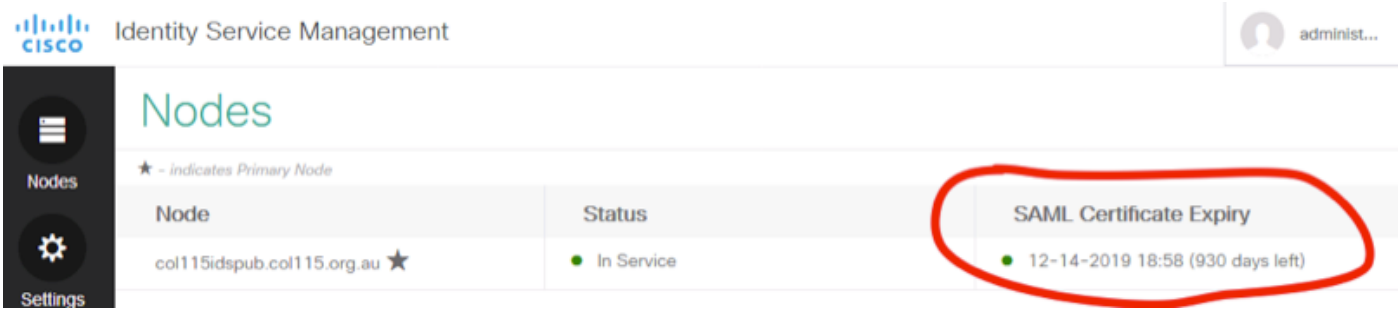
암호화가 활성화되지 않았습니다.

Part D. Cisco IDS 측 인증서

- SAML 인증서
- 암호화 키
- 서명 키

SAML 인증서

이 인증서는 IDS 서버(자체 서명)에 의해 생성됩니다. 기본적으로 3년간 유효합니다.

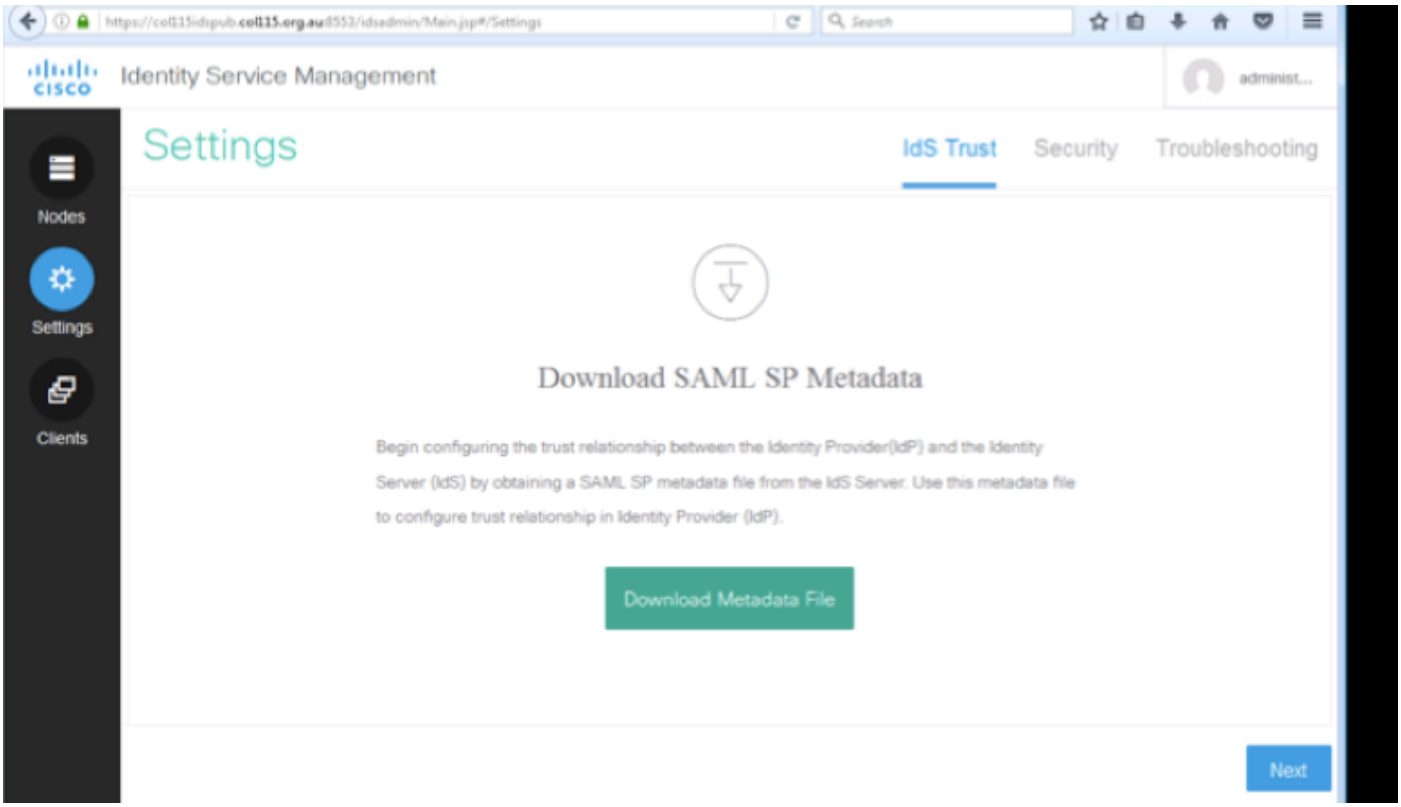


이 인증서는 SAML 요청에 서명하고 IDP(ADFS)에 전송하는 데 사용됩니다. 이 공개 키는 IDS 메타데이터에 있으며 ADFS 서버로 가져와야 합니다.

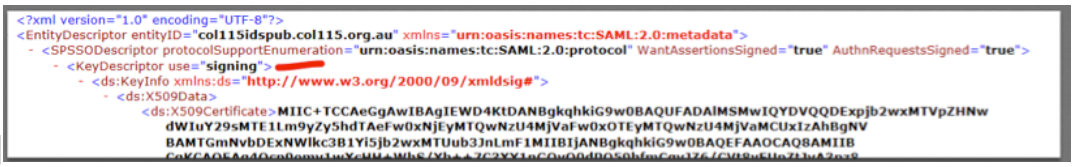
1. IDS 서버에서 SAML SP 메타데이터를 다운로드합니다.

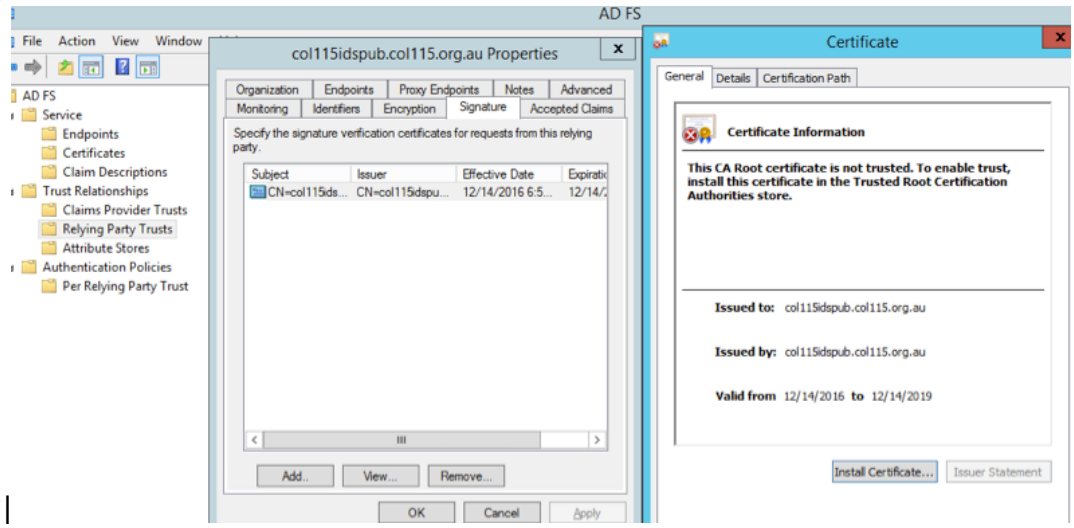
2. https://<ids server FQDN>:8553/idsadmin/으로 이동합니다.

3. 설정을 선택하고 SAML SP 메타데이터를 다운로드하여 저장합니다.



IDS 서버의 메타데이터



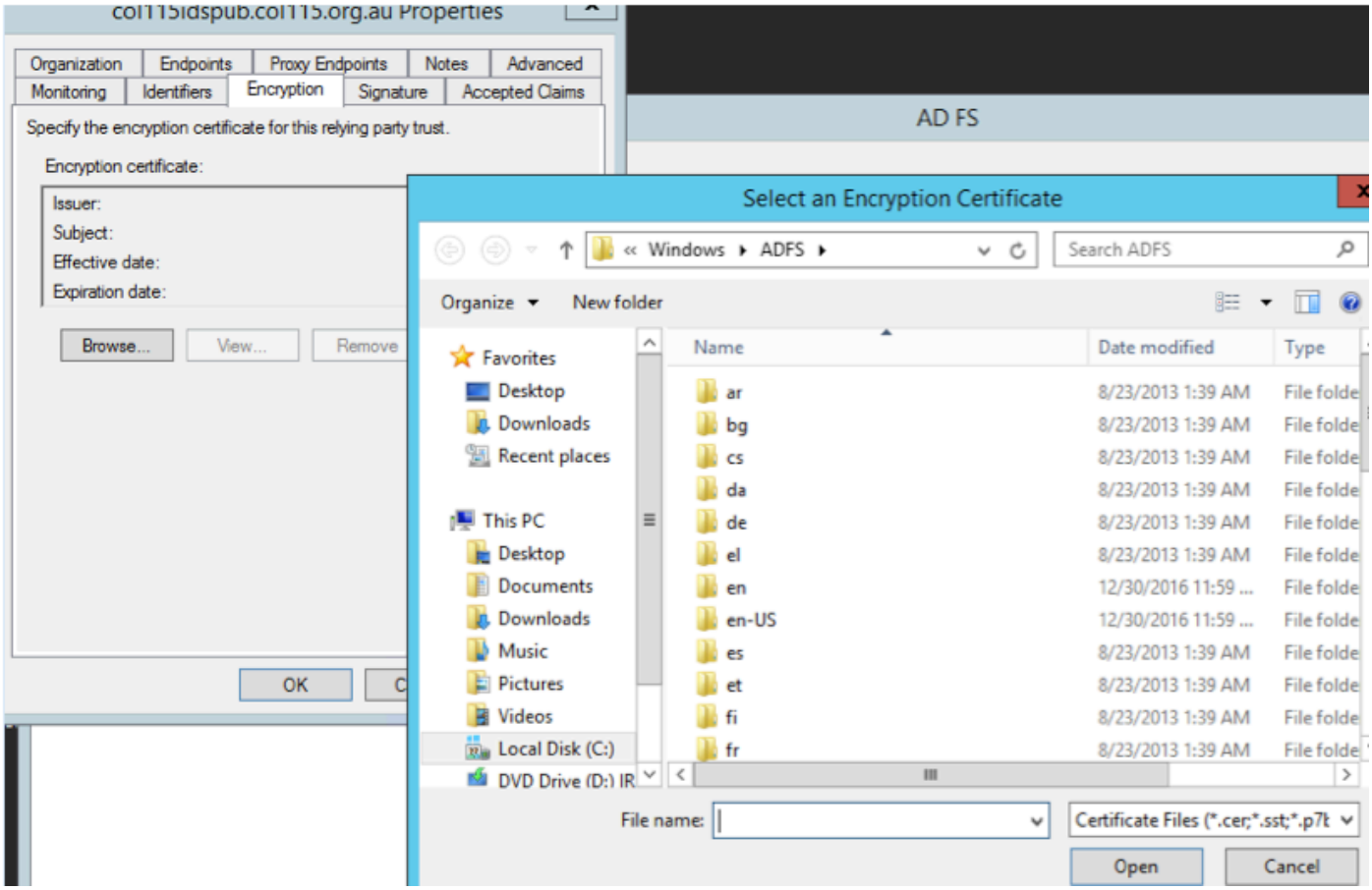


AD FS 서버로 가져오기
AD FS 측에서 확인

IDS가 SAML 인증서를 다시 생성할 때 SAML 요청에 서명하는 데 사용되며 메타데이터 교환을 수행합니다.

암호화/서명 키

암호화는 기본적으로 활성화되어 있지 않습니다. 암호화가 활성화된 경우 AD FS에 업로드해야 합니다.



참조:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_ent
features-guide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf

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.