ECE에서 에이전트 및 파티션 관리자를 위한 SSO 구성 및 문제 해결

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

배경 정보

컨피그레이션 단계

- ECE에 대한 당사자 Trust 구성
- ID 제공자 구성
- 인증서 생성 및 가져오기
- 에이전트 단일 로그인 구성
- 파티션 설정에서 웹 서버/LB URL 설정
- 파티션 관리자를 위한 SSO 구성

문제 해결

- 추적 수준 설정
- 문제 해결 시나리오 1
  - 오류
  - 로그 분석
  - 해결
- 문제 해결 시나리오 2
  - 오류
  - 로그 분석
  - 해결
- 문제 해결 시나리오 3
  - 오류
  - 로그 분석
  - 해결

관련 정보

소개

이 문서에서는 ECE 솔루션에서 에이전트 및 파티션 관리자를 위한 SSO(Single Sign-On)를 구성하는 데 필요한 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

Cisco PCCE(Packaged Contact Center Enterprise)

Cisco UCCE(Unified Contact Center Enterprise)

ECE(Enterprise Chat and Email)

Microsoft Active Directory

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

UCCE 버전: 12.6(1)

ECE 버전: 12.6(1)

Windows Server 2016의 Microsoft ADFS(Active Directory Federation Service)

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

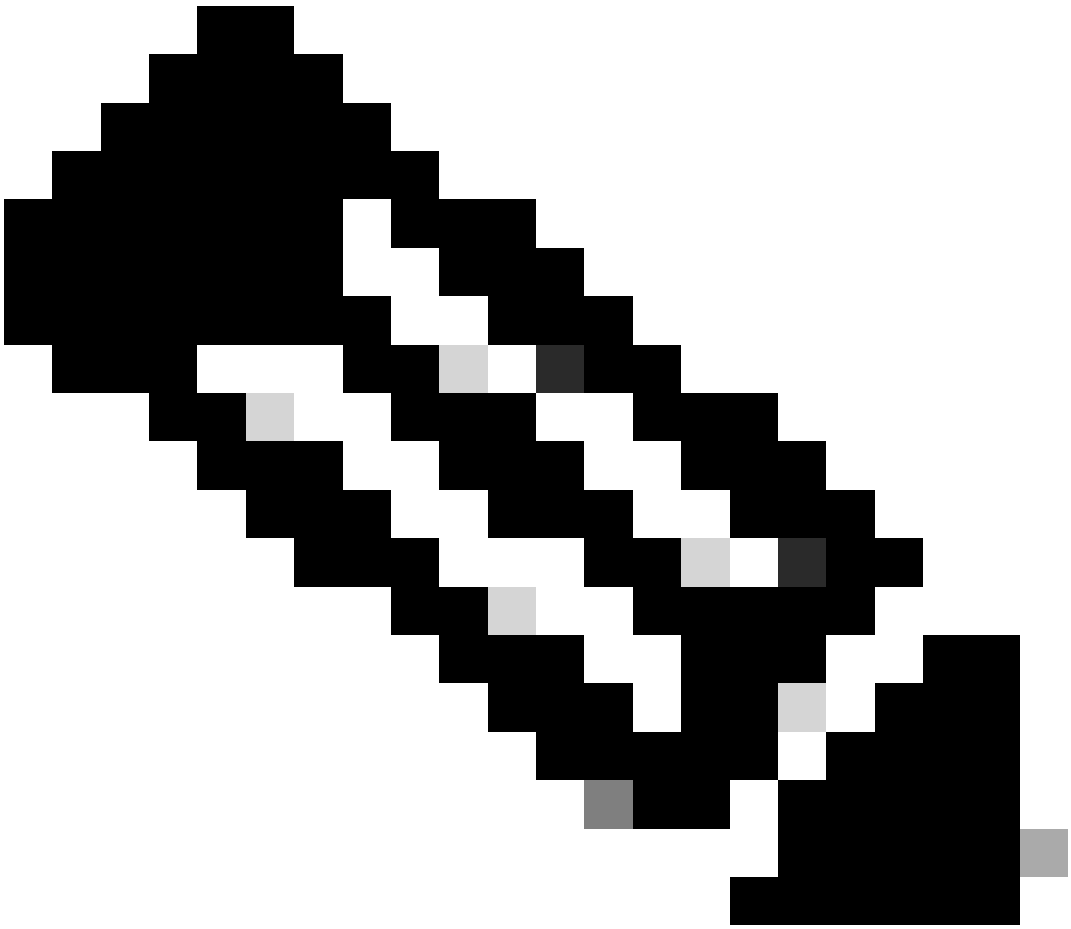
ECE(Enterprise Chat and Email) 콘솔은 Finesse 외부에서 액세스할 수 있지만 에이전트와 수퍼바이저가 Finesse를 통해 ECE에 로그인할 수 있도록 SSO를 활성화해야 합니다.

새 파티션 관리자를 위해 Single Sign-On도 구성할 수 있습니다. 이렇게 하면 Cisco Administrator Desktop에 로그인하는 새 사용자에게 Enterprise Chat and Email Administration Console 액세스 권한이 부여됩니다.

Single Sign-On에 대한 중요 참고 사항:

- Single Sign-On에 대한 시스템 구성 프로세스는 파티션 사용자가 필요한 작업(응용 프로그램 보안 보기 및 응용 프로그램 보안 관리)을 사용하여 파티션 수준에서 보안 노드에 대해 수행해야 합니다.
- 수퍼바이저 및 관리자가 에이전트 콘솔 이외의 콘솔에 로그인하려면 SSO가 활성화된 후 파티션 설정에서 응용 프로그램의 유효한 외부 URL을 제공해야 합니다. 자세한 내용은 일반 파티션 설정을 참조하십시오.
- 관리자 또는 수퍼바이저 역할을 가진 사용자가 SSO 로그인 자격 증명을 사용하여 Finesse 외부의 ECE 파티션 1에 로그인할 수 있도록 SSO를 구성하려면 JKS(Java Keystore) 인증서가 필요합니다. JKS 인증서를 받으려면 IT 부서에 문의하십시오.
- Cisco IDS의 SSL(Secure Sockets Layer) 인증서를 설치 시 모든 애플리케이션 서버로 가져와야 합니다. 필요한 SSL 인증서 파일을 얻으려면 IT 부서나 Cisco IDS 지원에 문의하십시오.
- Unified CCE의 DB 서버 데이터 정렬은 대/소문자를 구분합니다. 사용자 정보 엔드포인트 URL에서 반환되는 클레임의 사용자 이름과 Unified CCE의 사용자 이름이 동일해야 합니다.

동일하지 않으면 SSO(Single Sign-On) 에이전트가 로그인한 것으로 인식되지 않으며 ECE에서 Unified CCE에 에이전트 가용성을 보낼 수 없습니다.
- Cisco IDS에 대해 SSO를 구성하면 Unified CCE에서 SSO(Single Sign-On)를 구성하도록 구성된 사용자에게 영향을 줍니다. ECE에서 SSO를 활성화하려는 사용자가 Unified CCE에서 SSO에 대해 구성되어 있는지 확인합니다. 자세한 내용은 Unified CCE 관리자에게 문의하십시오.



참고:

- ECE에서 SSO를 활성화하려는 사용자가 Unified CCE에서 SSO에 대해 구성되어 있는지 확인합니다.
- 이 문서에서는 리소스 페더레이션 서버 및 계정 페더레이션 서버가 동일한 컴퓨터에 설치된 단일 AD FS 배포에서 ECE에 대한 Relying Part Trust를 구성하는 단계를 지정합니다.
- Split AD FS(분할 AD FS) 구축의 경우 해당 버전에 대한 ECE Install and Configure(ECE 설치 및 구성) 설명서로 이동합니다.

컨피그레이션 단계

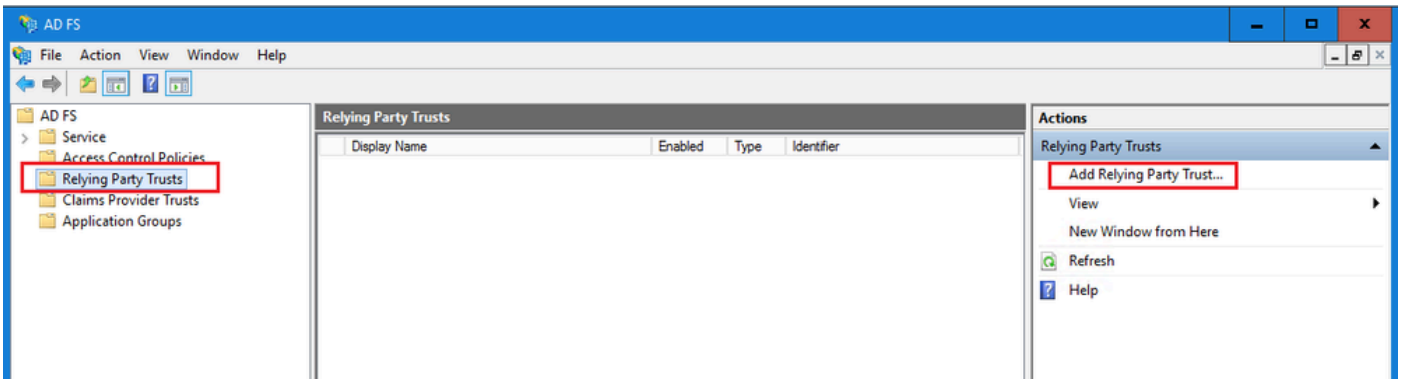
ECE에 대한 당사자 Trust 구성

1단계

AD FS Management Console을 열고 AD FS > Trust Relationships > Relying Party Trust로 이동합니다.

2단계

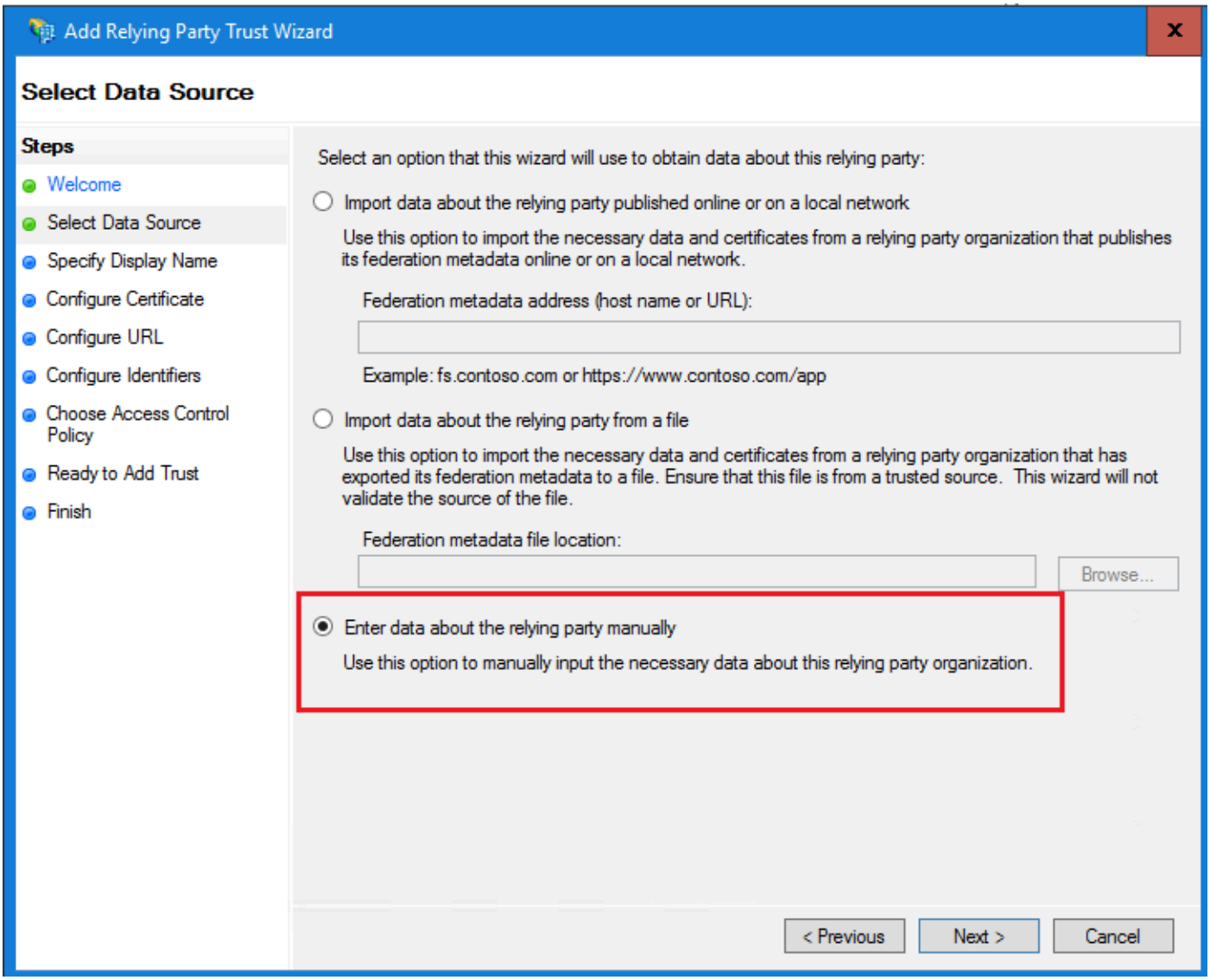
Actions(작업) 섹션에서 Add Relying Party Trust...를 클릭합니다.



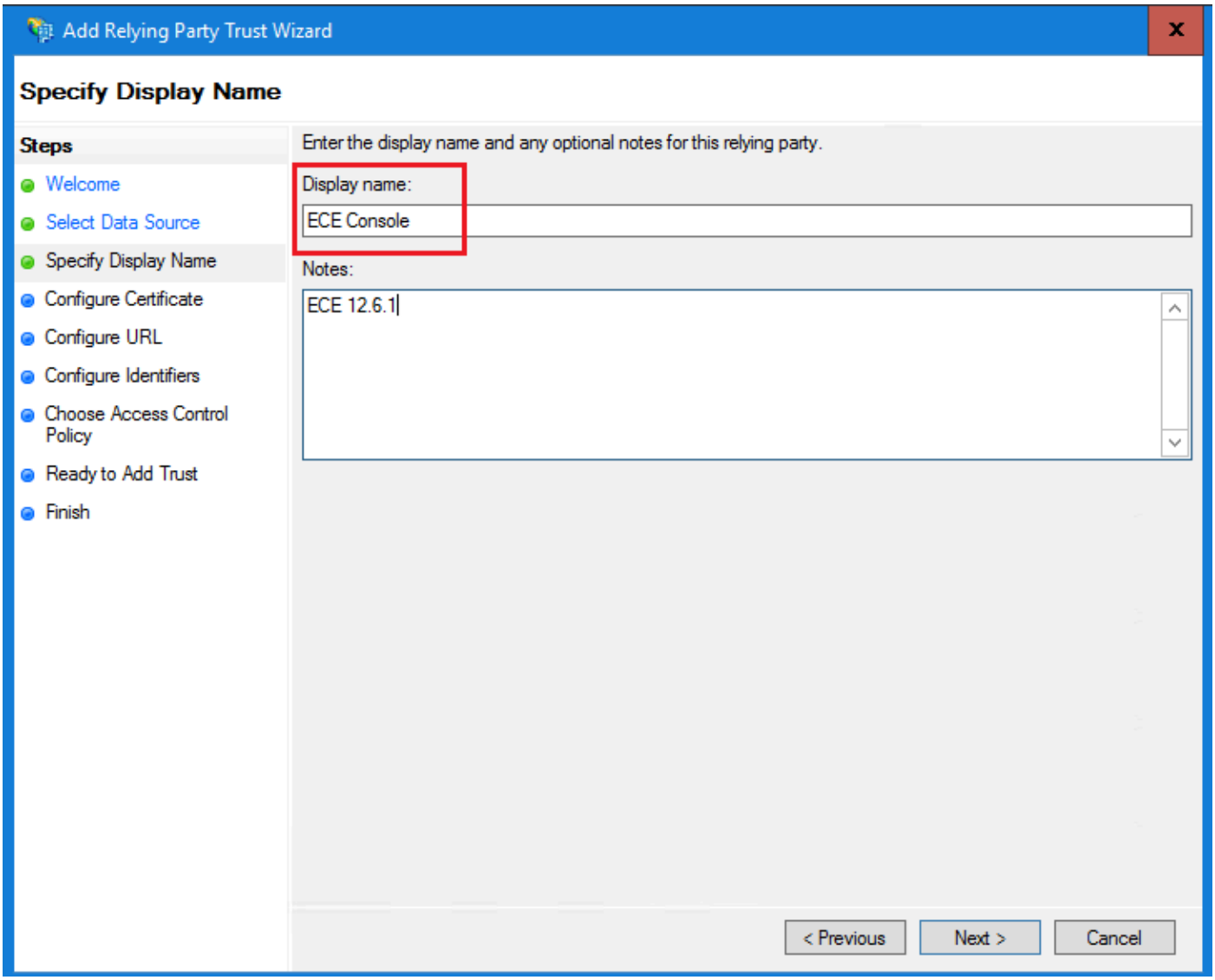
3단계

Add Relying Party Trust(당사자 Trust 추가) 마법사에서 Start(시작)를 클릭하고 다음 단계를 완료합니다.

a. [데이터 소스 선택] 페이지에서 응답 당사자에 대한 데이터 수동 입력 옵션을 선택하고 다음을 누릅니다.



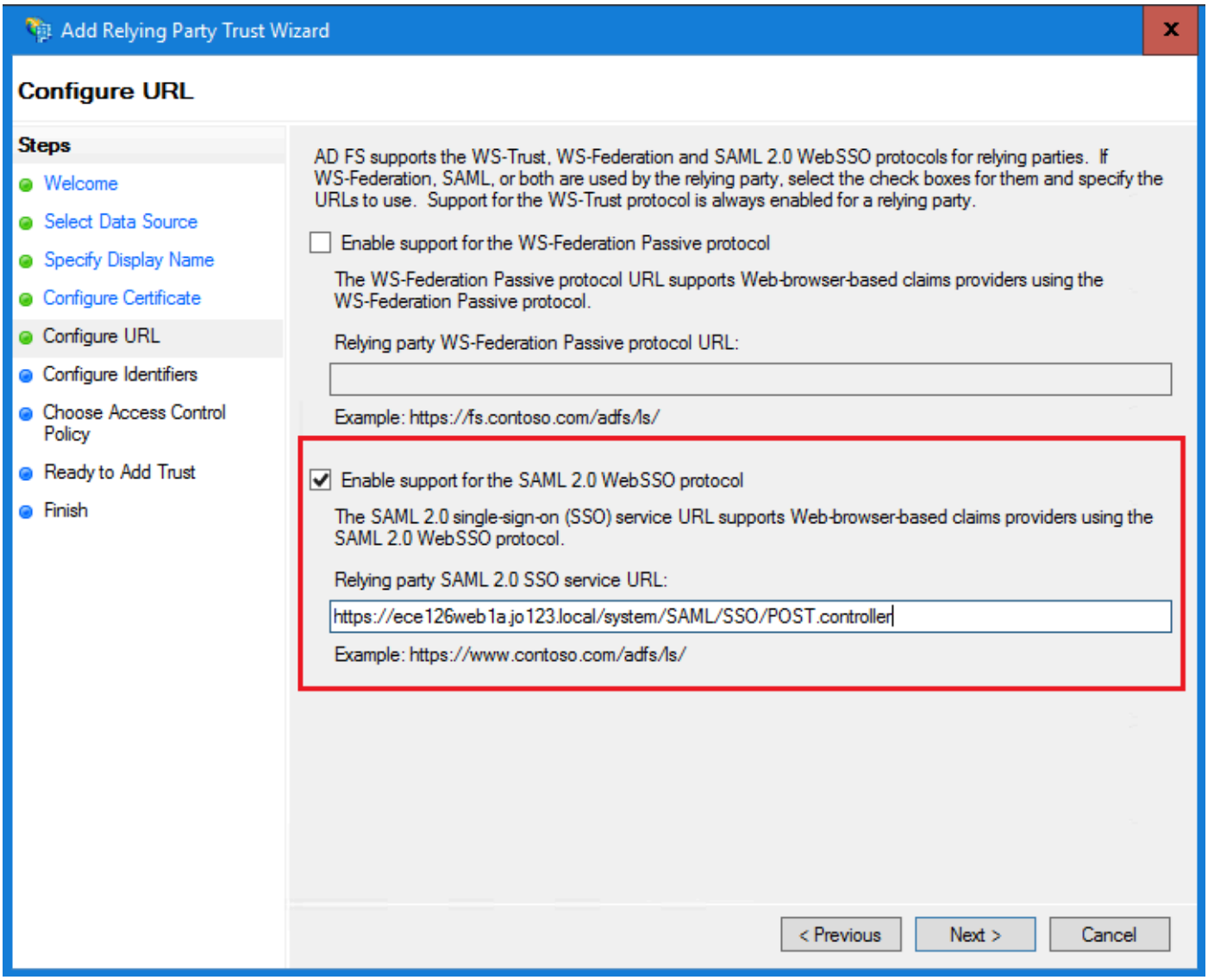
b. Specify Display Name 페이지에서 신뢰 당사자에 대한 표시 이름을 제공합니다. Next(다음)를 클릭합니다.



c. Configure URL(URL 구성) 페이지에서

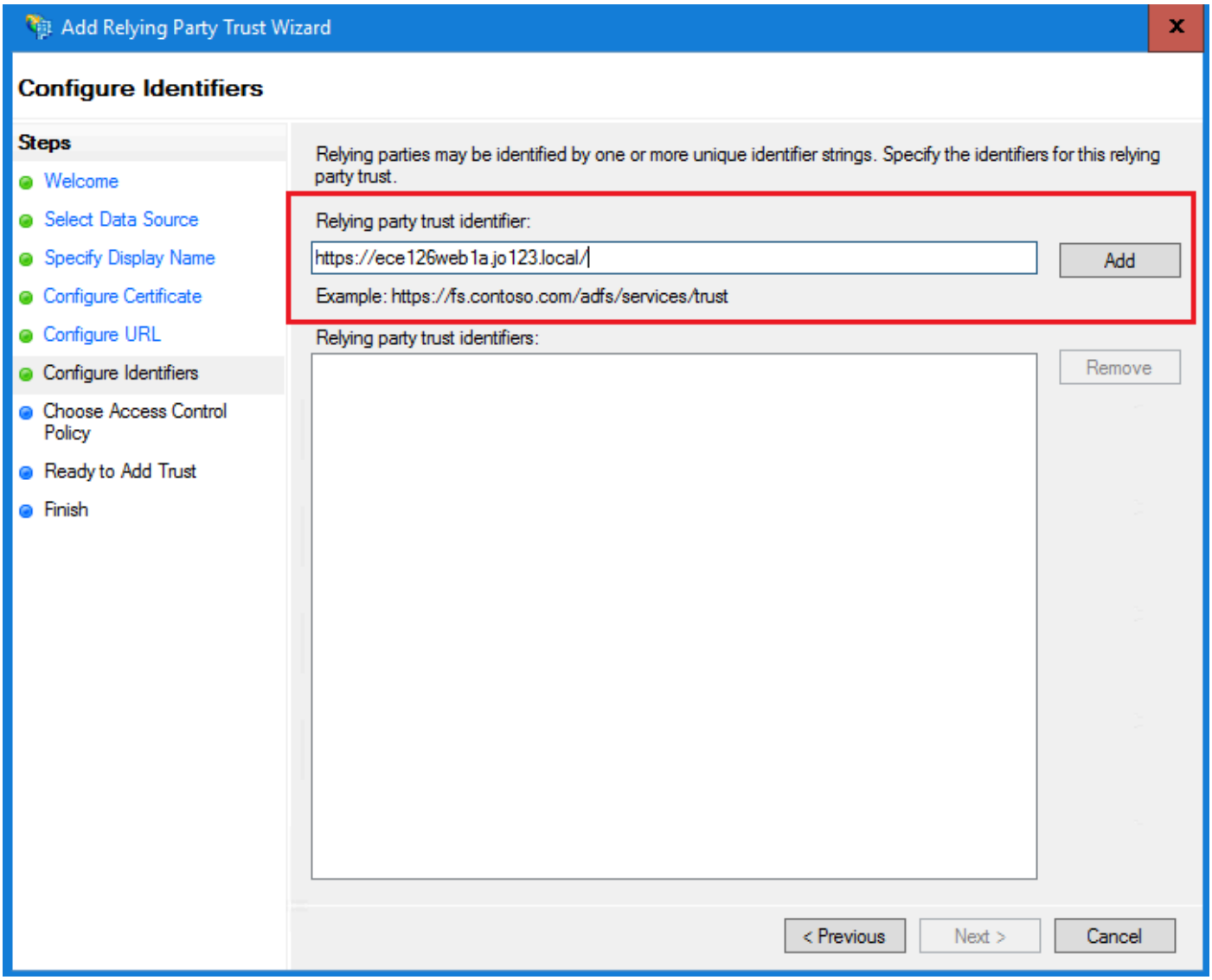
i. Enable support for the SAML 2.0 Web SSO protocol(SAML 2.0 웹 SSO 프로토콜 지원 활성화) 옵션을 선택합니다.

ii. Relying Party SAML 2.0 SSO 서버 URL 필드에서 https://<Web-Server-Or-Load-Balancer-FQDN>/system/SAML/SSO/POST.controller 형식으로 URL을 제공합니다.

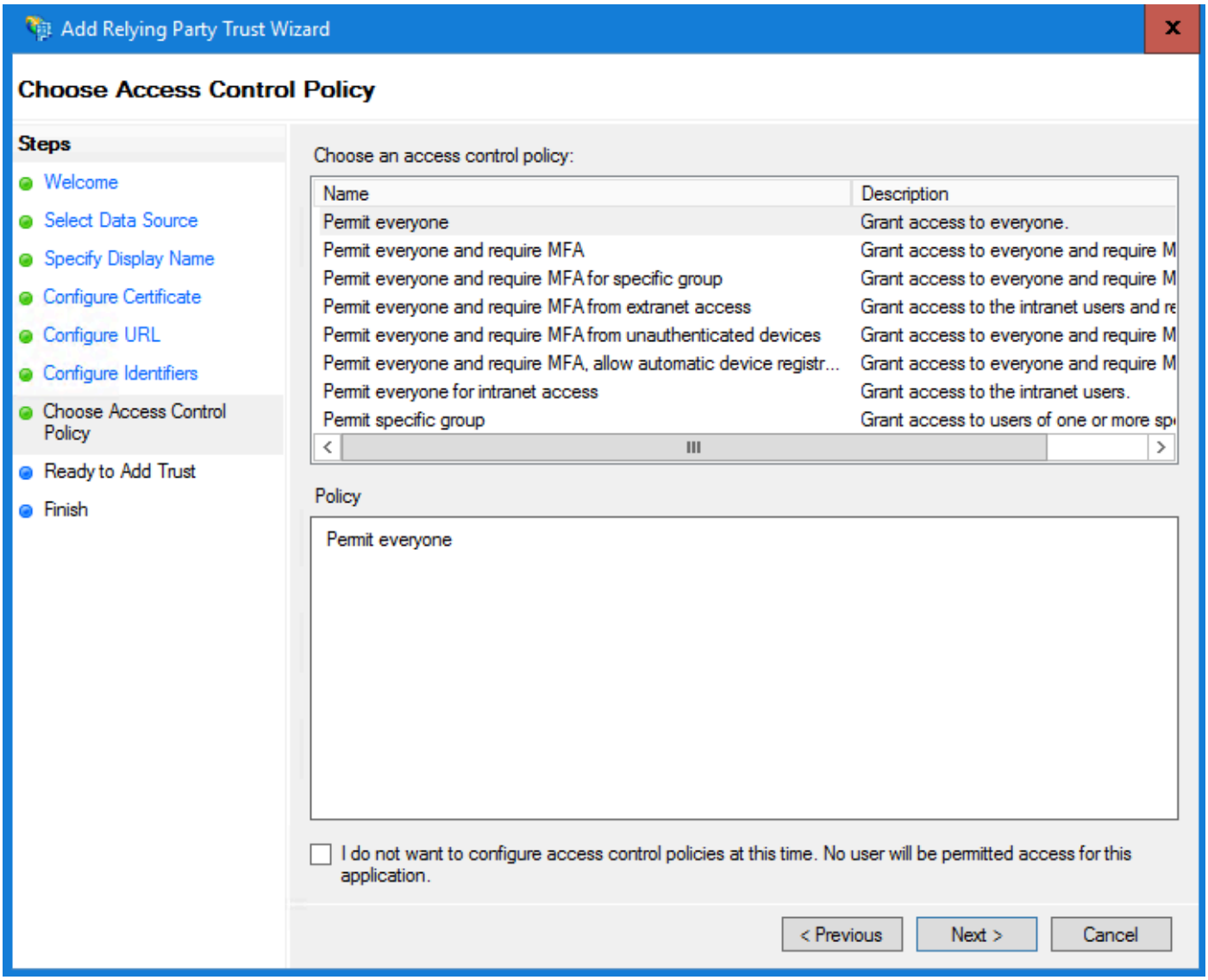


d. Configure Identifiers(식별자 구성) 페이지에서 Relying party trust identifier(신뢰 당사자 트러스트 식별자)를 제공하고 Add(추가)를 클릭합니다.

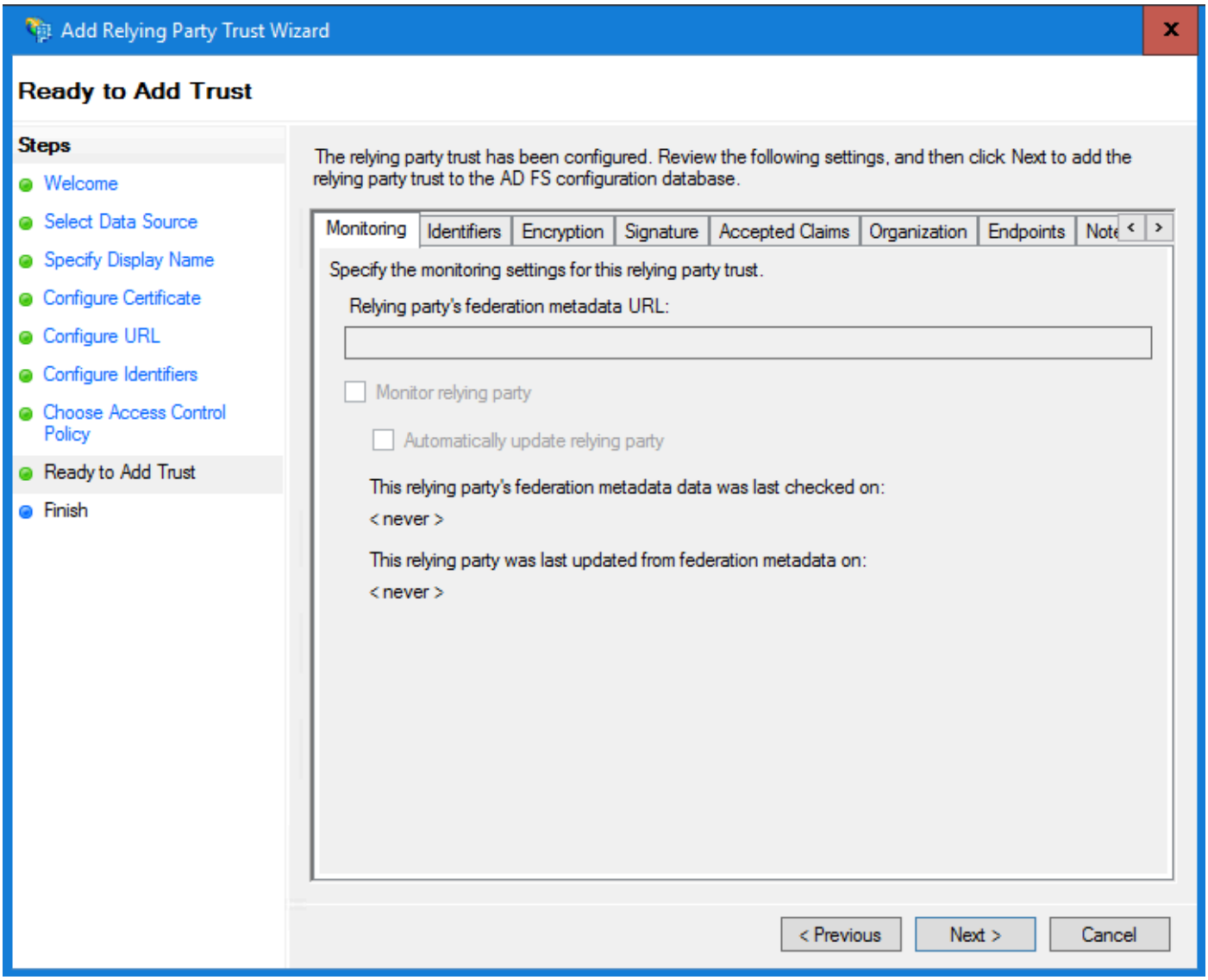
- 값은 https://<Web-Server-Or-Load-Balancer-FQDN>/ 형식이어야 합니다.



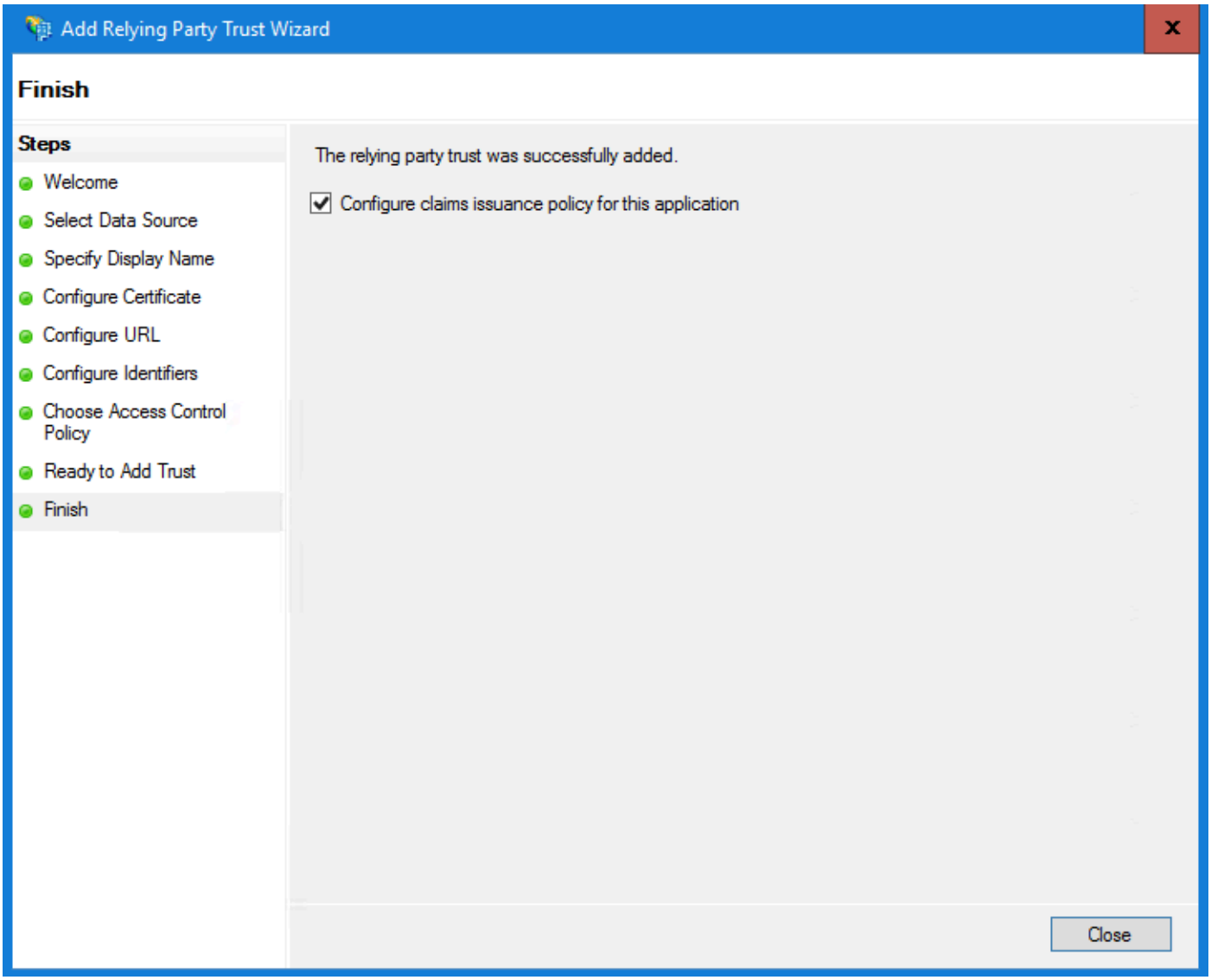
e. Choose Access Control Policy(액세스 제어 정책 선택) 페이지에서 기본값 'Permit everyone' 정책을 사용하여 다음을 클릭합니다.



f. Ready to Add Trust(트러스트 추가 준비) 페이지에서 Next(다음)를 클릭합니다.

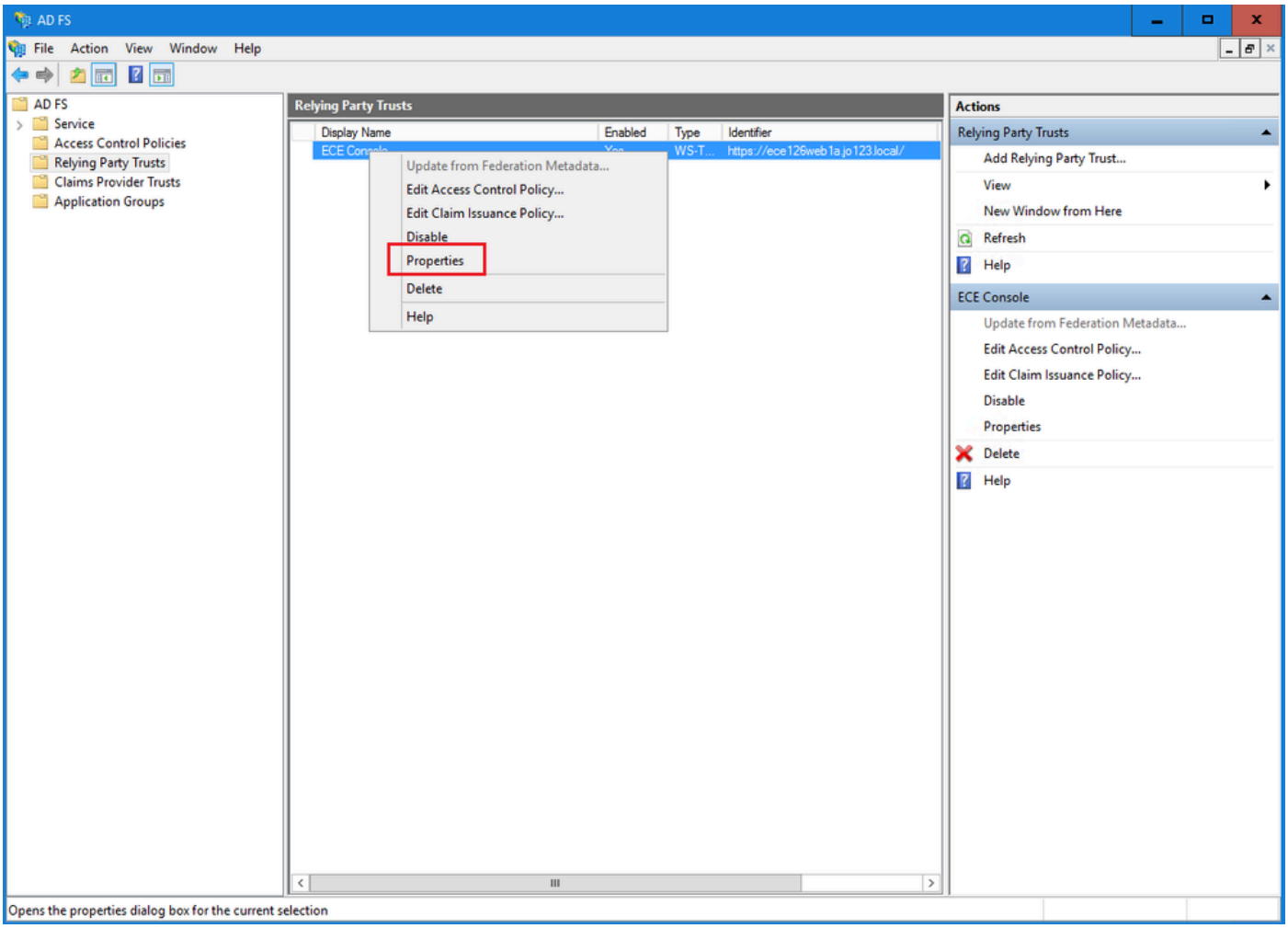


g. 신뢰 당사자 트러스트가 성공적으로 추가되면 Close(닫기)를 클릭합니다.



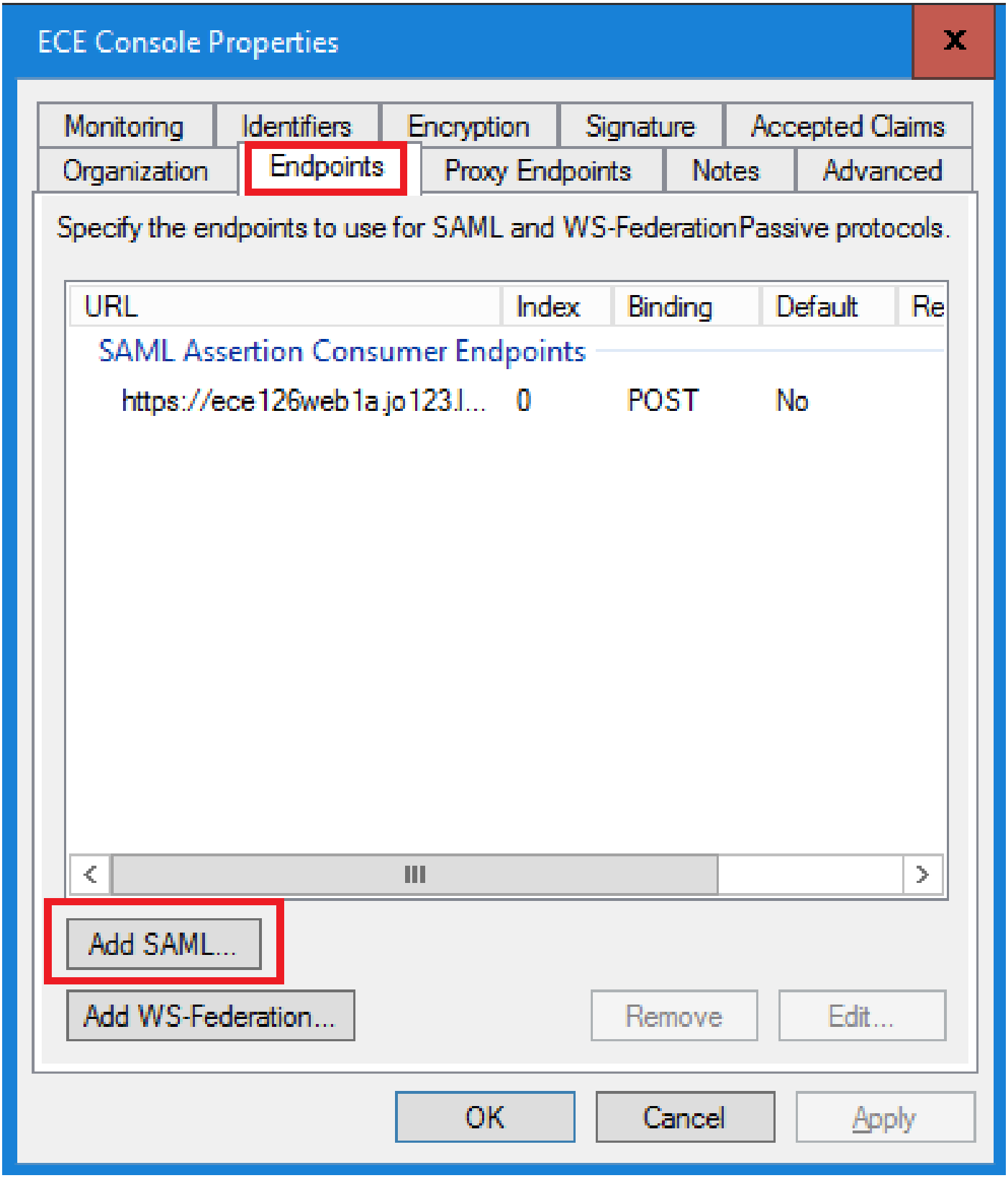
4단계

Relying Provider Trust(신뢰 제공자 신뢰) 목록에서 ECE에 대해 생성된 신뢰 당사자 신뢰를 선택하고 작업 섹션에서 Properties(속성)를 클릭합니다.



5단계

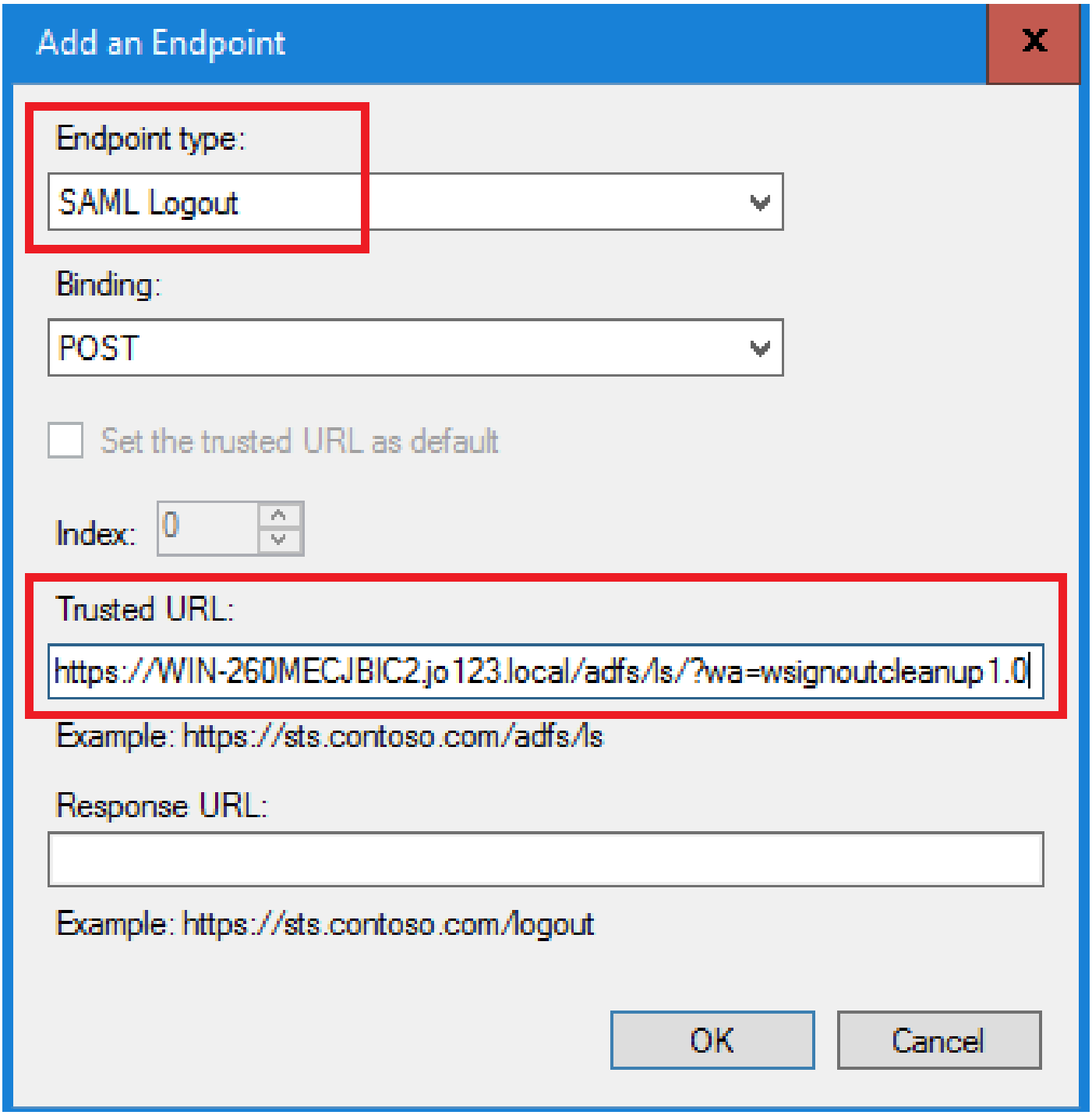
속성 창에서 엔드포인트 탭으로 이동하고 SAML 추가 ... 단추



6단계

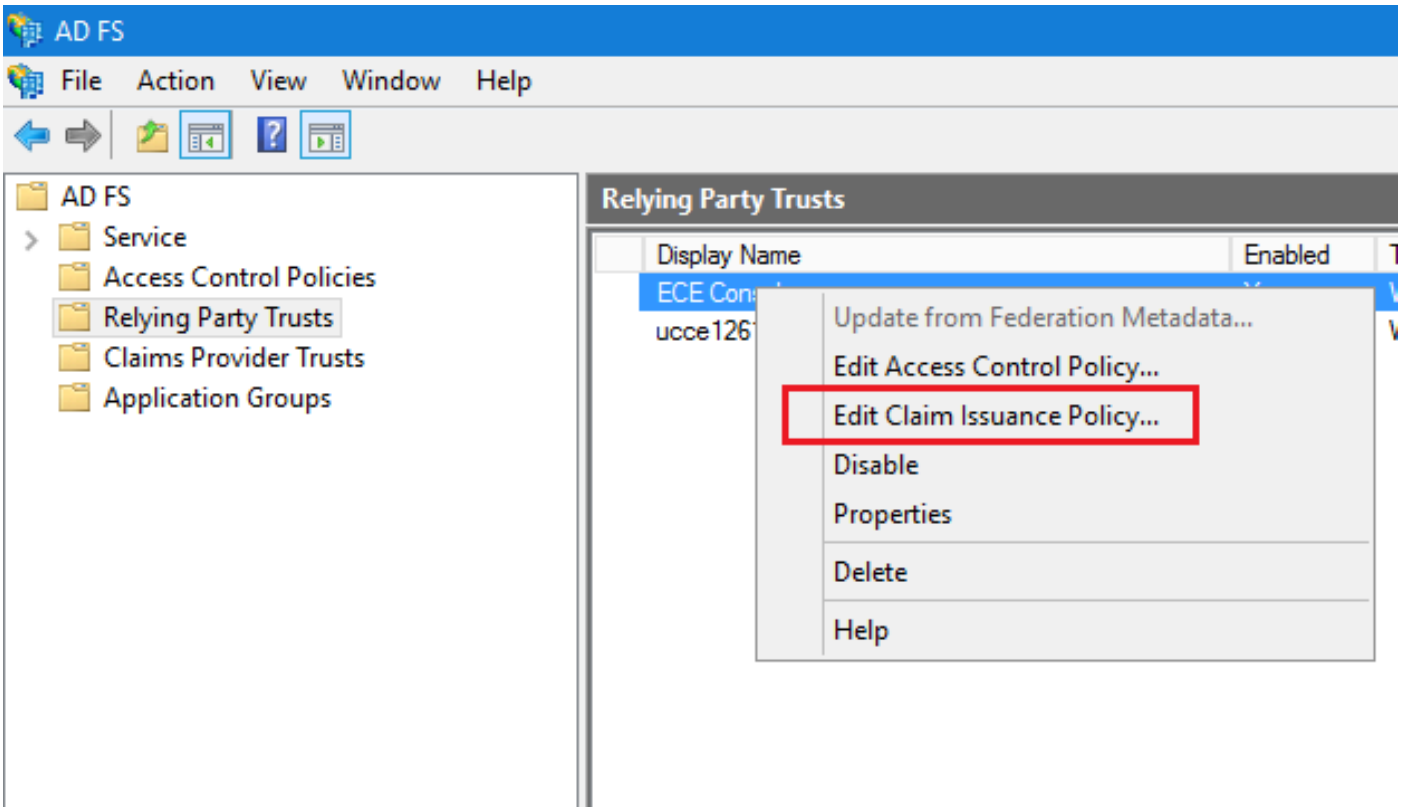
Add an Endpoint(엔드포인트 추가) 창에서 다음과 같이 구성합니다.

1. 엔드포인트 유형을 SAML 로그아웃으로 선택합니다.
2. 신뢰할 수 있는 URL을 https://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0으로 지정합니다.
3. OK(확인)를 클릭합니다.



7단계

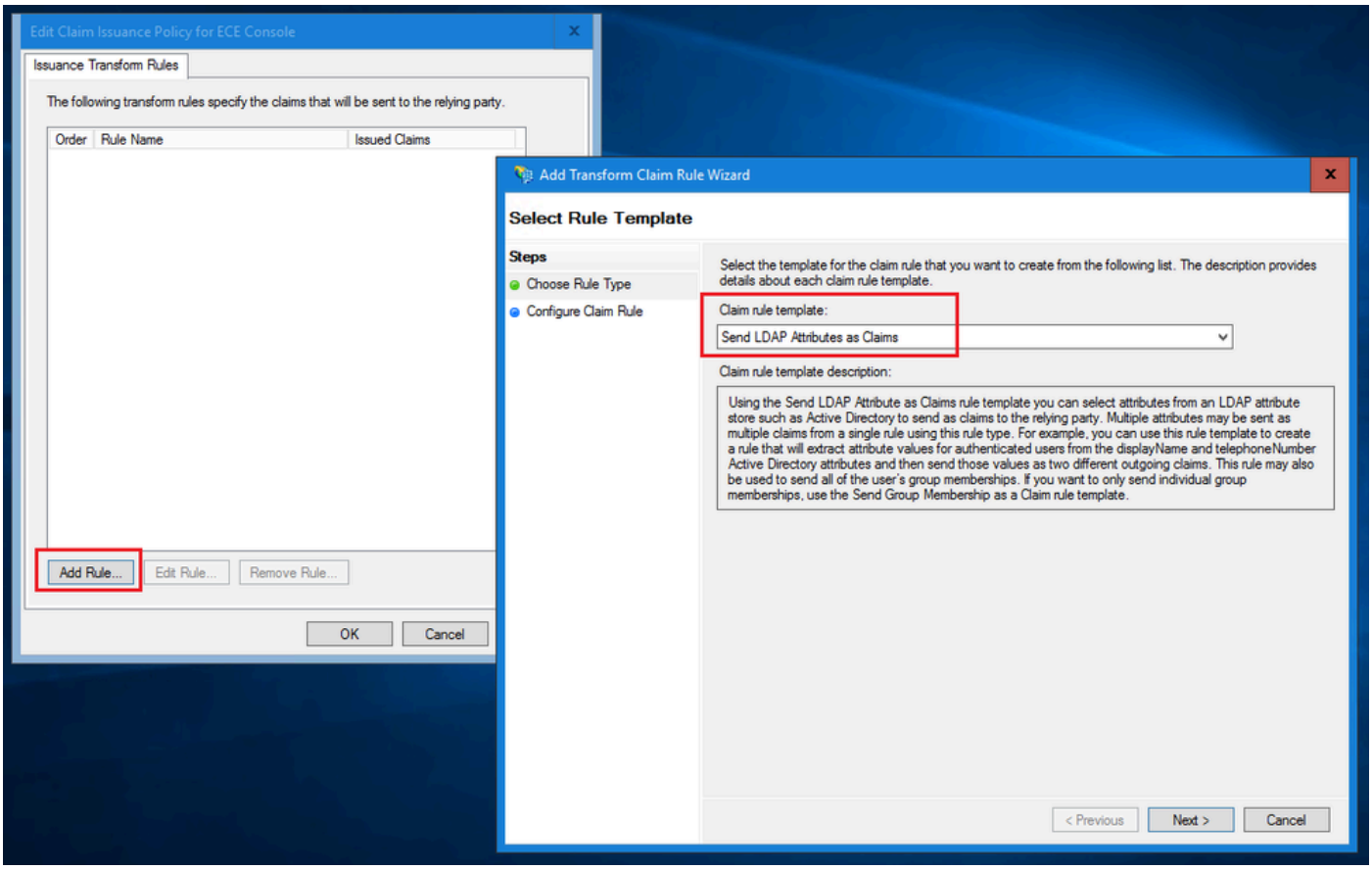
Relying Provider Trust 목록에서 ECE에 대해 생성된 트러스트를 선택하고 작업 섹션에서 Edit Claim Insurance Policy를 클릭합니다.



8단계

Edit Claim Insurance Policy(클레임 보험 정책 수정) 창의 Issuance Transform Rules(발급 변환 규칙) 탭에서 Add Rule...(규칙 추가...) 버튼을 클릭하고 다음과 같이 구성합니다.

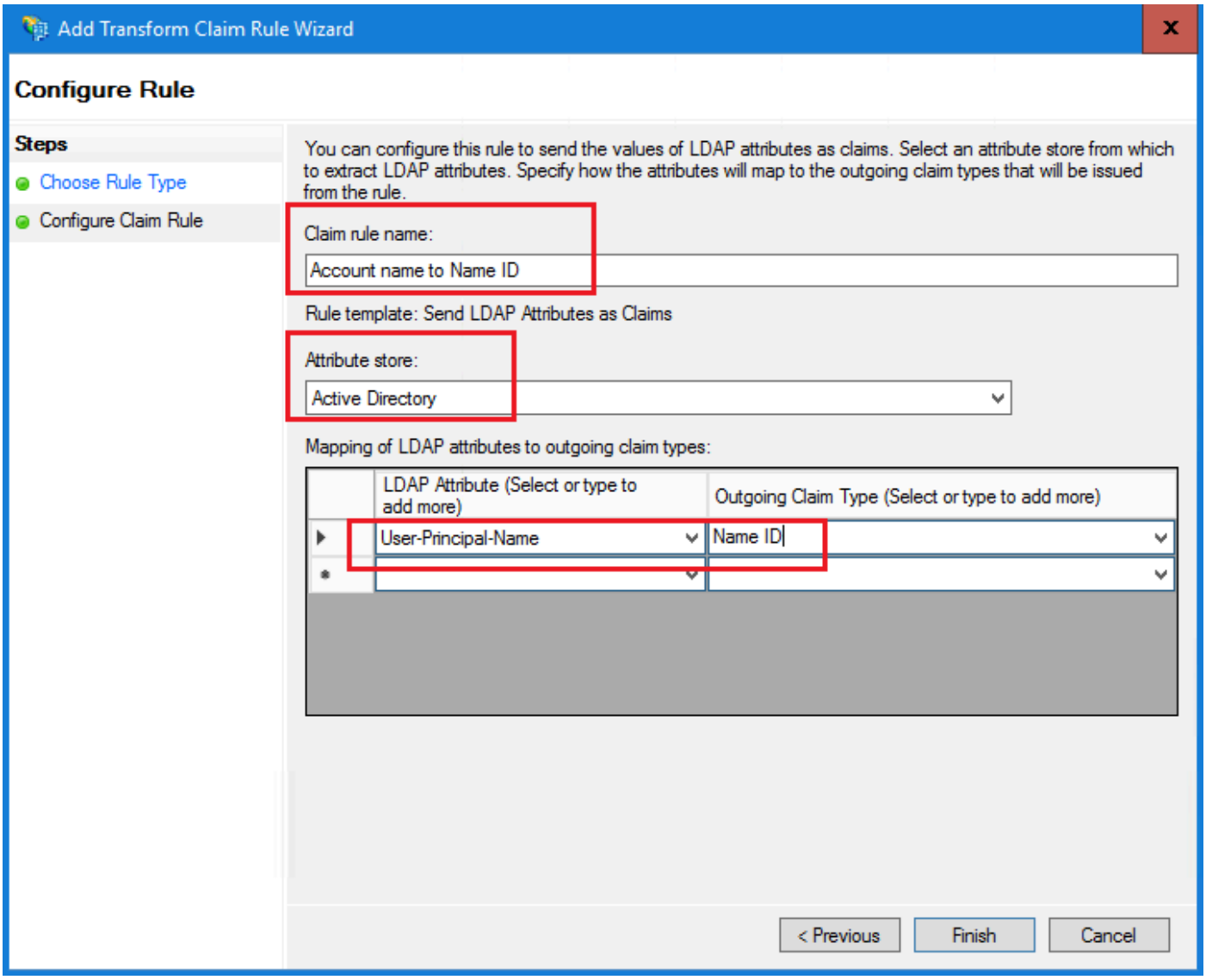
a. Choose Rule Type(규칙 유형 선택) 페이지의 드롭다운에서 Send LDAP Attributes as Claims(LDAP 특성을 클레임으로 보내기)를 선택하고 Next(다음)를 클릭합니다.

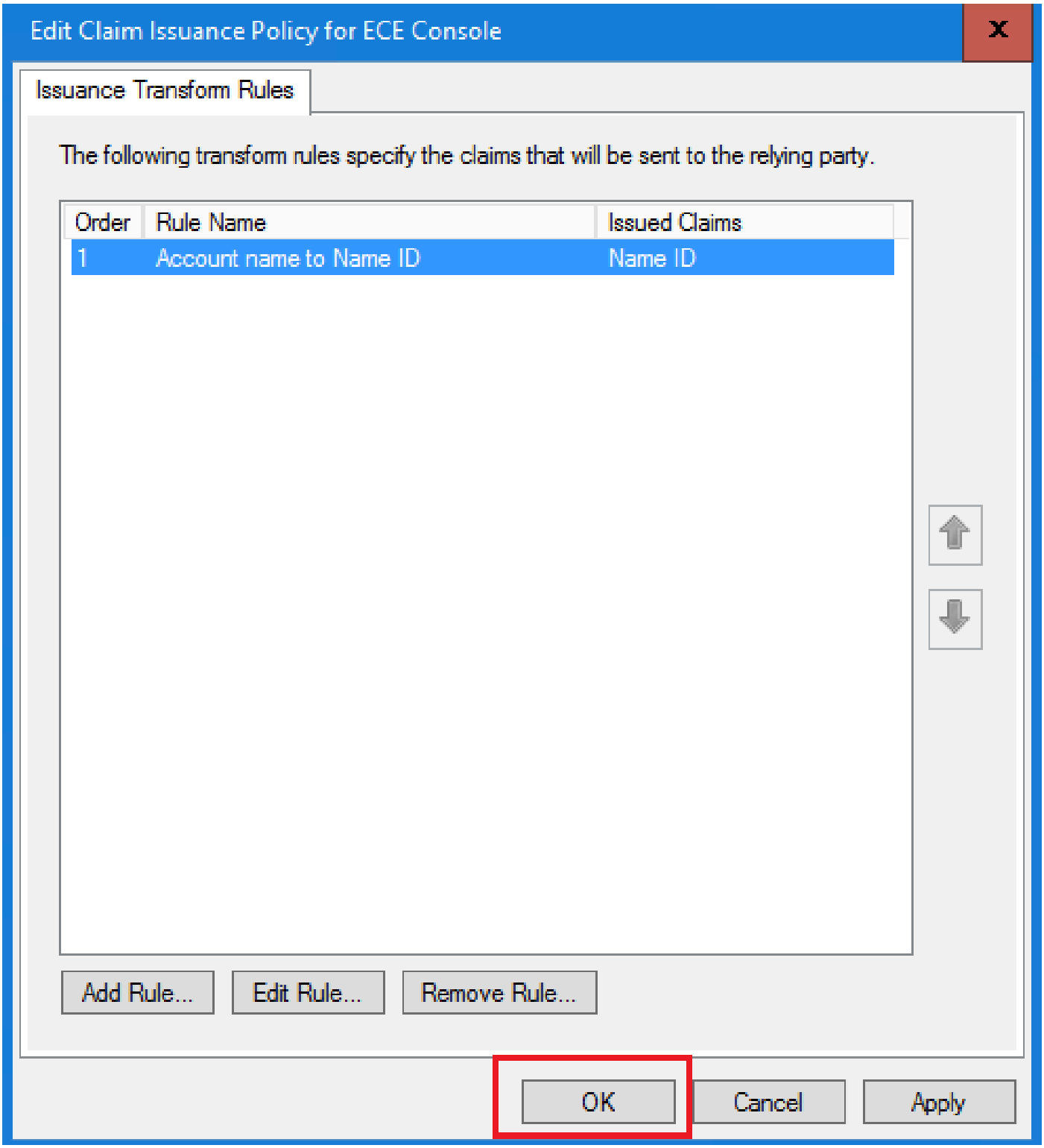


b. Configure Claim Rule 페이지에서 다음을 수행합니다.

1. 클레임 규칙 이름을 제공하고 특성 저장소를 선택합니다.
2. LDAP 특성 및 발신 클레임 유형의 매핑을 정의합니다.

- 발신 클레임 유형 이름으로 Name ID를 선택합니다.
- 마침을 눌러 청구 보험 정책 편집 창으로 되돌아가 확인을 누릅니다.

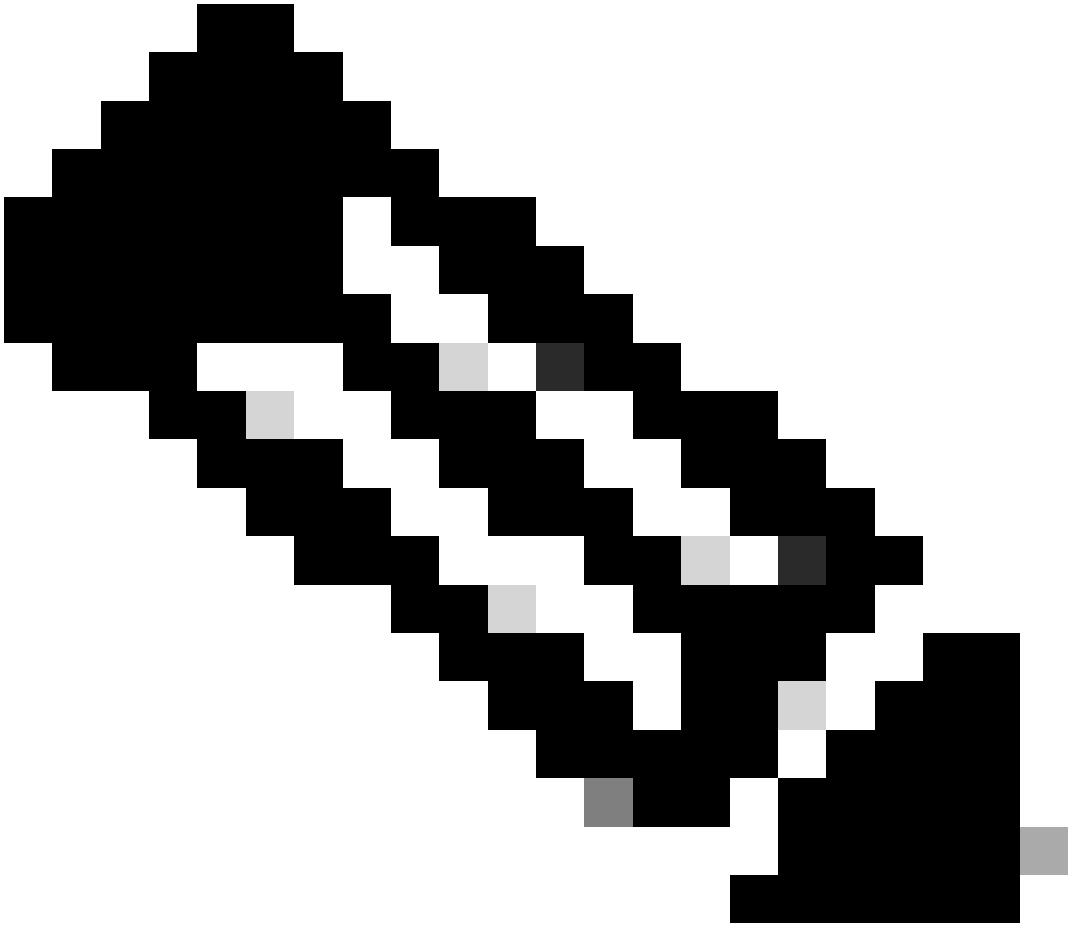

Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.
Claim rule name:
Account name to Name ID
Rule template: Send LDAP Attributes as Claims
Attribute store:
Active Directory
Mapping of LDAP attributes to outgoing claim types:
LDAP Attribute (Select or type to add more)
Outgoing Claim Type (Select or type to add more)
User-Principal-Name
Name ID
< Previous
Finish
Cancel



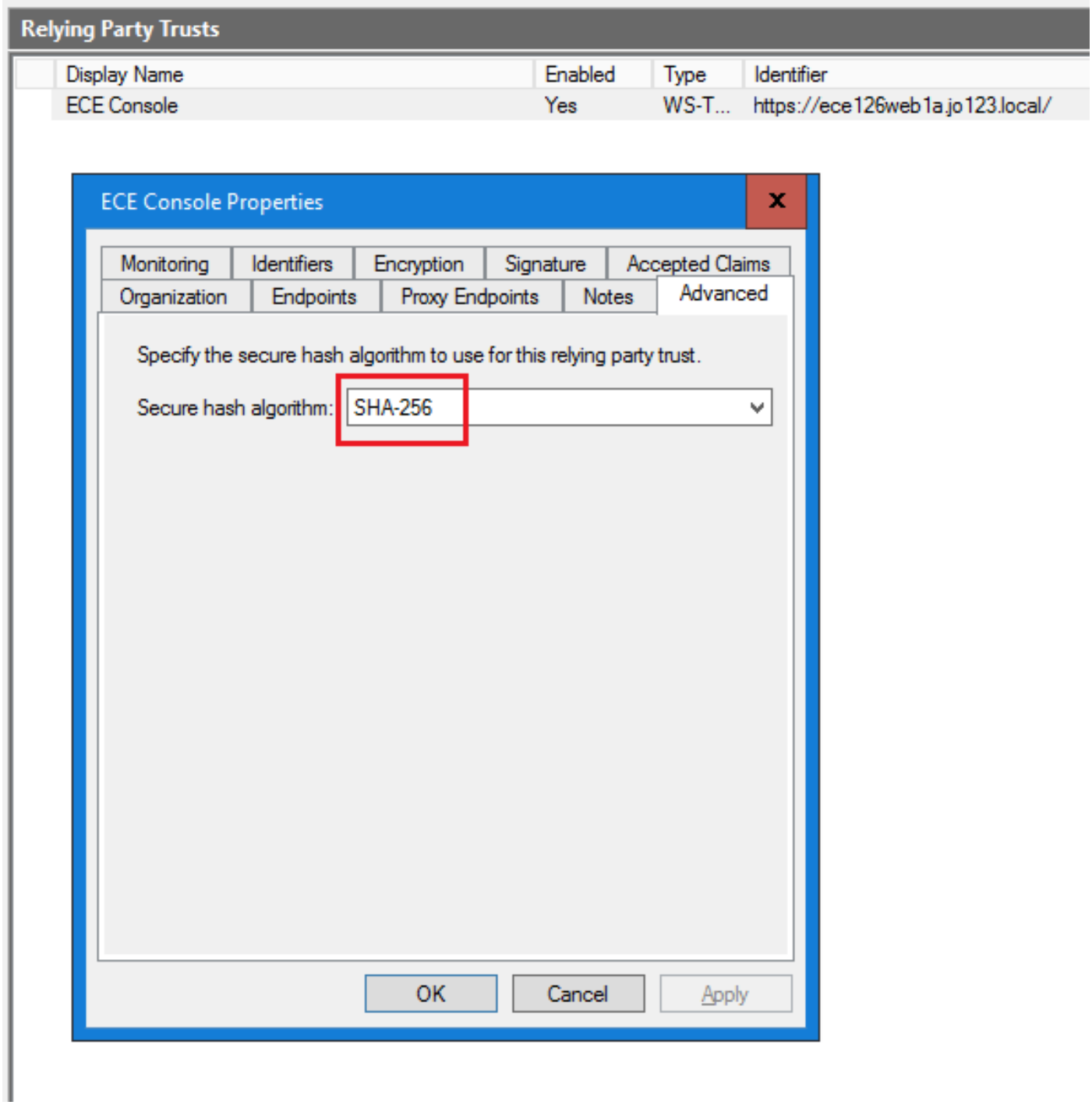
9단계

Relying Provider Trust 목록에서 생성한 ECE 신뢰 당사자 트러스트를 두 번 클릭합니다.

Properties(속성) 창이 열리면 Advanced(고급) 탭으로 이동하여 Secure hash(보안 해시) 알고리즘을 SHA-1 또는 SHA-256으로 설정합니다. OK(확인)를 클릭하여 창을 닫습니다.



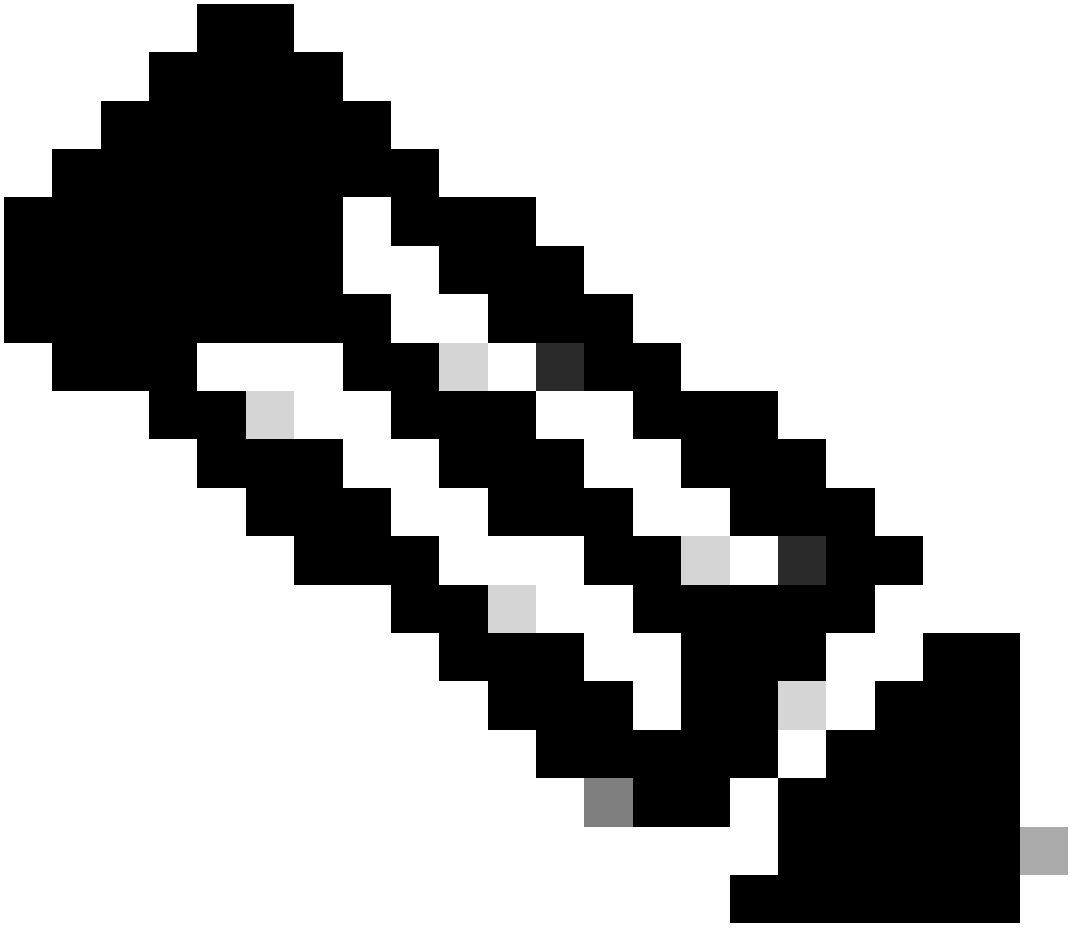
참고: 이 값은 ECE의 SSO 구성에서 '서비스 공급자'에 대해 설정된 '서명 알고리즘' 값과 일치해야 합니다.



10단계

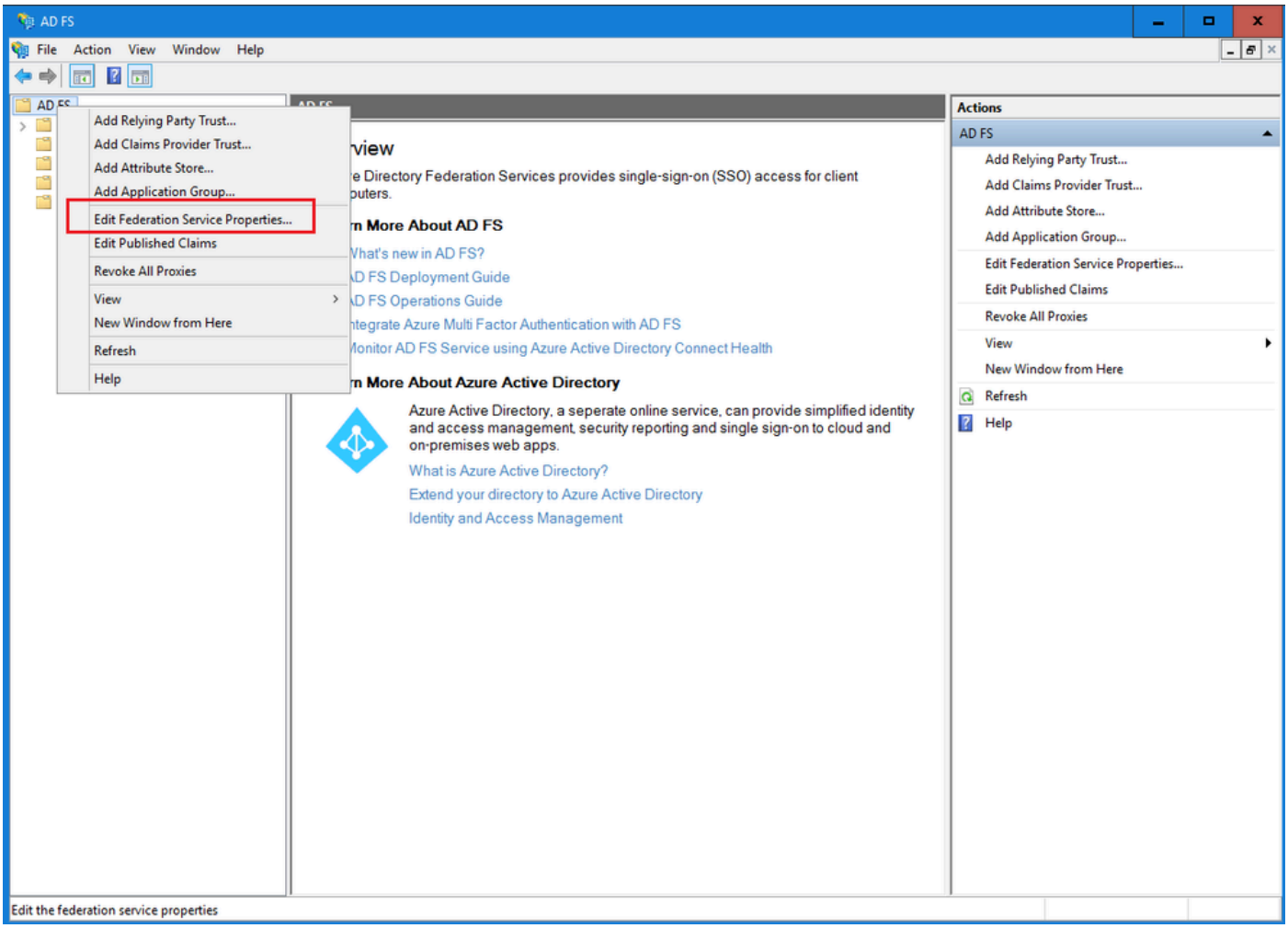
페더레이션 서비스 식별자 값을 확인하고 기록해 둡니다.

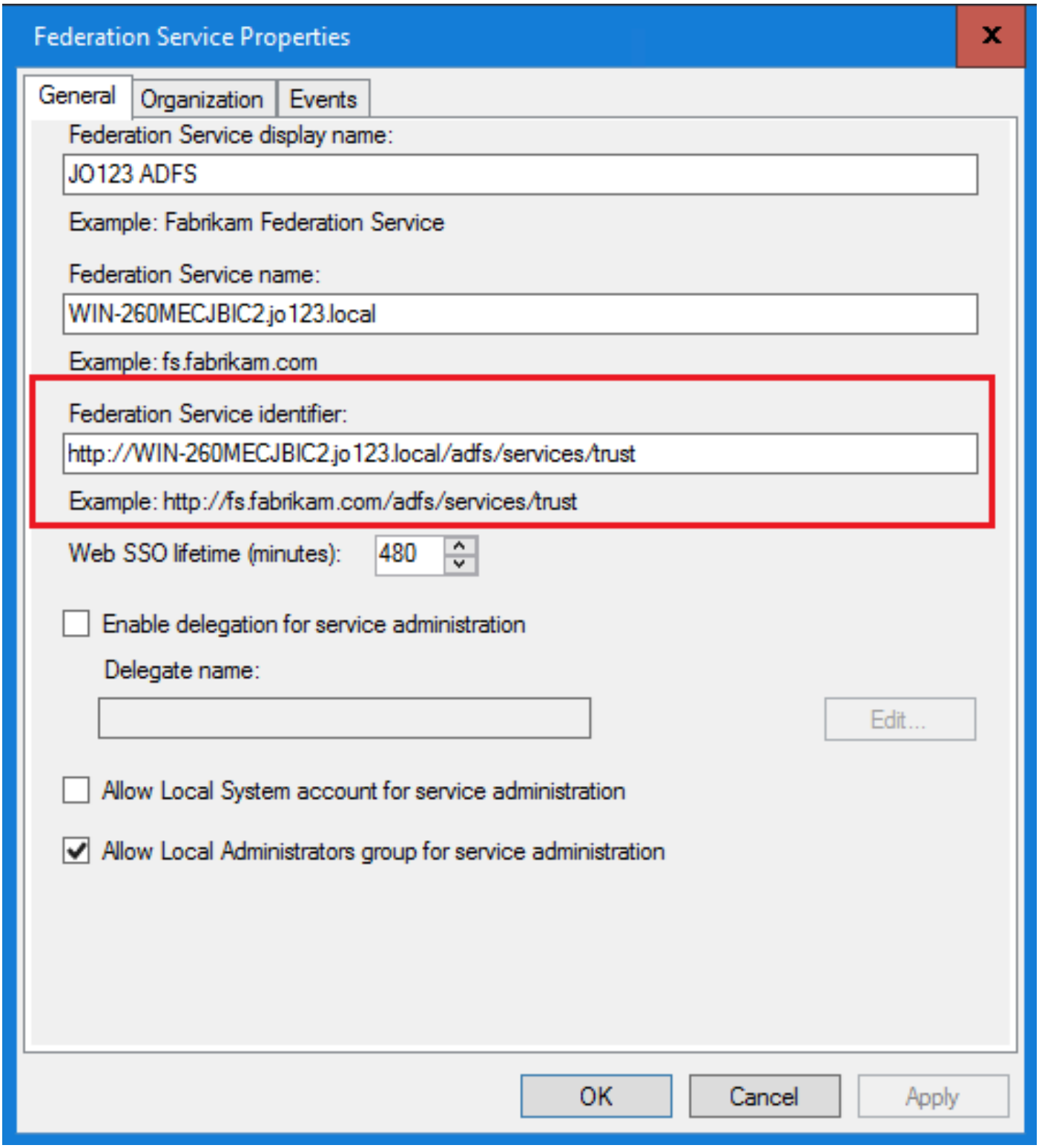
- AD FS Management 콘솔에서 AD FS > Edit Federation Service Properties > General 탭 > Federation Service Identifier를 선택하고 마우스 오른쪽 버튼으로 클릭합니다



참고:

- 이 값은 ECE의 SSO Configurations(SSO 컨피그레이션)에서 ID 공급자에 대한 'Entity ID' 값을 구성할 때와 동일하게 추가해야 합니다.
- http://을 사용한다고 해서 AD FS가 안전하지 않은 것은 아니며 단순히 식별자일 뿐입니다.


AD FS
File Action View Window Help
Add Relying Party Trust...
Add Claims Provider Trust...
Add Attribute Store...
Add Application Group...
Edit Federation Service Properties...
Edit Published Claims
Revoke All Proxies
View
New Window from Here
Refresh
Help
view
e Directory Federation Services provides single-sign-on (SSO) access for client
puters.
rn More About AD FS
What's new in AD FS?
D FS Deployment Guide
D FS Operations Guide
tegrate Azure Multi Factor Authentication with AD FS
Monitor AD FS Service using Azure Active Directory Connect Health
rn More About Azure Active Directory
Azure Active Directory, a seperate online service, can provide simplified identity
and access management, security reporting and single sign-on to cloud and
on-premises web apps.
What is Azure Active Directory?
Extend your directory to Azure Active Directory
Identity and Access Management
Actions
AD FS
Add Relying Party Trust...
Add Claims Provider Trust...
Add Attribute Store...
Add Application Group...
Edit Federation Service Properties...
Edit Published Claims
Revoke All Proxies
View
New Window from Here
Refresh
Help
Edit the federation service properties



ID 제공자 구성

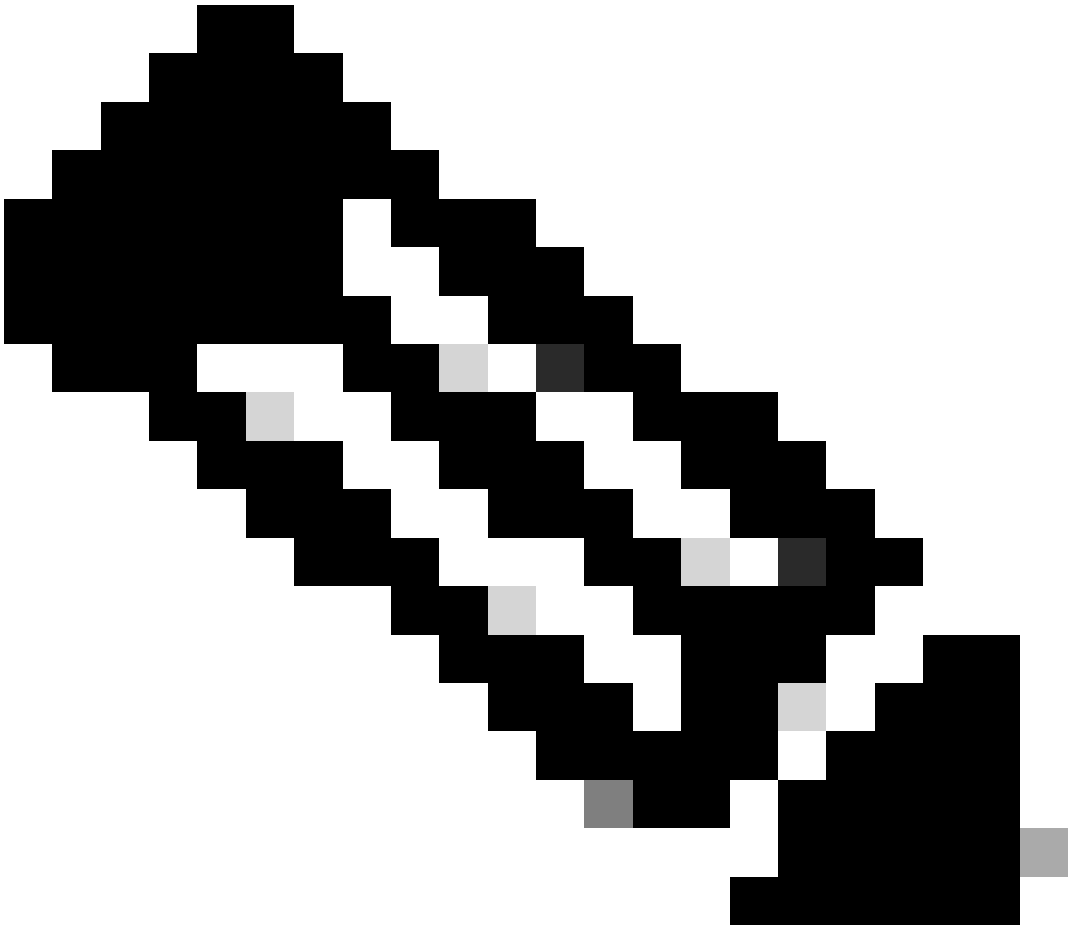
11단계

관리자 또는 수퍼바이저 역할을 가진 사용자가 SSO 로그인 자격 증명을 사용하여 Finesse 외부의 ECE 파티션에 로그인할 수 있도록 SSO를 구성하려면 JKS(Java Keystore) 인증서가 필요합니다.

관리자 또는 수퍼바이저 역할이 있는 사용자가 SSO 로그인 자격 증명을 사용하여 Finesse 외부에서 ECE 파티션에 로그인할 수 있도록 SSO를 구성하려면 JKS(Java Keystore) 인증서를 공개 키 인

증서로 변환하고 ECE용 IdP 서버에 생성된 당사자 Trust에서 구성해야 합니다.

JKS 인증서를 받으려면 IT 부서에 문의하십시오.

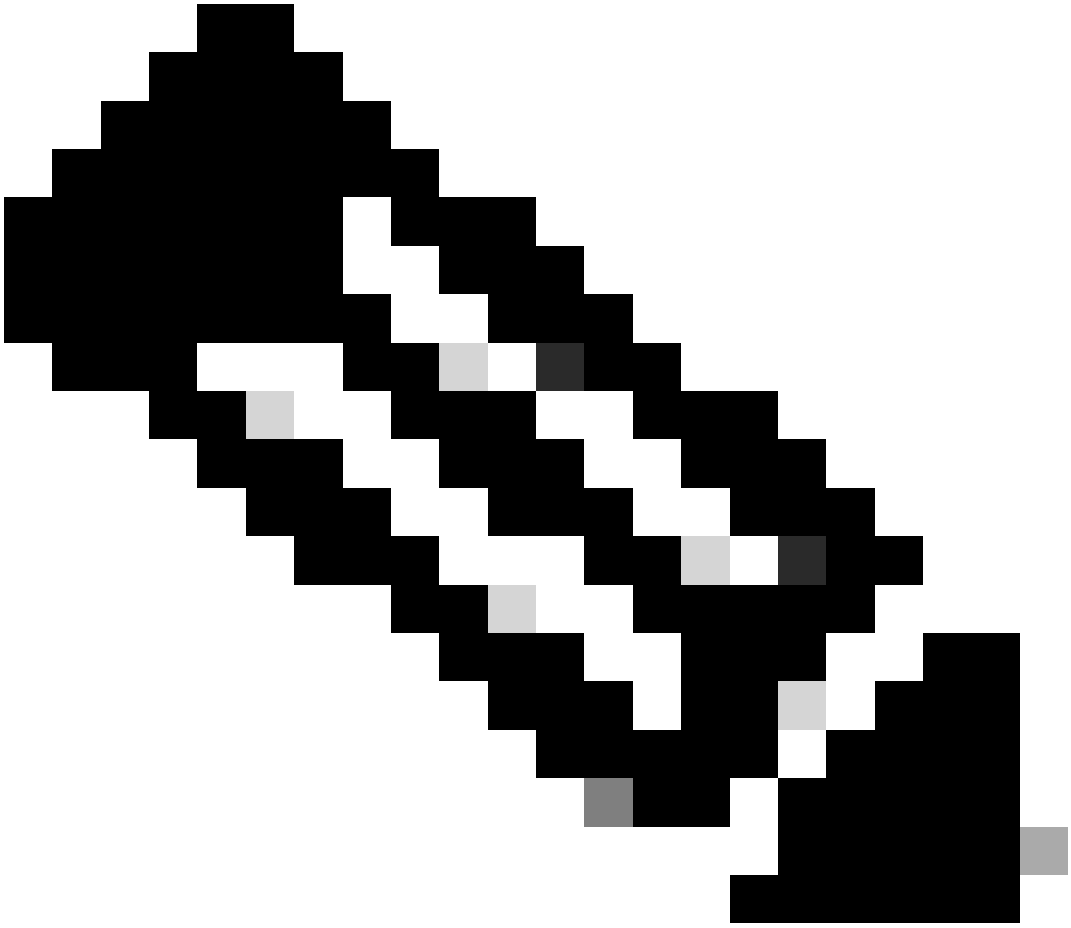


> 참고: 이 단계는 AD FS를 ID 공급자로 사용하는 시스템에 적용할 수 있습니다. 다른 ID 공급자는 공개 키 인증서를 구성하는 다른 방법을 가질 수 있습니다.

다음은 Lab에서 JKS 파일이 생성된 방법의 예입니다.

a. JKS 생성:

```
keytool -genkey -keyalg RSA -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -keysize 204
```



참고: 여기에 입력한 키 저장소 암호, 별칭 이름 및 키 암호는 ECE의 SSO 구성에서 '서비스 공급자' 구성을 구성하는 동안 사용됩니다.

```
C:\Users\administrator.JO123>keytool -genkey -keyalg RSA -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -keysize 2048 -validity 1825
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  ece126app1a.jo123.local
What is the name of your organizational unit?
  [Unknown]:  TAC
What is the name of your organization?
  [Unknown]:  Cisco
What is the name of your City or Locality?
  [Unknown]:  RTP
What is the name of your State or Province?
  [Unknown]:  NC
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=ece126app1a.jo123.local, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US correct?
  [no]:  yes

Enter key password for <ece126web1a_saml>
        (RETURN if same as keystore password):
```

b. 인증서 내보내기:

이 keytool 명령은 파일 이름 ece126web1a_saml.crt를 사용하여 .crt 형식의 인증서 파일을 C:\Temp 디렉토리로 내보냅니다.

```
keytool -exportcert -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -rfc -file C:\Temp\e
```

12단계

ID 제공자 구성

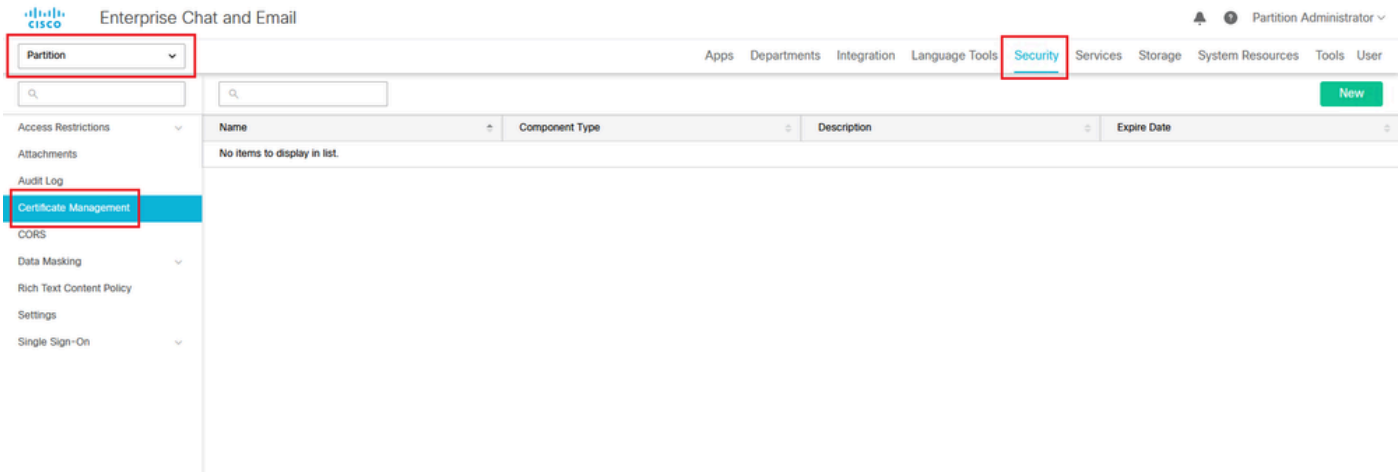
1. AD FS 관리 콘솔에서 ECE에 대해 생성된 당사자 Trust를 선택하고 마우스 오른쪽 버튼으로 클릭합니다.
2. 트러스트에 대한 속성 창을 열고 서명 탭에서 추가 단추를 클릭합니다.
3. 공용 인증서(.crt 파일은 이전 단계에서 생성됨)를 추가하고 OK(확인)를 클릭합니다.

인증서 생성 및 가져오기

13단계

에이전트의 Single Sign-On에 Cisco IDS를 사용하도록 SSO를 구성하기 전에 Cisco IdS 서버의 Tomcat 인증서를 애플리케이션으로 가져와야 합니다.

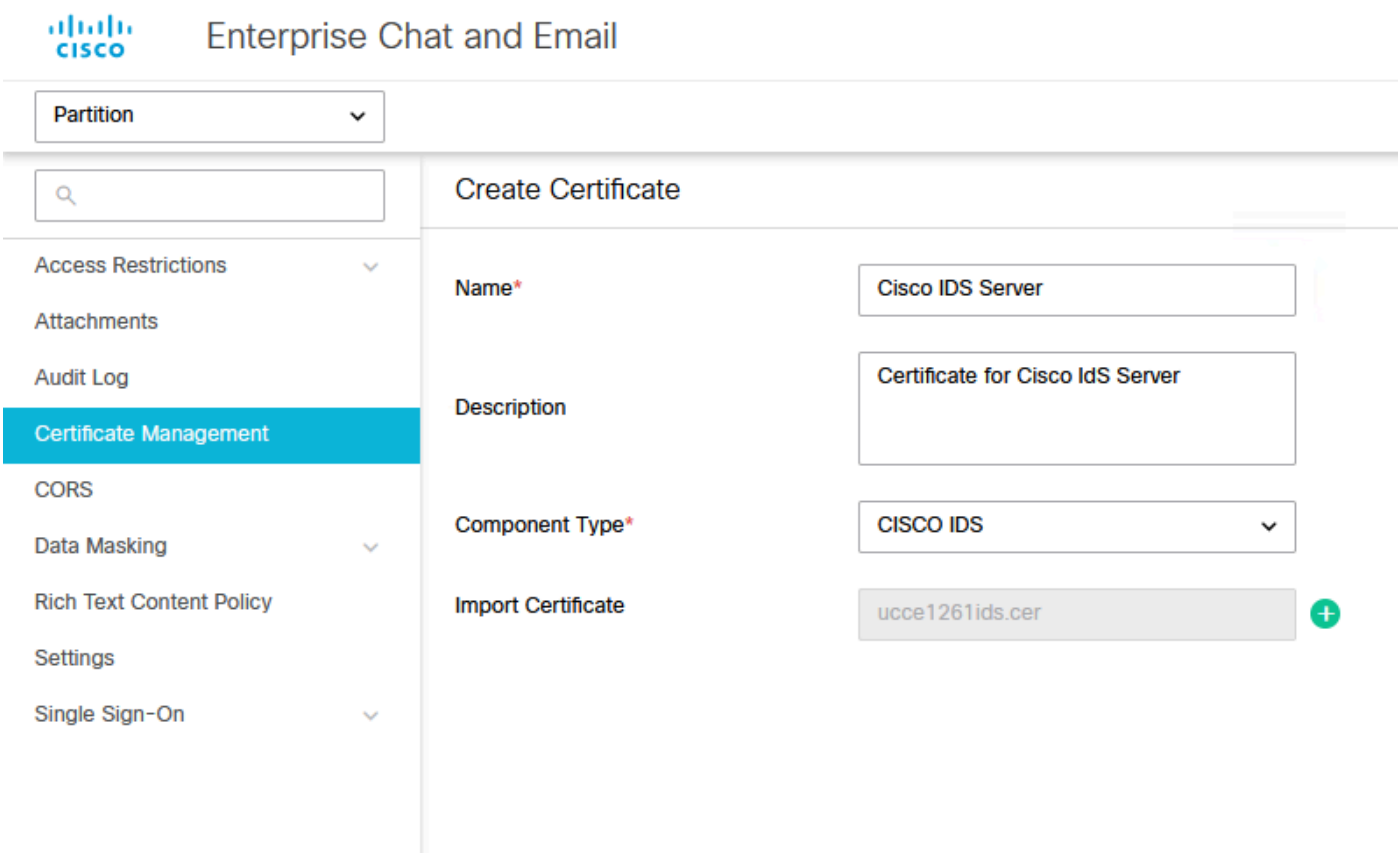
a. ECE 관리 콘솔의 파티션 레벨 메뉴에서 보안 옵션을 클릭한 다음 왼쪽 메뉴에서 인증서 관리를 선택합니다.



b. Certificate Management(인증서 관리) 영역에서 New(새로 만들기) 버튼을 클릭하고 적절한 세부 정보를 입력합니다.

- Name(이름): 인증서의 이름을 입력합니다.
- Description(설명): 인증서에 대한 설명을 추가합니다.
- Component Type(구성 요소 유형): CISCO IDS를 선택합니다.
- Import Certificate(인증서 가져오기): 인증서를 가져오려면 Search and Add(검색 및 추가) 버튼을 클릭하고 요청된 세부 정보를 입력합니다.
- 인증서 파일: Browse(찾아보기) 버튼을 클릭하고 가져올 인증서를 선택합니다. 인증서는 .pem, .der(BINARY) 또는 .cer/cert 형식으로만 가져올 수 있습니다.
- Alias Name(별칭 이름): 인증서의 별칭을 제공합니다.

c. 저장을 클릭합니다.

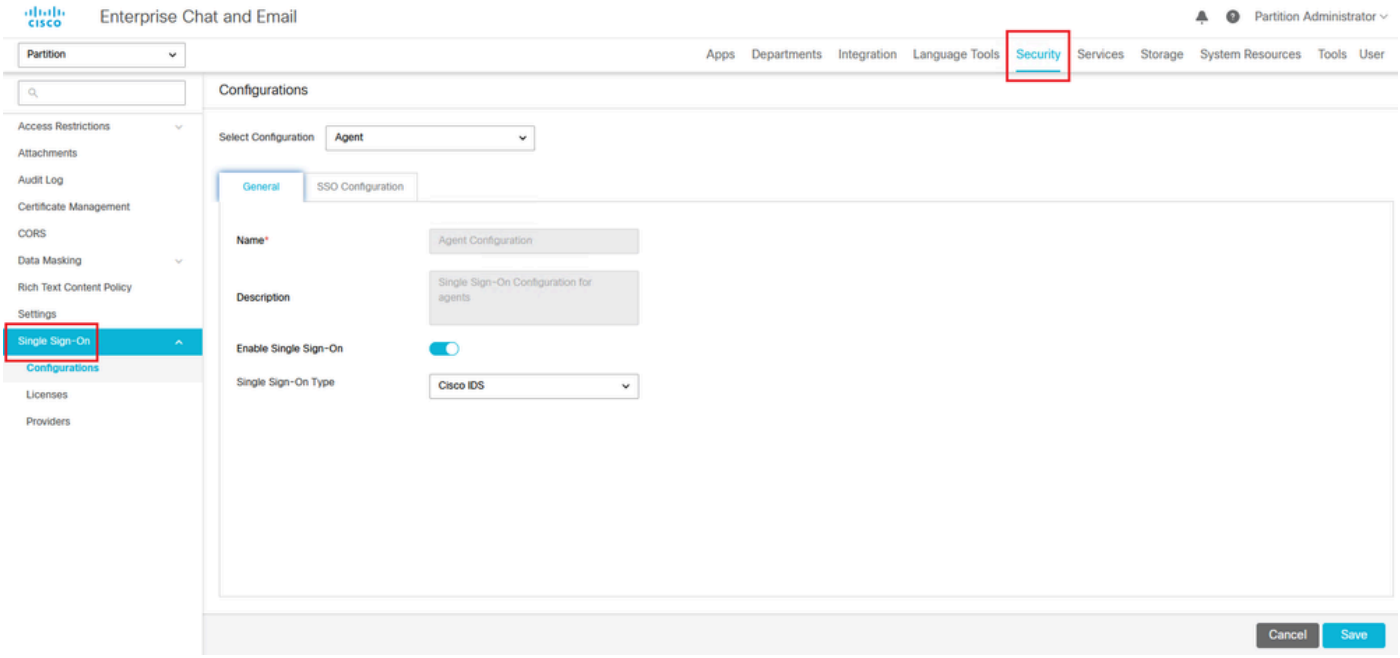


에이전트 단일 로그인 구성

14단계

1. ECE 관리 콘솔의 파티션 레벨 메뉴에서 보안 옵션을 클릭한 다음 왼쪽 메뉴에서 Single Sign-On > Configurations를 선택합니다.
2. 구성 선택 드롭다운에서 에이전트를 선택하고 일반 탭에서 구성을 설정합니다.

- Enable Single Sign-On(단일 로그인 활성화): SSO를 활성화하려면 Toggle(토글) 버튼을 클릭합니다.
- Single Sign-On Type(단일 로그인 유형): Cisco IDS를 선택합니다.



15단계

SSO Configuration(SSO 컨피그레이션) 탭을 클릭하고 컨피그레이션 세부 정보를 제공합니다.

a. OpenID 연결 공급자

기본 사용자 정보 엔드포인트 URL

- 기본 Cisco IDS 서버의 사용자 정보 엔드포인트 URL입니다.
- 이 URL은 사용자 토큰/사용자 정보 API를 검증합니다.
- https://cisco-ids-1:8553/ids/v1/oauth/userinfo 형식이며 cisco-ids-1은 기본 Cisco IDS 서버의 FQDN(Fully Qualified Domain Name)을 나타냅니다.

사용자 ID 클레임 이름

- Unified 또는 Packaged CCE에서 사용자 이름을 식별하는 사용자 정보 엔드포인트 URL에서 반환되는 클레임의 이름입니다.
- Unified CCE 또는 Packaged CCE의 클레임 이름과 사용자 이름이 일치해야 합니다.
- 이는 Bearer 토큰 검증에 대한 응답으로 얻은 클레임 중 하나입니다.
- Unified CCE 또는 Packaged CCE의 에이전트 사용자 이름이 User Principal Name(사용자 계정 이름)과 일치하는 경우 User Identity Claim name(사용자 ID 클레임 이름) 필드에 "upn"을 입력합니다.
- Unified CCE 또는 Packaged CCE의 에이전트 사용자 이름이 SAM Account Name(SAM 계정 이름)과 일치하는 경우 User Identity Claim name(사용자 ID 클레임 이름) 필드의 값으로 "sub"를 입력합니다.

보조 사용자 정보 엔드포인트 URL

- Cisco IDS 서버의 보조 사용자 정보 엔드포인트 URL입니다.
- https://cisco-ids-2:8553/ids/v1/oauth/userinfo 형식이며 cisco-ids-2는 보조 Cisco IDS 서버의 FQDN(Fully Qualified Domain Name)을 나타냅니다.

사용자 정보 엔드포인트 URL 메서드

- ECE에서 사용자 정보 끝점 URL에 전달자 토큰 유효성 검사를 호출하는 데 사용하는 HTTP 메서드입니다.
- 표시된 옵션 목록에서 POST를 선택합니다(IDS 서버의 방법과 일치하도록 여기서 POST를 선택합니다).

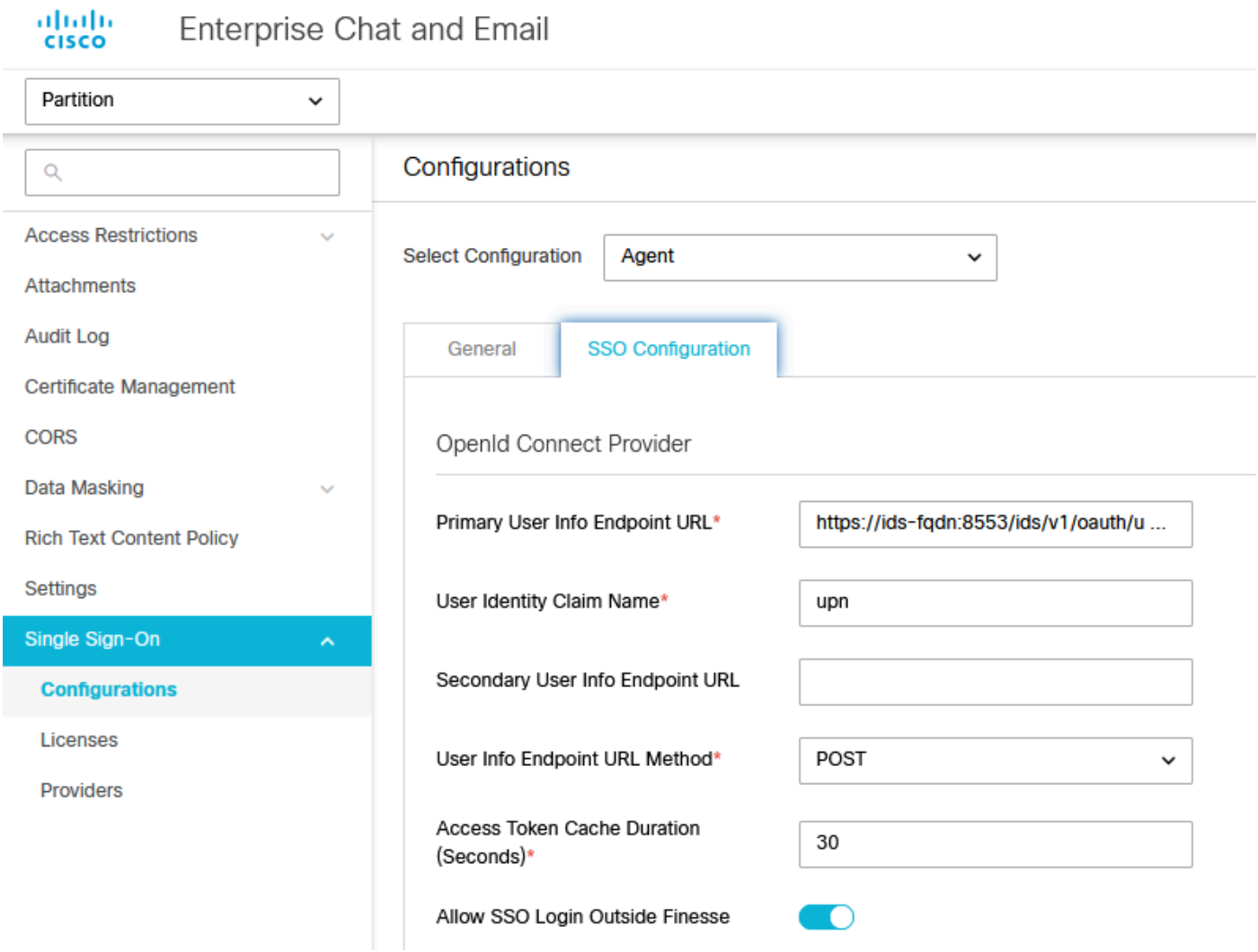
POST: 지정된 엔드포인트의 Cisco IDS 서버로 데이터를 전송하는 데 사용되는 방법입니다.

액세스 토큰 캐시 기간(초)

- ECE에서 전달자 토큰을 캐시해야 하는 기간(초)입니다.
- 검증 호출이 성공한 베어러 토큰은 캐시에만 저장됩니다. (최소값: 1, 최대값: 30)

Finesse 외부에서 SSO 로그인 허용

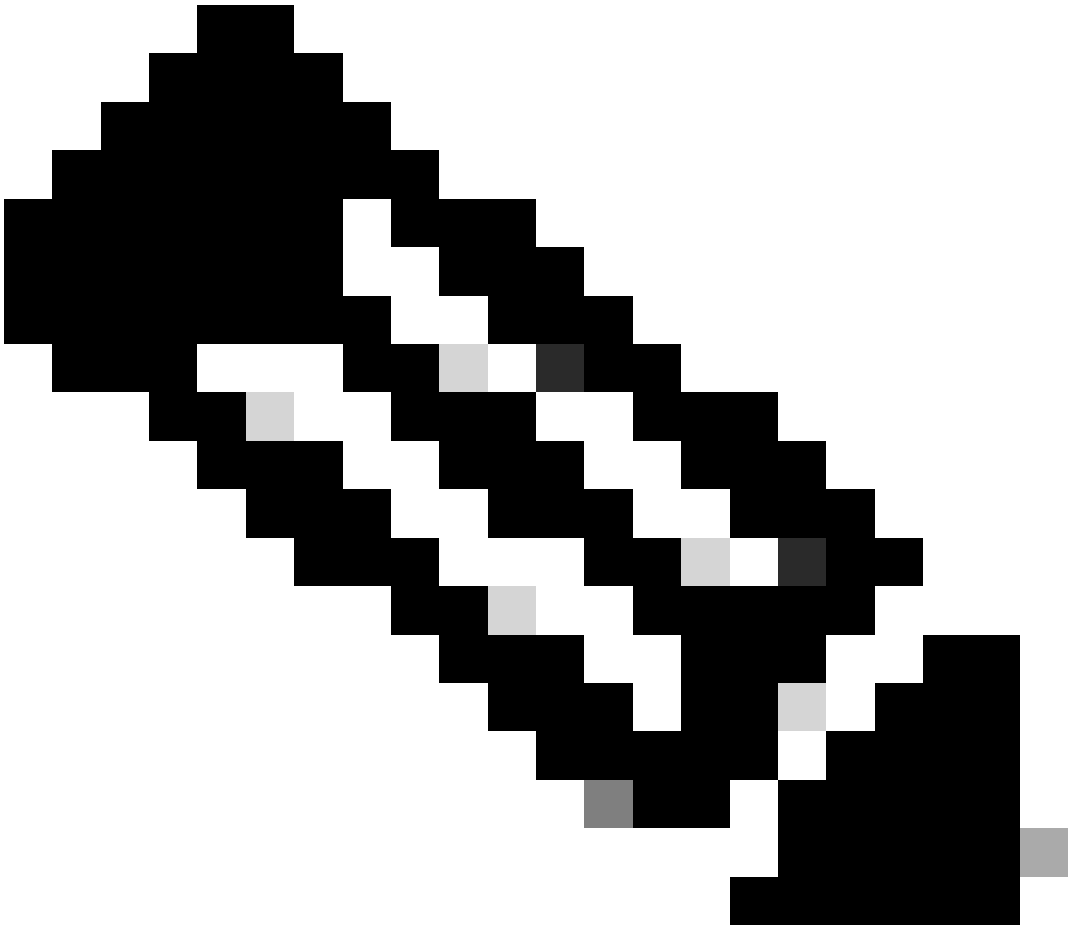
- 관리자 또는 수퍼바이저 역할을 가진 사용자가 SSO 로그인 자격 증명을 사용하여 Finesse 외부의 ECE 파티션에 로그인할 수 있도록 허용하려면 이 전환 버튼을 클릭합니다.
- 활성화된 경우 ID 제공자 및 서비스 제공자 섹션 아래에 정보를 제공해야 합니다.
- 이를 위해서는 IdP 컨피그레이션에서 공유 IdP 서버를 허용해야 합니다.



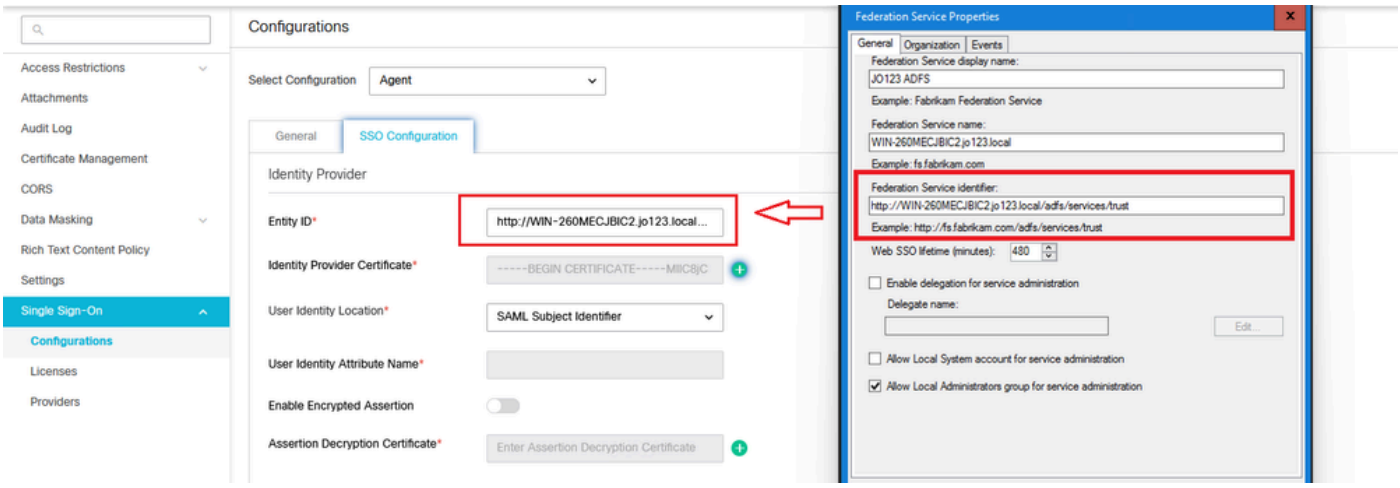
b. ID 공급자

엔티티 ID

- IdP 서버의 엔터티 ID입니다.

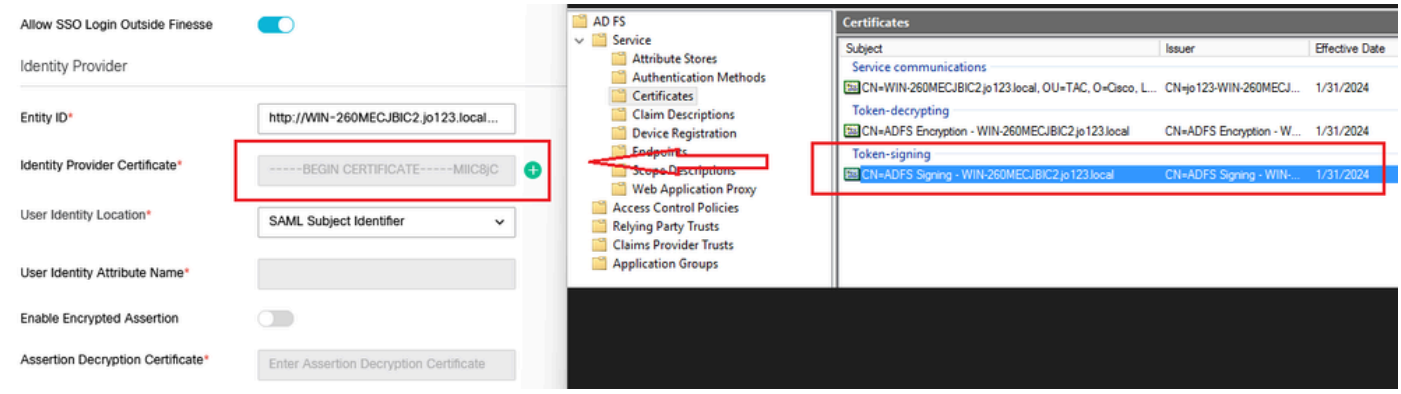


참고: 이 값은 AD FS 관리 콘솔의 '페더레이션 서비스 식별자' 값과 정확히 일치해야 합니다
.



ID 공급자 인증서

- 공개 키 인증서
- 인증서는 "-----BEGIN CERTIFICATE-----"로 시작하고 "-----END CERTIFICATE"로 끝나야 합니다-----
- AD FS Management Console(AD FS 관리 콘솔) > Service(서비스) > Certificates(인증서) > Token-signing(토큰 서명)의 토큰 서명 인증서입니다.



사용자 ID 위치

- SAML Subject Identifier를 선택하여 인증서의 ID 위치를 SAML 어설션의 주체(예: <saml:Subject>의 사용자 이름)와 같은 기본 SAML 주체 식별자로 설정합니다.
- SAML Attribute를 선택하여 인증서의 특정 특성(예: email.address)에 ID 위치를 할당합니다. User Identity Attribute Name 필드에 특성을 제공합니다.

사용자 ID 속성 이름

- 사용자 ID 위치 값이 SAML 특성인 경우에만 적용됩니다.
- SAML 어설션 내에서 이를 조정하여 이메일 주소와 같은 사용자 인증을 위한 다른 속성을 선택하는 데 사용할 수 있습니다.
- 또한 SAML 속성을 사용하여 새 사용자를 생성하는 데 사용할 수 있습니다.
- 예를 들어, 사용자가 email.address 속성에 제공된 값을 통해 식별되고 제공된 이메일 주소의 값이 시스템의 어떤 사용자와도 일치하지 않는 경우 제공된 SAML 속성으로 새 사용자가 생성됩니다.

Enable Encrypted Assertion(암호화된 어설션 활성화)(선택 사항)

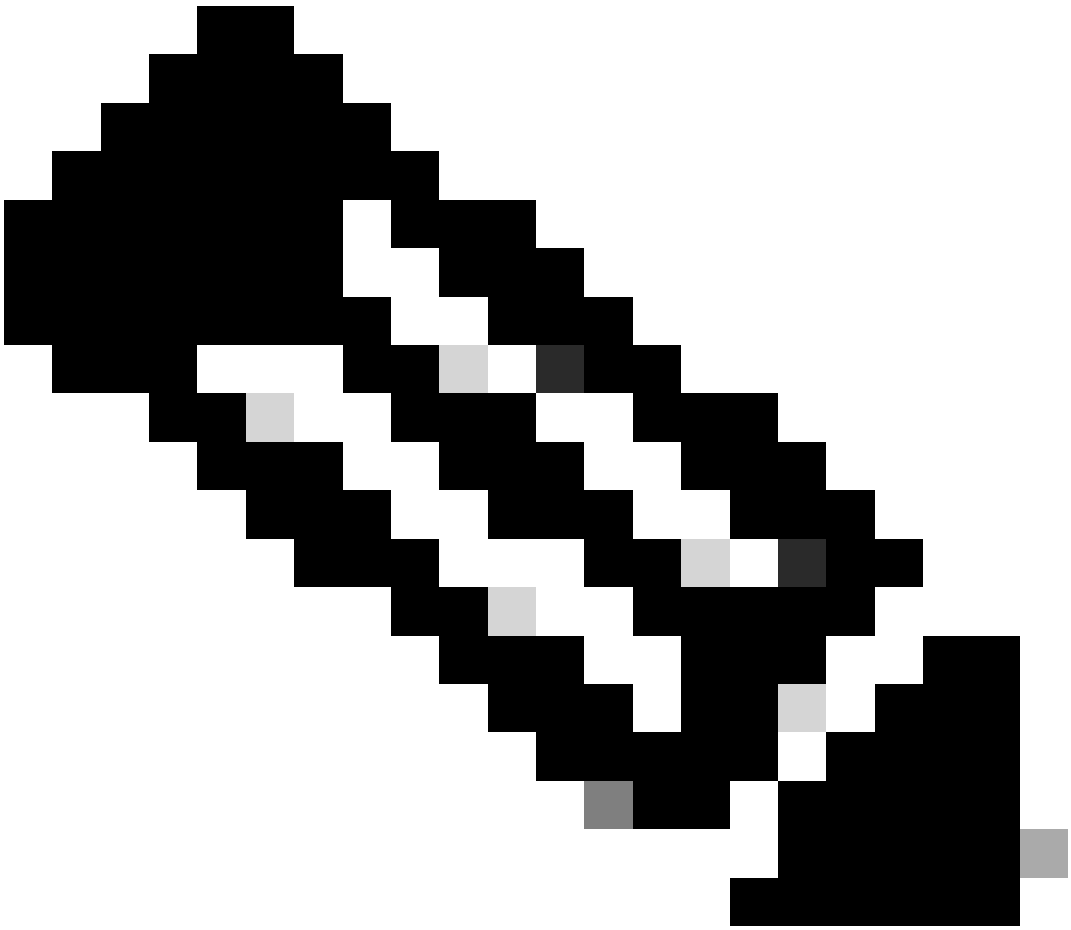
- 콘솔 로그인을 위해 ID 공급자로 암호화된 어설션을 활성화하려면 Toggle(전환) 버튼을 클릭하여 값을 Enabled(활성화됨)로 설정합니다.
- 그렇지 않은 경우 값을 Disabled(비활성화됨)로 설정합니다.

어설션 암호 해독 인증서

Enable encrypted assertion(암호화된 어설션 활성화)이 Enabled(활성화됨)로 설정된 경우 Search and Add(검색 및 추가) 버튼을 클릭하고 인증서 변경을 위한 선택 사항을 확인합니다.

Assertion Decryption Certificate(어설션 암호 해독 인증서) 창에 세부 정보를 제공합니다.

- Java 키 저장소 파일: Java 키 저장소 파일의 파일 경로를 제공합니다. 이 파일은 .jks 형식이며, ID 제공자가 보호하는 파일에 액세스하는 데 필요한 암호 해독 키를 포함합니다.
- Alias Name(별칭 이름): 암호 해독 키의 고유 식별자입니다.
- 키 저장소 비밀번호: Java 키 저장소 파일에 액세스하는 데 필요한 비밀번호입니다.
- 키 암호: 별칭의 암호 해독 키에 액세스하는 데 필요한 암호입니다.



참고: AD FS 관리 콘솔에서 구성된 ECE Relying Party Trust의 'Encryption' 탭에 있는 인증서와 일치해야 합니다.

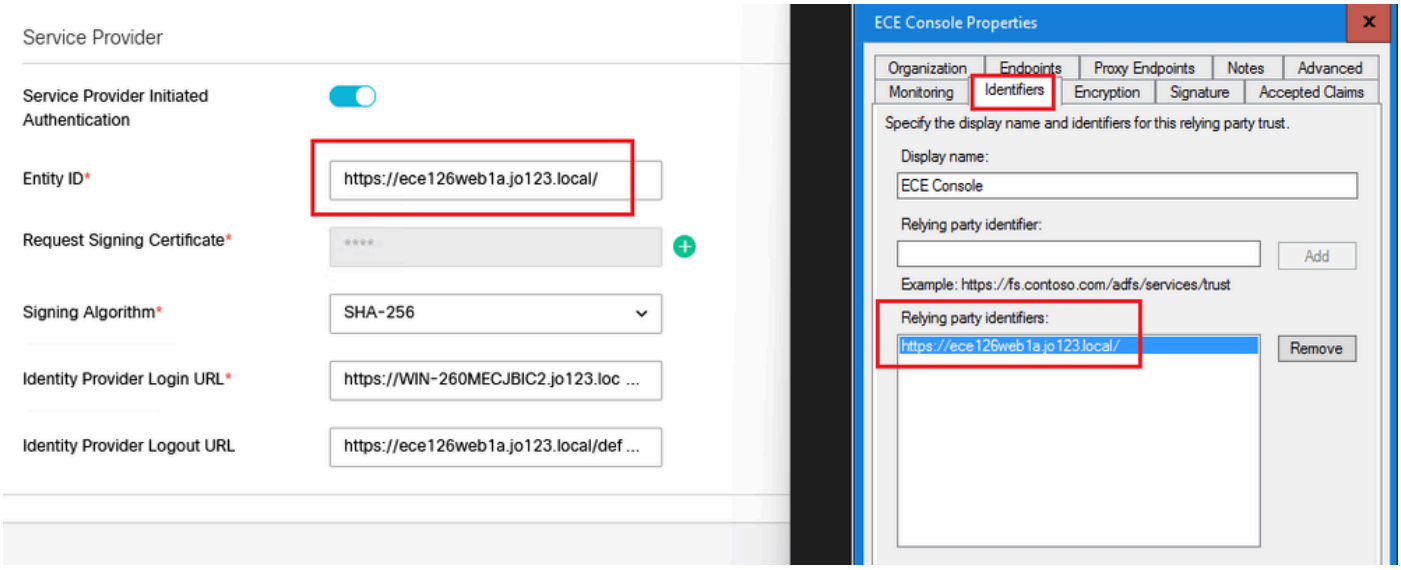
c. 서비스 공급자

서비스 공급자가 인증 시작

- 토글 단추를 사용으로 설정합니다.

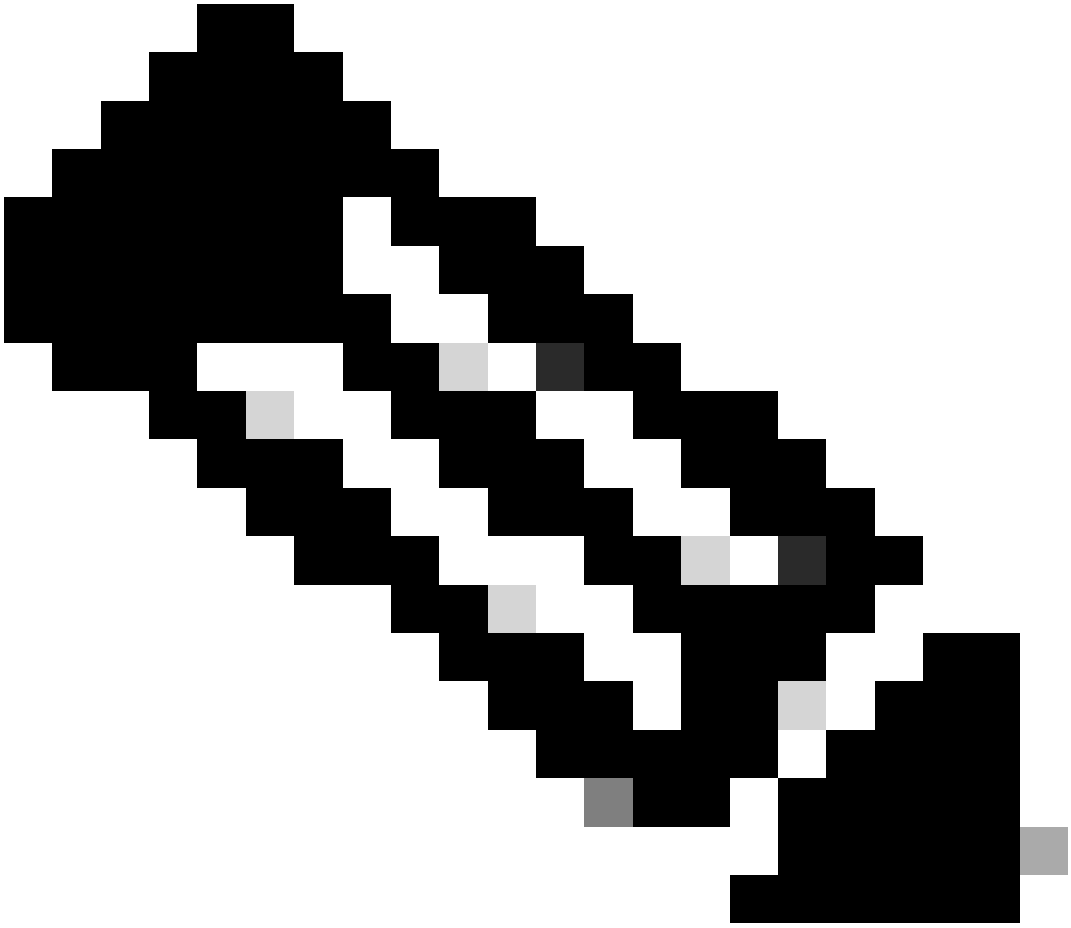
엔티티 ID

- ECE 애플리케이션의 외부 URL을 제공합니다.

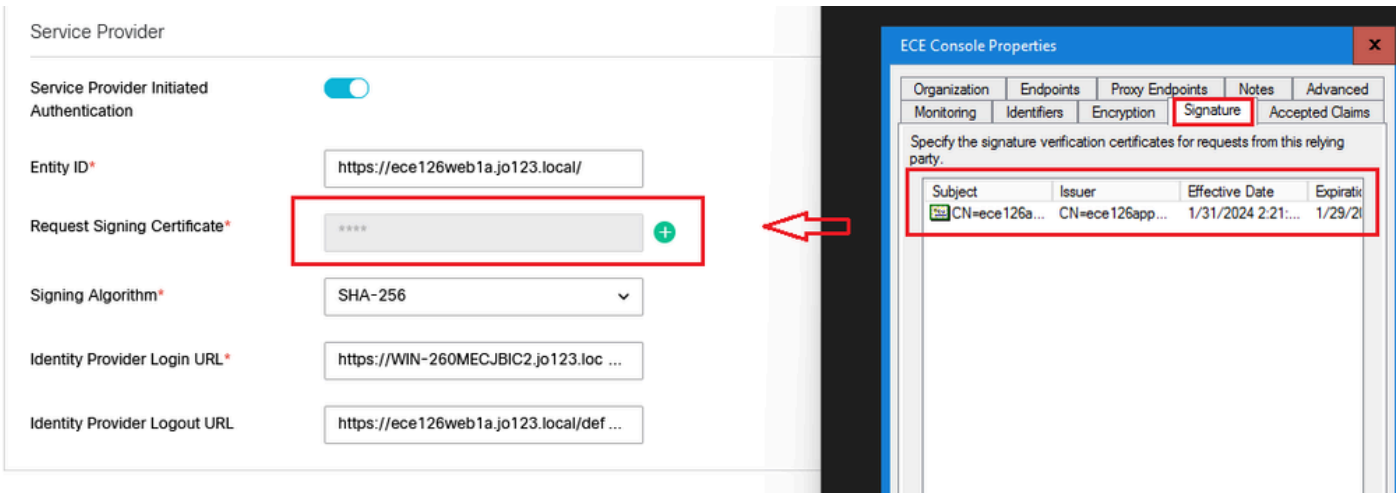


서명 인증서 요청

- 필요한 정보를 제공하려면 JKS(Java Keystore) 인증서가 필요합니다.
- 11단계에서 생성한 별칭 이름 및 키 저장소/키 비밀번호를 사용하여 .jks 파일을 업로드합니다.

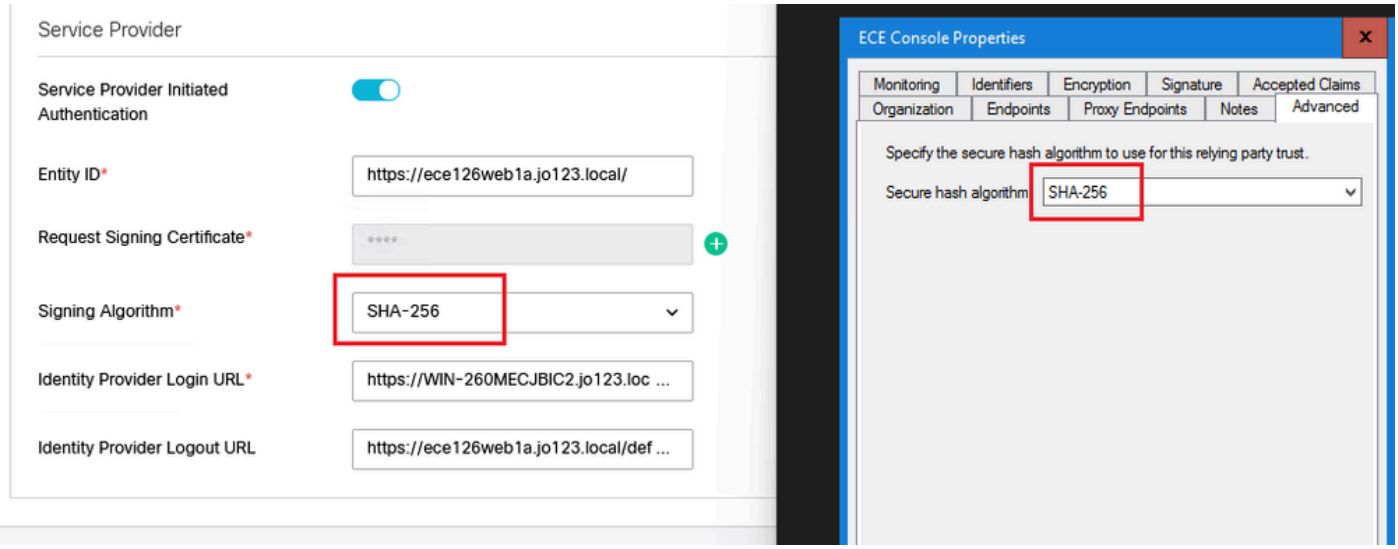


참고: 이는 AD FS 관리 콘솔에서 구성된 ECE Relying Party Trust의 'Signature' 탭에 업로드된 인증서와 일치해야 합니다.



서명 알고리즘

- 서비스 공급자에 대한 서명 알고리즘을 설정합니다.
- AD FS를 사용하는 경우 이 값은 Advanced(고급) 탭의 ECE에 대해 생성된 신뢰 당사자 트러스트에서 선택한 알고리즘과 일치해야 합니다.



ID 공급자 로그인 URL

- SAML 인증을 위한 URL입니다.
- 예를 들어 AD FS의 경우 http://<AD FS>/adfs/ls입니다.

ID 공급자 로그아웃 URL

- 로그아웃 시 사용자가 리디렉션되는 URL입니다. 이는 선택 사항이며 모든 URL이 될 수 있습니다.
- 예를 들어 상담원은 SSO 로그아웃 후 https://www.cisco.com 또는 기타 URL로 리디렉션될 수 있습니다.

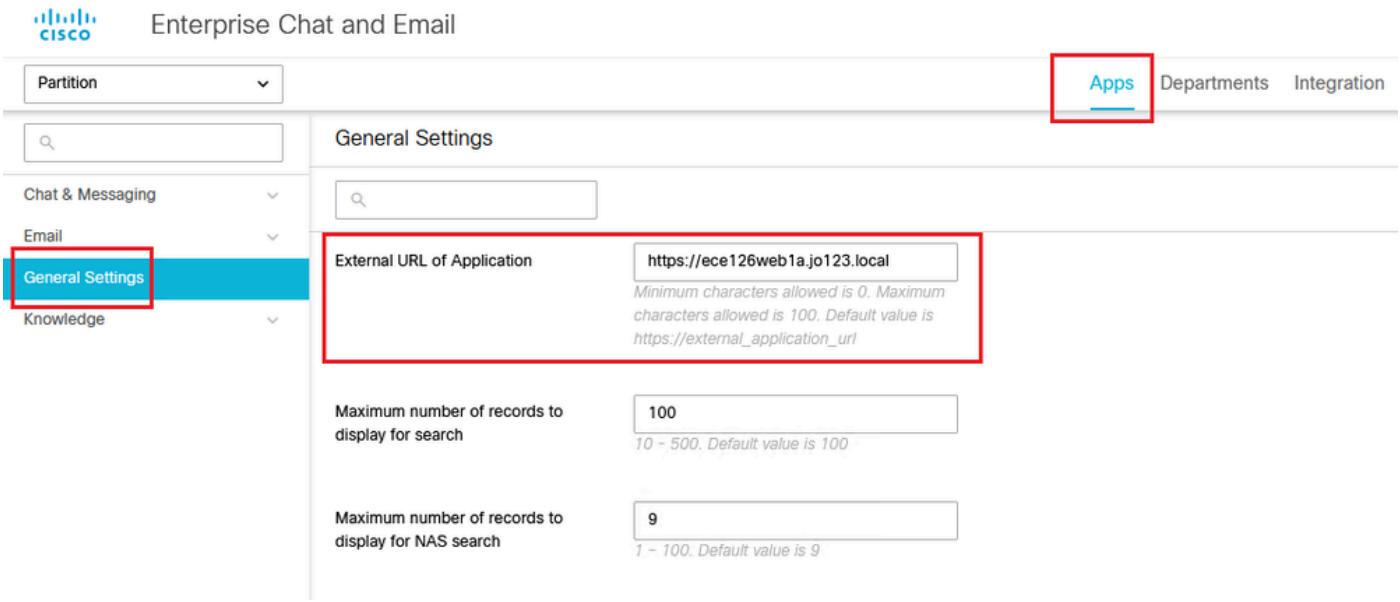
16단계

Save(저장)를 클릭합니다.

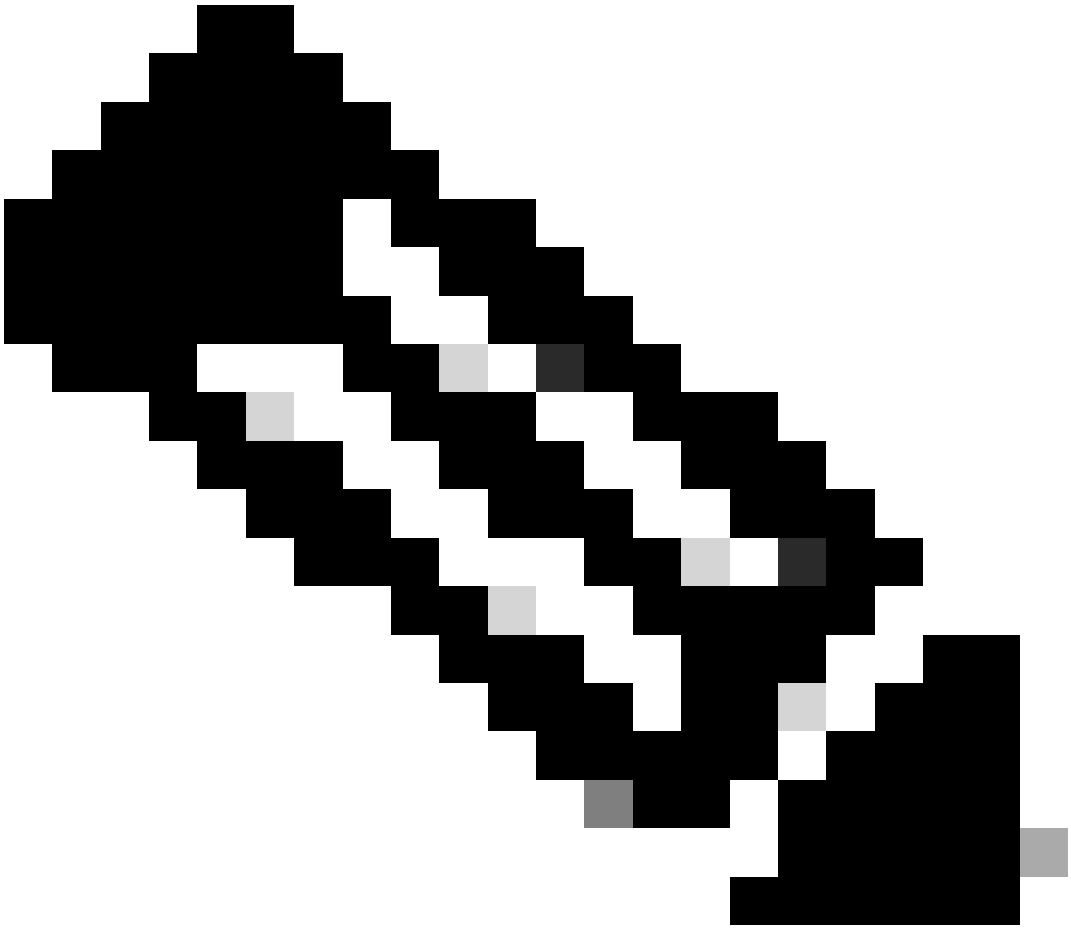
파티션 설정에서 웹 서버/LB URL 설정

17단계

Partition settings(파티션 설정) > Apps(앱) 탭에서 올바른 웹 서버/LB URL을 입력했는지 확인하고 General Settings(일반 설정) > External URL of the Application(애플리케이션 외부 URL)로 이동합니다.



파티션 관리자를 위한 SSO 구성



참고:

- 이 단계는 PCCE에만 적용됩니다.
- CCE 관리 웹 인터페이스 https:///cceadmin에서 액세스하는 ECE 가젯에 사용됩니다.

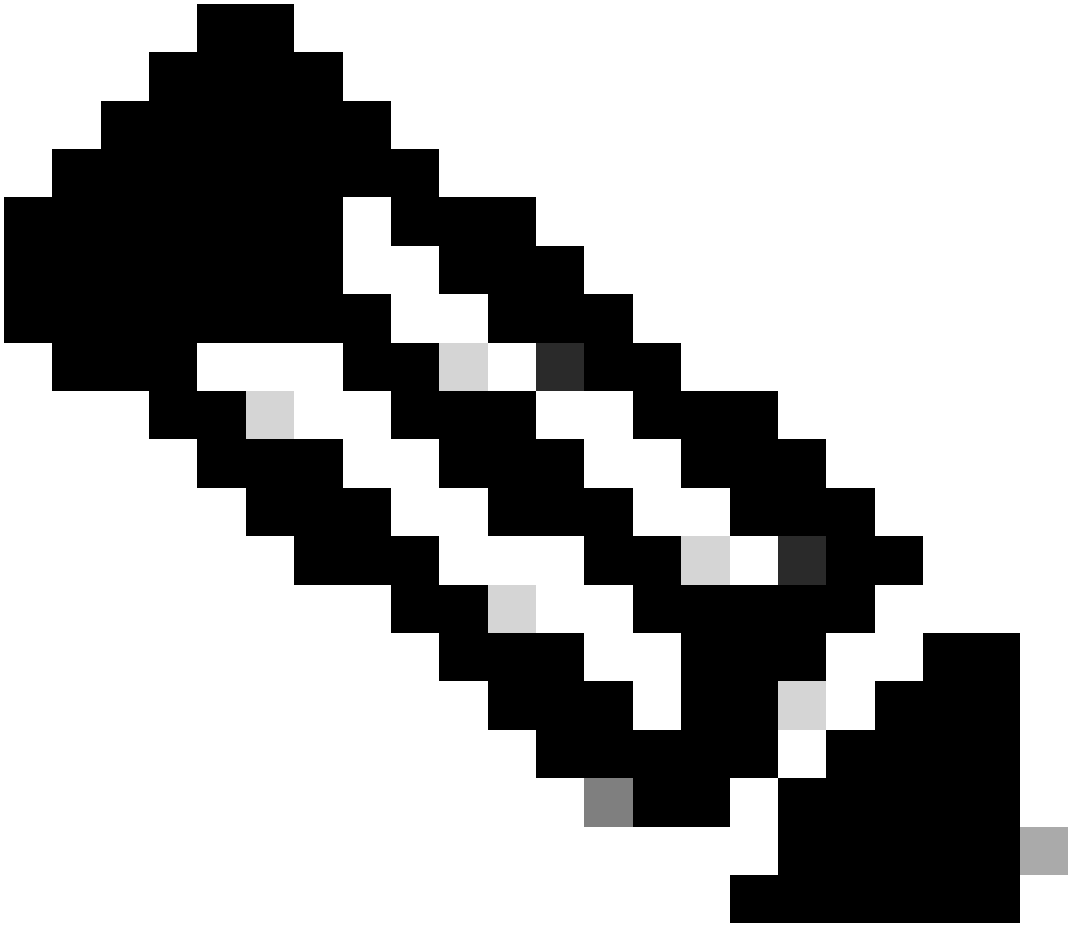
18단계

파티션 관리자를 위해 SSO를 구성하려면

1. ECE 관리 콘솔의 파티션 레벨 메뉴에서 보안 옵션을 클릭한 다음 왼쪽 메뉴에서 Single Sign-On > 구성을 선택합니다.
2. Select Configuration(컨피그레이션 선택) 드롭다운에서 Partition Administrators(파티션 관리자)를 선택하고 컨피그레이션 세부 정보를 입력합니다.

LDAP URL

- LDAP 서버의 URL입니다.
- LDAP 서버의 도메인 컨트롤러 URL(예: ldap://LDAP_server:389) 또는 글로벌 카탈로그 URL(예: ldap://LDAP_server:3268)일 수 있습니다.
- ECE가 LDAP 조회로 구성된 경우 CCE 관리 콘솔을 통해 ECE에 액세스하면 파티션이 시스템에 자동으로 추가될 수 있습니다.
- 그러나 단일 포리스트에 여러 도메인이 있거나 대체 UPN이 구성된 Active Directory 구축에서는 표준 LDAP 포트가 389 및 636인 도메인 컨트롤러 URL을 사용할 수 없습니다.
- 포트 3268 및 3269와 함께 글로벌 카탈로그 URL을 사용하도록 LDAP 통합을 구성할 수 있습니다.



참고: 글로벌 카탈로그 URL을 사용하는 것이 좋습니다. GC를 사용하지 않는 경우 ApplicationServer 로그의 오류는 다음과 같습니다.

- LDAP 인증 <@>의 예외 javax.naming.PartialResultException: 처리되지 않은 연속 참조; 나머지 이름 'DC=example,DC=com'

DN 특성

- 사용자 로그인 이름을 포함하는 DN의 특성입니다.
- 예: userPrincipalName.

기본

- Base에 대해 지정된 값은 애플리케이션에서 검색 기반으로 사용됩니다.
- Search base는 LDAP 디렉토리 트리에서 검색하기 위한 시작 위치입니다.
- 예를 들어, DC=mycompany, DC=com입니다.

LDAP 검색을 위한 DN

- LDAP 시스템에서 익명 바인딩을 허용하지 않는 경우 LDAP 디렉토리 트리에 대한 검색 권한이 있는 사용자의 DN(Distinguished Name)을 제공합니다.
- LDAP 서버에서 익명 바인딩을 허용하는 경우 이 필드를 비워 둡니다.

암호

- LDAP 시스템에서 익명 바인딩을 허용하지 않는 경우 LDAP 디렉토리 트리에 대한 검색 권한이 있는 사용자의 비밀번호를 제공합니다.
- LDAP 서버에서 익명 바인딩을 허용하는 경우 이 필드를 비워 둡니다.

19단계

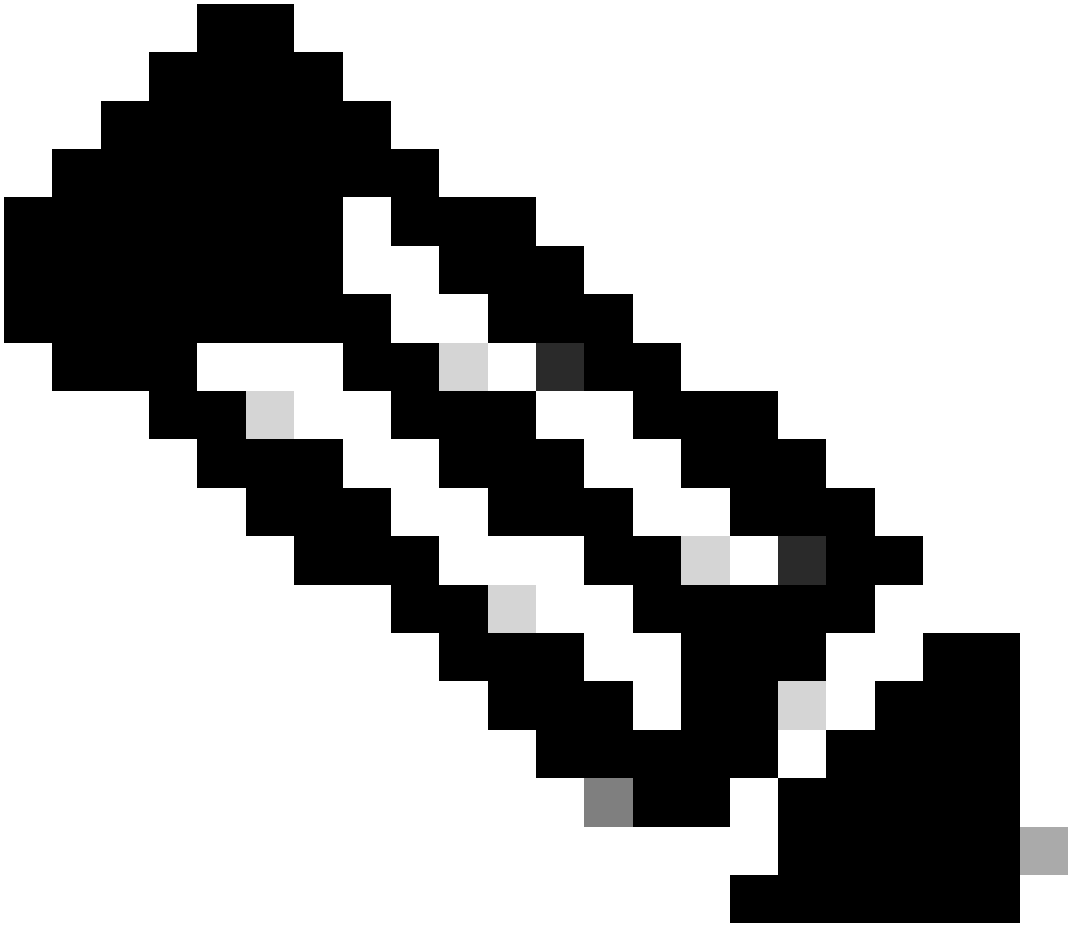
Save(저장)를 클릭합니다.

이제 ECE의 에이전트 및 파티션 관리자에 대한 Single Sign-On 컨피그레이션이 완료되었습니다.

문제 해결

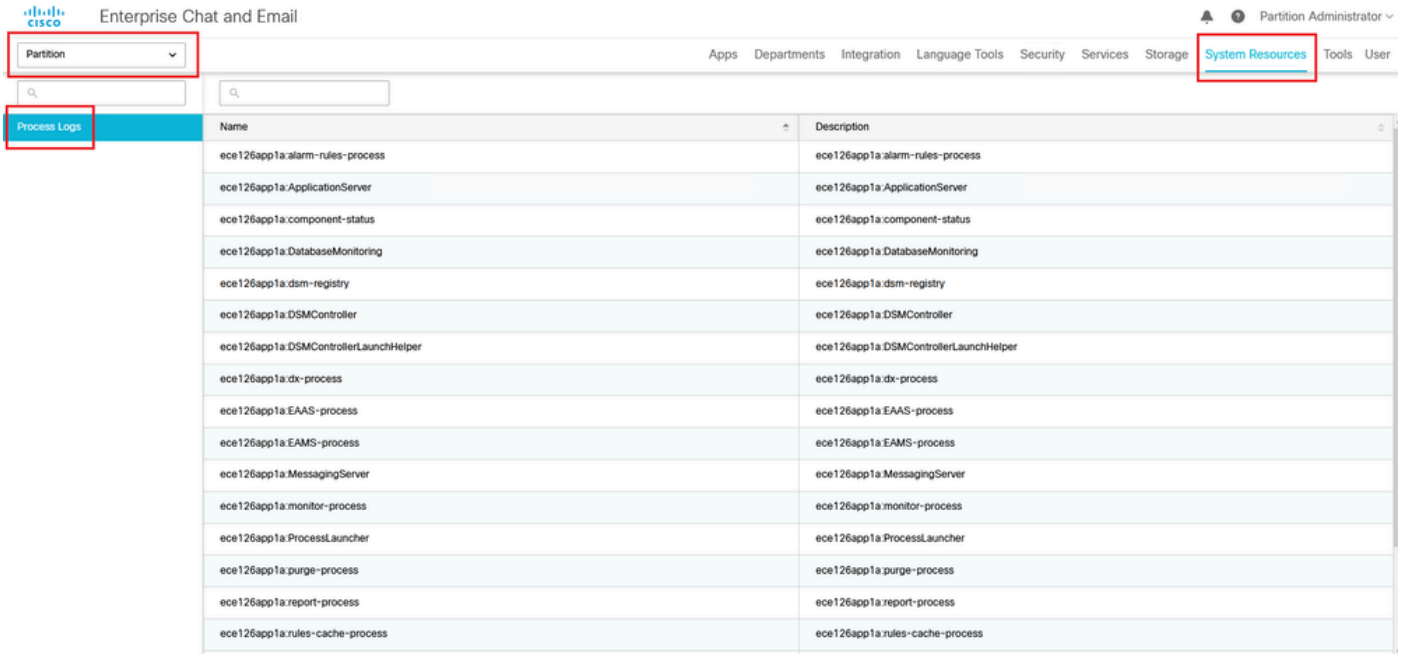
추적 수준 설정

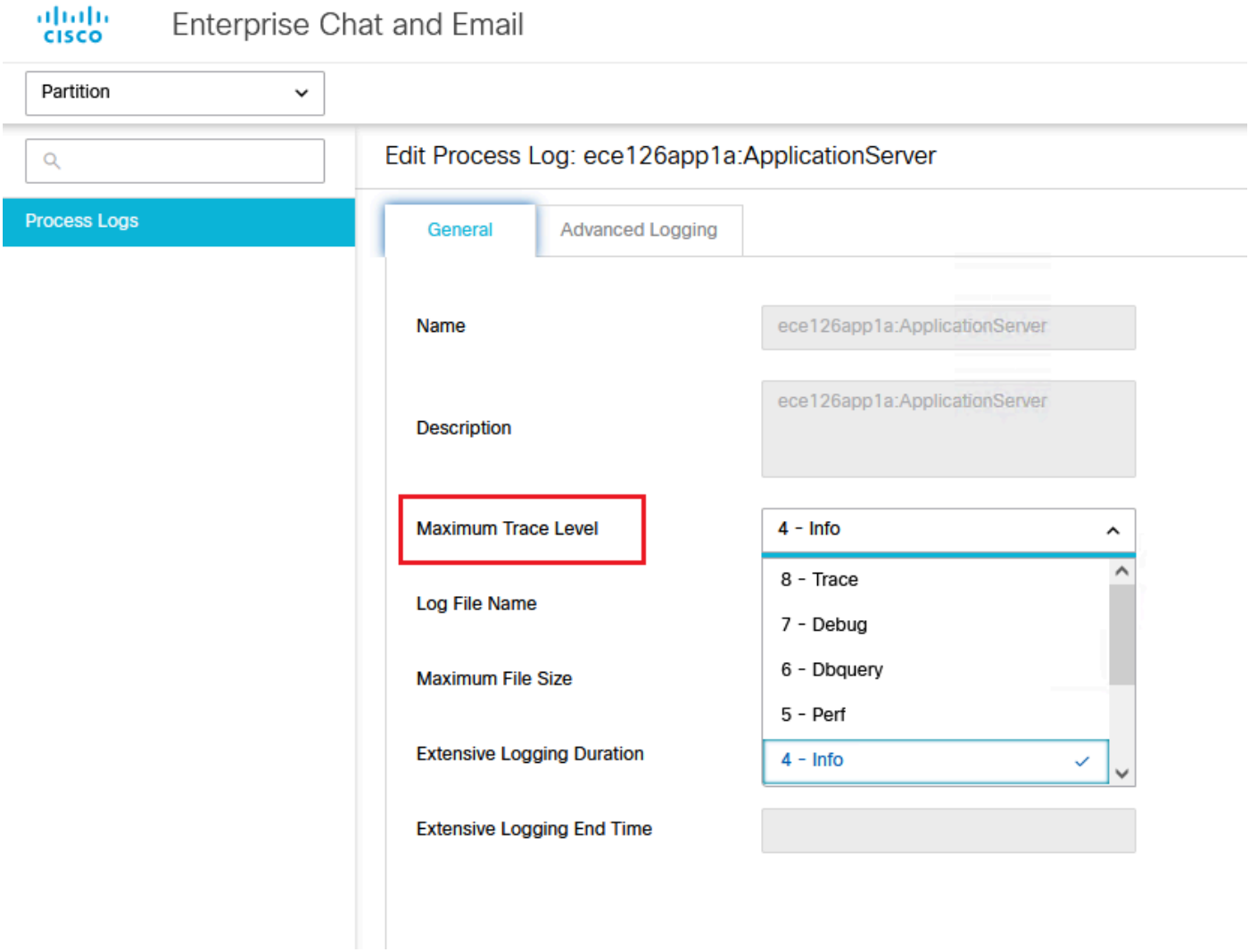
1. ECE 관리 콘솔의 파티션 레벨 메뉴에서 시스템 리소스 옵션을 클릭한 다음 왼쪽 메뉴에서 프로세스 로그를 선택합니다.
2. 프로세스 목록에서 ApplicationServer 프로세스를 선택하고 '최대 추적 레벨' 드롭다운 메뉴에서 원하는 추적 레벨을 설정합니다.



참고:

- 초기 설정 또는 재컨피그레이션 중 SSO 로그인 오류를 해결하려면 ApplicationServer 프로세스 추적을 레벨 7로 설정합니다.
- 오류가 재현되면 로그를 덮어쓰지 않도록 추적 수준을 기본 수준 4로 다시 설정합니다.





문제 해결 시나리오 1

오류

- 오류 코드: 500
- 오류 설명: ID 공급자 로그인에 실패하여 현재 응용 프로그램에서 사용자를 로그인할 수 없습니다.

로그 분석

- IdP 로그인 실패 - <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder" /></samlp:Status>
- 여기서 상태 "Responder"는 AD FS 측에 문제가 있음을 나타냅니다. 이 경우 주로 ECE 관리 콘솔(SSO Configuration > Service Provider)에 업로드된 "Request Signing Certificate" 및 'Signature' 탭의 ECE Relying Party Trust에 업로드된 인증서가 사용됩니다.
- Java 키 저장소 파일을 사용하여 생성되는 인증서입니다.

응용 프로그램 서버 로그 - 추적 수준 7:

<#root>

unmarshallAndValidateResponse:

2022-09-21 18:18:15.002 GMT+0000 <@> ERROR <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
2022-09-21 18:18:15.002 GMT+0000 <@> INFO <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID:

L10N_USER_STATUS_CODE_ERROR:

2022-09-21 18:18:15.002 GMT+0000 <@> ERROR <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_0
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Han
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Han
at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(OpenI
at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdmin
at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.j
.
.
.
.
at java.lang.Thread.run(Thread.java:834) ~[?:?]

errorCode=500&errorString=The application is not able to login the user at this time as Identity Provide

2022-09-21 18:18:15.003 GMT+0000 <@> DEBUG <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
2022-09-21 18:18:15.003 GMT+0000 <@> DEBUG <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID

해결

- '에이전트 Single Sign-On 구성 - 서비스 공급자' 섹션의 '서명 인증서 요청' 구성을 참조하십시오.
- 11단계에서 생성된 Java Keystore .jks 파일이 ECE 관리 콘솔의 SSO Configuration(SSO 구성) > Select Configuration 'Agent'(구성 '에이전트' 선택) > 'SSO Configuration'(SSO 구성) 탭

> Service Provider(통신 사업자) > Request Signing certificate(서명 인증서 요청) 아래에 있는 "Request Signing certificate(서명 인증서 요청)" 필드에 업로드되었는지 확인합니다.
- .crt 파일이 ECE 신뢰 당사자 트러스트의 '서명' 탭 아래에 업로드되었는지 확인합니다(12단계).

문제 해결 시나리오 2

오류

- 오류 코드: 400
- 오류 설명: SAML 응답 토큰이 잘못되었습니다. 서명 유효성 검사에 실패했습니다.

로그 분석

- 이 오류는 AD FS의 '토큰 서명 인증서'와 ECE SSO 구성의 'ID 공급자 인증서' 간에 인증서가 일치하지 않음을 나타냅니다.

응용 프로그램 서버 로그 - 추적 수준 7:

<#root>

```
Entering 'validateSSOCertificate' and validating the saml response against certificate:


2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.520 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
.....
-----END CERTIFICATE----- <@>
2022-10-07 15:27:34.523 GMT+0000 <@> INFO <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID:


Error: Could not parse certificate: java.io.IOException: Incomplete data:


2022-10-07 15:27:34.523 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.524 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID


Signature validation failed:


2022-10-07 15:27:34.525 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> INFO <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID:
2022-10-07 15:27:34.525 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
```

해결

- 로그 스니펫에 나타나는 오류 '인증서를 구문 분석할 수 없습니다. java.io.IOException: 불완전한 데이터'는 'ID 공급자 인증서' 내용이 올바르게 입력되지 않았음을 나타냅니다
- 이 문제를 해결하려면: AS FS Management(AS FS 관리) > AD FS > Service(서비스) > Certificates(인증서) > Token-Signing(토큰 서명) > Export this certificate(이 인증서 내보내기)에서 텍스트 편집기에서 Open(열기) > Copy all contents(모든 콘텐츠 복사) > Save(저장)에서 SSO configuration(SSO 컨피그레이션) > Save(저장)를 클릭합니다.
- '에이전트 Single Sign-On 구성 - ID 공급자' 섹션 아래의 'ID 공급자 인증서' 구성을 참조하십시오(15단계).

문제 해결 시나리오 3

오류

- 오류 코드: 401-114
- 오류 설명: SAML 특성에서 사용자 ID를 찾을 수 없습니다.

로그 분석

응용 프로그램 서버 로그 - 추적 수준 7:

<#root>

getSSODataFromSAMLToken:

2024-02-01 01:44:32.081 GMT+0000 <@> ERROR <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
2024-02-01 01:44:32.081 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@

L10N_USER_IDENTIFIER_NOT_FOUND_IN_ATTRIBUTE:

2024-02-01 01:44:32.081 GMT+0000 <@> ERROR <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
com.egain.platform.module.security.sso.exception.SSOLoginException: null
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.getSSODataFromSAMLToken(SAML2_0_Hand
*at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_*
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(Open
at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdmi
at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.
.
.
.
at java.lang.Thread.run(Thread.java:830) [?:?]

errorCode=401-114&errorString=User Identity not found in SAML attribute: 'upn':

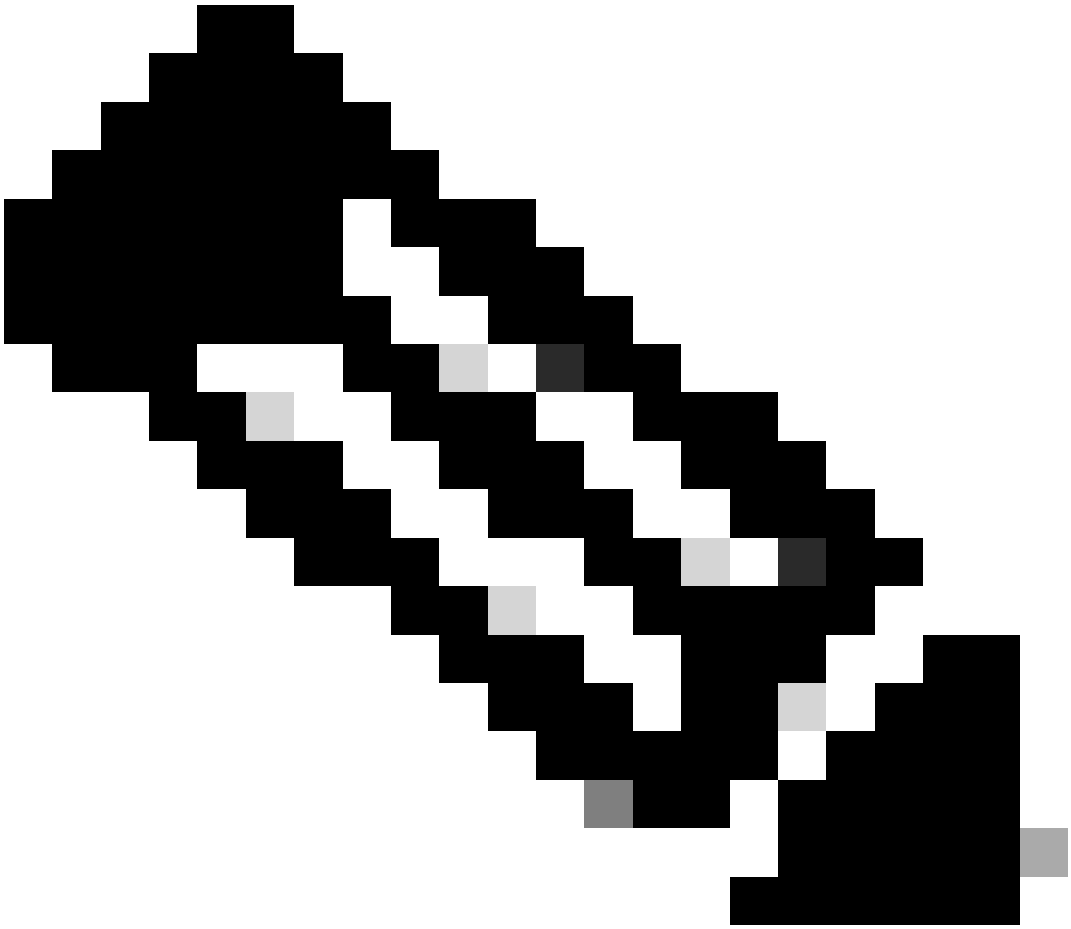
2024-02-01 01:44:32.083 GMT+0000 <@> DEBUG <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
2024-02-01 01:44:32.083 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@

해결

- 이 오류는 '사용자 ID 위치' 및 '사용자 ID 특성 이름' 필드에서 구성 문제/불일치를 나타냅니다.
- ECE 관리 콘솔에서 '사용자 ID 위치' 및 '사용자 ID 속성 이름'을 확인하고 수정하려면 Single Sign-On > Configurations > Select Configuration 드롭다운 메뉴에서 Agent > SSO Configuration 탭 > Identify Provider를 선택합니다(15단계).

관련 정보

ECE 설치 또는 통합을 시작하기 전에 반드시 철저하게 검토해야 하는 주요 문서입니다. 이것은 ECE 문서의 포괄적인 목록이 아닙니다.



참고:

- 대부분의 ECE 문서에는 두 가지 버전이 있습니다. PCCE용 버전을 다운로드하여 사용하고 있는지 확인하십시오. 문서 제목에는 버전 번호 뒤에 Packaged Contact

---

Center Enterprise용 또는 (PCCE용) 또는 (UCCE 및 PCCE용)이 있습니다.
- Cisco Enterprise Chat and Email 설명서의 시작 페이지에서 설치, 업그레이드 또는 통합 전에 업데이트가 있는지 확인합니다.
- https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

---

ECE 버전 12.6(1)

- 엔터프라이즈 채팅 및 이메일 관리자 가이드

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.