ISE를 사용하여 Catalyst Center 외부 인증 TACACS 구성

목차

소개

이 문서에서는 TACACS+ 인증을 활성화하기 위해 Cisco Identity Services Engine을 Catalyst Center와 통합하는 데 필요한 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 및 Cisco Catalyst Center에 대한 관리자 액세스.
- AAA(Authentication, Authorization, Accounting) 개념에 대한 기본 이해.
- TACACS+ 프로토콜에 대한 실무 지식.
- Catalyst Center와 ISE 서버 간 네트워크 연결.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco Catalyst Center 버전 2.3.7.x
- Cisco ISE(Identity Services Engine) 버전 3.x 이상
- 외부 사용자 인증을 위한 TACACS+ 프로토콜

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

이러한 통합을 통해 외부 사용자는 Catalyst Center에 로그인하여 관리 액세스 및 관리를 수행할 수 있습니다.

구성

Cisco ISE(Identity Services Engine)

TACACS+ 서비스 라이센스 및 활성화

ISE에서 TACACS+ 컨피그레이션으로 시작하기 전에 올바른 라이센스가 설치되고 기능이 활성화되었는지 확인해야 합니다.

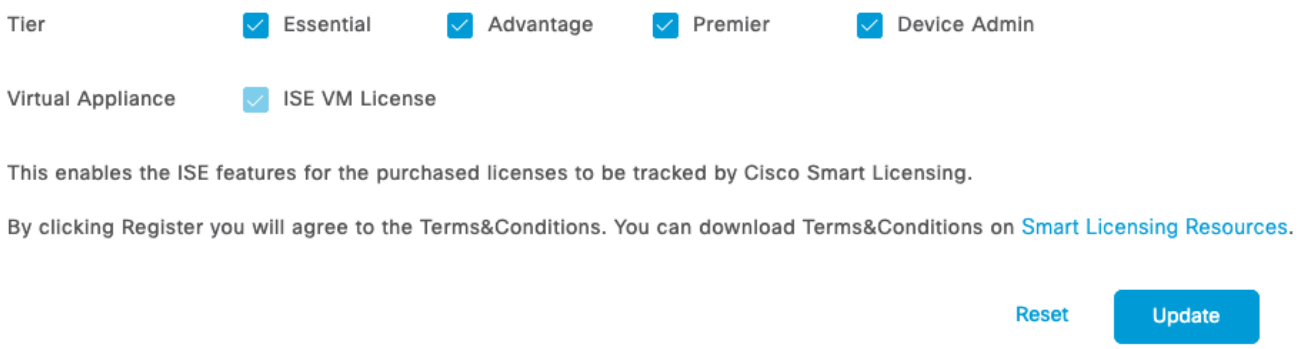
1. Cisco Smart Software Manage 또는 Cisco License Central 포털에서 PID 라이센스 L-ISE-TACACS-ND=이 있는지 확인합니다.

ISE 라이센싱 포털에서 디바이스 관리를 활성화합니다.

- 디바이스 관리자 라이센스(PID: L-ISE-TACACS-ND=)는 PSN(Policy Service Node)에서 TACACS+ 서비스를 활성화합니다.
- 다음으로 이동합니다.

  Administration(관리) > System(시스템) > Licensing(라이센스)

- Tier(계층) 옵션에서 Device Admin(디바이스 관리)의 확인란을 선택합니다.



장치 관리자

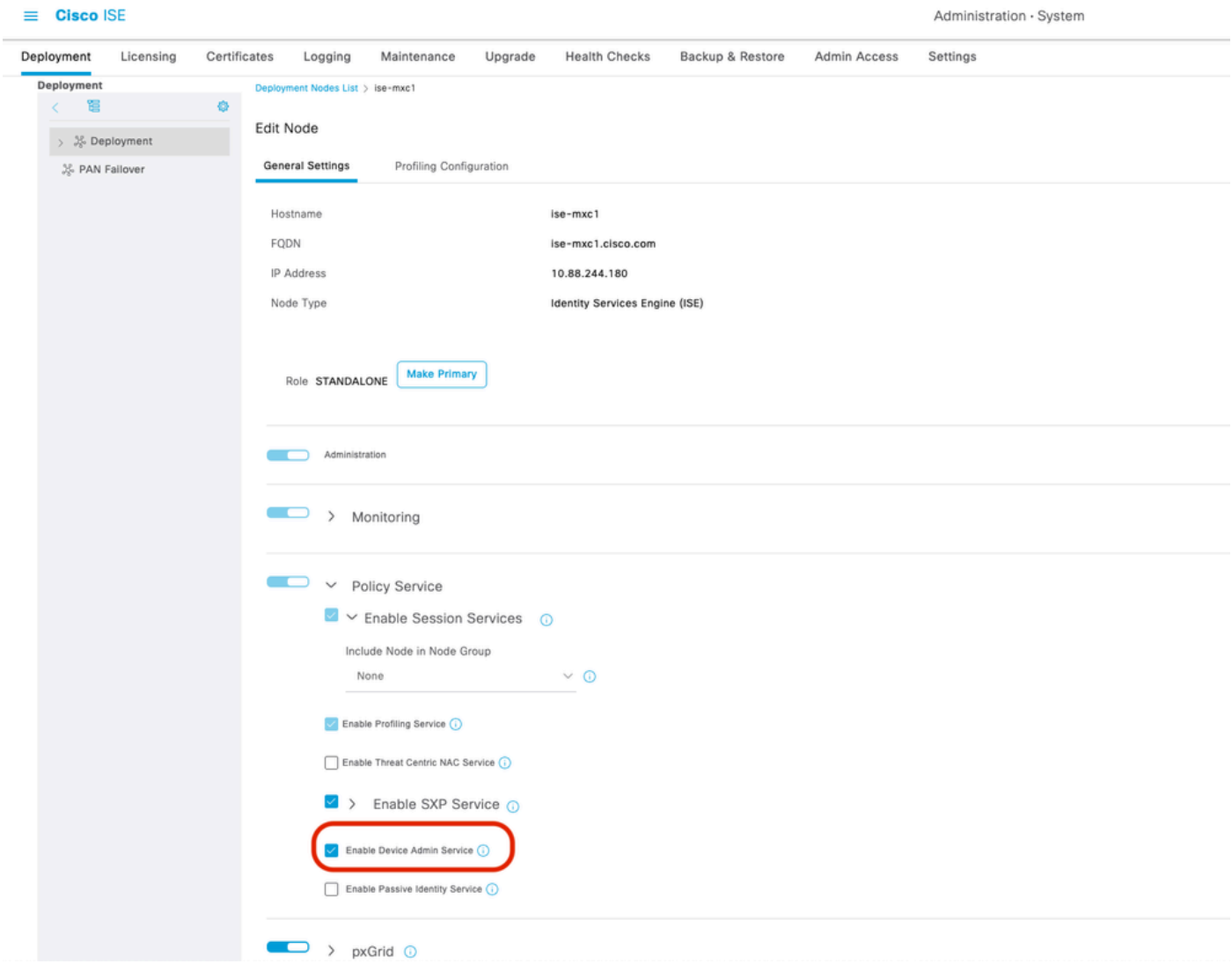
라이센스 디바이스 관리

3. TACACS+ 서비스를 실행하는 ISE 노드에서 Device Admin Service를 활성화합니다.

- 다음으로 이동합니다.

  관리 > 시스템 > 구축 > 노드를 선택 합니다

- Enable Device Admin Service(디바이스 관리 서비스 활성화) 옵션을 선택합니다.



장치 관리 서비스 사용

관리자 사용자 생성 및 네트워크 디바이스 추가

1. 관리자 사용자를 생성합니다.

- 이 사용자 계정은 ISE 인증을 통해 Catalyst Center UI에 로그인하는 데 사용됩니다.
- 다음으로 이동합니다.

Work Centers(작업 센터) > Network Access(네트워크 액세스) > Identity(ID) > Network Access User(네트워크 액세스 사용자)

- 새 사용자(예: catc-user)를 추가합니다.
- 사용자가 이미 존재하는 경우 다음 단계로 진행합니다.

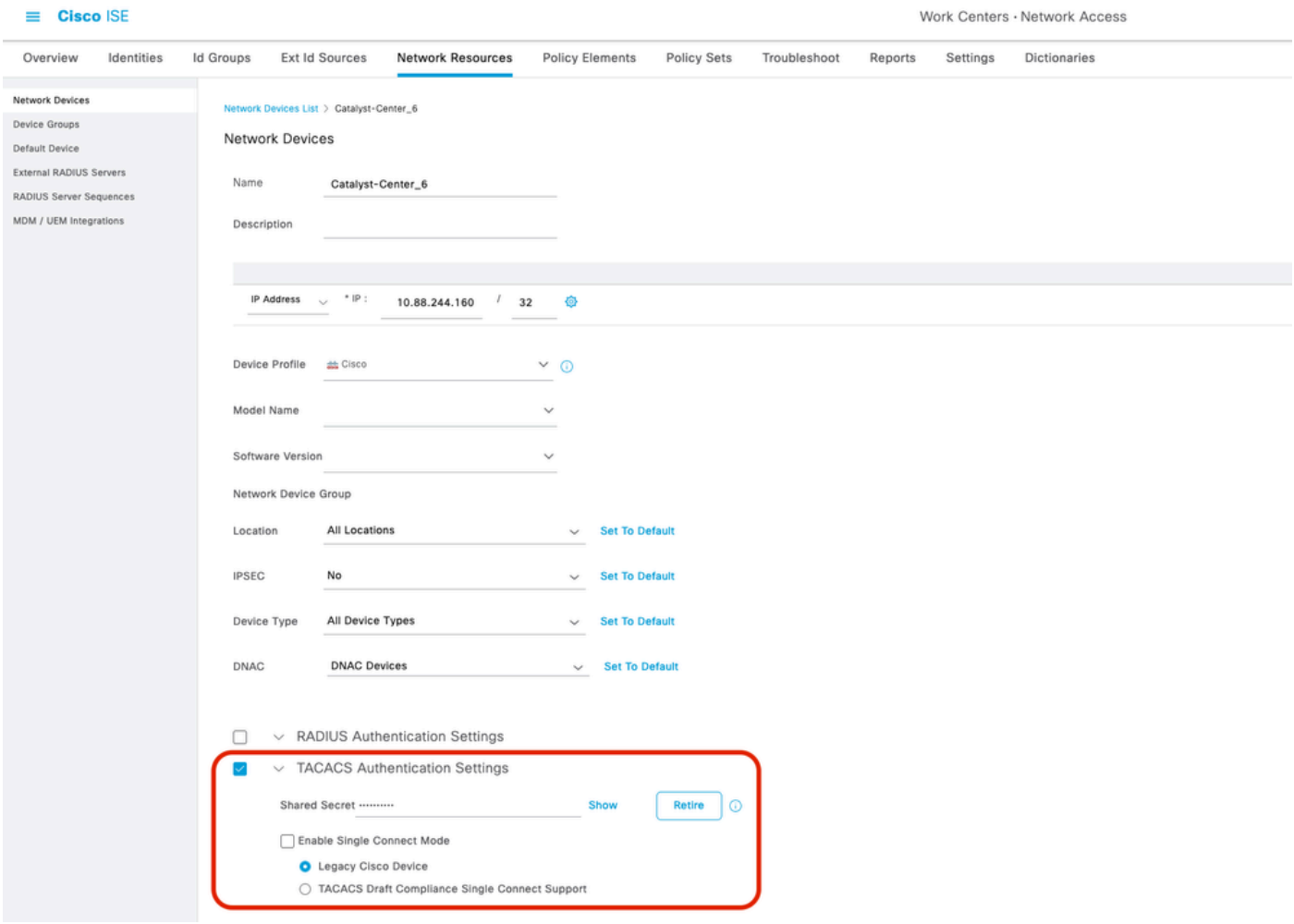
2. 네트워크 장치를 만듭니다.

- 다음으로 이동합니다.

Work Centers(작업 센터) > Network Access(네트워크 액세스) > Identity(ID) > Network

Resource(네트워크 리소스)

- Catalyst Center의 IP 주소를 추가하거나 Catalyst Center IP가 있는 서브넷을 정의합니다.
- 디바이스가 이미 있는 경우 다음 매개변수가 포함되어 있는지 확인합니다.
  - TACACS 인증 설정이 활성화됩니다.
  - 공유 암호가 구성되고 알려졌습니다(나중에 Catalyst Center에서 필요하므로 이 값을 저장하십시오).



TACACS 인증 설정

TACACS+ 프로파일 구성

1. 새 TACACS+ 프로파일을 생성합니다.

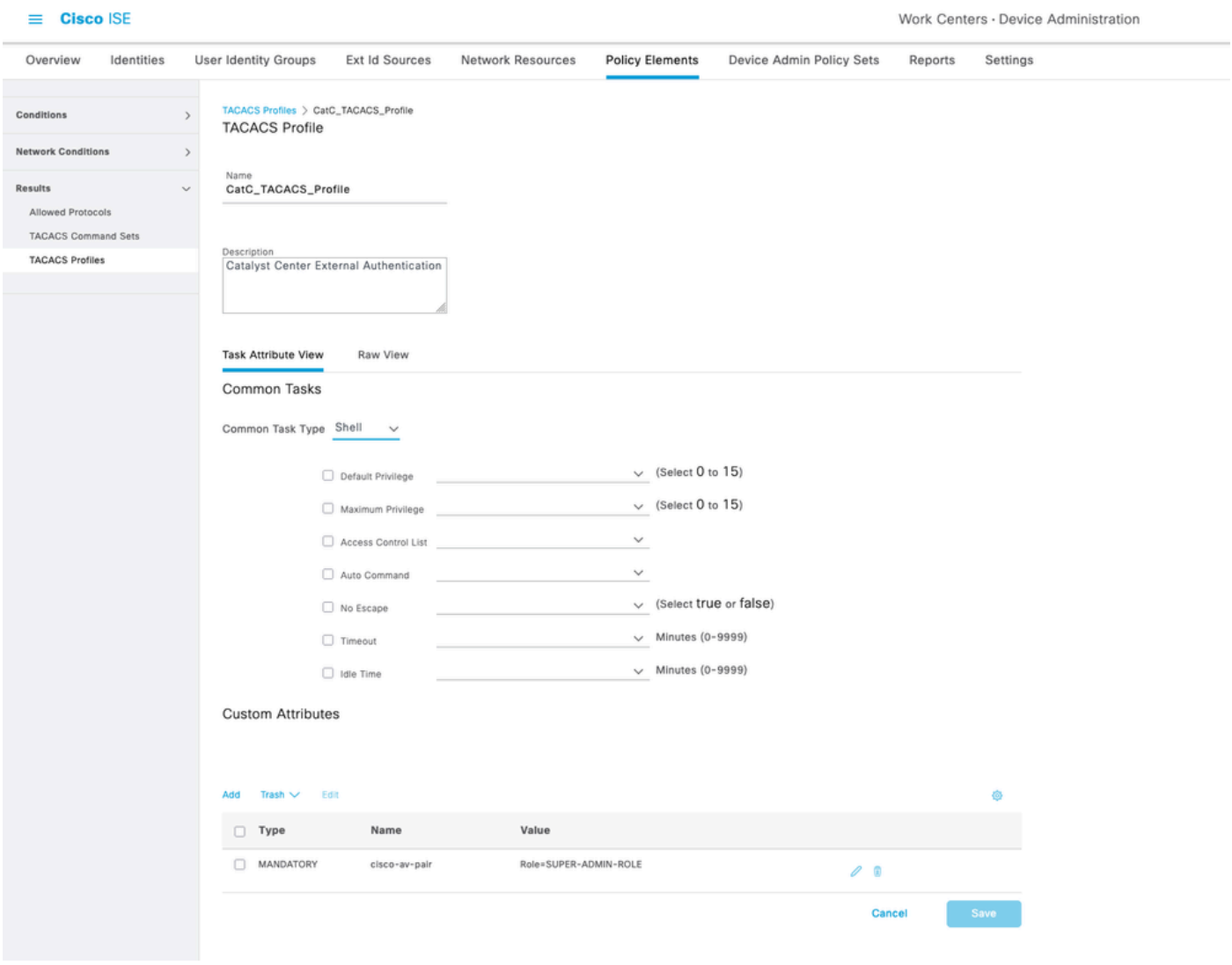
- 다음으로 이동합니다.

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로필)

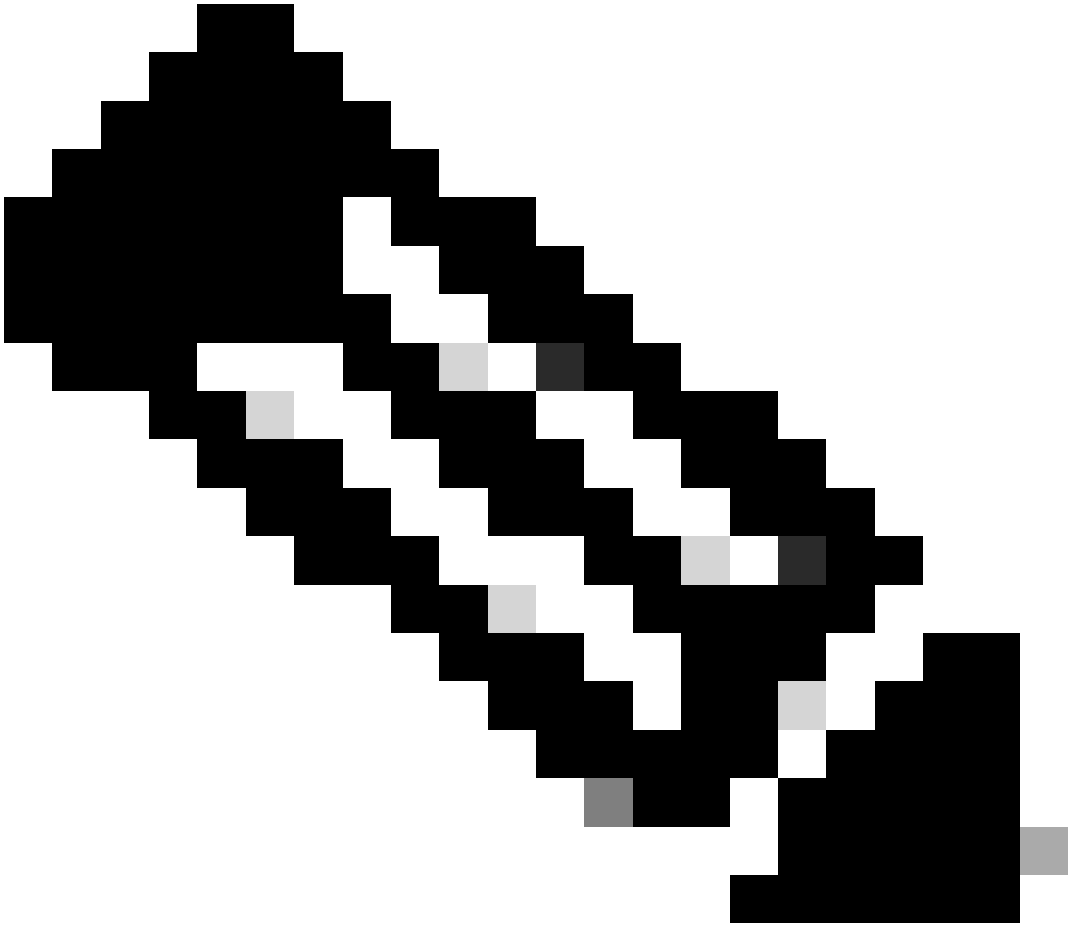
- 프로필 이름을 추가합니다.
- 다음과 같이 사용자 지정 특성을 추가합니다.

- 유형: 필수
- 이름: cisco av 쌍
- 가치: 역할=수퍼 관리자 역할

- 프로파일을 저장합니다.



TACACS+ 프로파일



참고: Cisco Catalyst Center는 액세스 제어를 위해 외부 AAA(Authentication, Authorization and Accounting) 서버를 지원합니다. 외부 사용자의 인증 및 권한 부여에 외부 서버를 사용하는 경우 Cisco Catalyst Center에서 외부 인증을 활성화할 수 있습니다. 기본 AAA 특성 설정은 기본 사용자 프로필 특성과 일치합니다.

TACACS 프로토콜 기본 AAA 특성 값은 cisco-av-pair입니다.

RADIUS 프로토콜 기본 AAA 특성 값은 Cisco-AVPair입니다.

변경 사항은 AAA 서버가 사용자 프로필에 사용자 지정 특성을 갖는 경우에만 필요합니다. AAA 서버에서 AAA 특성 값의 형식은 Role=role1입니다. Cisco ISE(Cisco Identity Services Engine) 서버에서 RADIUS 또는 TACACS 프로파일을 구성하는 동안 사용자는 Cisco av 쌍을 AAA 특성으로 선택하거나 입력할 수 있습니다.

예를 들어, AAA 특성을 수동으로 선택하고 cisco-av-pair=Role=SUPER-ADMIN-ROLE 또는 Cisco-AVPair=Role=SUPER-ADMIN-ROLE로 구성할 수 있습니다.

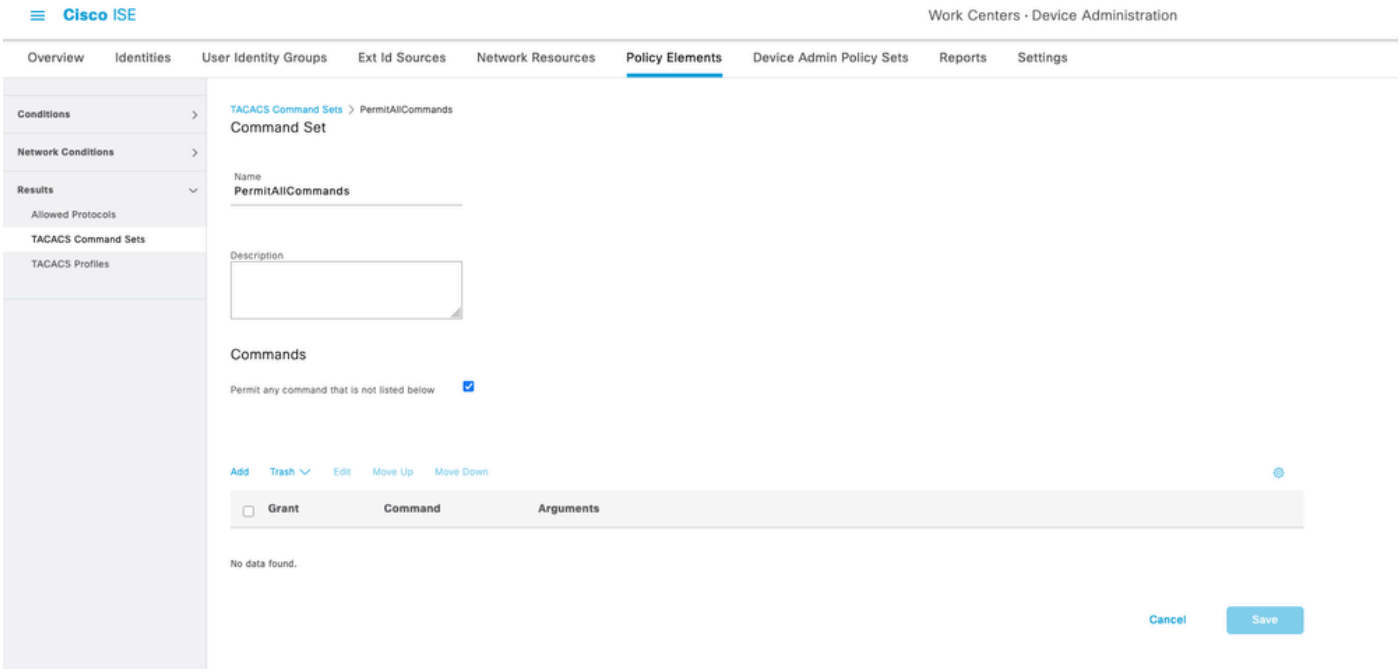
---

2. TACACS+ 명령 집합을 생성합니다.

- 다음으로 이동합니다.

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Command Sets(TACACS 명령 집합)

- 이름을 추가합니다.
- 아래에 나열되지 않은 모든 명령 허용 옵션을 선택합니다.
- 명령 세트를 저장합니다.



TACACS 명령 집합

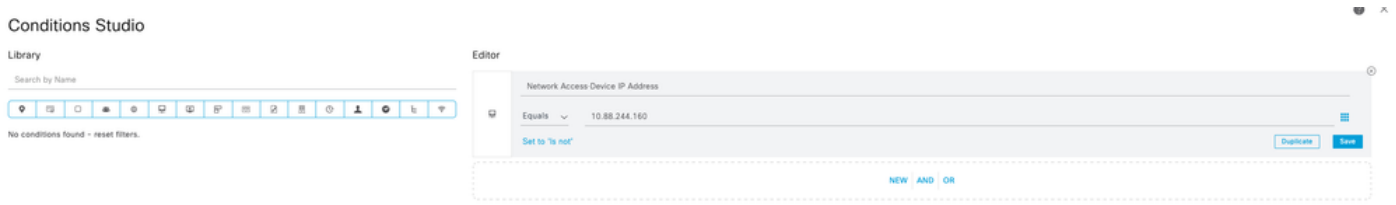
TACACS+ 정책 구성

1. 새 TACACS+ 정책 집합을 생성합니다.

- 다음으로 이동합니다.

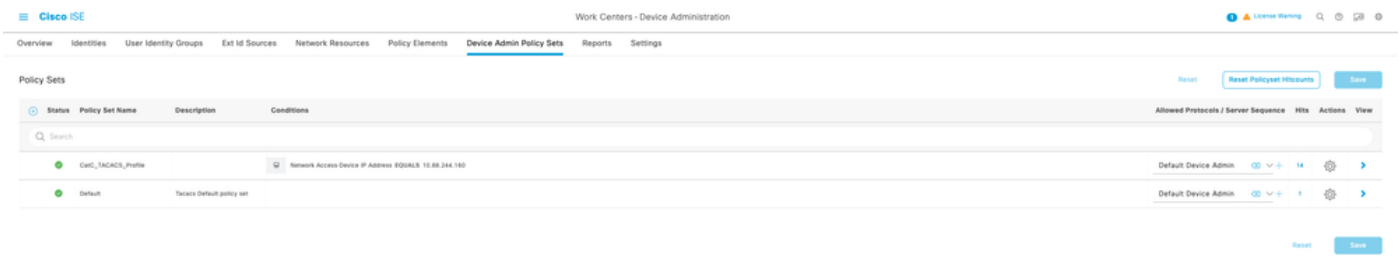
Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Set(디바이스 관리 정책 집합)

- 정책 세트의 이름을 추가합니다.
- 조건을 구성합니다.
  - 이 예에서는 조건이 Catalyst Center IP 주소와 일치합니다.



Catalyst Center IP 주소

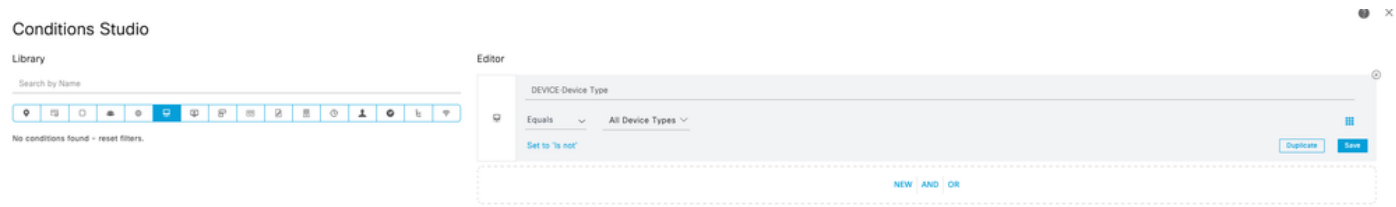
1.3 Allowed Protocols/Server Sequence(허용된 프로토콜/서버 시퀀스)에서 Default Device Admin(기본 디바이스 관리)을 선택합니다.



Default Device Admin(기본 디바이스 관리)을 선택합니다.

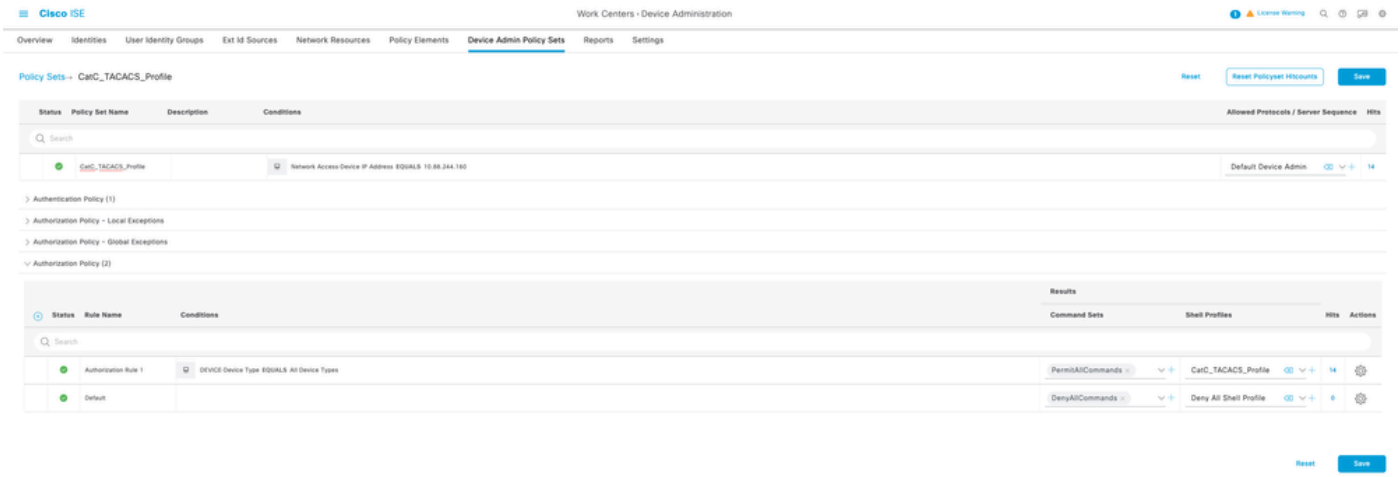
2. 정책 집합을 구성합니다.

- 오른쪽의 화살표(>)를 클릭하여 Policy Set을 확장하고 구성합니다.
- Authorization Policy(권한 부여 정책)에 새 규칙을 추가합니다.
- 다음과 같이 새 규칙을 구성합니다.
  - 이름: 설명이 포함된 규칙 이름을 입력합니다.
  - 조건: 이 예에서는 조건이 모든 디바이스 유형과 일치합니다.



모든 장치 유형

- 명령 집합: 앞서 생성한 TACACS+ 명령 집합을 선택합니다.
- 셸 프로파일: 이전에 생성한 TACACS+ 프로파일을 선택합니다.



TACACS+ 명령 집합

Cisco Catalyst 센터

ISE/AAA 서버 구성

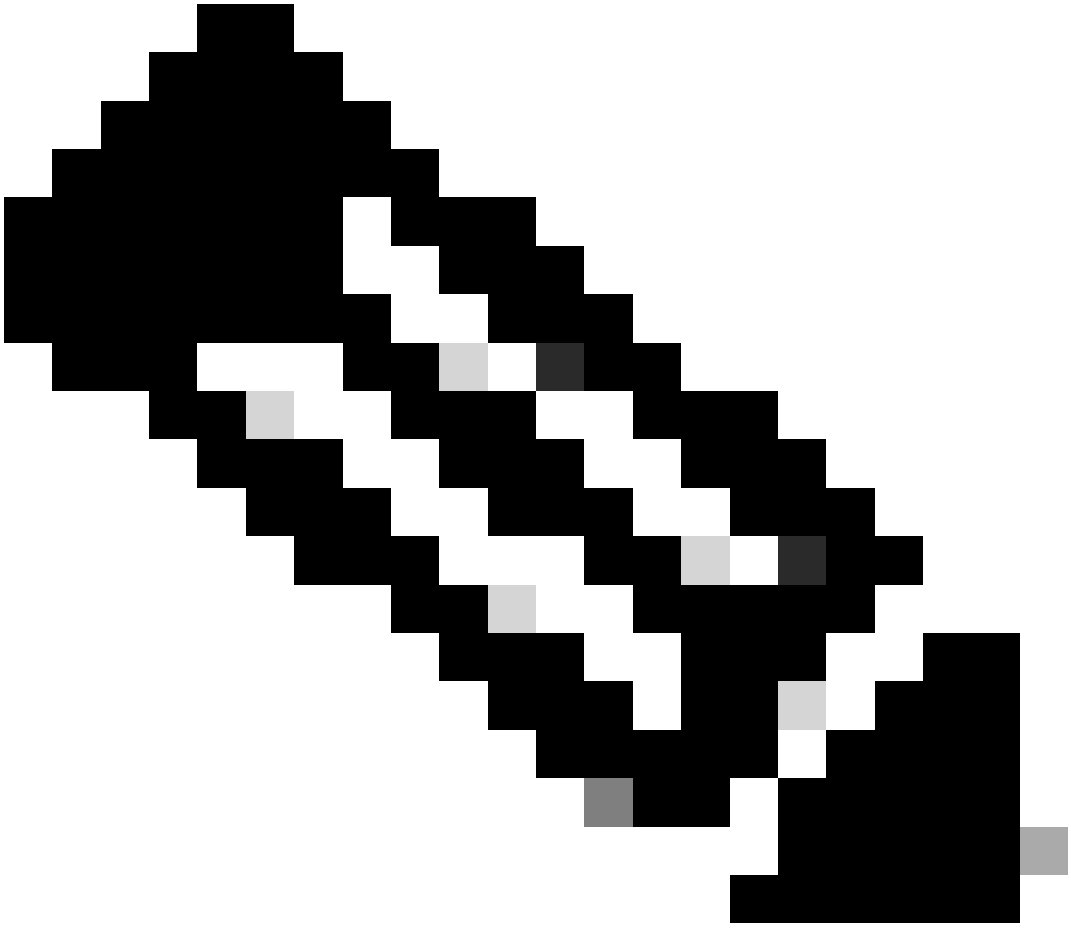
1. Catalyst Center 웹 인터페이스에 로그인합니다.

- 다음으로 이동합니다.

주 메뉴 > 시스템 > 설정 > 외부 서비스 > 인증 및 정책 서버

2. 새 서버를 추가합니다. ISE 또는 AAA를 선택할 수 있습니다.

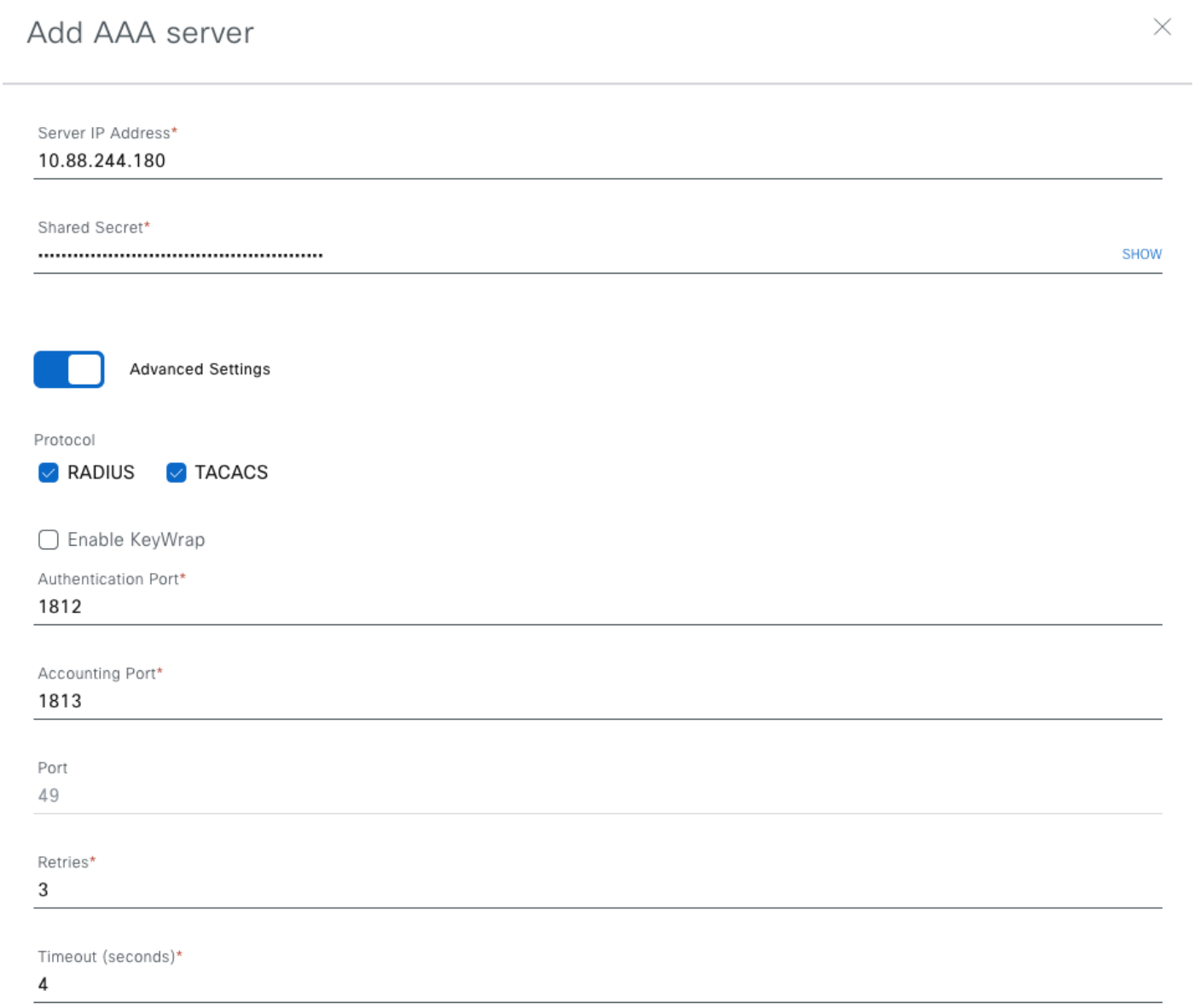
- 이 데모에서는 AAA 서버 옵션이 사용됩니다.



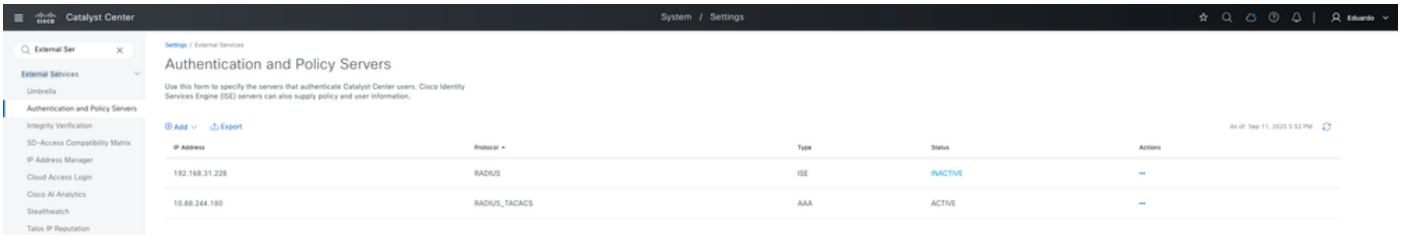
참고: Catalyst Center 클러스터에는 ISE 클러스터를 하나만 구성할 수 있습니다.

3. 다음 옵션을 구성한 다음 저장합니다.

- AAA 서버의 IP 주소를 입력합니다.
- 공유 암호(Cisco ISE 네트워크 리소스에 구성된 동일한 암호)를 추가합니다.
- Advanced Settings(고급 설정)를 On(켜기)으로 전환합니다.
- TACACS 옵션을 선택합니다.



인증 및 정책 서버



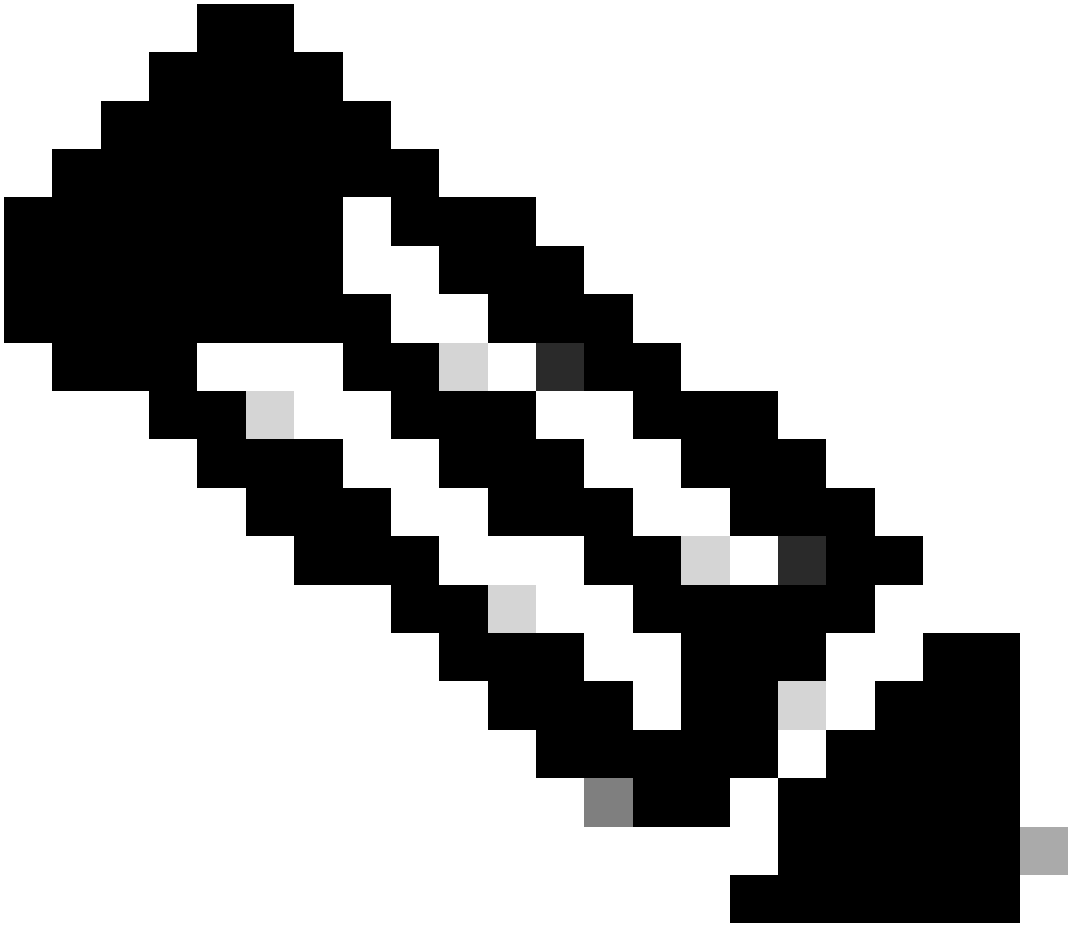
고급 설정

외부 인증을 활성화하고 구성합니다.

1. 외부 인증 페이지로 이동합니다.

    주 메뉴 > 시스템 > 사용자 및 역할 > 외부 인증

2. AAA 특성 cisco-av-pair를 추가하고 Update(업데이트)를 클릭하여 변경 사항을 저장합니다.



참고: TACACS+의 기본 특성이 이미 cisco-av-pair이므로 이 단계는 필수 단계는 아니지만 명시적으로 구성하는 것이 좋습니다.

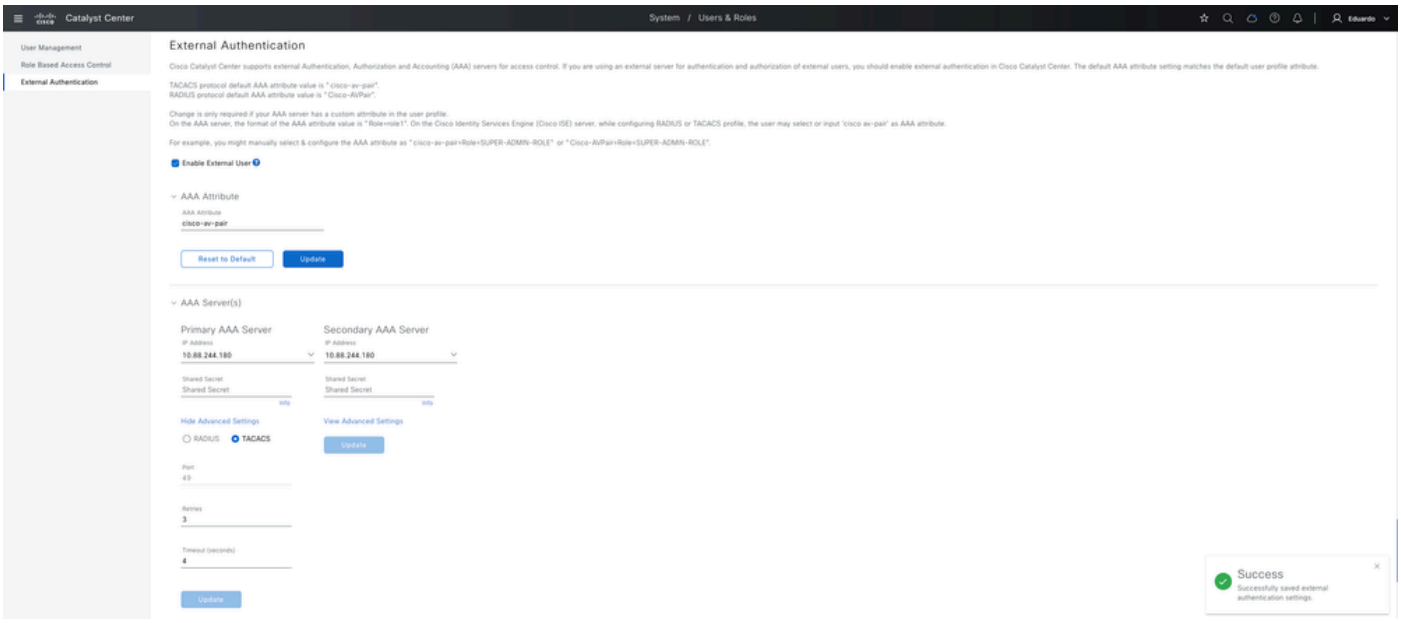
---

3. Primary AAA Server(기본 AAA 서버) 아래에서 이전에 구성한 AAA 서버를 선택합니다.

- 추가 옵션을 표시하려면 View Advanced Settings(고급 설정 보기)를 클릭합니다.
- TACACS+ 옵션을 선택합니다.
- Cisco ISE의 네트워크 리소스에 구성 된 공유 암호를 입력 합니다.
- Update(업데이트)를 클릭하여 변경 사항을 저장합니다.

4. 외부 사용자 확인란을 활성화합니다.

- 이 작업을 수행하면 컨피그레이션이 자동으로 저장됩니다.



외부 인증

다음을 확인합니다.

1. 새 브라우저 세션을 열거나 익명 모드를 사용하고 Cisco ISE에 구성된 사용자 계정으로 Catalyst Center 웹 페이지에 로그인합니다.
2. Catalyst Center에서 로그인이 성공했는지 확인합니다.

ISE를 사용하여 Catalyst Center 외부 인증 TACACS 구성에 로그인

3. Cisco ISE에서 로그를 검증합니다.

   Operations(운영) > TACACS > Live Logs(라이브 로그)

- 인증 상태: 통과
- 권한 부여 상태: 통과

라이브 로그

4. Authorization Details(권한 부여 세부 정보)에서 다음 출력과 비교합니다.

- 메시지 텍스트: 장치 관리: 세션 권한 부여 성공
- 모든 응답 특성: cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

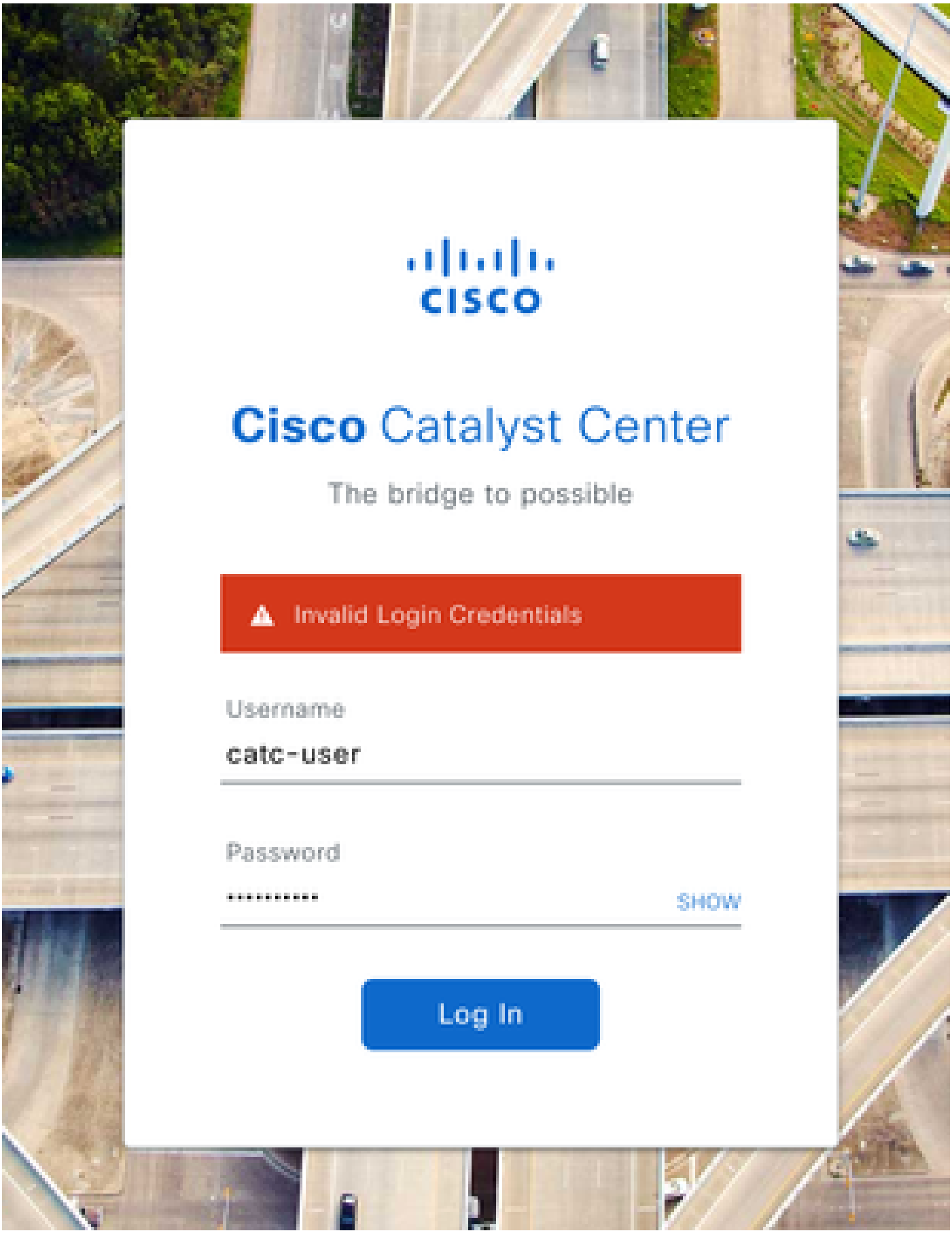
cisco av-pair=역할=슈퍼 관리자-역할

문제 해결

다음은 통합 중에 발생할 수 있는 몇 가지 일반적인 문제와 이러한 문제를 식별하는 방법입니다.

1. 특성 컨피그레이션 오류

Catalyst Center의 증상: 잘못된 로그인 자격 증명



잘못된 특성 컨피그레이션

- Cisco ISE의 증상(TACACS 로그):

- 인증: 통과
- 인증: 통과

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:20.801...	✓		catc-user	Authorization		CatC_TACACS_Profile >> Authoriz...	ise-mac1	Catalyst-Center_6	10.88.244.160	Device Type#All D...	Location#All Locati...	console		10.189.17.203		CatC_TACACS_Pr...
Sep 12, 2025 12:12:20.788...	✓		catc-user	Authentication	CatC_TACACS_Profile >> Default		ise-mac1	Catalyst-Center_6	10.88.244.160	Device Type#All D...	Location#All Locati...	console		10.189.17.203		

잘못된 특성 컨피그레이션

- 가능한 원인:
  - 특성 값에 공백이 있습니다.

예:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

잘못된 특성 컨피그레이션

- 특성이 잘못 구성되었으며 Role= 키워드가 누락되었습니다.

  예:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

잘못된 특성 컨피그레이션

2. 공유 암호가 일치하지 않습니다.

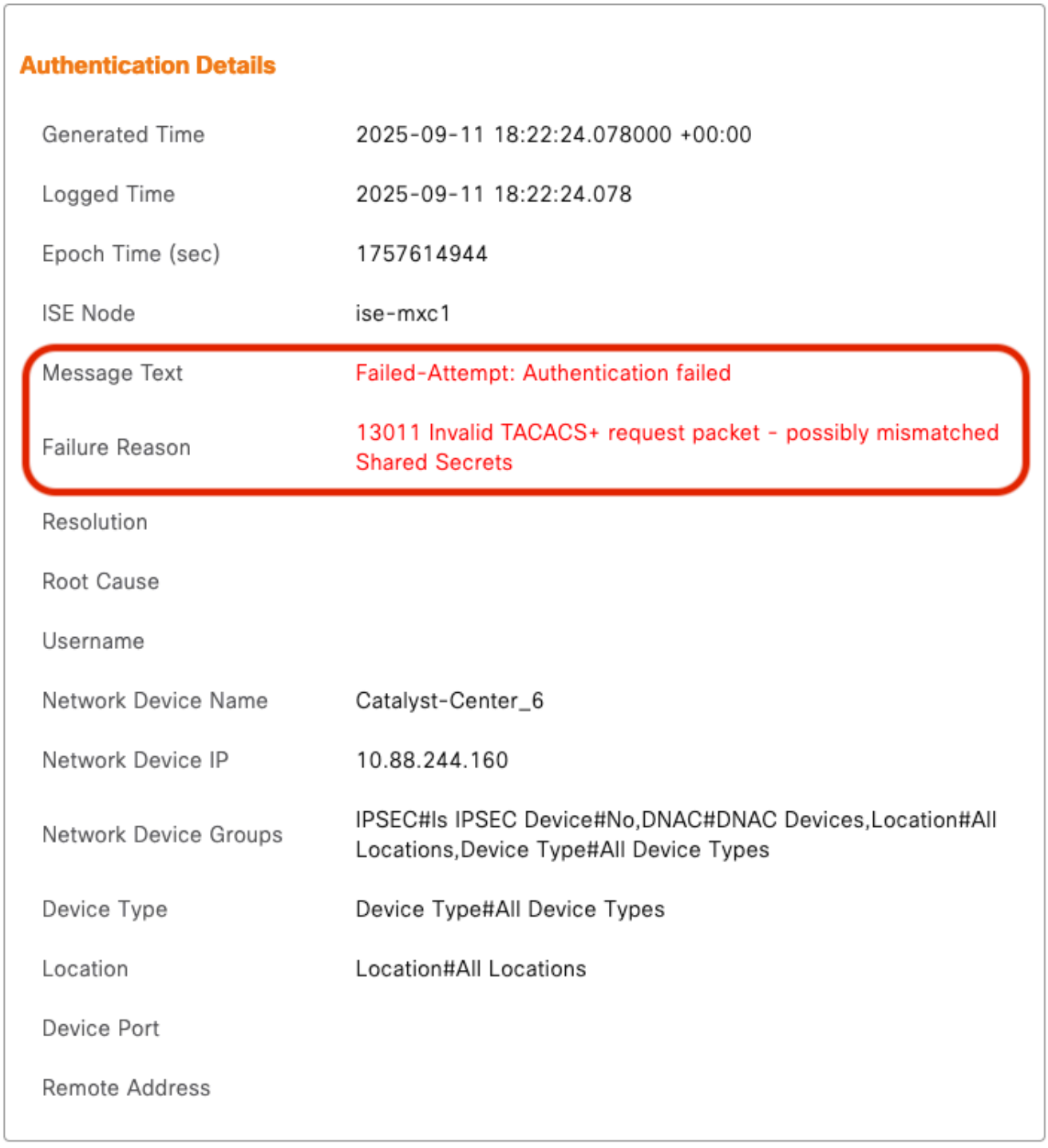
- 증상: Catalyst Center와 Cisco ISE 간에 인증 패킷이 실패합니다.

- 가능한 원인: ISE의 네트워크 리소스에 구성된 공유 암호가 Catalyst Center > 외부 인증 페이지에 구성된 것과 일치하지 않습니다.

확인 방법:

- ISE의 네트워크 리소스 컨피그레이션을 확인합니다.
- 공유 암호를 Catalyst Center > External Authentication의 구성과 비교합니다.

예:



공유 암호 불일치

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.