ISE에서 외부 TACACS 서버 구성 및 문제 해결

목차

소개

이 문서에서는 ISE(Identity Service Engine)를 프록시로 사용하여 구축에서 외부 TACACS+ 서버를 활용하는 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

- ISE에서 디바이스 관리에 대한 기본적인 이해
- 이 문서는 Identity Service Engine 버전 2.0을 기반으로 하며, 2.0보다 높은 버전의 Identity Service Engine에 적용됩니다.

사용되는 구성 요소

> **참고:**이 문서의 ACS에 대한 모든 참조는 외부 TACACS+ 서버에 대한 참조로 해석될 수 있습니다.그러나 ACS의 컨피그레이션 및 다른 TACACS 서버의 컨피그레이션은 다를 수 있습니다.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

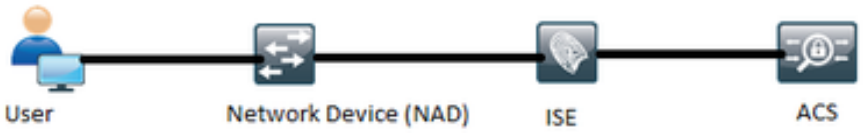
- Identity Service Engine 2.0
- ACS(Access Control System) 5.7

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 컨피그레이션 변경의 잠재적 영향을 이해해야 합니다.

구성

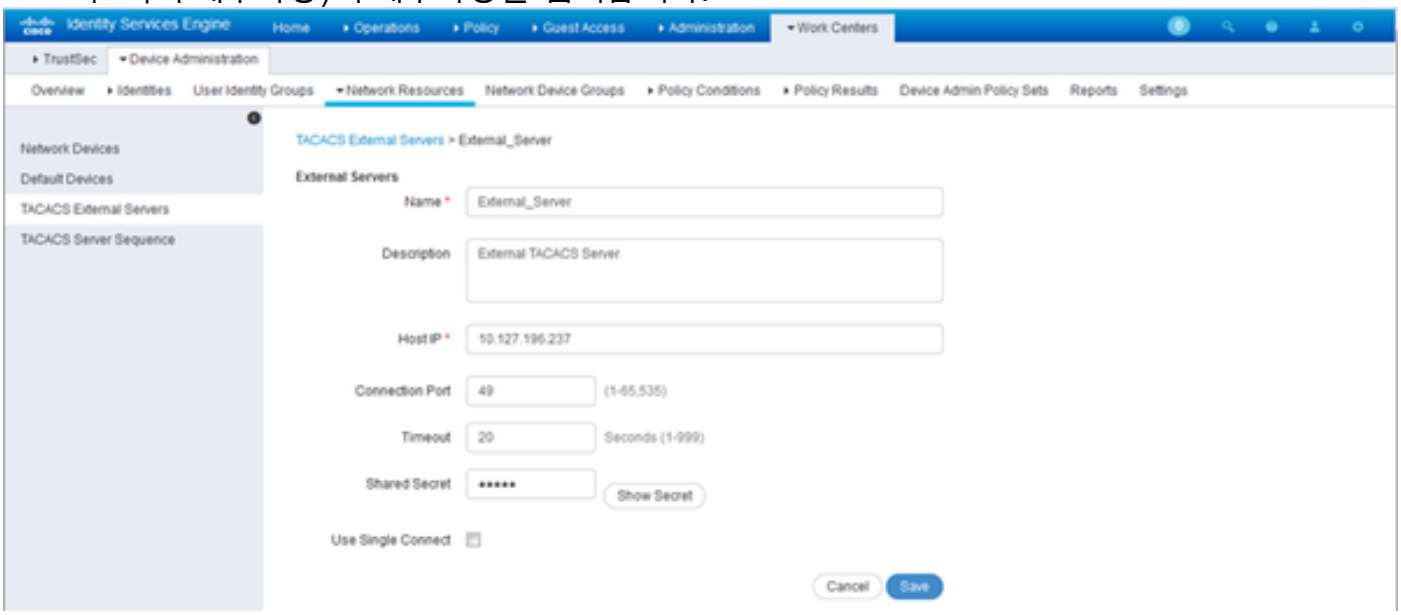
이 섹션에서는 ACS에 대한 TACACS+ 요청을 프록시하도록 ISE를 구성하는 데 도움이 됩니다.

네트워크 다이어그램



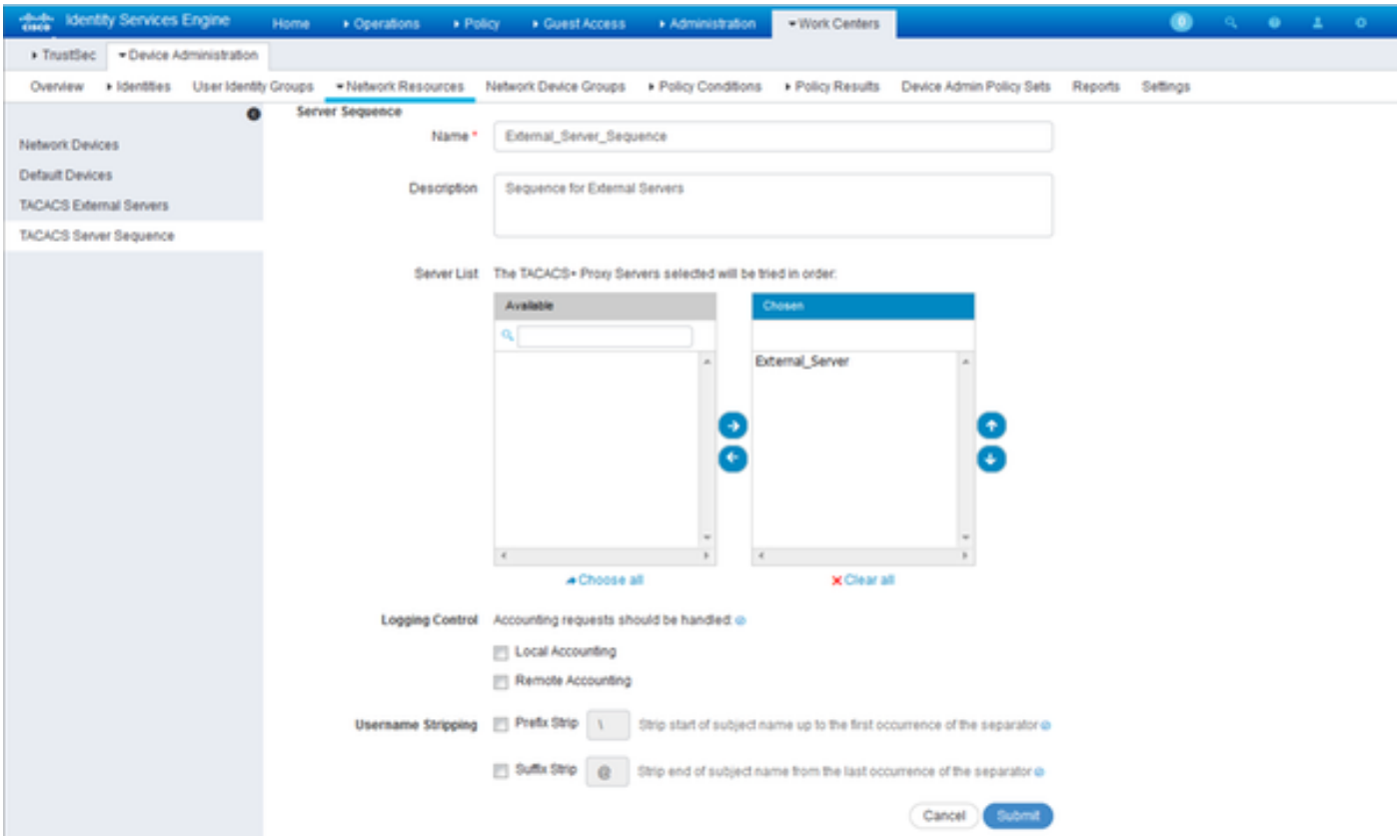
ISE 구성

1. 여러 외부 TACACS 서버를 ISE에 구성할 수 있으며 사용자를 인증하는 데 사용할 수 있습니다.ISE에서 외부 TACACS+ 서버를 구성하려면 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > TACACS External Servers(TACACS 외부 서버)로 이동합니다.**Add(**추가**)를 클릭하고 External Server Details(외부 서버 세부사항)의 세부사항을 입력합니다.



이 섹션에서 제공하는 공유 암호는 ACS에서 사용하는 암호와 동일해야 합니다.

2. 구성된 외부 TACACS 서버를 활용하려면 정책 세트에 사용할 TACACS 서버 시퀀스에 추가해야 합니다.TACACS Server Sequence를 구성하려면 Work Centers(작업 센터) > Device Administration(디바이스 관리) **> Network Resources(네트워크 리소스) > TACACS Server Sequence(TACACS 서버 시퀀스)로 이동합니다.**Add(**추가**)를 클릭하고 세부 정보를 입력한 다음 해당 시퀀스에 사용할 서버를 선택합니다.

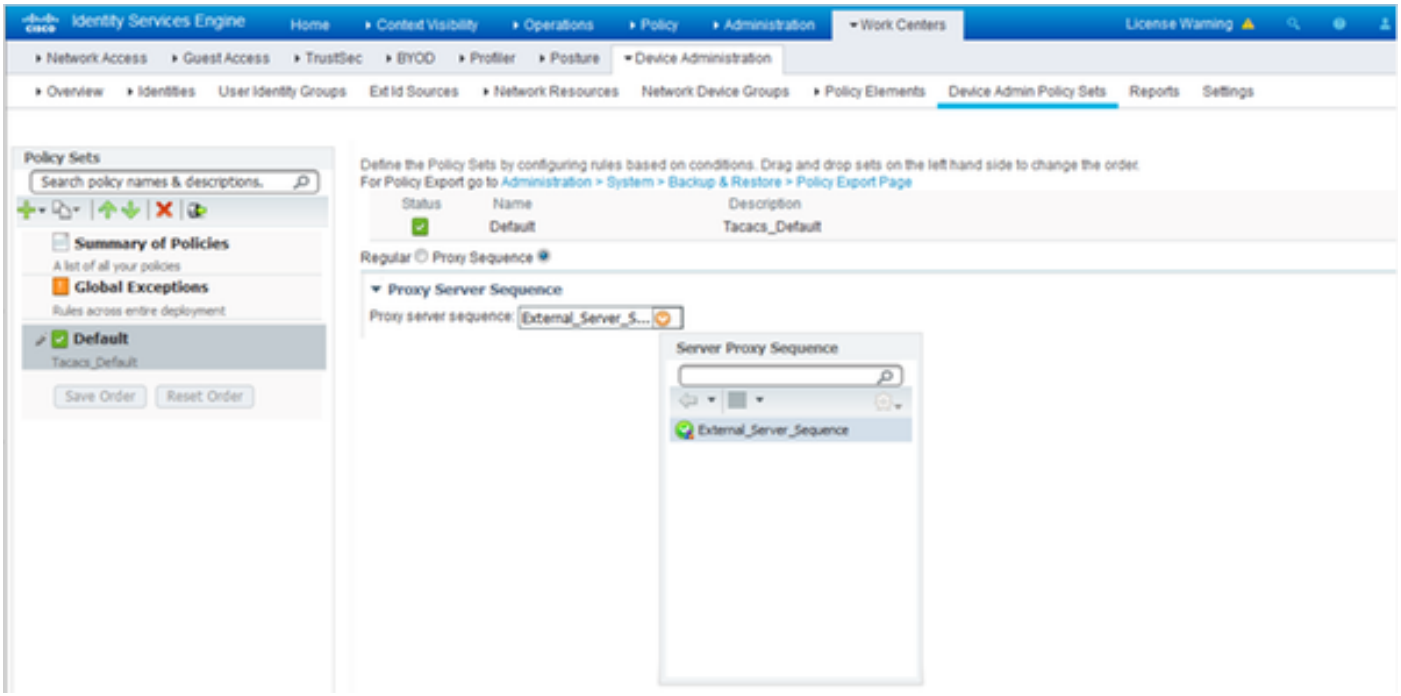


서버 시퀀스 외에도 두 가지 다른 옵션이 제공됩니다.로깅 제어 및 사용자 이름 스트리핑.

Logging Control(로깅 제어)은 ISE에서 어카운팅 요청을 로컬로 기록하거나 인증을 처리하는 외부 서버에 어카운팅 요청을 로깅하는 옵션을 제공합니다.

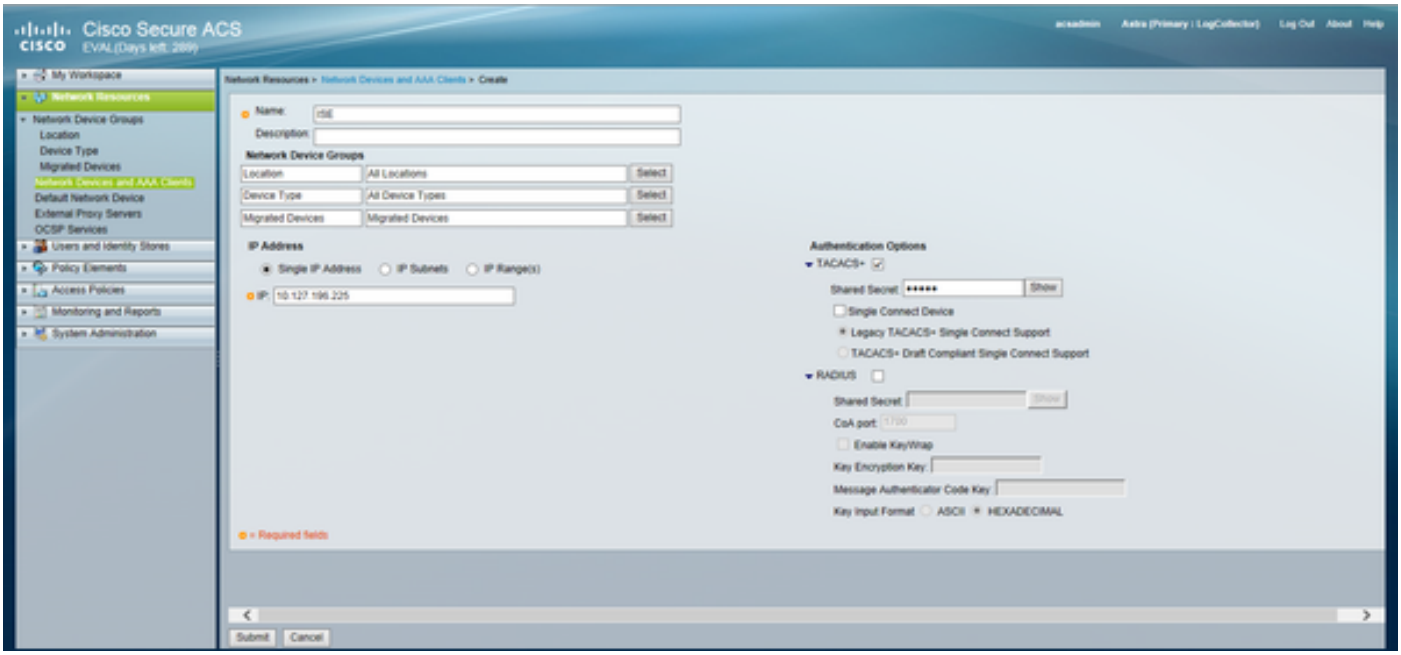
Username Strip은 외부 TACACS 서버로 요청을 전달하기 전에 구분 기호를 지정하여 접두사 또는 접미사를 제거하는 데 사용됩니다.

3. 구성된 외부 TACACS 서버 시퀀스를 사용하려면 생성된 시퀀스를 사용하도록 정책 세트를 구성해야 합니다.외부 서버 시퀀스를 사용하도록 정책 세트를 구성하려면 **Work Centers(작업 센터) > Device Administration(디바이스 관리) >** Device Admin Policy Sets(**디바이스 관리 정책 집합) > [정책 집합 선택]으로 이동합니다.**프록시 시퀀스라는 라디오 버튼**을 토글합니다.**생성된 외부 서버 시퀀스를 선택합니다.

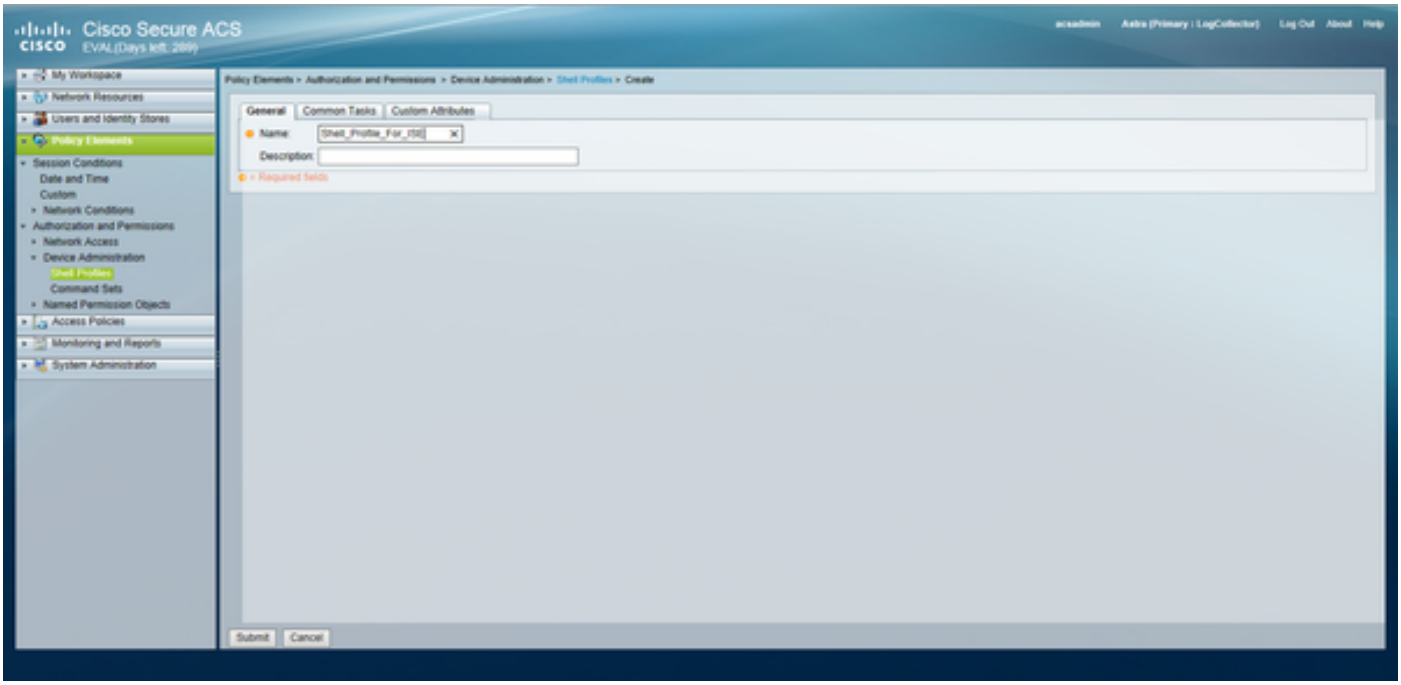


ACS 구성

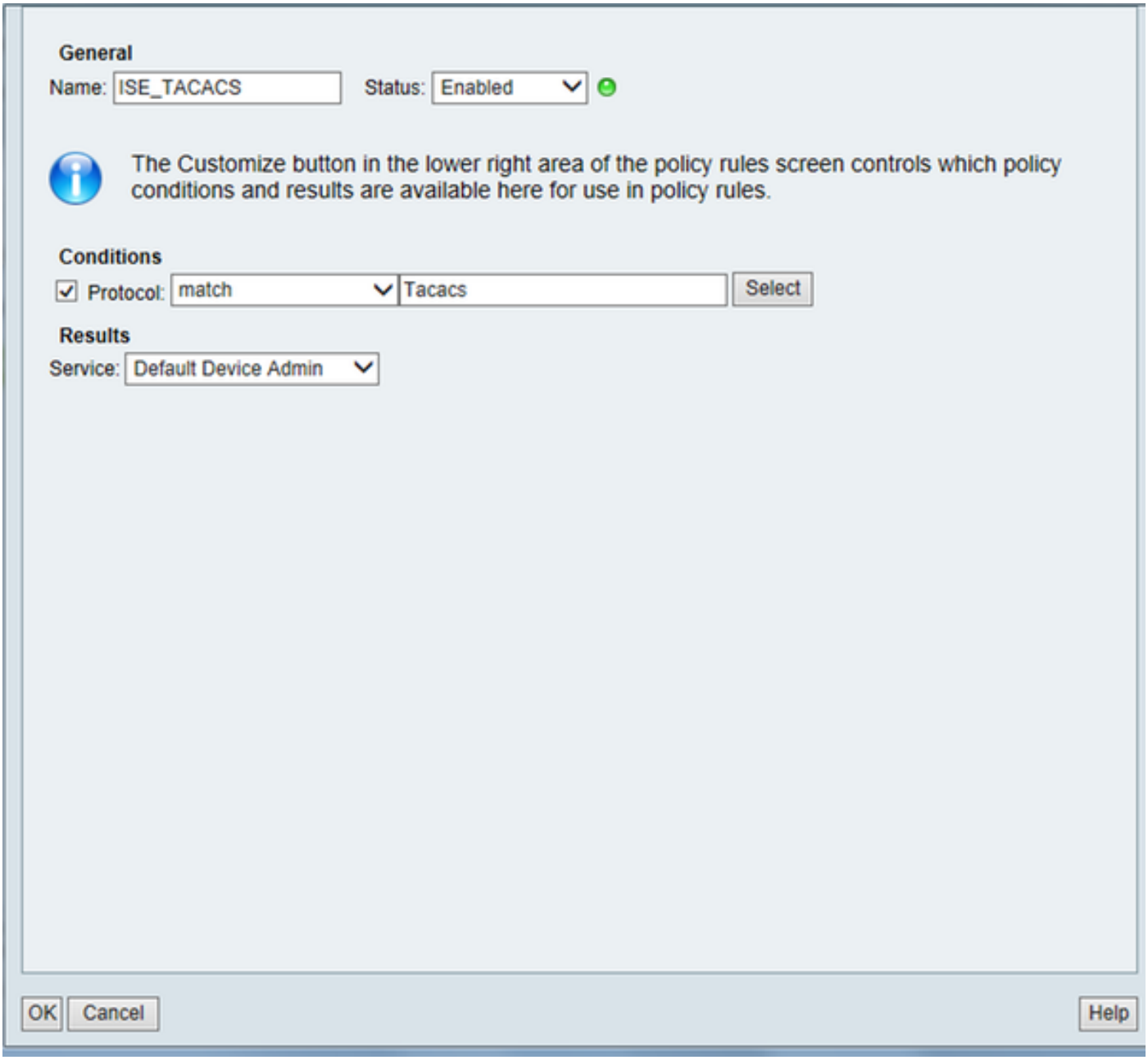
ACS의 경우, ISE는 TACACS 요청을 전송할 다른 네트워크 디바이스일 뿐입니다.ACS에서 ISE를 네트워크 디바이스로 구성하려면 Network Resources(네트워크 리소스) **> Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트)로 이동합니다.**Create(**생성**)를 클릭하고 ISE에 구성된 것과 동일한 공유 암호를 사용하여 ISE 서버의 세부 정보를 입력합니다.



ACS에서 셸 프로파일 및 명령 집합인 디바이스 관리 매개변수를 구성합니다.셸 프로필을 구성하려면 Policy Elements(정책 요소) **> Authorization and Permissions(권한 부여 및 권한) > Device Administration(디바이스 관리) > Shell Profiles(셸 프로파일)로 이동합니다.**Create(**생성**)를 클릭하고 요구 사항에 따라 이름, Common Tasks(공통 작업) 및 Custom Attributes(사용자 지정 특성)를 구성합니다.



명령 집합을 구성하려면 **정책 요소 > 권한 부여 및 권한 > 장치 관리 > 명령 집합으로** 이동합니다. **생성**을 클릭하고 요구 사항에 따라 세부 정보를 입력합니다.



요구 사항에 따라 서비스 선택 규칙에서 선택한 액세스 서비스를 구성합니다.액세스 서비스 규칙을 구성하려면 **액세스 정책 > 액세스 서비스 > 기본 장치 관리자 > 인증을 위해** 사용해야 하는 ID 저장소를 선택할 수 있는 ID로 이동합니다.권한 부여 규칙은 Access Policies(**액세스 정책) > Access Services(액세스 서비스) > Default Device Admin(기본 디바이스 관리자) > Authorization(권한 부여)으로** 이동하여 구성할 수 **있습니다.**

> **참고:**특정 디바이스에 대한 권한 부여 정책 및 셸 프로파일 컨피그레이션은 다를 수 있으며 이 문서의 범위를 벗어납니다.

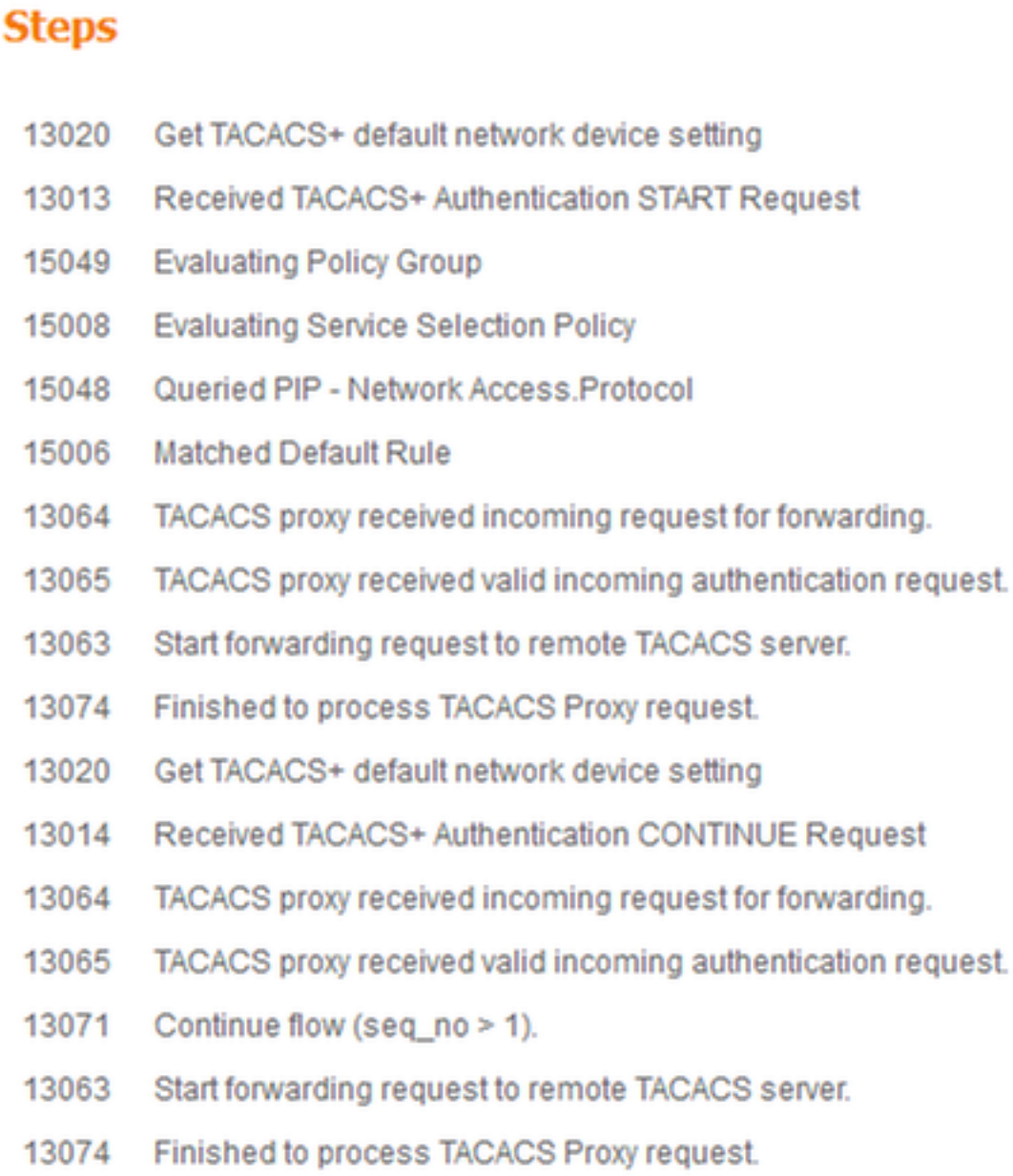
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

ISE와 ACS 모두에서 확인을 수행할 수 있습니다.ISE 또는 ACS의 컨피그레이션에서 오류가 발생하면 인증 오류가 발생합니다.ACS는 인증 및 권한 부여 요청을 처리할 기본 서버이며, ISE는 ACS 서버에서 ACS에 대한 권한을 가지고 요청에 대한 프록시 역할을 합니다.패킷이 두 서버를 모두 통과하므로 두 서버에서 인증 또는 권한 부여 요청을 확인할 수 있습니다.

네트워크 디바이스는 ACS가 아닌 TACACS 서버로 ISE로 구성됩니다.따라서 요청이 먼저 ISE에 도달하고 구성된 규칙을 기반으로 ISE는 요청이 외부 서버로 전달되어야 하는지 여부를 결정합니다.이는 ISE의 TACACS Live 로그에서 확인할 수 있습니다.

ISE에서 라이브 로그를 보려면 Operations(작업) **> TACACS > Live Logs(라이브 로그)로 이동합니다.**이 페이지에서 라이브 보고서를 볼 수 있으며 관심 있는 특정 요청에 대한 돋보기 아이콘을 클릭하여 특정 요청의 세부 정보를 확인할 수 있습니다.


Steps

13020 Get TACACS+ default network device setting
13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Network Access.Protocol
15006 Matched Default Rule
13064 TACACS proxy received incoming request for forwarding.
13065 TACACS proxy received valid incoming authentication request.
13063 Start forwarding request to remote TACACS server.
13074 Finished to process TACACS Proxy request.
13020 Get TACACS+ default network device setting
13014 Received TACACS+ Authentication CONTINUE Request
13064 TACACS proxy received incoming request for forwarding.
13065 TACACS proxy received valid incoming authentication request.
13071 Continue flow (seq_no > 1).
13063 Start forwarding request to remote TACACS server.
13074 Finished to process TACACS Proxy request.

ACS에서 인증 보고서를 보려면 **Monitoring and Reports(모니터링 및 보고서 실행) > Launch Monitoring and Report Viewer(모니터링 및 보고서 실행) > Monitoring and Reports(모니터링 및 보고서) > Reports(보고서) > AAA Protocol(AAA 프로토콜) > TACACS Authentication(TACACS 인증)으로** 이동합니다. ISE와 마찬가지로 관심 있는 특정 요청에 대한 돋보기 아이콘을 눌러 특정 요청의 세부 정보를 확인할 수 있습니다

문제 해결

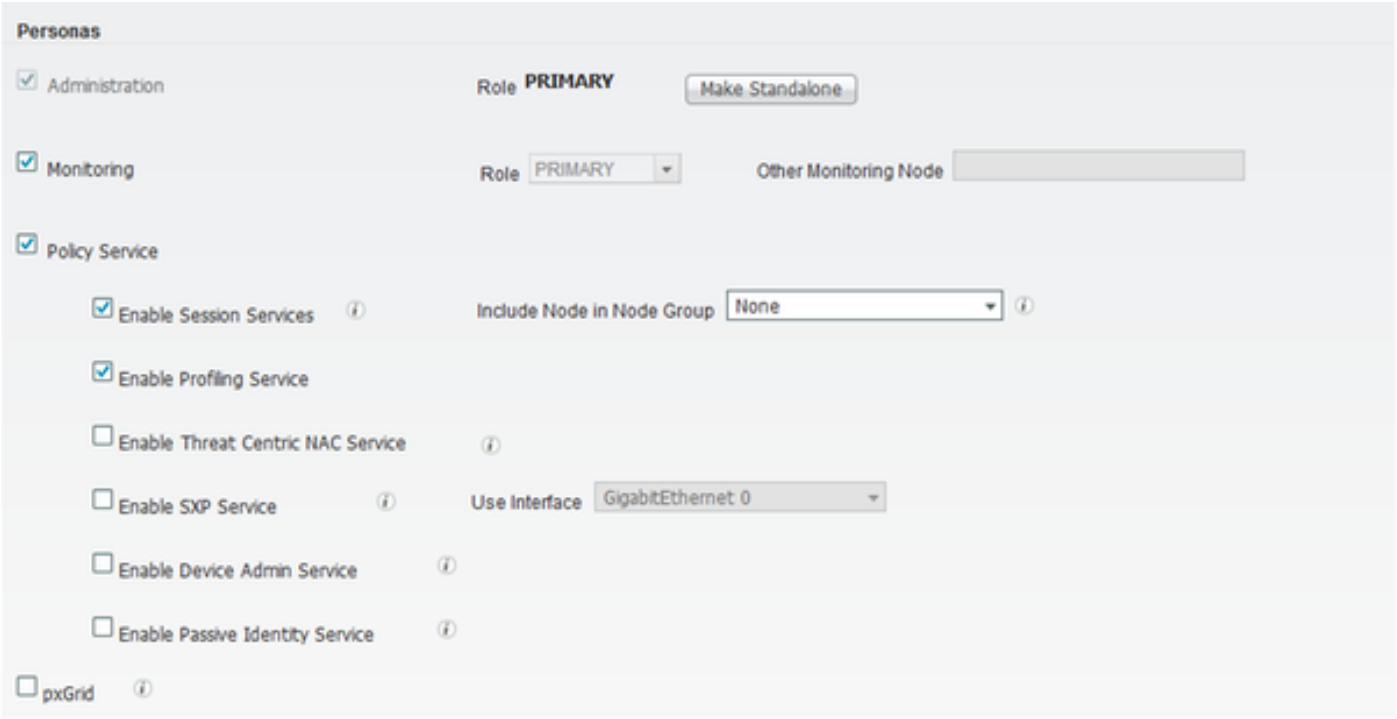
이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다

1. ISE에 대한 보고서의 세부사항에 그림에 표시된 오류 메시지가 표시되면 ISE 또는 네트워크 디바이스(NAD)에 구성된 잘못된 공유 비밀임을 나타냅니다.

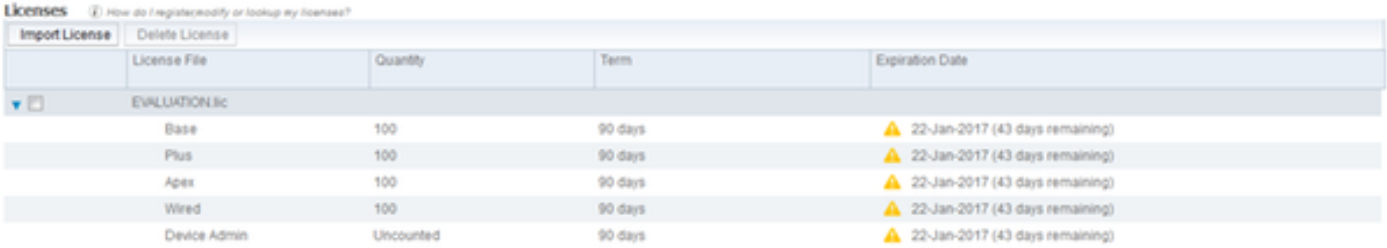
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. ISE에 대한 요청에 대한 인증 보고서가 없지만 최종 사용자가 네트워크 디바이스에 대한 액세스를 거부하면 일반적으로 몇 가지 사항이 표시됩니다.

- 요청 자체가 ISE 서버에 연결되지 않았습니다.
- ISE에서 Device Administration 페르소나를 비활성화하면 ISE에 대한 TACACS+ 요청이 자동으로 삭제됩니다.보고서 또는 라이브 로그에 동일함을 나타내는 로그가 표시되지 않습니다.이를 확인하려면 Administration(관리) **> System(시스템) > Deployment(구축) > [select the node](노드 선택)로 이동합니다.**Edit(**수정**)를 클릭하고 그림에 표시된 대로 General Settings(**일반 설정**) 탭 아래에 있는 "Enable Device Admin Service(**디바이스 관리 서비스 활성화**)" 확인란을 확인합니다.디바이스 관리가 ISE에서 작동하려면 이 확인란을 선택해야 합니다.



- 디바이스 관리 라이센스가 만료되지 않은 경우 모든 TACACS+ 요청이 자동으로 삭제됩니다.동일한 GUI에 로그가 표시되지 않습니다.Administration(**관리) > System(시스템) > Licensing(라이센싱)**으로 이동하여 디바이스 관리 라이센스를 확인합니다.



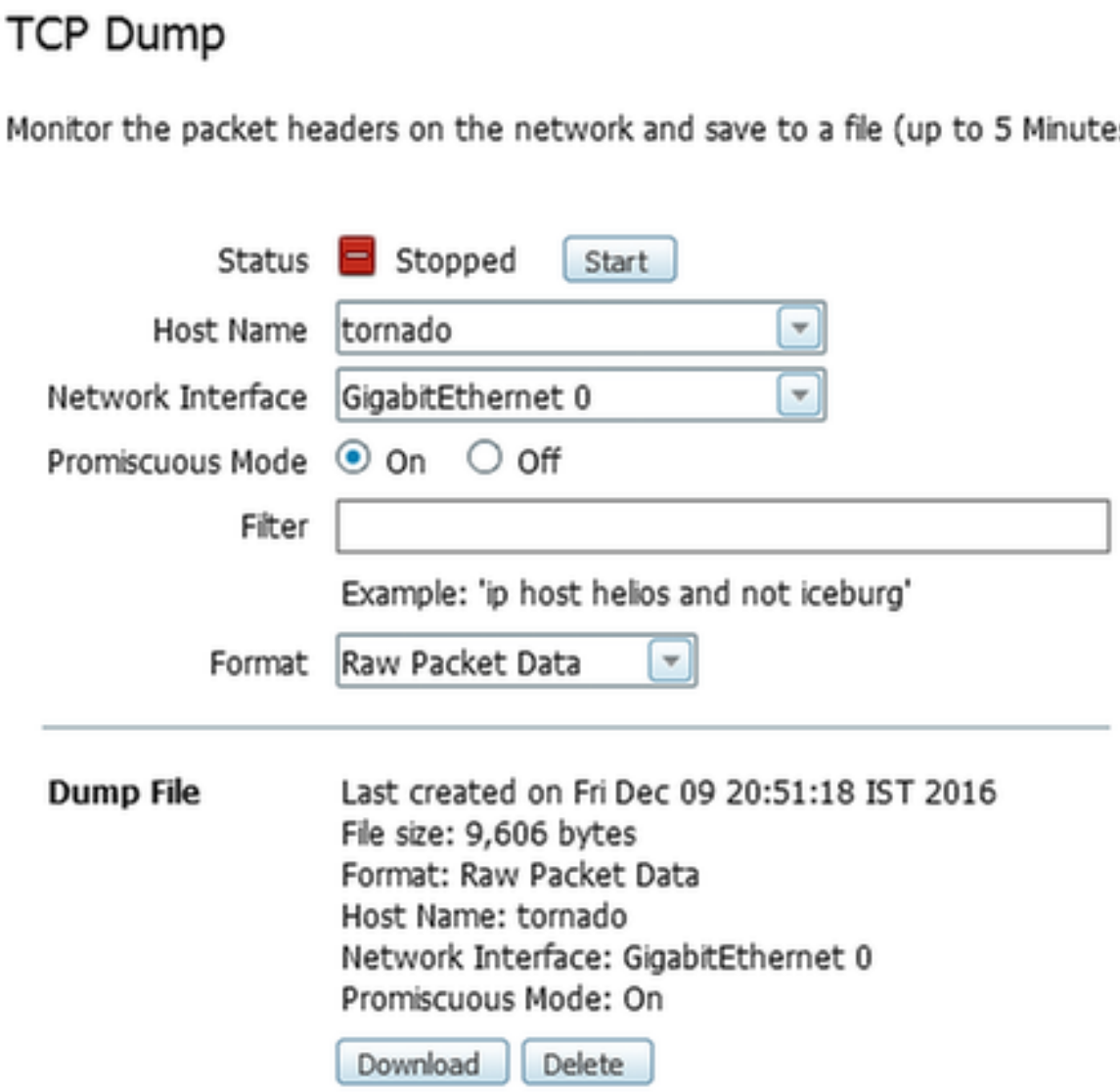
- 네트워크 디바이스가 구성되지 않았거나 ISE에 잘못된 네트워크 디바이스 IP가 구성된 경우 ISE는 패킷을 자동으로 삭제합니다.클라이언트로 응답이 전송되지 않으며 GUI에 로그가 표시되지 않습니다.이는 ACS와 비교하여 TACACS+에 대한 ISE의 동작 변화이며, 이는 요청이 알려지지 않은 네트워크 디바이스 또는 AAA 클라이언트에서 수신되었음을 알립니다.

- 요청이 ACS에 도달했지만 응답이 ISE로 다시 돌아오지 않았습니다.이 시나리오는 그림에 표시된 대로 ACS의 보고서에서 확인할 수 있습니다.일반적으로 이는 ISE에 대해 구성된 ACS 또는 ACS에 대해 구성된 ISE에서 유효하지 않은 공유 비밀 때문입니다.

- ISE가 구성되지 않았거나 ISE의 관리 인터페이스의 IP 주소가 네트워크 디바이스 컨피그레이션의 ACS에 구성되지 않은 경우에도 응답이 전송되지 않습니다.이러한 시나리오에서는 그림의 메시지를 ACS에서 볼 수 있습니다.

- ACS에서 성공적인 인증 보고서가 확인되었지만 ISE에 보고서가 표시되지 않고 사용자가 거부되는 경우 네트워크에서 문제가 될 수 있습니다.이는 필요한 필터를 사용하여 ISE의 패킷 캡처에서 확인할 수 있습니다.ISE에서 패킷 캡처를 수집하려면 Operations(작업) **> Troubleshoot(문**

제 해결) > Diagnostic Tools(진단 도구) > General tools(일반 툴) > TCP Dump(TCP 덤프)로 이동합니다.



3. ISE에서 보고서를 볼 수 있지만 ACS에서는 볼 수 없는 경우, ISE에 대한 상세 보고서를 기반으로 문제 해결할 수 있는 ISE에서 정책 집합을 잘못 구성했거나 ACS에서 패킷 캡처로 식별할 수 있는 네트워크 문제로 인해 요청이 ACS에 도달하지 않은 것일 수 있습니다.

4. 보고서가 ISE와 ACS에서 모두 확인되었지만 사용자가 여전히 액세스 거부 상태인 경우, ACS에 대한 상세 보고서에 따라 문제 해결을 수행할 수 있는 ACS의 액세스 정책 구성에서 문제가 되는 경우가 더 많습니다.또한 ISE에서 네트워크 디바이스로의 반환 트래픽이 허용되어야 합니다.