ISE에서 외부 RADIUS 서버 구성

목차

소개

이 문서에서는 프록시 및 권한 부여 서버로 ISE의 RADIUS 서버 구성에 대해 설명합니다. 여기서는 두 개의 ISE 서버가 사용되며 하나는 외부 서버 역할을 합니다. 그러나 모든 RFC 호환 RADIUS 서버를 사용할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RADIUS 프로토콜에 대한 기본 지식
- ISE(Identity Services Engine) 정책 컨피그레이션에 대한 전문 지식

사용되는 구성 요소

이 문서의 정보는 Cisco ISE 버전 2.2 및 2.4를 기반으로 합니다.

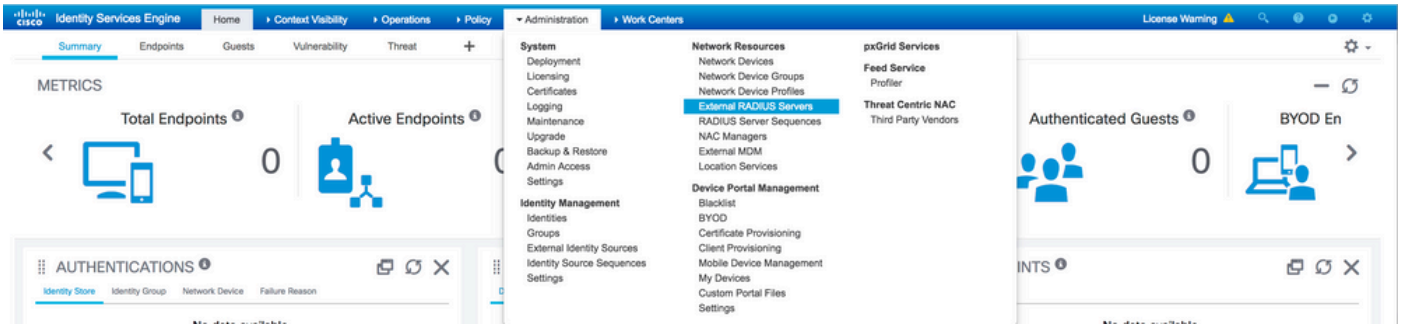
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

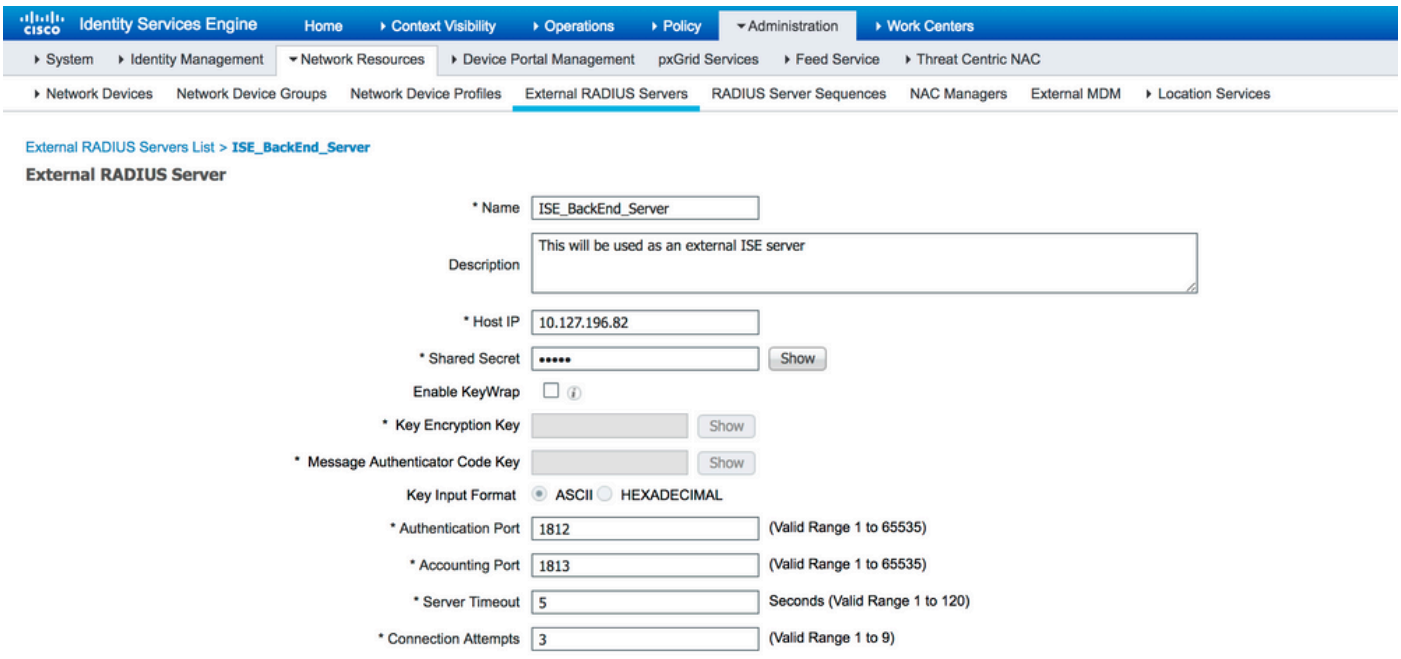
구성

네트워크 다이어그램

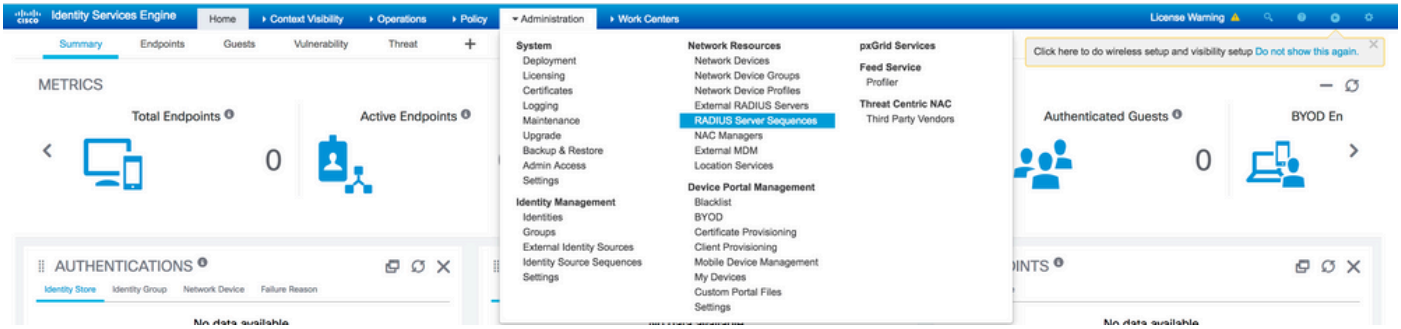
ISE(프런트 엔드 서버) 구성

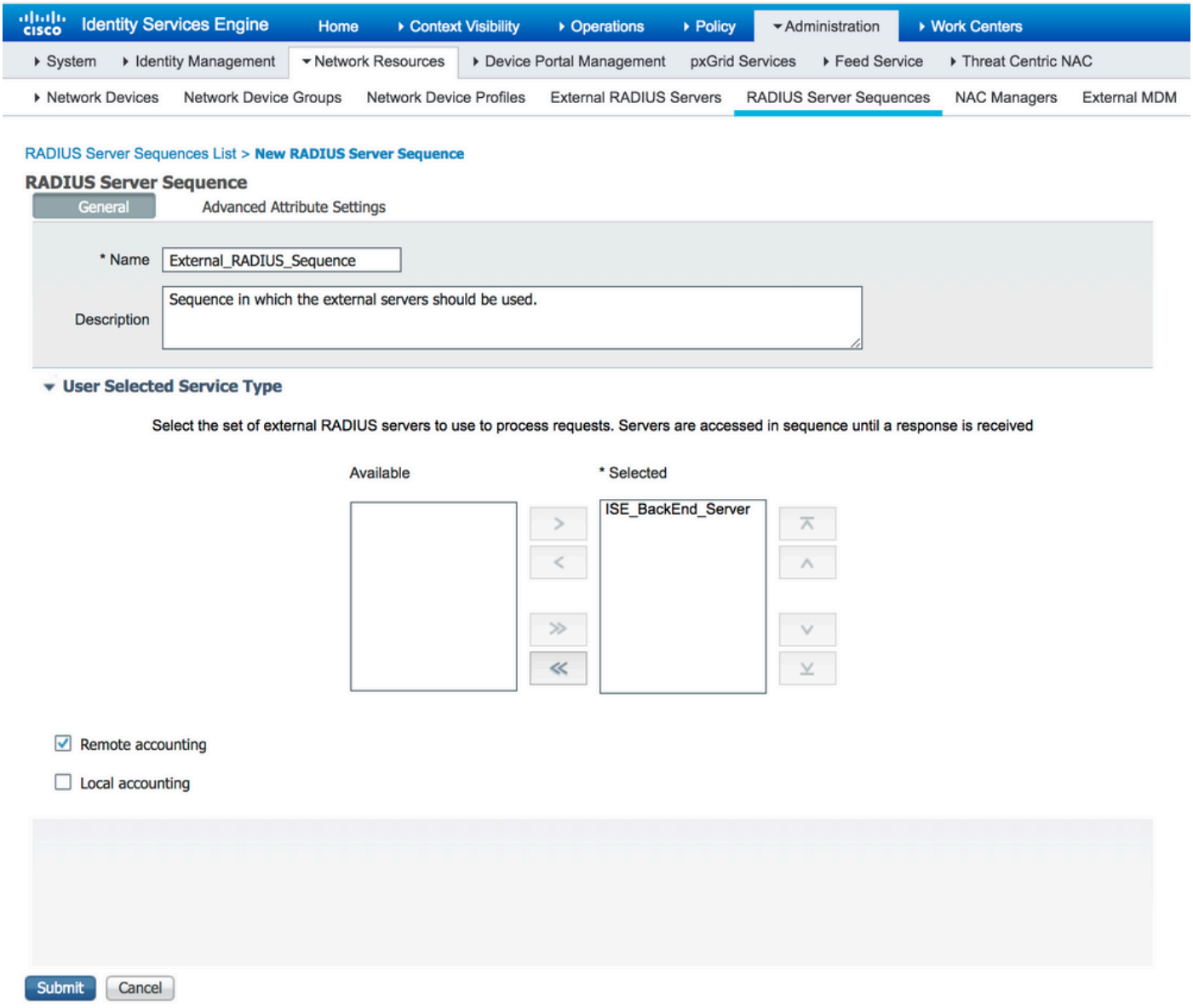
1단계. ISE에서 사용자를 인증하기 위해 여러 외부 RADIUS 서버를 구성하고 사용할 수 있습니다. 외부 RADIUS 서버를 구성하려면 Administration > Network Resources > External RADIUS Servers > Add, 이미지에 표시된 대로





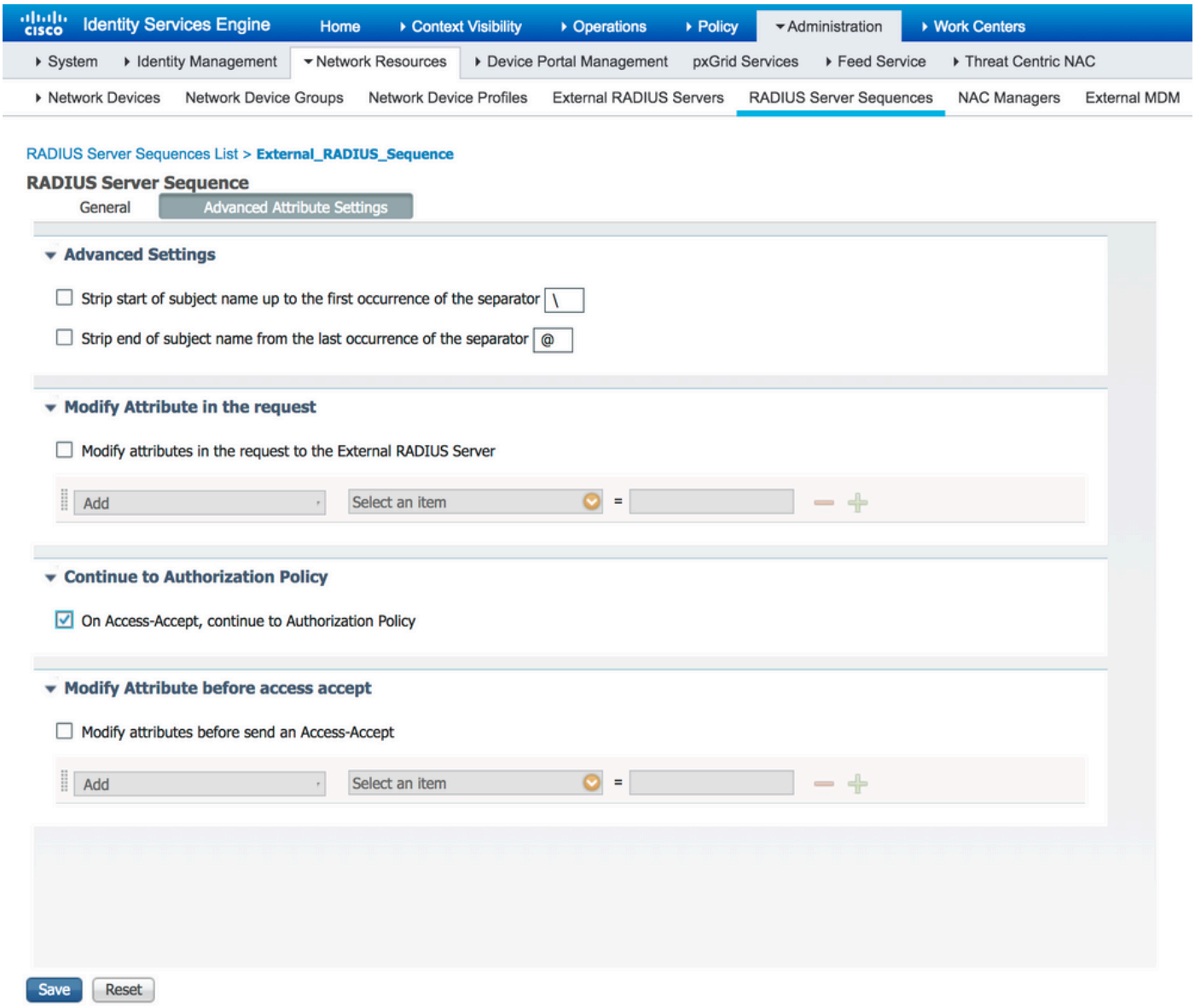
2단계. 구성된 외부 RADIUS 서버를 사용하려면 ID 소스 시퀀스와 유사하게 RADIUS 서버 시퀀스를 구성해야 합니다. 동일한 를 구성하려면 다음으로 이동합니다. Administration > Network Resources > RADIUS Server Sequences > Add에 나와 있는 것처럼.





참고: 서버 시퀀스가 생성될 때 사용할 수 있는 옵션 중 하나는 어카운팅이 ISE에서 로컬로 수행되어야 하는지 또는 외부 RADIUS 서버에서 수행되어야 하는지를 선택하는 것입니다. 여기서 선택한 옵션에 따라 ISE는 어카운팅 요청을 프록시할지 아니면 해당 로그를 로컬에 저장할지를 결정합니다.

3단계. ISE가 외부 RADIUS 서버에 요청을 프록시할 때 ISE가 어떻게 동작해야 하는지 좀 더 유연하게 설명하는 추가 섹션이 있습니다. Cisco Security Solutions Engine의 Advance Attribute Settings에 나와 있는 것처럼.



- 고급 설정: 구분 기호를 사용하여 RADIUS 요청에서 사용자 이름의 시작 또는 끝을 제거하는 옵션을 제공합니다.
- 요청의 속성 수정: RADIUS 요청의 모든 RADIUS 속성을 수정할 수 있는 옵션을 제공합니다. 이 목록에는 추가/제거/업데이트할 수 있는 특성이 표시됩니다.

```
User-Name--[1]
NAS-IP-Address--[4]
NAS-Port--[5]
Service-Type--[6]
Framed-Protocol--[7]
Framed-IP-Address--[8]
Framed-IP-Netmask--[9]
Filter-ID--[11]
Framed-Compression--[13]
Login-IP-Host--[14]
Callback-Number--[19]
State--[24]
VendorSpecific--[26]
Called-Station-ID--[30]
Calling-Station-ID--[31]
```

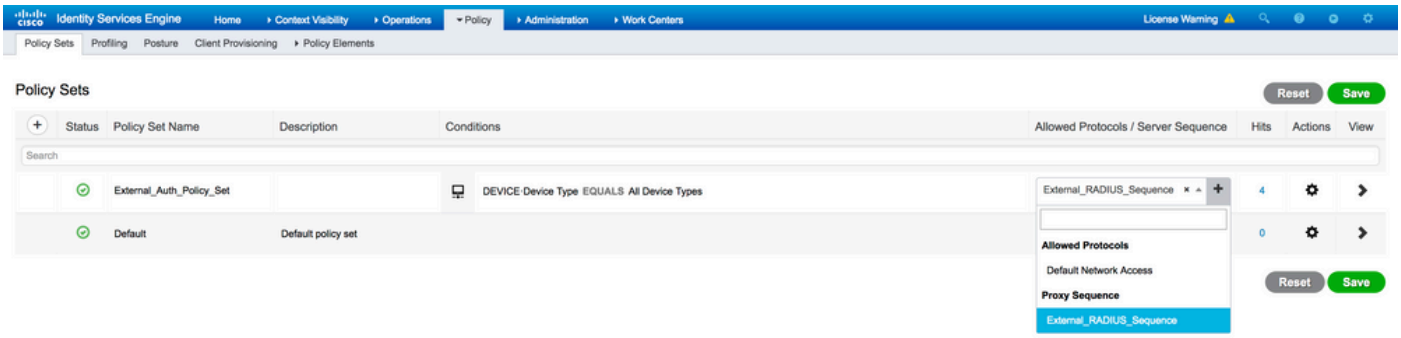
```
NAS-Identifier--[32]
Login-LAT-Service--[34]
Login-LAT-Node--[35]
Login-LAT-Group--[36]
Event-Timestamp--[55]
Egress-VLANID--[56]
Ingress-Filters--[57]
Egress-VLAN-Name--[58]
User-Priority-Table--[59]
NAS-Port-Type--[61]
Port-Limit--[62]
Login-LAT-Port--[63]
Password-Retry--[75]
Connect-Info--[77]
NAS-Port-Id--[87]
Framed-Pool--[88]
NAS-Filter-Rule--[92]
NAS-IPv6-Address--[95]
Framed-Interface-Id--[96]
Framed-IPv6-Prefix--[97]
Login-IPv6-Host--[98]
Error-Cause--[101]
Delegated-IPv6-Prefix--[123]
Framed-IPv6-Address--[168]
DNS-Server-IPv6-Address--[169]
Route-IPv6-Information--[170]
Delegated-IPv6-Prefix-Pool--[171]
Stateful-IPv6-Address-Pool--[172]
```

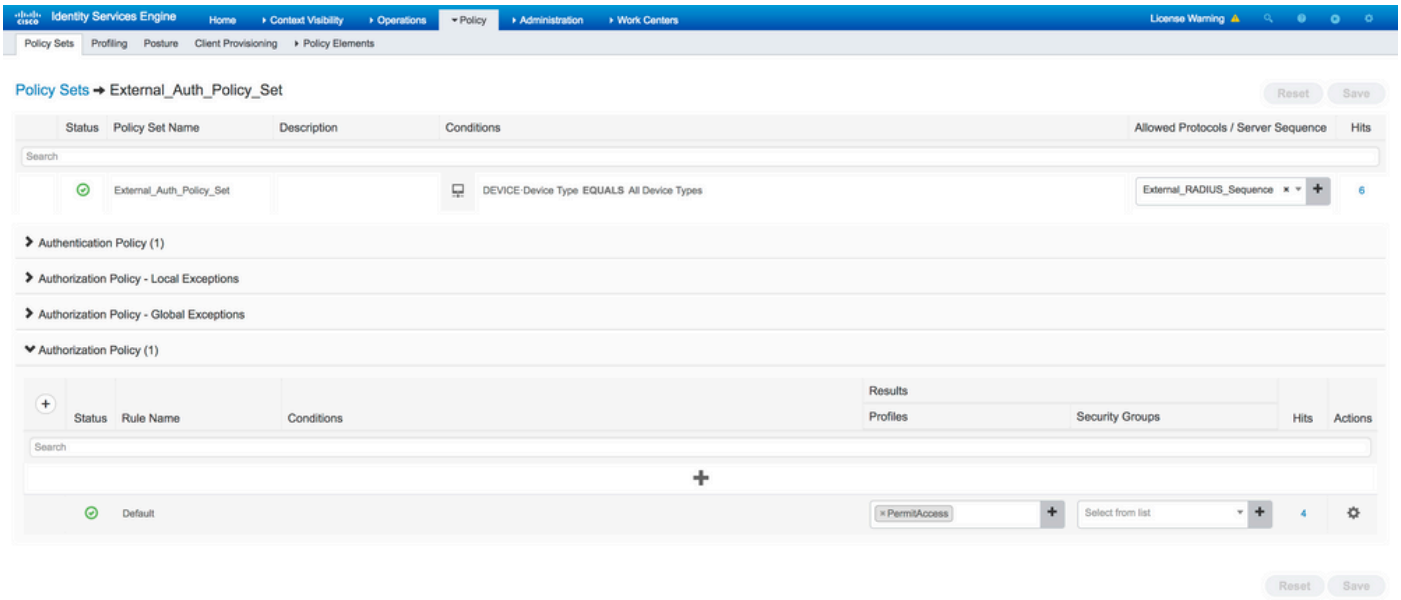
- Continue to Authorization Policy on Access-Accept: ISE에서 Access-Accept를 그대로 전송해야 하는지 또는 외부 RADIUS 서버에서 제공하는 권한 부여가 아니라 ISE에 구성된 권한 부여 정책을 기반으로 액세스를 제공해야 하는지를 선택할 수 있는 옵션을 제공합니다. 이 옵션을 선택하면 외부 RADIUS 서버에서 제공하는 권한 부여가 ISE에서 제공하는 권한 부여로 덮어쓰기됩니다.

> 참고: 이 옵션은 외부 RADIUS 서버에서 Access-Accept 프록시된 RADIUS 액세스 요청에 대한 응답.

- Modify Attribute before Access-Accept(액세스 수락 전에 특성 수정): Modify Attribute in the request, 앞서 언급 한 속성은 네트워크 장치로 전송 되기 전에 외부 RADIUS 서버에 의해 전송 된 Access-Accept에 존재 추가 / 제거 / 업데이트 할 수 있습니다.

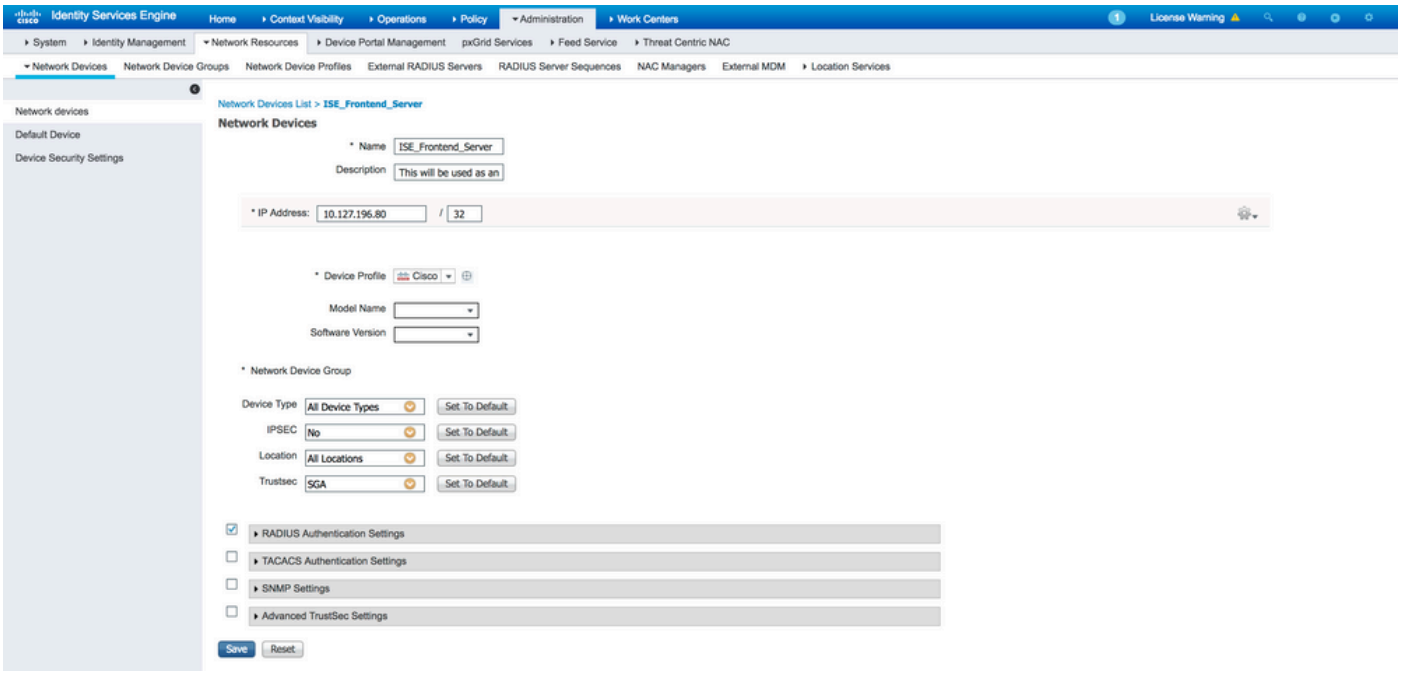
4단계. 다음 부분은 외부 RADIUS 서버로 요청이 전송되도록 허용된 프로토콜 대신 RADIUS 서버 시퀀스를 사용하도록 정책 집합을 구성하는 것입니다. 구성 가능한 구성 Policy > Policy Sets. 권한 부여 정책은 Policy Set 하지만 이 경우 Continue to Authorization Policy on Access-Accept 옵션을 선택합니다. 그렇지 않은 경우, ISE는 이 정책 집합에 대해 구성된 조건과 매칭하기 위해 RADIUS 요청에 대한 프록시 역할을 합니다.



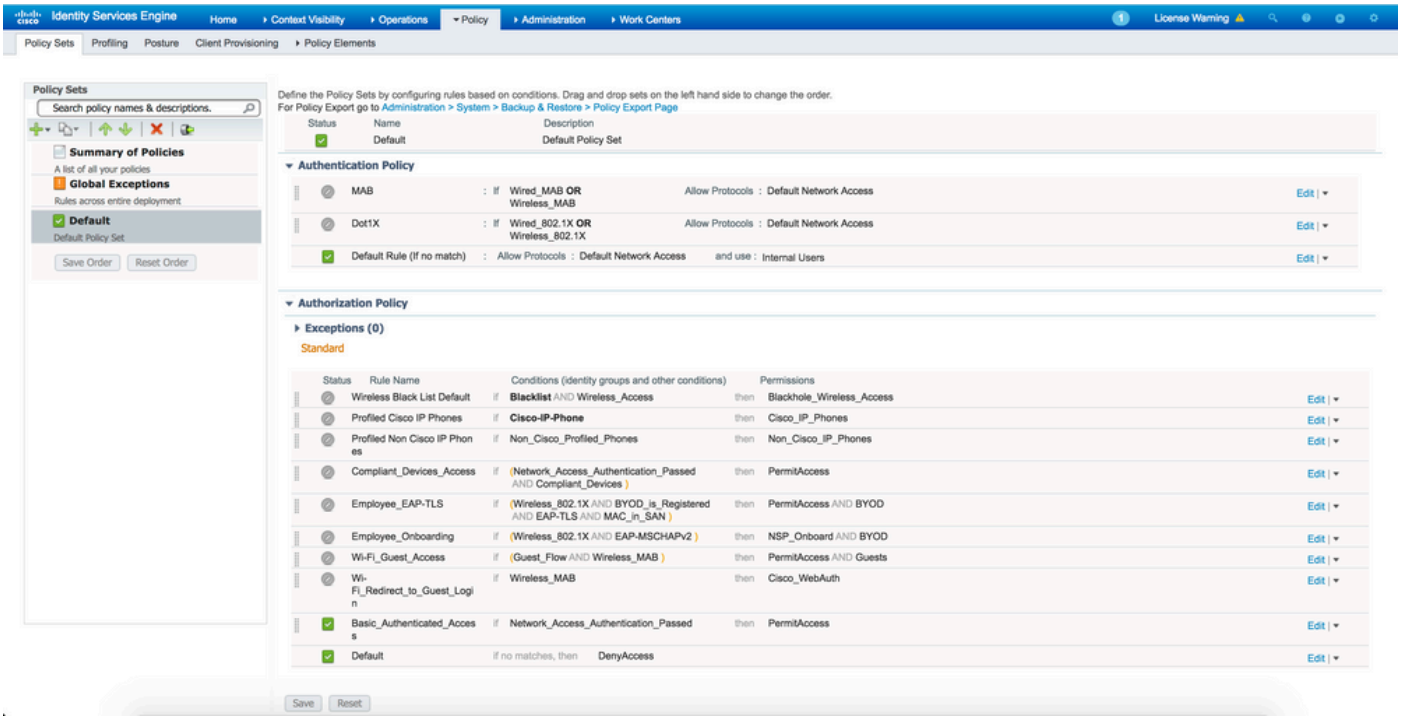


외부 RADIUS 서버 구성

1단계. 이 예에서는 다른 ISE 서버(버전 2.2)가 외부 RADIUS 서버로 사용됩니다 ISE_Backend_Server. ISE(ISE_Frontend_Server)는 네트워크 디바이스로 구성되거나 외부 RADIUS 서버에서 전통적으로 NAS라고 합니다(ISE_Backend_Server 이 예에서는 NAS-IP-Address 외부 RADIUS 서버로 전달 된 액세스 요청의 속성은 의 IP 주소로 대체 됩니다.ISE_Frontend_Server. 구성할 공유 비밀은 의 외부 RADIUS 서버에 대해 구성된 것과 동일합니다. ISE_Frontend_Server.



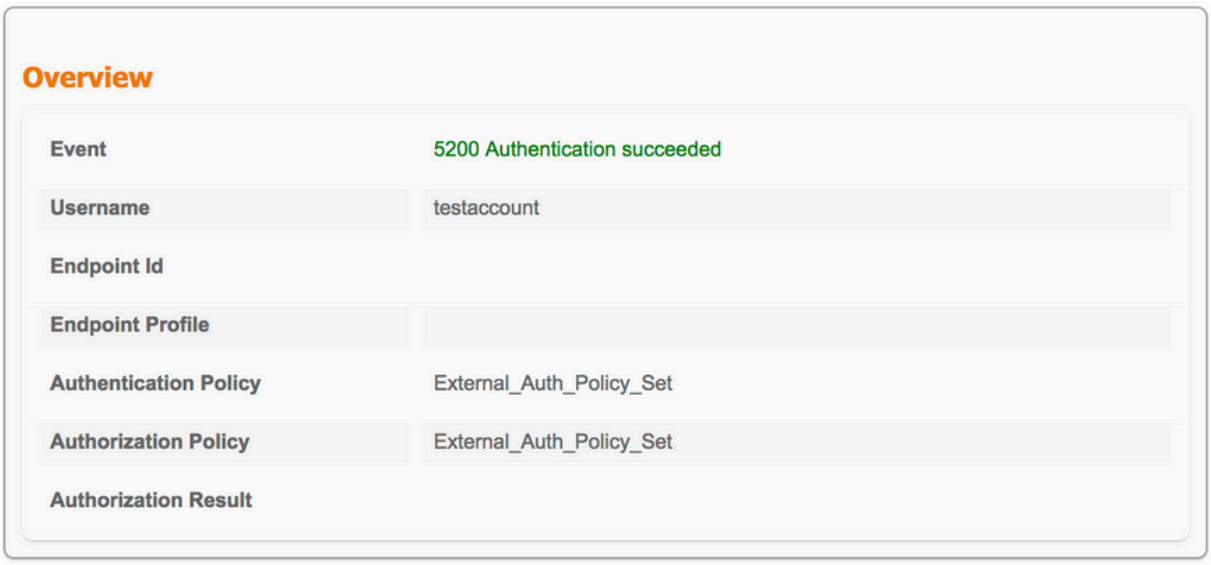
2단계. 외부 RADIUS 서버는 ISE에서 프록시한 요청을 처리하기 위해 자체 인증 및 권한 부여 정책으로 구성할 수 있습니다. 이 예에서는 내부 사용자의 사용자를 확인한 다음 인증된 경우 액세스를 허용하도록 간단한 정책을 구성합니다.



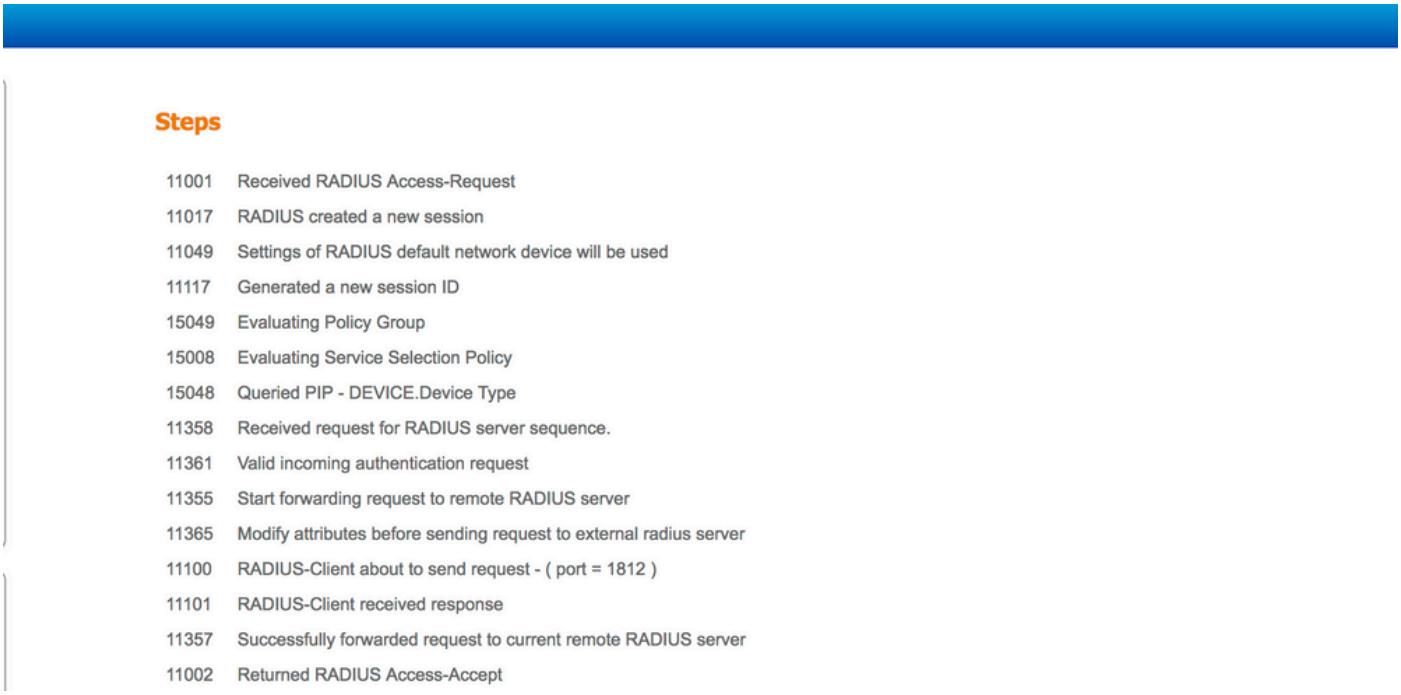
다음을 확인합니다.

1단계. 이미지에 표시된 대로 요청이 수신되면 ISE 라이브 로그를 확인합니다.

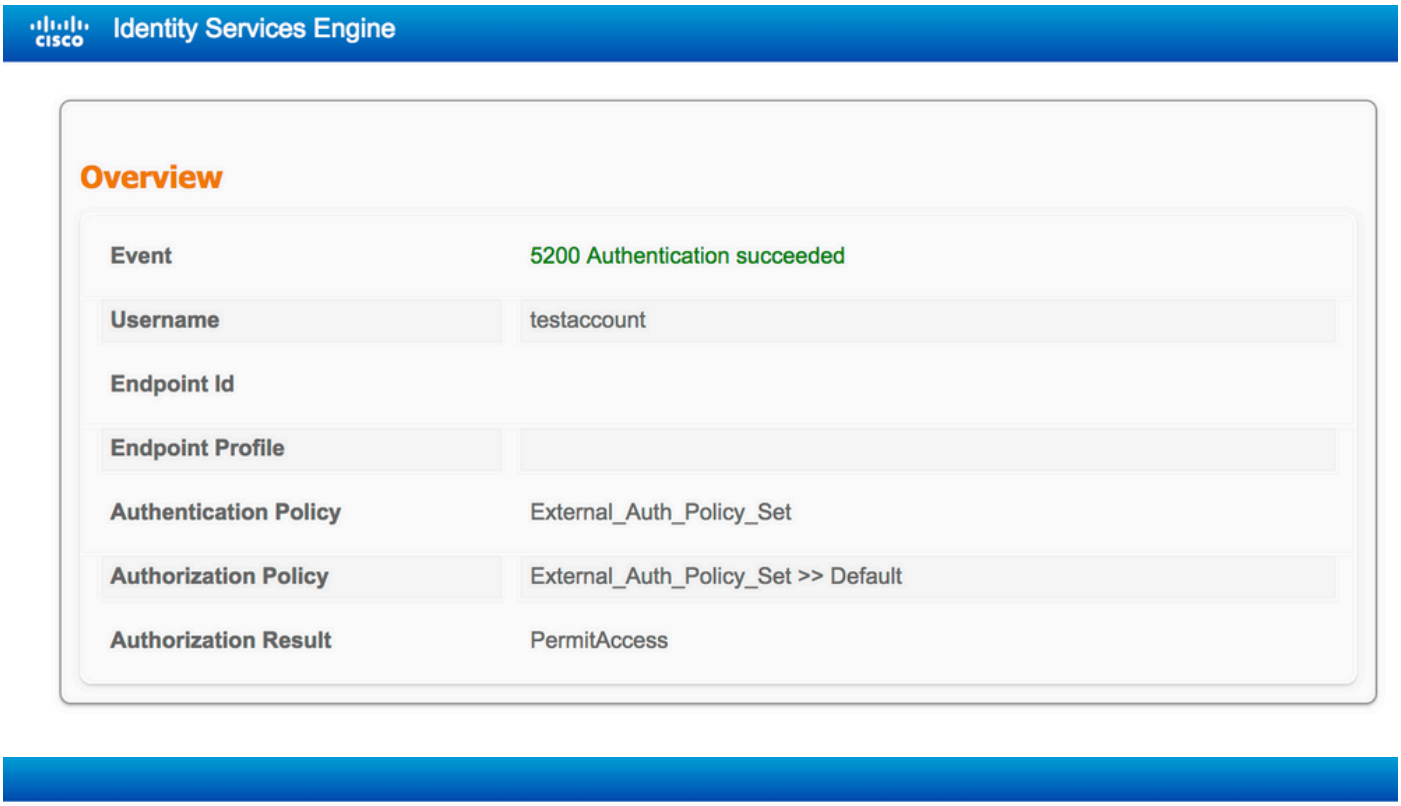
2단계. 이미지에 표시된 대로 올바른 정책 집합이 선택되었는지 확인합니다.

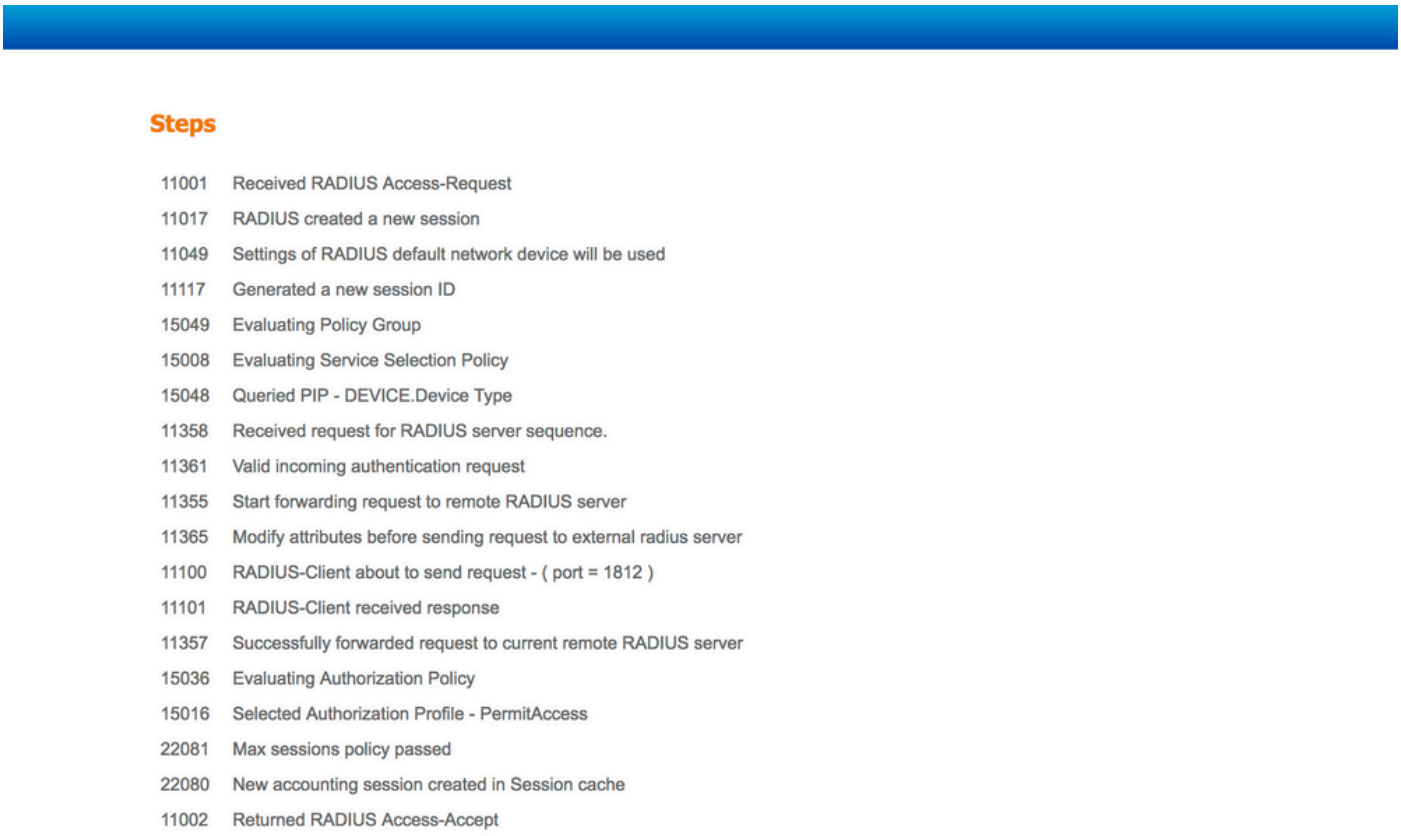


3단계. 요청이 외부 RADIUS 서버로 전달되는지 확인합니다.



4. 다음과 같은 경우 Continue to Authorization Policy on Access-Accept 옵션을 선택하고 권한 부여 정책을 평가하는지 확인합니다.



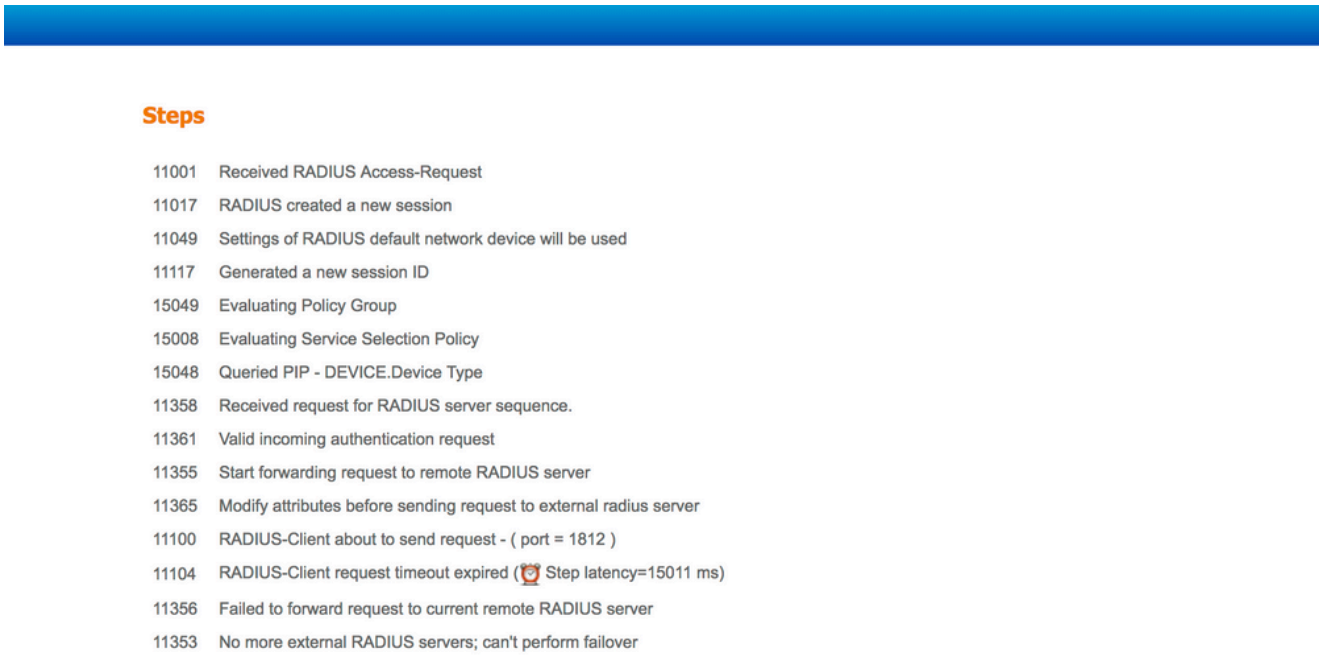


문제 해결

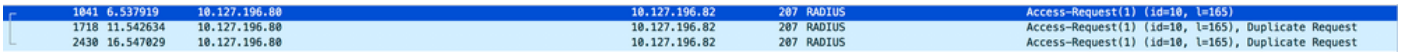
시나리오 1. 이벤트 - 5405 RADIUS 요청 삭제됨

- 반드시 검증해야 할 가장 중요한 것은 세부 인증 보고서의 단계이다. 단계에 RADIUS-Client request timeout expired그러면 ISE가 구성된 외부 RADIUS 서버로부터 어떤 응답도 받지 못했음을 의미합니다. 다음과 같은 경우에 발생할 수 있습니다.

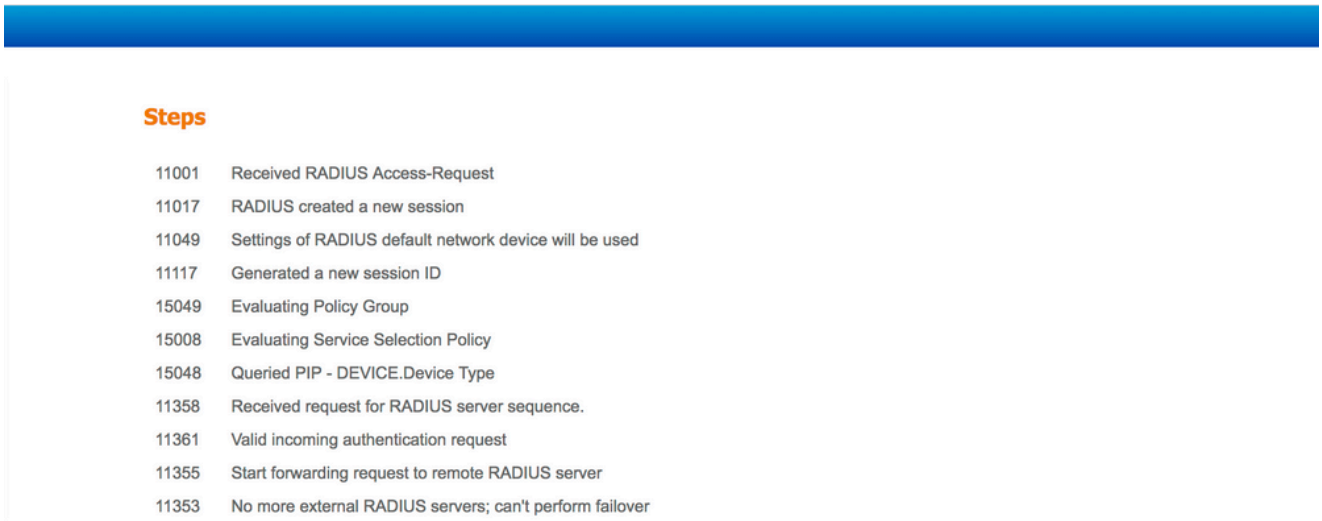
1. 외부 RADIUS 서버에 연결 문제가 있습니다. ISE가 구성된 포트에서 외부 RADIUS 서버에 연결할 수 없습니다.
2. ISE는 외부 RADIUS 서버에서 네트워크 디바이스 또는 NAS로 구성되지 않습니다.
3. 외부 RADIUS 서버는 구성에 의해 또는 외부 RADIUS 서버의 일부 문제 때문에 패킷을 삭제합니다.



패킷 캡처도 확인하여 잘못된 메시지가 아닌지 확인합니다. 즉, ISE가 서버에서 패킷을 다시 받지만 요청 시간이 초과되었음을 보고합니다.



- 다음 단계를 수행하면 Start forwarding request to remote RADIUS server 그리고 즉각적인 단계는 No more external RADIUS servers; can't perform failover, 그러면 구성된 모든 외부 RADIUS 서버가 현재 데드(dead)로 표시되고 데드 타이머가 만료된 후에만 요청이 처리됨을 의미합니다.



참고: ISE의 외부 RADIUS 서버에 대한 기본 데드 시간은 5분입니다. 이 값은 하드 코드이므로 이 버전에서는 수정할 수 없습니다.

- 다음 단계를 수행하면 RADIUS-Client encountered error during processing flow 그 뒤에 Failed to forward request to current remote RADIUS server; an invalid response was received,그러면 외부 RADIUS 서버에 대한 요청이 전달되는 동안 ISE에 문제가 발생했음을 의미합니다. 일반적으로 네트워크 디바이스/NAS에서 ISE로 전송된 RADIUS 요청에 NAS-IP-Address 하나의 특성으로 간주합니다. 없는 경우 NAS-IP-Address 외부 RADIUS 서버가 사용 중이 아닌 경우 ISE는 NAS-IP-Address 패킷의 소스 IP가 있는 필드. 그러나 외부 RADIUS 서버를 사용 중인 경우에는 적용되지 않습니다.

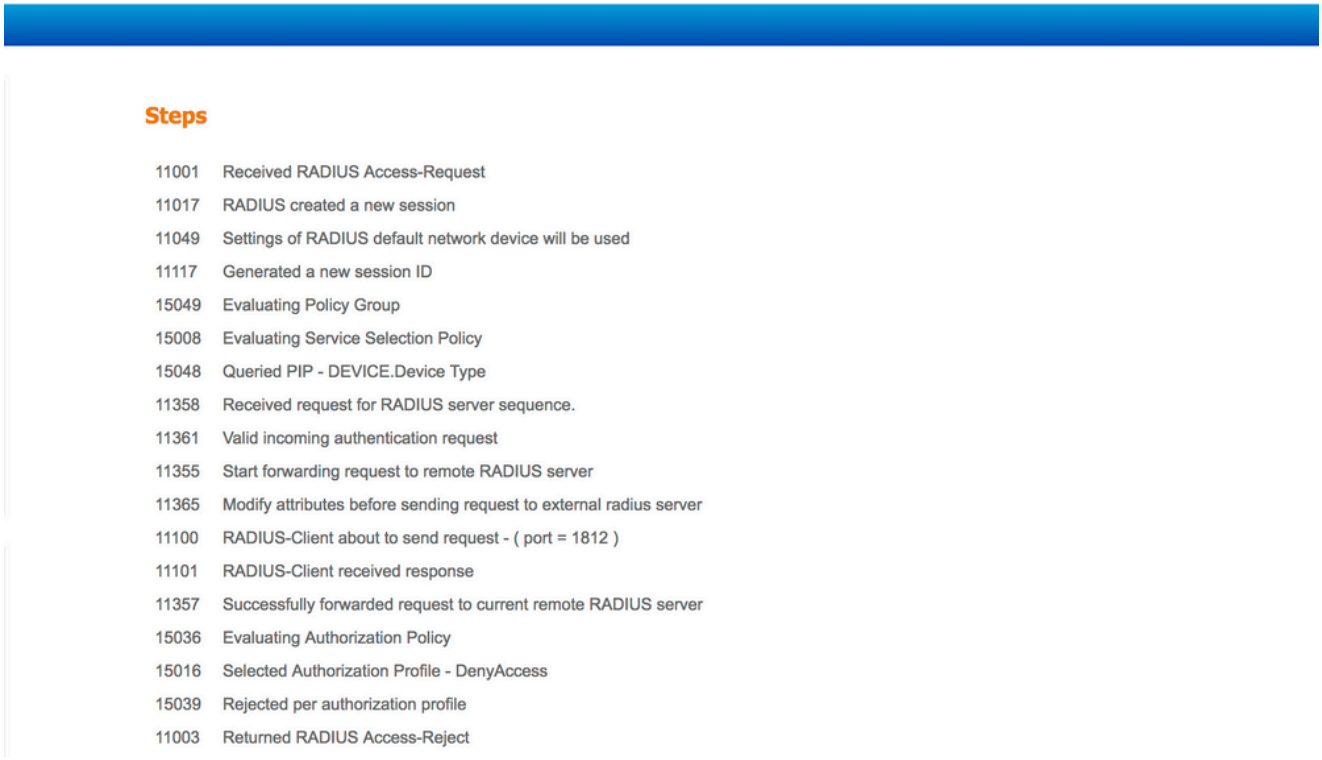
시나리오 2. 이벤트 - 5400 인증 실패

- 이 경우 단계에서 11368 Please review logs on the External RADIUS Server to determine the precise failure reason그러면 외부 RADIUS 서버 자체에서 인증이 실패했으며 Access-Reject를 전송했음을 의미합니다.

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response
11368	Please review logs on the External RADIUS Server to determine the precise failure reason.
11357	Successfully forwarded request to current remote RADIUS server
11003	Returned RADIUS Access-Reject

- 다음 단계를 수행하면 15039 Rejected per authorization profile즉, ISE가 외부 RADIUS 서버로부터 Access-Accept를 수신했지만 구성된 권한 부여 정책에 따라 ISE가 권한 부여를 거부합니다.



Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response
11357	Successfully forwarded request to current remote RADIUS server
15036	Evaluating Authorization Policy
15016	Selected Authorization Profile - DenyAccess
15039	Rejected per authorization profile
11003	Returned RADIUS Access-Reject

- 이 Failure Reason ISE에는 인증 실패의 경우 여기에 언급된 것과 다른 어떤 것도 있으며, 이는 컨피그레이션 또는 ISE 자체와 관련된 잠재적인 문제를 의미할 수 있습니다. 이 시점에서 TAC 케이스를 여는 것이 좋습니다.

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.