ISE(Identity Services Engine)와 함께 디바이스 관리에 RADIUS 사용

목차

소개

이 문서에서는 다양한 Cisco 및 타사 제품이 Cisco ISE와 같은 AAA 서버로부터 수신할 것으로 예상되는 특성의 컴파일에 대해 설명합니다.

배경 정보

Cisco 및 타사 제품은 AAA(Authentication, Authorization, and Accounting) 서버에서 특성 컴파일을 수신하려고 합니다. 이 경우 서버는 Cisco ISE이며 ISE는 권한 부여 프로파일(RADIUS)의 일부로서 Access-Accept와 함께 이러한 특성을 반환합니다.

이 문서에서는 사용자 지정 특성 권한 부여 프로파일을 추가하는 방법에 대한 단계별 지침을 제공하며, 디바이스에서 AAA 서버에서 반환되는 RADIUS 특성 및 디바이스 목록을 포함합니다. 모든 항목에는 예제가 포함되어 있습니다.

이 문서에 제공된 특성 목록은 완전한 것도 아니고 권위 있는 것도 아니며 이 문서를 업데이트하지 않으면 언제든지 변경할 수 있습니다.

네트워크 디바이스의 디바이스 관리는 일반적으로 TACACS+ 프로토콜을 통해 수행되지만, 네트워

크 디바이스가 TACACS+를 지원하지 않거나 ISE에 디바이스 관리 라이센스가 없는 경우, 네트워크 디바이스가 RADIUS 디바이스 관리를 지원하는 경우에도 RADIUS를 통해 수행할 수 있습니다. 일부 디바이스는 두 프로토콜을 모두 지원하며, 사용자가 어떤 프로토콜을 사용할지 결정할 수 있습니다. 그러나 TACACS+는 명령 권한 부여 및 명령 어카운팅과 같은 기능이 있으므로 유리할 수 있습니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 사항에 대해 알고 있는 것이 좋습니다.

- Cisco ISE는 관심 네트워크에서 Radius 서버로 사용
- Radius 프로토콜의 워크플로 - RFC2865

사용되는 구성 요소

이 문서의 정보는 Cisco ISE(Identity Services Engine) 3.x 이상 버전의 ISE를 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

1단계. VSA(Vendor-Specific Attribute) 생성

판매업체별로 다양한 사전이 생성될 수 있으며, 이러한 사전 각각에 속성을 추가할 수 있습니다. 각 사전에는 권한 부여 프로파일에서 사용할 수 있는 여러 특성이 있을 수 있습니다. 일반적으로 각 특성은 사용자가 네트워크 디바이스에 로그인할 때 얻을 수 있는 디바이스 관리의 서로 다른 역할을 정의합니다. 그러나 이 속성은 네트워크 디바이스에서의 동작 또는 컨피그레이션의 다른 목적을 위해 사용될 수 있습니다.

ISE는 일부 벤더에 대해 사전 정의된 특성을 제공합니다. 판매업체가 목록에 없으면 특성을 가진 사전으로 추가할 수 있습니다. 일부 네트워크 디바이스의 경우 특성을 구성할 수 있으며 다양한 액세스 유형에 대해 변경할 수 있습니다. 이러한 경우 ISE는 네트워크 디바이스가 다양한 액세스 유형에 대해 기대하는 특성으로 구성해야 합니다.

Radius Access-Accept를 사용하여 전송할 속성은 다음과 같이 정의됩니다.

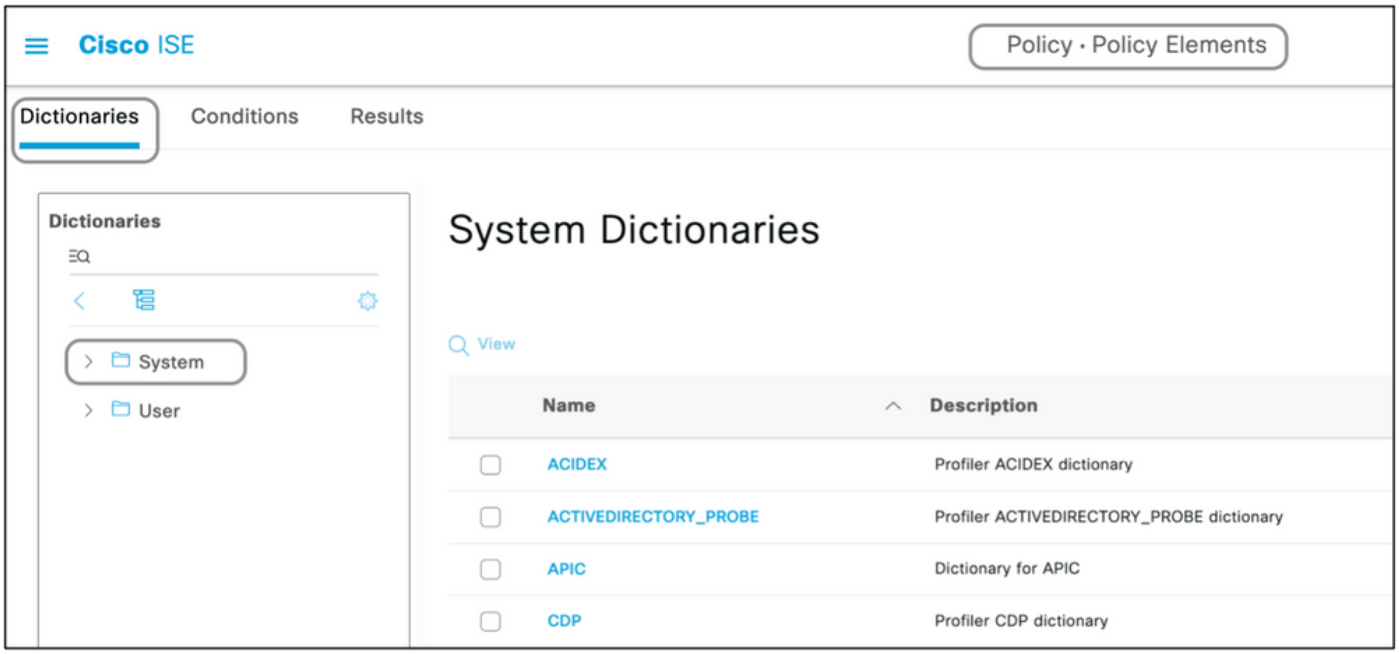
1. Policy(**정책) > Policy Elements(정책 요소) > Dictionaries(사전) > System(시스템) > Radius > Radius Vendors(RADIUS 벤더) > Add(추가)로 이동합니다**.
2. 이름 및 공급업체 ID를 입력하고 저장합니다.
3. 저장된 Radius Vendor를 **클릭하고 Dictionary** Attributes(**사전 특성)로 이동합니다**.
4. Add(**추가**)를 클릭하고 대소문자를 구분하는 Attribute Name(특성 이름), Data Type(데이터 유

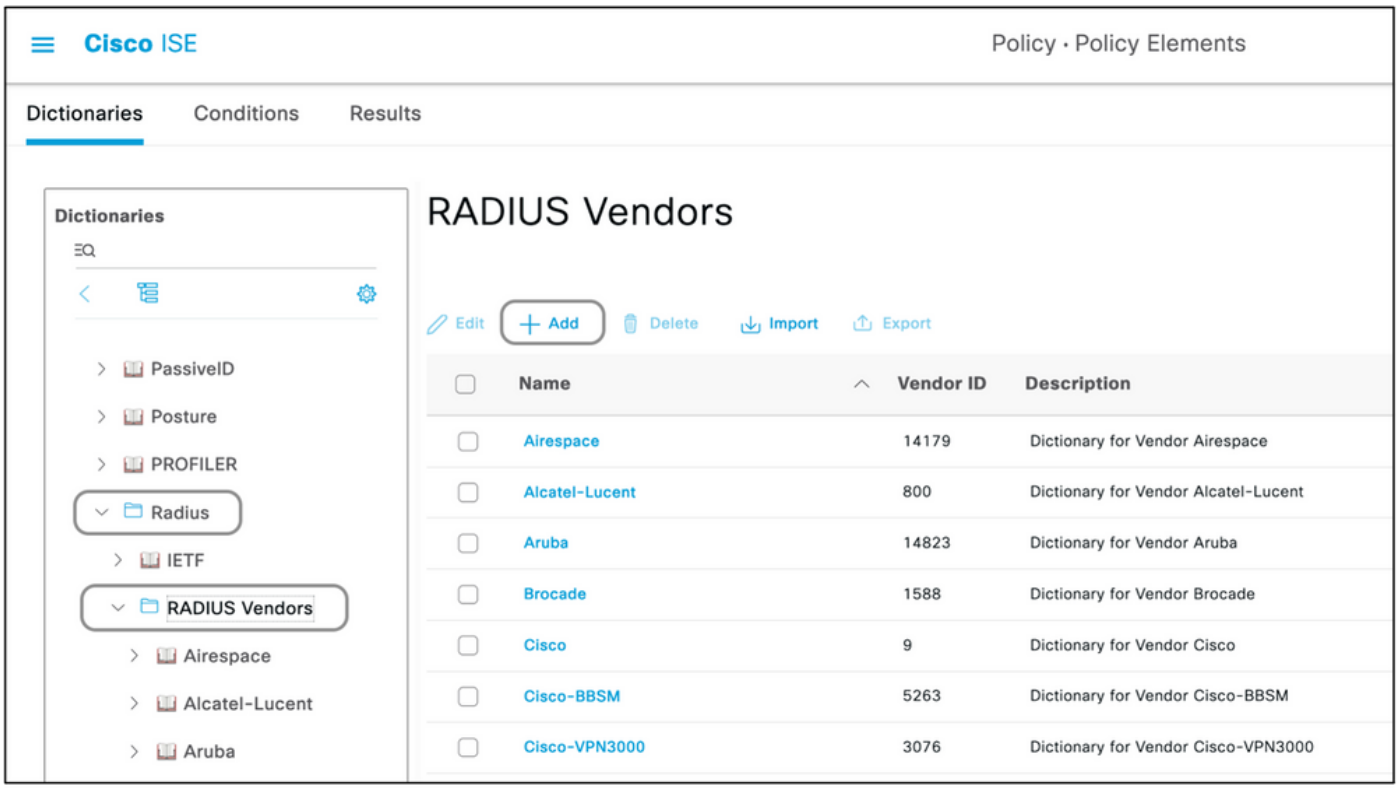
형), Direction(방향) 및 ID를 입력합니다.

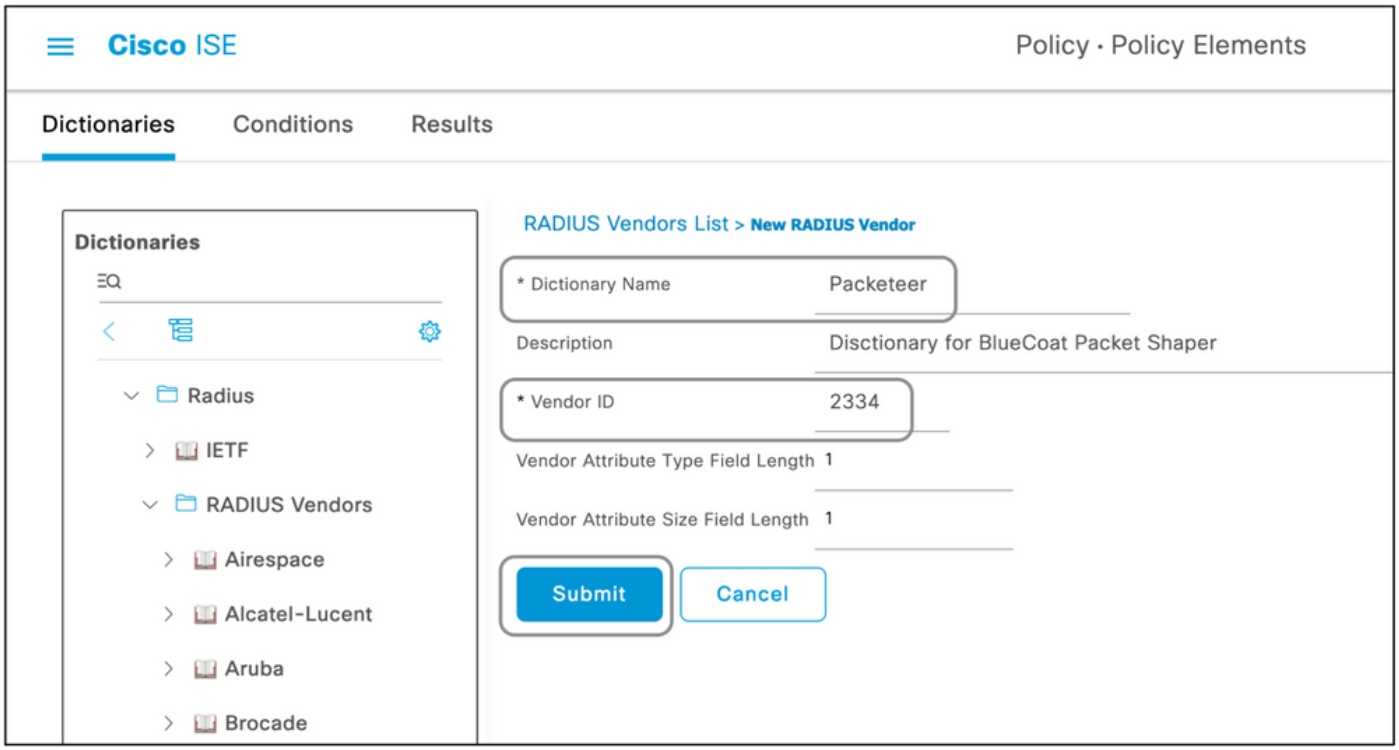
5. **특성**을 저장합니다.

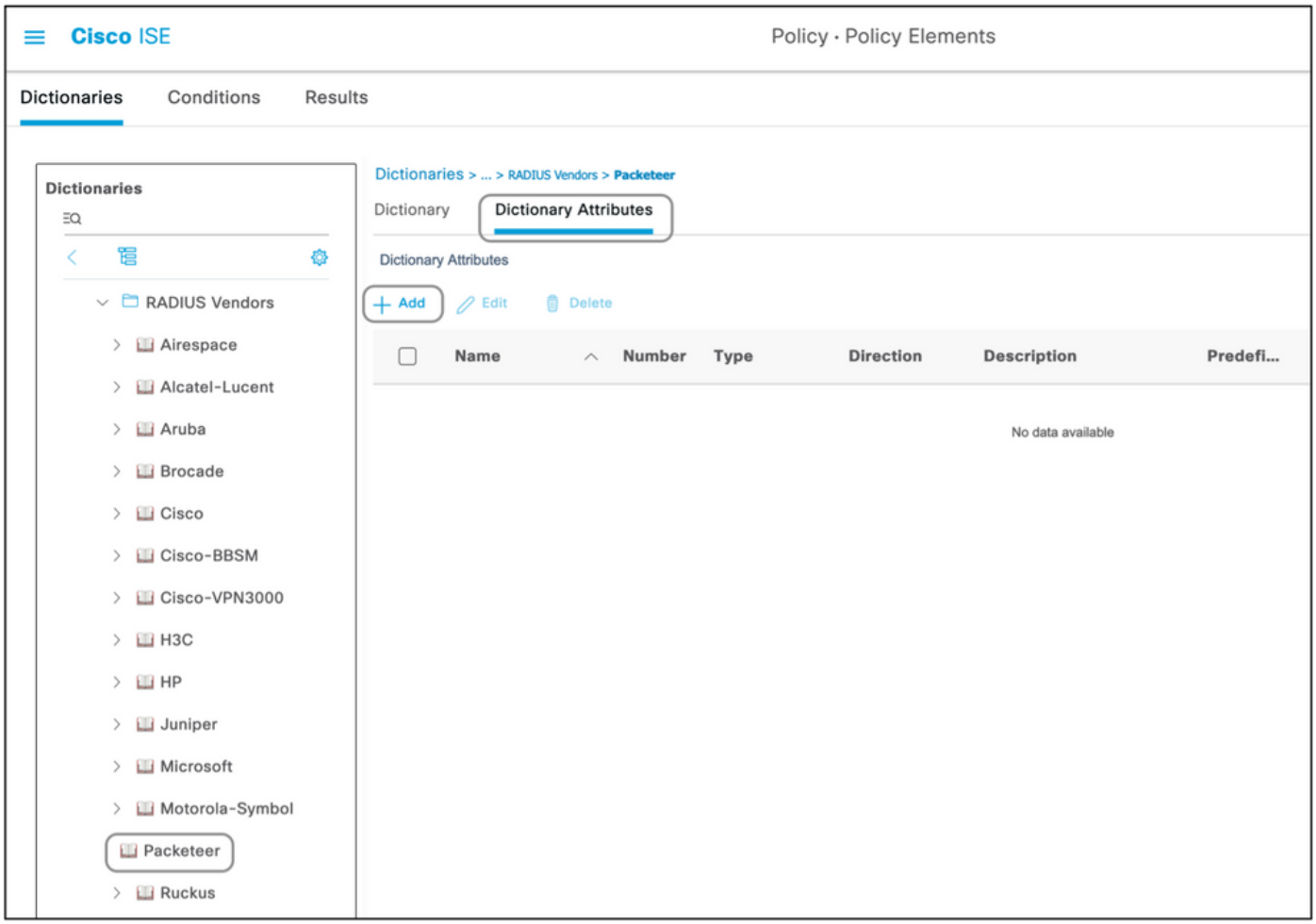
6. 동일한 사전에 추가할 속성이 여러 개인 경우 동일한 페이지에 다른 속성을 추가합니다.

참고: 이 섹션에 값으로 입력된 각 필드는 판매업체가 직접 제공해야 합니다. 판매업체 웹 사이트를 방문하거나 모르는 경우 판매업체 지원 팀에 문의할 수 있습니다.






Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
Radius
IETF
RADIUS Vendors
Airespace
Alcatel-Lucent
Aruba
Brocade
RADIUS Vendors List > New RADIUS Vendor
* Dictionary Name
Packeteer
Description
Disctionary for BlueCoat Packet Shaper
* Vendor ID
2334
Vendor Attribute Type Field Length
1
Vendor Attribute Size Field Length
1
Submit
Cancel


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
RADIUS Vendors
Airespace
Alcatel-Lucent
Aruba
Brocade
Cisco
Cisco-BBSM
Cisco-VPN3000
H3C
HP
Juniper
Microsoft
Motorola-Symbol
Packeteer
Ruckus
Dictionaries > ... > RADIUS Vendors > Packeteer
Dictionary
Dictionary Attributes
Dictionary Attributes
Add
Edit
Delete
Name
Number
Type
Direction
Description
Predefi...
No data available

참고: 일부 벤더에서는 특정 사전을 추가할 필요가 없습니다. 공급업체가 ISE에 이미 존재하는 IETF에 의해 정의된 RADIUS 특성을 사용할 수 있는 경우 이 단계를 건너뛸 수 있습니다.

2단계. 네트워크 디바이스 프로파일 생성

이 섹션은 필수가 아닙니다. 네트워크 디바이스 프로필은 추가된 네트워크 디바이스 유형을 분리하고 해당 유형에 적합한 권한 부여 프로필을 생성하는 데 도움이 됩니다. ISE는 radius 사전과 마찬가지로 사용할 수 있는 몇 가지 미리 정의된 프로필을 가지고 있습니다. 아직 없는 경우 새 디바이스 프로필을 생성할 수 있습니다.

다음은 네트워크 프로필을 추가하기 위한 절차입니다.

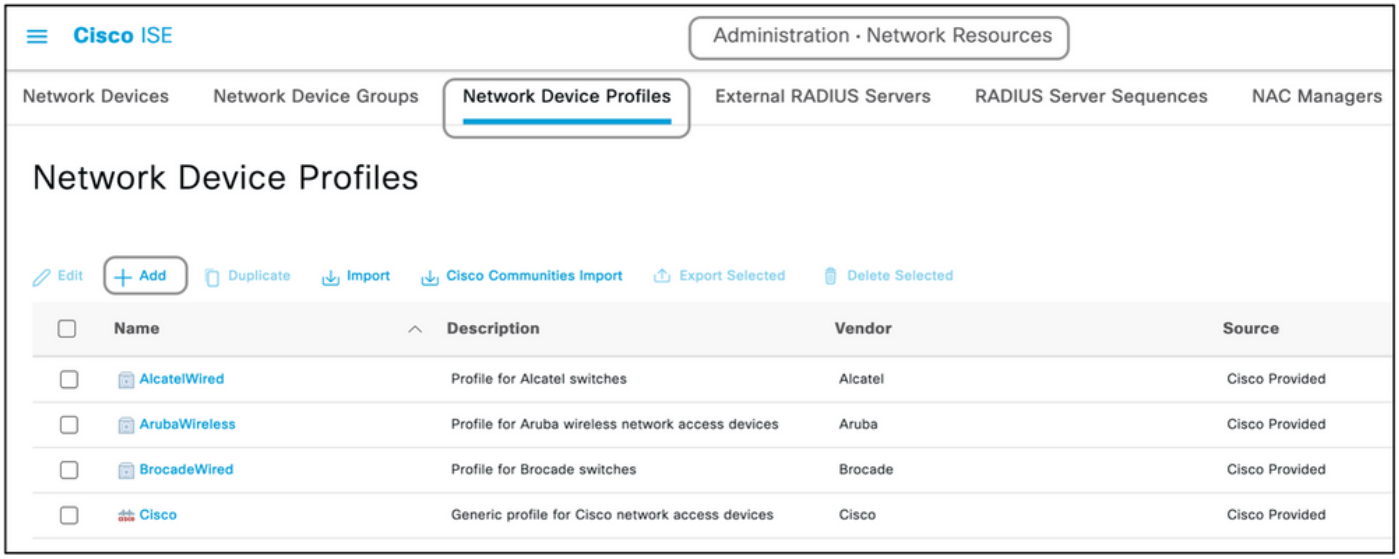
1. 탐색 **Administration(관리) > Network Resources(네트워크 리소스) > Network Device Profiles(네트워크 디바이스 프로파일) > Add(추가)**

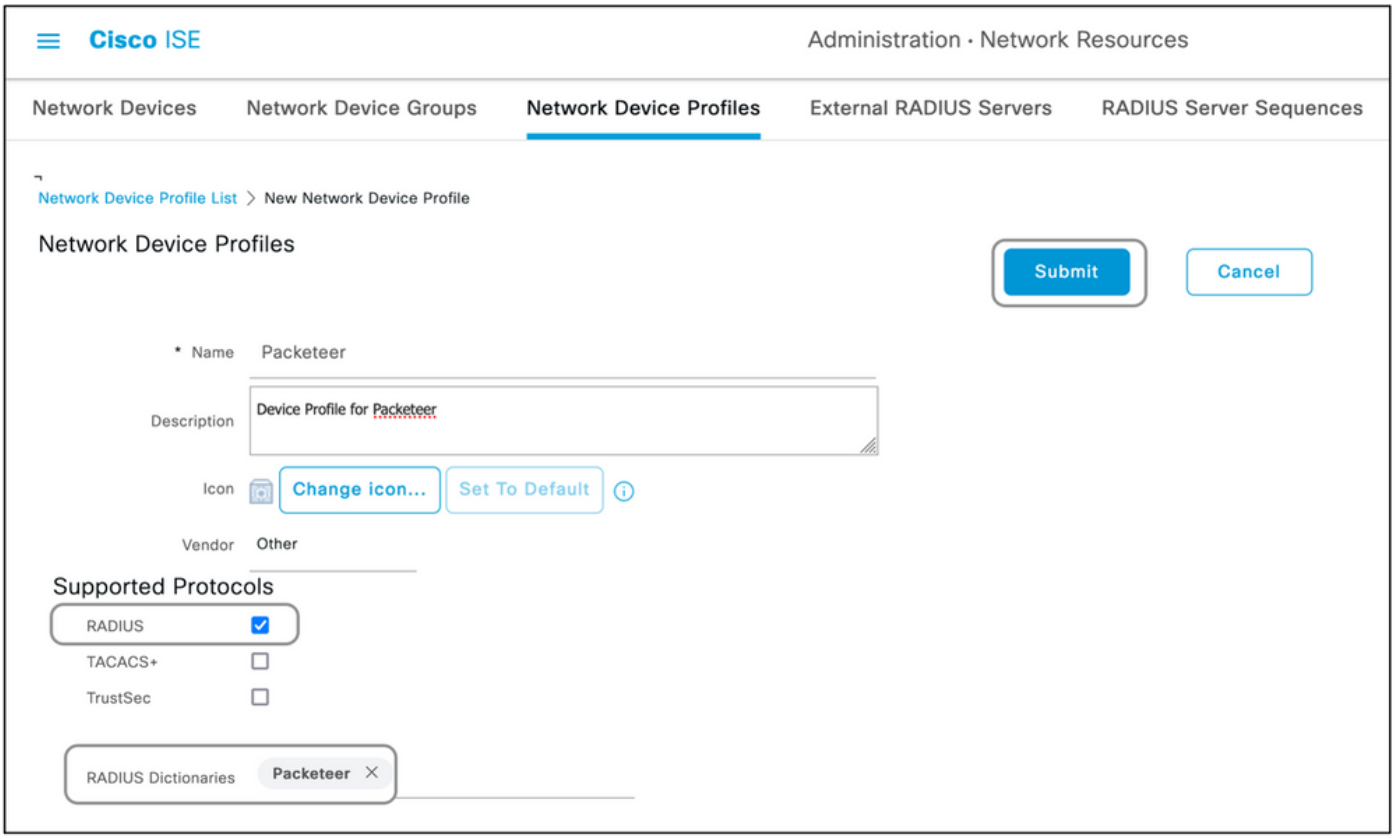
2. 이름을 지정하고 RADIUS 확인란을 **선택합니다**.

3. RADIUS Dictionaries(**RADIUS 사전**) 아래에서 이전 섹션에서 생성한 사전을 선택합니다.

4. 동일한 디바이스 유형에 대해 여러 사전이 생성된 경우 RADIUS Dictionaries(RADIUS 사전)에서 모두 선택할 **수 있습니다**.

5. **프로파일**을 저장합니다.





3단계. ISE에 네트워크 디바이스 추가

디바이스 관리가 달성되는 네트워크 디바이스는 네트워크 디바이스에 정의된 키와 함께 ISE에 추가되어야 합니다. 네트워크 디바이스에서 ISE는 이 키를 사용하여 radius AAA 서버로 추가됩니다.

ISE에서 디바이스를 추가하는 절차는 다음과 같습니다.

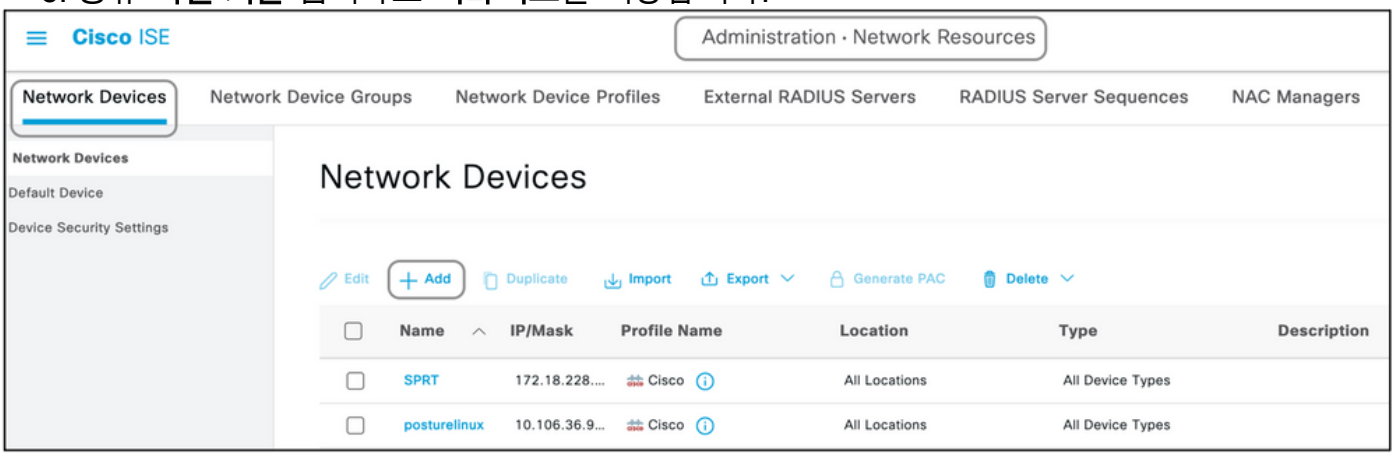
1. 탐색 **Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > Add(추가)**

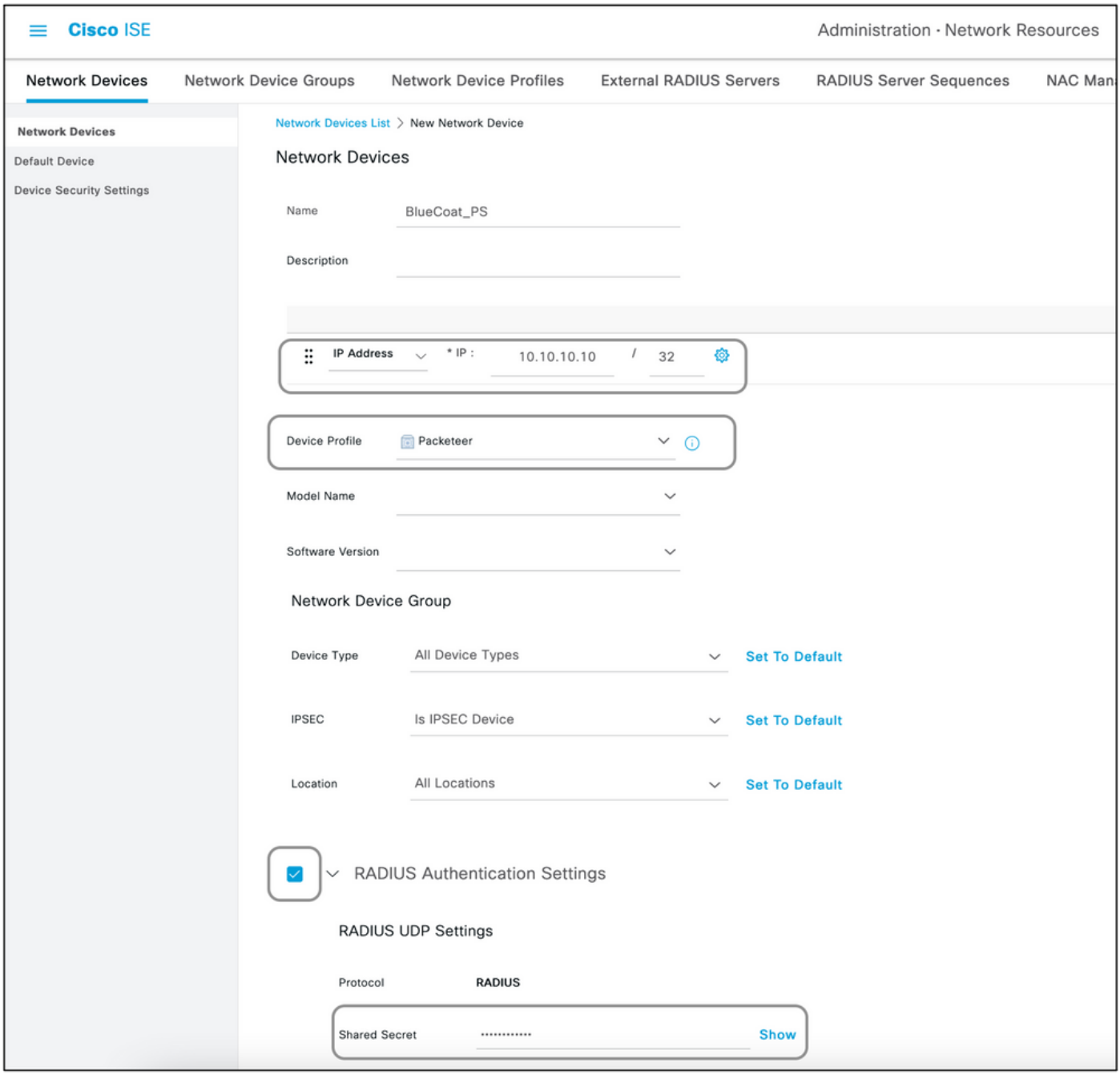
2. 이름과 IP 주소를 지정합니다.

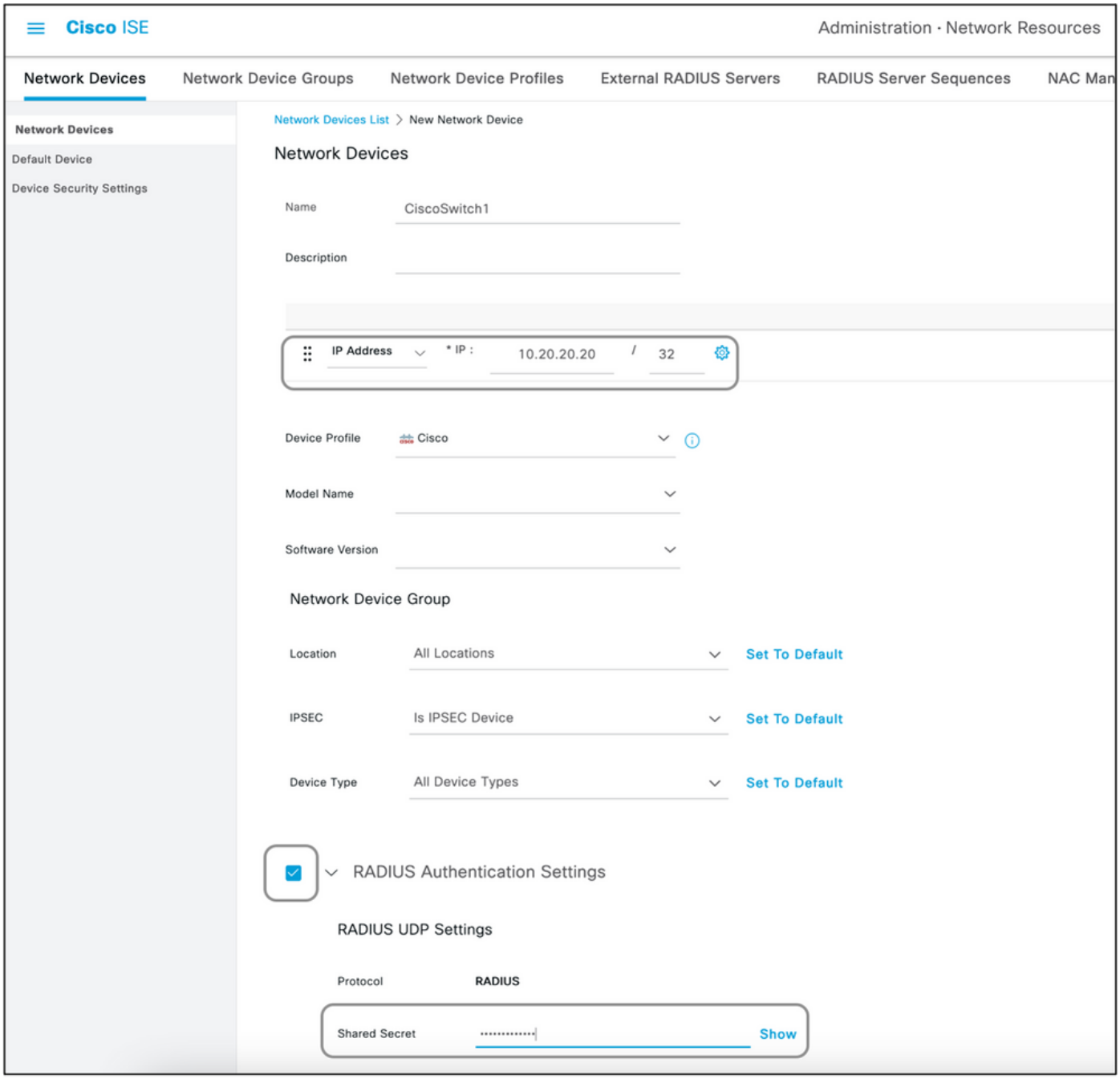
3. 드롭다운 목록에서 이전 섹션에서 정의한 디바이스 프로필을 선택할 수 있습니다. 프로파일이 생성되지 않은 경우 기본 Cisco를 그대로 사용할 수 있습니다.

4. Radius Authentication Settings(Radius 인증 설정)를 확인합니다.

5. 공유 **비밀 키를** 입력하고 **디바이스**를 저장합니다.







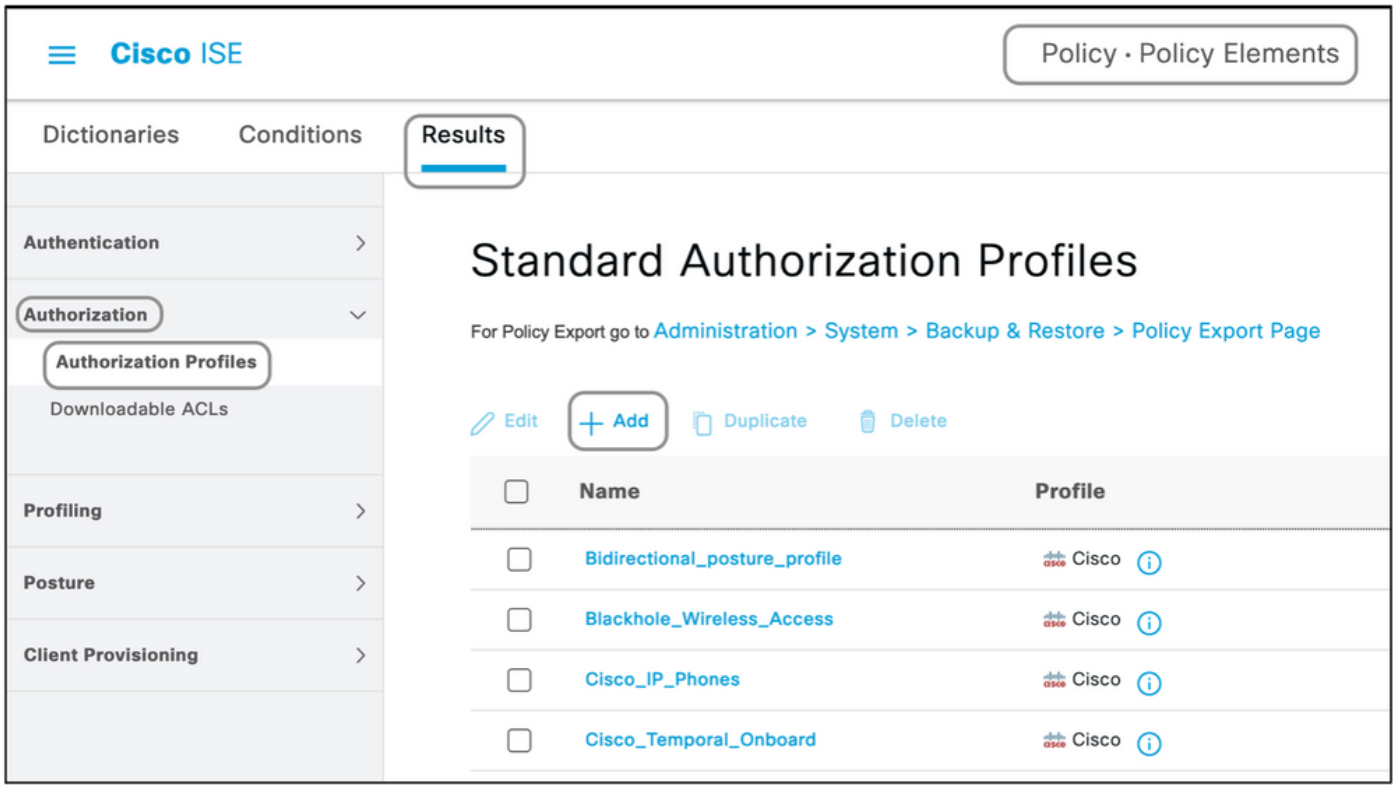
4단계. 권한 부여 프로파일 생성

ISE에서 Access-Accept 또는 Access-Reject로 푸시되는 최종 결과는 권한 부여 프로파일에서 정의됩니다. 각 권한 부여 프로파일은 네트워크 디바이스에 필요한 추가 특성을 푸시할 수 있습니다.

다음은 권한 부여 프로파일을 생성하는 절차입니다.

1. 탐색 **Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)**

2. Standard Authorization **Profiles(표준 권한 부여 프로파일)** 아래에서 Add(추가)**를 클릭합니다**.



추가할 수 있는 프로파일의 유형은 Access-Accept 및 Access-Reject입니다.

Access-Accept 프로필 만들기

이 프로파일은 네트워크 디바이스에 대한 일종의 액세스에 사용됩니다. 이 프로필에는 여러 특성이 함께 전달될 수 있습니다. 단계는 다음과 같습니다.

1. 적절한 이름을 지정하고 Access Type(액세스 유형)을 Access-Accept(액세스 수락)로 선택합니다.

2. 이전 섹션 중 하나에서 생성된 네트워크 디바이스 프로필을 선택합니다. 프로파일이 생성되지 않은 경우 기본 Cisco를 사용할 수 있습니다.

3. 선택한 프로필 유형이 서로 다르면 이 페이지에서 구성 옵션을 제한합니다.

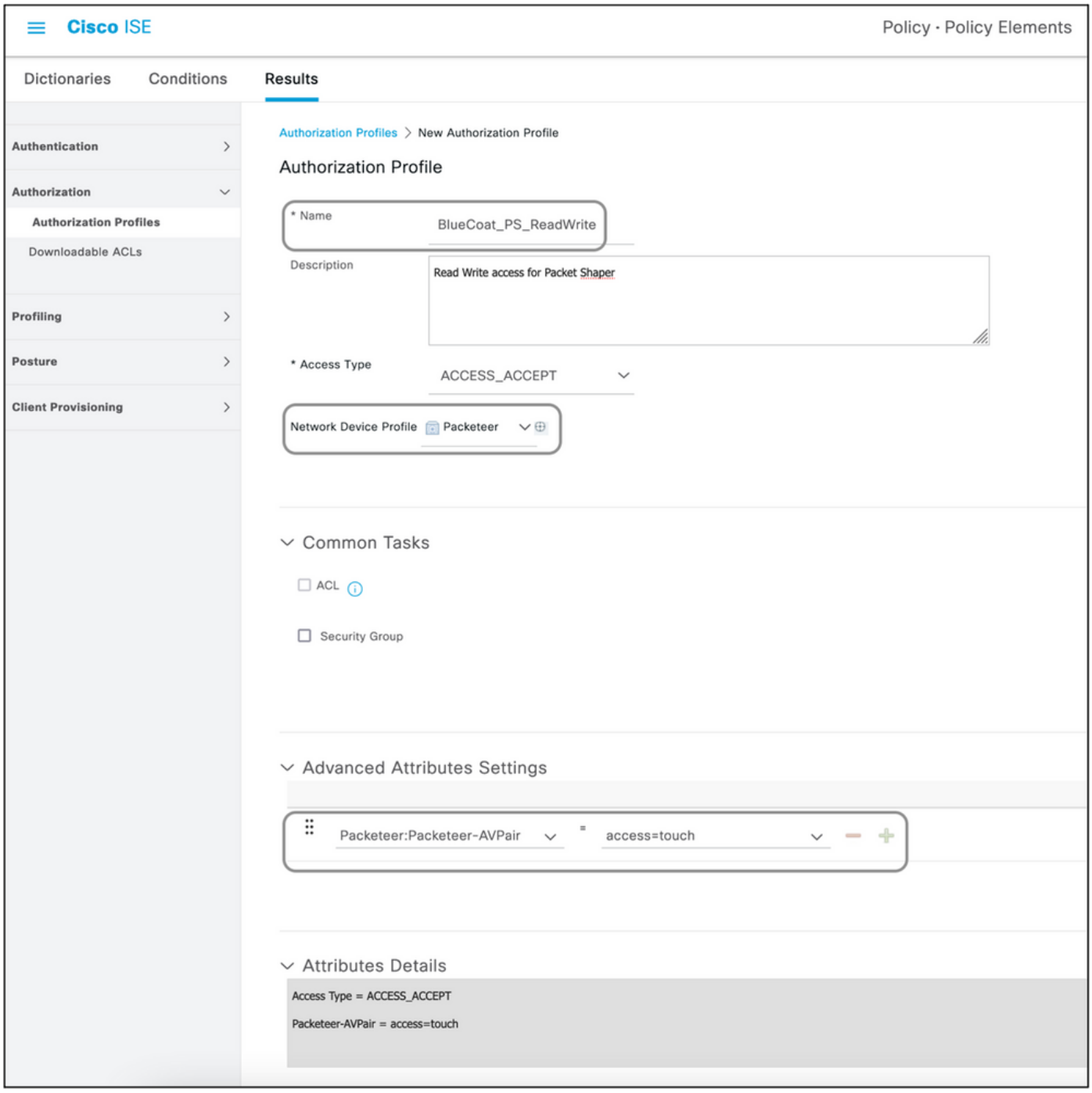
4. **Advanced Attributes Settings(고급 특성 설정)** 아래에서 사전 및 해당 특성(LHS)을 선택합니다.

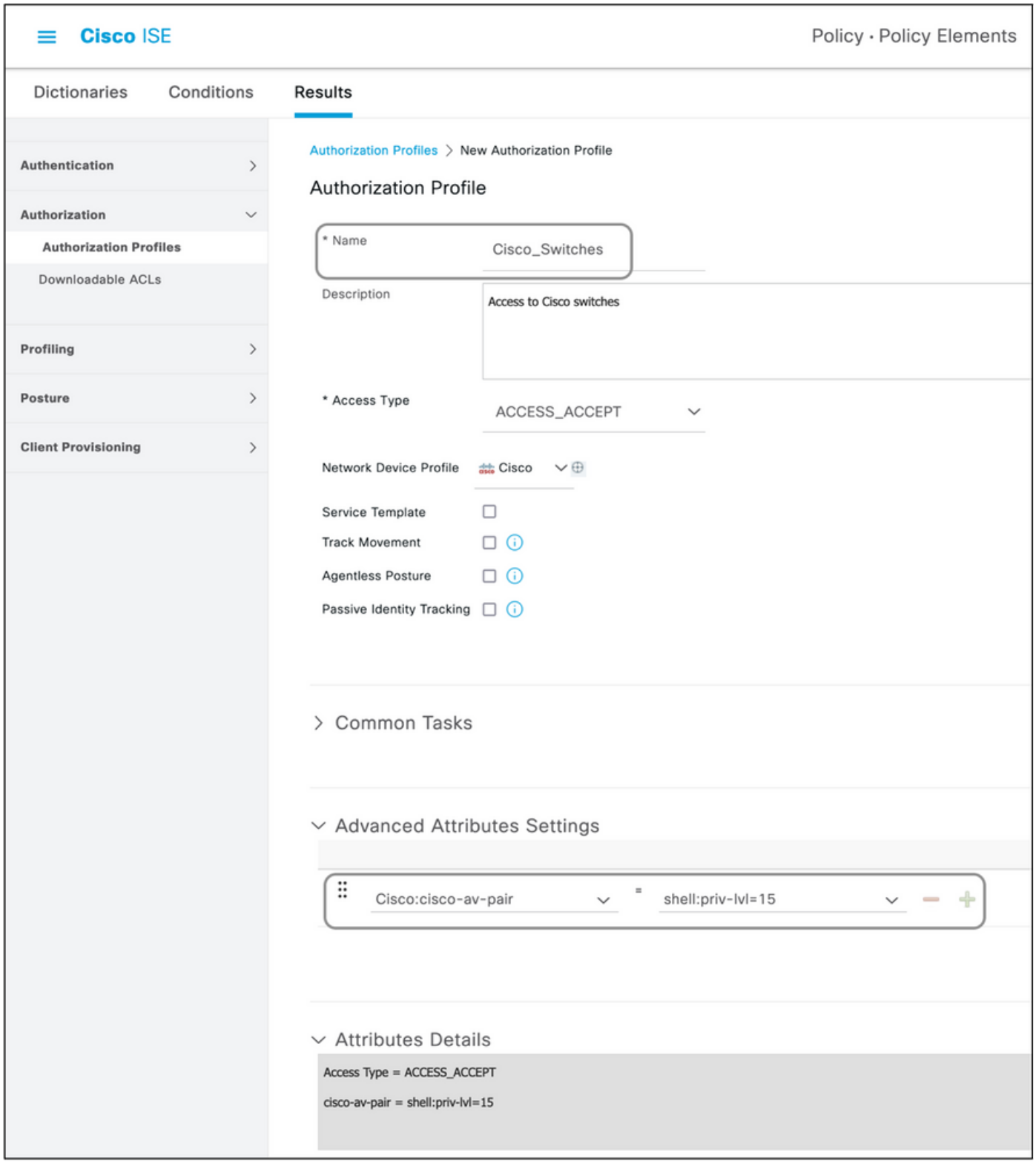
5. 사용 가능한 경우 드롭다운에서 특성에 값(RHS)을 할당하거나 예상 값을 입력합니다.

6. 동일한 결과의 일부로 전송할 속성이 더 있는 경우 + 아이콘을 클릭하고 4단계와 5단계를 반복합니다.

ISE에서 전송할 각 결과/역할/권한 부여에 대해 여러 권한 부여 프로파일을 생성합니다.

주: 통합된 속성은 속성 상세내역 필드에서 확인할 수 있습니다.


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Authorization Profiles > New Authorization Profile
Authorization Profile
* Name
BlueCoat_PS_ReadWrite
Description
Read Write access for Packet Shaper
* Access Type
ACCESS_ACCEPT
Network Device Profile
Packeteer
Common Tasks
ACL
Security Group
Advanced Attributes Settings
Packeteer:Packeteer-AVPair
=
access=touch
Attributes Details
Access Type = ACCESS_ACCEPT
Packeteer-AVPair = access=touch



액세스 거부 프로필 만들기

이 프로파일은 디바이스 관리에 대한 거부를 전송하는 데 사용되지만, 속성과 함께 전송하는 데에는 계속 사용할 수 있습니다. 이는 Radius Access-Reject 패킷을 전송하는 데 사용됩니다. 이 단계는 액세스 유형에 대해 Access-Accept 대신 Access-Reject를 선택해야 하는 1단계를 제외하고는 동일합니다.

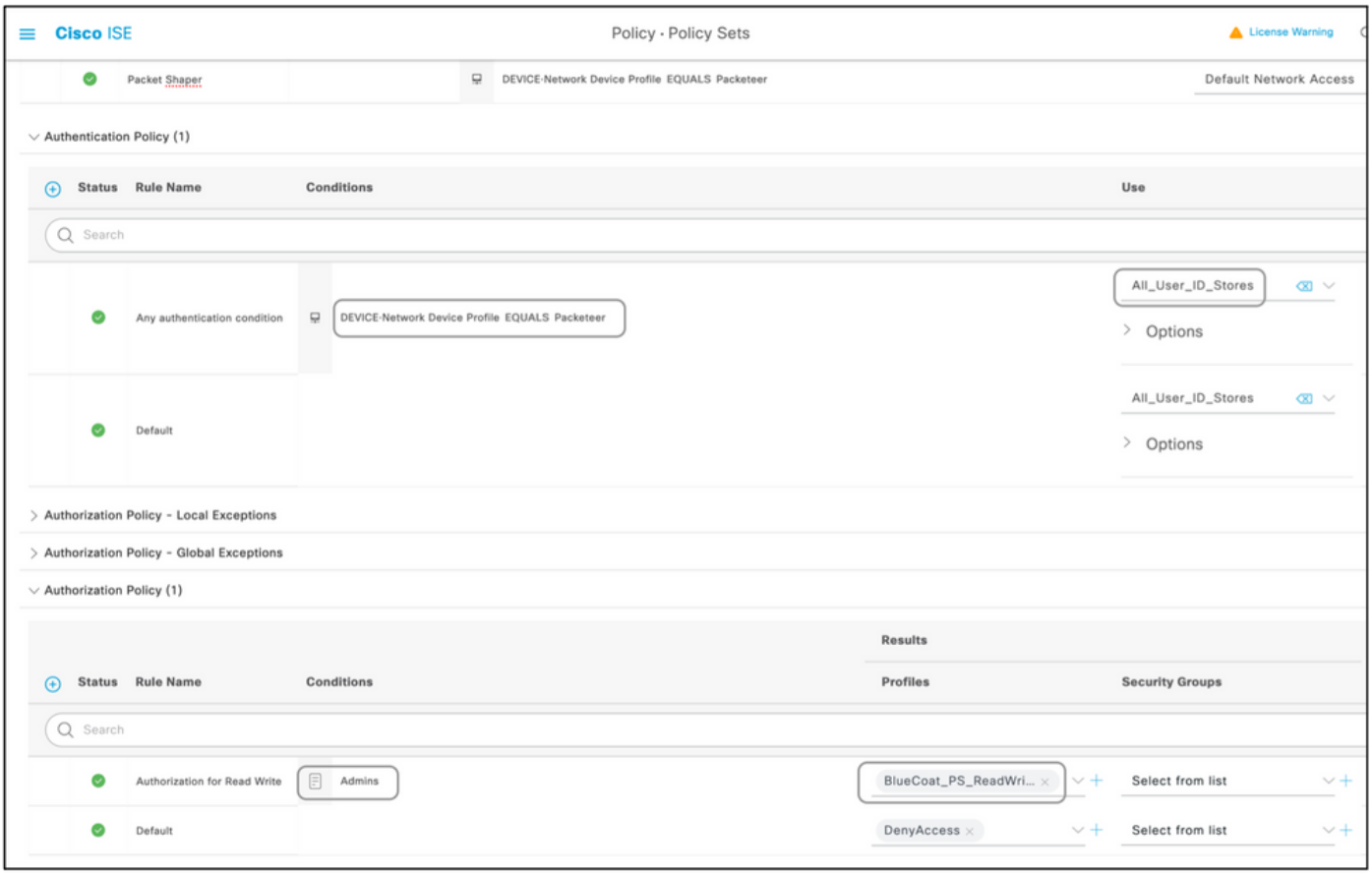
5단계. 정책 집합 생성

ISE의 정책 세트는 하향식으로 평가되며, 정책 세트에 설정된 조건을 충족하는 첫 번째 정책 세트는 네트워크 디바이스에서 보낸 Radius Access-Request 패킷에 대한 ISE의 응답을 담당합니다.

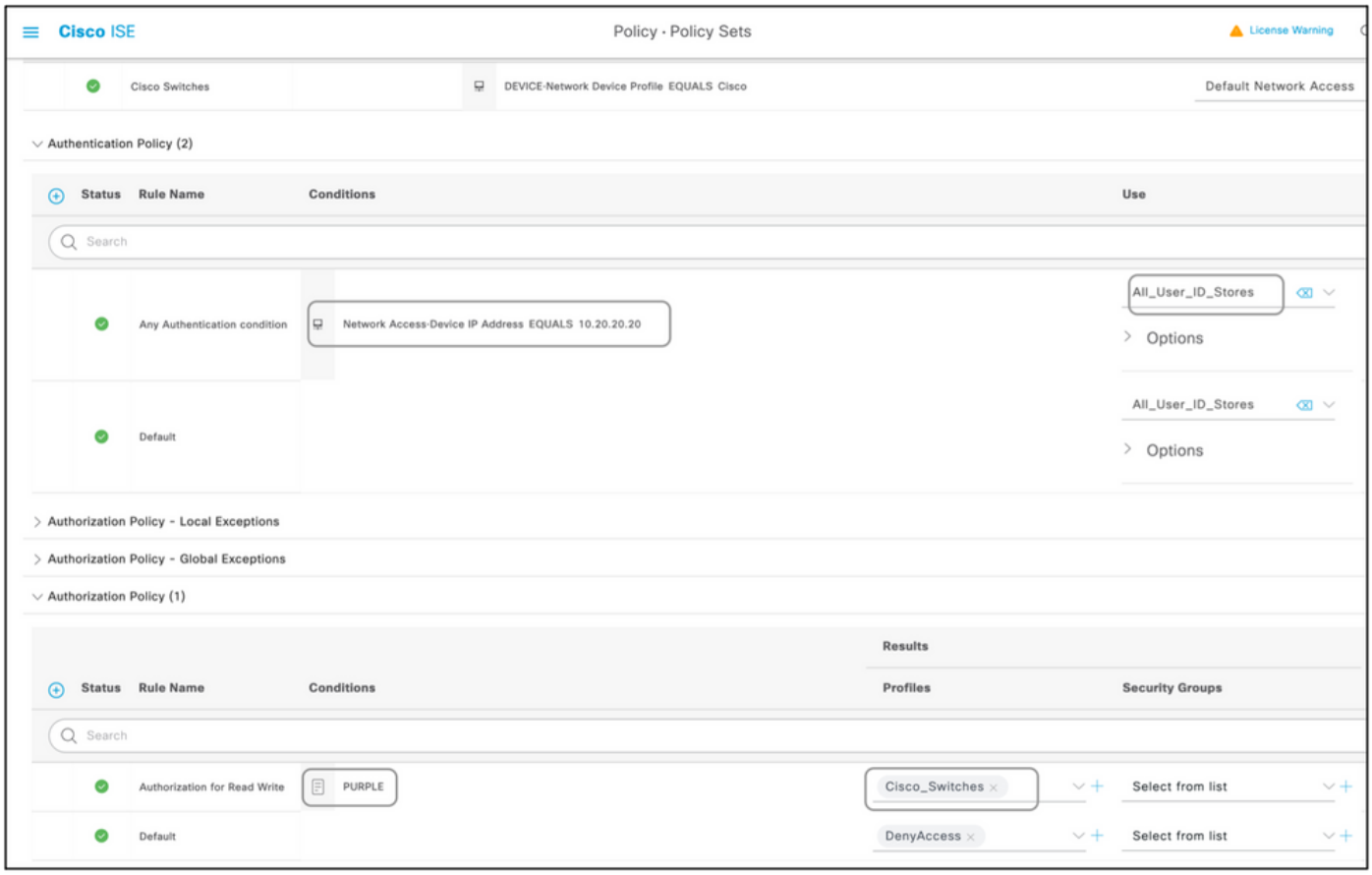
Cisco에서는 각 디바이스 유형에 대해 고유한 정책 세트를 권장합니다. 사용자의 인증 및 권한 부여를 평가 할 조건은 평가 시 발생 합니다. ISE에 외부 ID 소스가 있는 경우 권한 부여 유형에 사용할 수 있습니다.

일반적인 정책 집합은 다음과 같이 생성됩니다.

1. Policy(정책) **> Policy Sets(정책 집합) > +로 이동합니다**.
2. 이름 바꾸기 **새 정책 집합 1.**
3. 조건을 이 장치에 대해 고유하도록 설정합니다.
4. Policy Set(정책 **집합)를 확장합니다**.
5. Authentication **Policy(인증 정책**)를 확장하여 인증 규칙을 설정합니다. 외부 소스 또는 내부 사용자는 ISE가 사용자를 확인하는 ID 소스 시퀀스로 사용할 수 있는 예입니다.
6. 인증 정책이 모두 설정되었습니다. 이 시점에서 정책을 저장할 수 있습니다.
7. Authorization **Policy(권한 부여 정책**)를 확장하여 사용자에 대한 권한 부여 조건을 추가합니다. 예를 들어 특정 AD 그룹 또는 ISE 내부 ID 그룹을 확인하는 것입니다. 규칙의 이름도 이와 같이 지정합니다.
8. 권한 부여 규칙에 대한 결과는 드롭다운에서 선택할 수 있습니다.
9. 벤더가 지원하는 다양한 액세스 유형에 대한 여러 권한 부여 규칙을 생성합니다.


Cisco ISE
Policy · Policy Sets
License Warning
Packet Shaper
DEVICE-Network Device Profile EQUALS Packeteer
Default Network Access
Authentication Policy (1)
Status
Rule Name
Conditions
Use
Search
Any authentication condition
DEVICE-Network Device Profile EQUALS Packeteer
All_User_ID_Stores
Options
Default
All_User_ID_Stores
Options
Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy (1)
Results
Status
Rule Name
Conditions
Profiles
Security Groups
Search
Authorization for Read Write
Admins
BlueCoat_PS_ReadWri...
Select from list
Default
DenyAccess
Select from list


Cisco ISE
Policy - Policy Sets
License Warning
Policy Sets
Reset
Reset Policyset Hitcounts
Save
Status
Policy Set Name
Description
Conditions
Allowed Protocols / Server Sequence
Hits
Actions
View
Search
Cisco Switches
DEVICE-Network Device Profile EQUALS Cisco
Default Network Access
0



장치 목록

Radius를 통한 장치 관리를 지원하는 모든 장치는 이전 섹션에서 언급한 모든 단계를 몇 가지 수정하여 ISE에 추가할 수 있습니다. 따라서 이 문서에는 이 섹션에 제공된 정보와 함께 작동하는 디바이스 목록이 있습니다. 이 문서에 제공된 특성 및 값 목록은 완전하지도 권위적이지도 않으며 이 문서에 대한 업데이트 없이 언제든지 변경할 수 있습니다. 검증을 위해 공급업체 웹 사이트 및 공급업체 지원 서비스에 문의하십시오.

ASR(Aggregation Services Router)

ISE에 이미 있는 Cisco AV 쌍을 사용하므로 이를 위해 별도의 사전 및 VSA를 생성할 필요가 없습니다.

특성: **cisco av 쌍**

값: **shell:tasks="#<role-name>,<permission>:<process>"**

사용법:<role-name>의 값을 라우터에 로컬로 정의된 역할의 이름으로 설정합니다. 역할 계층 구조를 트리 형식으로 설명할 수 있습니다. 여기서 role#roots는 트리의 맨 위에 있으며 role#leafts는 추가 명령을 추가합니다. 다음의 경우 이 두 역할을 결합하여 다시 전달할 수 있습니다 **.shell:tasks="#root,#leaf"**.

개별 프로세스 단위로 권한을 다시 전달하여 사용자에게 특정 프로세스에 대한 읽기, 쓰기 및 실행 권한을 부여할 수도 있습니다. 예를 들어 BGP 프로세스에 대한 사용자 읽기 및 쓰기 권한을 부여하려면 값을:**shell:tasks="#root,rw:bgp"로 설정합니다**. 특성의 순서는 중요하지 않습니다. 값이 **toshell:tasks="#root,rw:bgp"**로 설정되는지 **아니면 toshell:tasks="rw:bgp,#root"로 설정되는지** 상관없이 결과는 동일합니다.

예: 권한 부여 프로파일에 특성을 추가합니다.

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-Cisco	cisco av 쌍	문자열	shell:tasks="#root,#leaf,rwx:bgp,r:ospf"

Cisco 스위치 IOS® 및 Cisco IOS® XE

ISE에 이미 있는 RADIUS 특성을 사용하므로 이를 위해 별도의 사전 및 VSA를 생성할 필요가 없습니다.

특성:**cisco av-pair**

값:**shell:priv-lvl=<level>**

사용법:<level>의 값을 기본적으로 보낼 권한 수인 숫자로 설정합니다. 일반적으로 15를 보내면 읽기-쓰기를, 7을 보내면 읽기 전용을 의미합니다.

예: 권한 부여 프로파일에 특성을 추가합니다.

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-Cisco	cisco av 쌍	문자열	셸:priv-lvl=15

BlueCoat 패킷 셰이퍼

속성:**Packet-AVPair**

값:**access=<level>**

Usage:<level>은 부여할 액세스 레벨입니다. 터치 액세스는 읽기-쓰기와 같지만 외관 액세스는 읽기 전용입니다.

이 문서에 표시된 대로 다음 값으로 사전을 만듭니다.

- Name(이름): Packeter
- 공급업체 ID: 2334
- 공급업체 길이 필드 크기: 1
- 공급업체 유형 필드 크기: 1

속성의 세부 정보를 입력 합니다.

- 속성:Packet-AVPair
- 설명: 액세스 수준을 지정하는 데 사용됩니다.
- 공급업체 특성 ID: 1
- 방향: OUT
- 다중 허용: False
- Allow Tagging(태그 지정 허용): 선택 취소됨
- 특성 유형: 문자열

예: 인증 프로파일에 특성을 추가합니다(읽기 전용 액세스용).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS 패킷	패킷-AVPair	문자열	액세스=표시

예: Authorization Profile(인증 프로파일)에 특성을 추가합니다(읽기/쓰기 액세스용).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS 패킷	패킷-AVPair	문자열	액세스=터치

BlueCoat 프록시 서버(AV/SG)

속성: **Blue-Coat-Authorization**

값: **<level>**

Usage:<level>은 부여할 액세스 레벨입니다. 0은 액세스 없음을, 1은 읽기 전용 액세스를, 2는 읽기-쓰기 액세스를 의미합니다. Blue-Coat-Authorization 특성은 액세스 수준을 담당하는 특성입니다.

이 문서에 표시된 대로 다음 값으로 사전을 만듭니다.

- 이름: BlueCoat
- 공급업체 ID: 14501
- 공급업체 길이 필드 크기: 1
- 공급업체 유형 필드 크기: 1

속성의 세부 정보를 입력 합니다.

- 속성: Blue-Coat-Group
- 공급업체 특성 ID: 1
- 방향: 둘 다
- 다중 허용: False
- Allow Tagging(태그 지정 허용): 선택 취소됨
- 특성 유형: Unsigned Integer 32(UINT32)

두 번째 속성의 세부 정보를 입력합니다.

- 특성: Blue-Coat-Authorization
- 설명: 액세스 수준을 지정하는 데 사용됩니다.
- 공급업체 특성 ID: 2
- 방향: 둘 다
- 다중 허용: False
- Allow Tagging(태그 지정 허용): 선택 취소됨
- 특성 유형: Unsigned Integer 32(UINT32)

예: Authorization Profile(권한 부여 프로파일)에 특성을 추가합니다(액세스 권한 없음).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-BlueCoat	블루 코트 그룹	UINT32	0

예: 인증 프로파일에 특성을 추가합니다(읽기 전용 액세스용).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-BlueCoat	블루 코트 그룹	UINT32	1

예: Authorization Profile(인증 프로파일)에 특성을 추가합니다(읽기/쓰기 액세스용).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-BlueCoat	블루 코트 그룹	UINT32	2

Brocade 스위치

ISE에 이미 있는 RADIUS 특성을 사용하므로 이를 위해 별도의 사전 및 VSA를 생성할 필요가 없습니다.

특성: **Tunnel-Private-Group-ID**

값:**U:<VLAN1>; T:<VLAN2>**

사용법:<VLAN1>을 데이터 VLAN 값으로 설정합니다. 음성 VLAN의 값으로 <VLAN2>를 설정합니다. 이 예에서 데이터 VLAN은 VLAN 10이고 음성 VLAN은 VLAN 21입니다.

예: 권한 부여 프로파일에 특성을 추가합니다.

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-IETF	터널 전용 그룹 ID	태그가 지정된 문자열	U:10;T:21

인포블록스

특성:**Infoblox-Group-Info**

값:**<group-name>**

Usage:<group-name>은 사용자에게 부여된 권한이 있는 그룹의 이름입니다. 이 그룹은 Infoblox 디바이스에서 구성해야 합니다. 이 컨피그레이션 예에서는 그룹 이름이 MyGroup입니다.

이 문서에 표시된 대로 다음 값으로 사전을 만듭니다.

- 이름: Infoblox
- 공급업체 ID: 7779
- 공급업체 길이 필드 크기: 1
- 공급업체 유형 필드 크기: 1

속성의 세부 정보를 입력 합니다.

- 특성: Infoblox-Group-Info
- 공급업체 특성 ID: 009
- 방향: OUT
- 다중 허용: False
- Allow Tagging(태그 지정 허용): 선택 취소됨
- 특성 유형: 문자열

예: 권한 부여 프로파일에 특성을 추가합니다.

사전 유형	RADIUS 특성	특성 유형	속성 값

RADIUS-Infoblox	Infoblox-Group-Info	문자열	내 그룹

Cisco Firepower Management Center

ISE에 이미 있는 RADIUS 특성을 사용하므로 이를 위해 별도의 사전 및 VSA를 생성할 필요가 없습니다.

특성:**cisco av-pair**

값: **Class-[25]=<역할>**

사용법:<role>의 값을 FMC에 로컬로 정의된 역할의 이름으로 설정합니다. FMC에서 admin 및 읽기 전용 사용자와 같은 여러 역할을 생성하고 FMC에서 수신할 ISE의 특성에 값을 할당합니다.

예: 권한 부여 프로파일에 특성을 추가합니다.

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-Cisco	cisco av 쌍	문자열	Class-[25]=NetAdmins

Nexus 스위치

ISE에 이미 있는 RADIUS 특성을 사용하므로 이를 위해 별도의 사전 및 VSA를 생성할 필요가 없습니다.

특성:**cisco av-pair**

값:**shell:roles="<role1> <role2>"**

사용법:<role1> 및<role2>의 값을 스위치에 로컬로 정의된 역할 이름으로 설정합니다. 여러 역할이 만들어지면 공백 문자로 구분합니다. 여러 역할이 AAA 서버에서 Nexus 스위치로 다시 전달될 경우 사용자는 세 역할 모두의 통합에 의해 정의된 명령에 액세스할 수 있습니다.

기본 제공 역할은 Configure User Accounts and RBAC에서 정의됩니다.

예: 권한 부여 프로파일에 특성을 추가합니다.

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-Cisco	cisco av 쌍	문자열	셸: roles= " 네트워크 관리자 vdc 관리 vdc 운영자 "

무선 LAN 컨트롤러(WLC)

ISE에 이미 있는 RADIUS 특성을 사용하므로 이를 위해 별도의 사전 및 VSA를 생성할 필요가 없습니다.

특성:**Service-Type**

값:**관리 (6) / NAS 프롬프트 (7)**

사용법: 사용자에게 WLC(Wireless LAN Controller)에 대한 읽기/쓰기 액세스 권한을 부여하려면 값

이 Administrative여야 하고, 읽기 전용 액세스의 경우 값이 NAS-Prompt여야 합니다.

자세한 내용은 WLC(Wireless LAN Controller)의 관리 사용자 RADIUS 서버 인증 컨피그레이션 예를 참조하십시오

예: 인증 프로파일에 특성을 추가합니다(읽기 전용 액세스용).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-IETF	서비스 유형	열거	NAS 프롬프트

예: Authorization Profile(인증 프로파일)에 특성을 추가합니다(읽기/쓰기 액세스용).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-IETF	서비스 유형	열거	관리

DCNM(Data Center Network Manager)

인증 방법을 변경한 후 DCNM을 다시 시작해야 합니다. 그렇지 않으면 network-admin 대신 network-operator 권한을 할당할 수 있습니다.

ISE에 이미 있는 RADIUS 특성을 사용하므로 이를 위해 별도의 사전 및 VSA를 생성할 필요가 없습니다.

특성:**cisco av-pair**

값:**셸:roles=<role>**

DCNM 역할	RADIUS Cisco AV 쌍
사용자	셸:역할 = "network-operator"
관리자	셸:역할 = "network-admin"

오디오코드

특성: **ACL-Auth-Level**

값: **ACL-Auth-Level = "<integer>"**

Usage:<integer>는 부여할 액세스 레벨입니다. 사용자의 경우 ACL-Auth-UserLevel 이름이 50인 ACL-Auth-Level 특성의 값, 관리자의 경우 ACL-Auth-AdminLevel 이름이 100인 ACL-Auth-Level 특성의 값, 보안 관리자의 경우 ACL-Auth-SecurityAdminLevel 이름이 200인 ACL-Auth-Level 값의 값 이름을 건너뛰고 특성의 값을 권한 부여 프로파일 고급 AV 쌍의 값으로 직접 지정할 수 있습니다.

이 문서에 표시된 대로 다음 값으로 사전을 만듭니다.

- 이름: AudioCodes
- 공급업체 ID: 5003
- 공급업체 길이 필드 크기: 1
- 공급업체 유형 필드 크기: 1

속성의 세부 정보를 입력 합니다.

- 특성: ACL-Auth-Level
- 설명: 액세스 수준을 지정하는 데 사용됩니다.
- 공급업체 특성 ID: 35
- 방향: OUT
- 다중 허용: False
- Allow Tagging(태그 지정 허용): 선택 취소됨
- 특성 유형: 정수

예: 권한 부여 프로파일에 특성을 추가합니다(사용자용).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-오디오코드	ACL 인증 레벨	정수	50

예: 권한 부여 프로파일에 특성을 추가합니다(관리자용).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-오디오코드	ACL 인증 레벨	정수	100

예: 인증 프로파일에 특성을 추가합니다(보안 관리자용).

사전 유형	RADIUS 특성	특성 유형	속성 값
RADIUS-오디오코드	ACL 인증 레벨	정수	200

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.