



# Cisco ISE 프로파일링 설계 가이드

*보안 액세스 방법 가이드 시리즈*

저자: **Craig Hys**

날짜: **2012년 8월**

# 목차

- 솔루션 개요 ..... 5
- 정책 아키텍처 및 구성 요소 ..... 5
- 시나리오 개요 ..... 6
- 프로파일링 서비스 요구 사항 ..... 10**
  - 라이센싱 ..... 10
  - 어플라이언스 요구 사항 ..... 10
  - 네트워크 요구 사항 ..... 11
- 프로파일링 서비스 전역 컨피그레이션 ..... 12**
  - ISE 프로파일링 전역 컨피그레이션 ..... 12
  - 전역 프로파일링 설정 구성 ..... 12
  - ISE 프로파일링 서비스 활성화 ..... 12
- 프로브 구성 ..... 15**
  - 프로브 개요 ..... 15
  - 프로브 컨피그레이션 ..... 16
  - RADIUS 프로브 구성 ..... 17
  - SNMP 트랩 프로브 구성 ..... 22
    - 시스템 쿼리 ..... 28
    - 인터페이스 쿼리 ..... 29
  - SNMP 쿼리 프로브 구성 ..... 30
    - DHCP SPAN 프로브 ..... 37
    - DHCP 특성 ..... 37
  - DHCP 및 DHCP SPAN 프로브 구성 ..... 38
    - URL 리디렉션을 사용한 HTTP 프로브 ..... 47
    - SPAN 을 사용한 HTTP 프로브 ..... 48
    - HTTP 프로브 및 IP-MAC 주소 바인딩 요구 사항 ..... 48
    - 클라이언트 프로비저닝을 사용한 URL 리디렉션 ..... 48
    - Central WebAuth 를 사용한 URL 리디렉션 ..... 49
  - HTTP 프로브 구성 ..... 49

DNS 프로브 구성.....	62
NetFlow 특성 .....	67
NetFlow 프로브 및 IP-MAC 주소 바인딩 요구 사항 .....	68
NetFlow 프로브 구성 .....	68
NMAP 프로브 검사 작업 .....	78
NMAP 프로브 네트워크 검사.....	80
NMAP 프로브 엔드포인트 검사 .....	80
NMAP 프로브 및 IP-MAC 주소 바인딩 요구 사항 .....	81
NMAP 프로브 구성 .....	81
<b>Device Sensor .....</b>	<b>90</b>
Device Sensor 개요 .....	90
Device Sensor 세부사항 .....	90
ISE 프로파일링에 맞게 Device Sensor 구성.....	93
<b>프로파일링 정책 구성 .....</b>	<b>106</b>
프로파일링 정책 컨피그레이션 개요.....	106
프로파일링 조건 .....	106
프로파일링 조건 구성.....	108
프로파일링 정책 및 규칙 .....	110
확실성 요인(CF).....	111
예외 및 NMAP 작업.....	114
엔드 포인트 ID 그룹.....	116
프로파일링 및 권한 부여 정책.....	120
프로파일 전환 및 COA(Change of Authorization) .....	122
예외 작업.....	123
권한 부여 정책이 변경되는 경우 프로파일 전환에 따른 자동 CoA.....	124
<b>프로파일링 설계 및 모범 사례.....</b>	<b>129</b>
프로파일링 설계 고려 사항 .....	129
프로브 선택 모범 사례.....	132
검색 단계 - 프로브 모범 사례 .....	137
유선 네트워크 - 프로브 모범 사례.....	139
무선 네트워크 - 프로브 모범 사례.....	141
프로파일링 계획 .....	143

---

부록 A: 참조 .....	146
Cisco TrustSec System: .....	146
디바이스 컨피그레이션 가이드: .....	146

## 솔루션 개요

Cisco ISE 프로파일링 서비스는 네트워크에 연결된 엔드포인트의 동적 탐지 및 분류를 제공합니다. ISE는 MAC 주소를 고유 식별자로 사용하여 각 네트워크 엔드포인트에서 내부 엔드포인트 데이터베이스를 작성하기 위한 다양한 특성을 수집합니다. 분류 프로세스는 수집된 특성을 사전 구성된 조건 또는 사용자 정의 조건과 일치시키며, 그러한 조건은 광범위한 프로파일 라이브러리와 상호 연결됩니다. 이러한 프로파일에는 모바일 클라이언트(iPad, Android 태블릿, BlackBerry 휴대폰 등), 데스크톱 운영 체제(예: Windows 7, Mac OS X, Linux 및 기타)와 수많은 비사용자 시스템(예: 프린터, 전화기, 카메라 및 게임 콘솔)을 비롯한 광범위한 디바이스 유형이 포함됩니다.

일단 분류된 엔드포인트의 경우 네트워크에 대한 권한이 부여되고 해당 프로파일을 기초로 액세스 권한이 부여됩니다. 예를 들어 IP 전화기 프로파일과 일치하는 엔드포인트는 인증 방법으로 MAB(MAC Authentication Bypass)를 사용하여 음성 VLAN에 배치될 수 있습니다. 또 다른 예는 사용되는 디바이스에 따라 사용자에 대해 차별화된 네트워크 액세스를 제공하는 것입니다. 예를 들어 직원이 회사 워크스테이션에서 네트워크에 액세스할 때는 전체 액세스 권한을 가질 수 있지만, 개인 iPhone에서 네트워크에 액세스할 때는 제한된 네트워크 액세스 권한이 부여될 수 있습니다.

## 정책 아키텍처 및 구성 요소

그림 3에서는 Cisco ISE 프로파일링 서비스에 대한 일반적인 정책 아키텍처 및 주요 구성 요소에 대해 중점적으로 설명합니다. 컨피그레이션 프로세스에서는 먼저 정책 서비스 페르소나를 실행하는 ISE 어플라이언스에서 특정 프로브를 활성화합니다. 서로 다른 종류의 엔드포인트 특성을 수집하는 여러 프로브가 있습니다. 이러한 특성은 조건과 일치하는지 비교되고 그 조건은 다시 디바이스 유형 또는 프로파일 라이브러리의 규칙과 일치하는지 비교될 수 있습니다. 일반 가중치 척도에 따라 각 일치 조건마다 서로 다른 가중치 또는 확실성 요인(CF)이 할당될 수 있습니다. 가중치나 CF는 조건이 특정 프로파일에 대한 디바이스 분류에 영향을 미치는 상대 값을 나타냅니다. 조건이 여러 프로파일에서 일치하더라도 엔드포인트의 누적 CF가 가장 높은 프로파일이 엔드포인트에 할당됩니다.

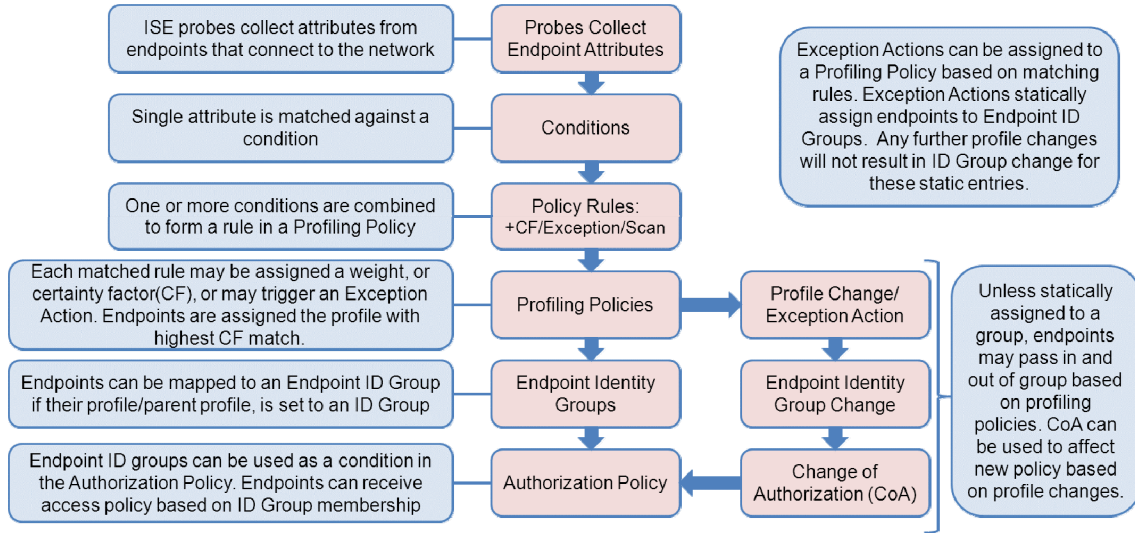


그림 1. ISE 프로파일링 정책 아키텍처 및 구성 요소

ISE 권한 부여 정책에 프로파일을 노출하려면 관리자는 일치하는 ID 그룹을 생성하기 위한 간단한 확인란을 통해 프로파일을 구성해야 합니다. 이 간단한 프로세스에서는 권한 부여 정책의 특정 조건으로 프로파일을 엔드포인트 ID 그룹 형태로 선택할 수 있습니다.

새 특성이 학습되거나 이전에 학습된 특성이 덮어쓰여지면 프로파일이 변경될 수 있습니다. 이러한 변경 사항은 프로파일링 정책이 변경되어도 발생할 수 있습니다. 경우에 따라 일반 HP 디바이스에서 HP-Color-LaserJet-4500과 같은 보다 구체적인 프로파일로 자동 전환될 수 있습니다. 한편, 관리자는 예외 작업 형태로 기본 정책을 우회하기 위한 작업을 수행해야 할 수 있습니다. 예외 작업을 통해 특성 수집 또는 상관 관계가 더 이상 할당된 프로파일 및 선택적 ID 그룹에 영향을 미치지 않도록 엔드포인트의 정적 할당을 특정 프로파일링 정책에 적용할 수 있습니다.

위의 각 경우마다(프로파일 전환 및 예외 작업) ISE에서 새로 할당된 프로파일을 기초로 엔드포인트에 새 액세스 정책을 적용하도록 허용하는 것이 좋습니다. RADIUS CoA(Change of Authorization)는 ISE에서 이러한 작업을 수행하기 위한 기능입니다. 엔드포인트가 연결된 디바이스에 액세스하기 위한 CoA 요청을 보내면 ISE에서 인증 및 권한 부여 정책을 기준으로 호스트를 다시 평가하도록 요구할 수 있습니다.

## 시나리오 개요

### 네트워크 토폴로지

그림 4에서는 이 가이드에 사용된 네트워크 토폴로지를 개괄적으로 보여줍니다. 그림 1에 나와 있는 모든 시나리오는 전체 TrustSec 아키텍처의 일부에 해당하며, 이 문서에서는 프로파일링에 대한 유선 및 무선 사용자 시나리오를 중점적으로 살펴봅니다. 프로파일링 데이터를 고유한 엔드포인트와 상호 연결하는 데 필요한 VPN 게이트웨이의 MAC 주소 정보가 없으므로 ISE 프로파일링 서비스는 현재 원격 액세스 VPN 활용 사례에 지원되지 않습니다.

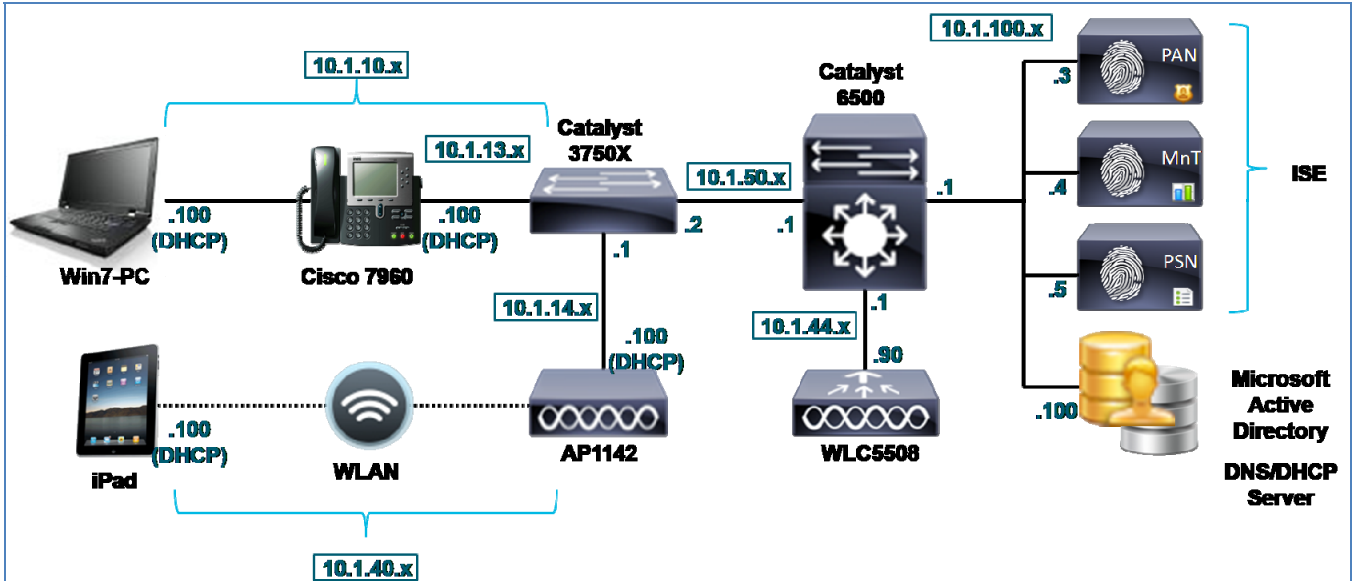


그림 2. ISE 프로파일링 토폴로지

구성 요소

표 1에는 이 가이드 작성 당시에 사용된 하드웨어 및 소프트웨어 구성 요소가 나와 있습니다.

표 1. Cisco TrustSec 2.0 시스템에서 테스트된 구성 요소

구성 요소	하드웨어	테스트한 기능	소프트웨어 릴리스
Cisco ISE (Identity Services Engine)	VMware ESXi4.1을 실행하는 Cisco UCS C200 M2 서버	통합 AAA, 정책 서버 및 프로파일링 서비스	Cisco ISE Software 버전 1.1.1 (기본 및 고급 기능 라이선스)
Cisco Catalyst 3000 Series 스위치	Cisco Catalyst 3560 Series	MAB(MAC Authentication Bypass), LWA(Local WebAuth), CWA(Central WebAuth), 802.1X 인증 및 CoA(Change of Authorization)를 포함한 Basic Identity 기능.  SNMP(Simple Network Management Protocol), RADIUS, Dynamic Host Configuration Protocol DHCP 릴레이 및 URL 리디렉션을 포함한 프로파일링 지원 서비스.	Cisco IOS® Software Release 12.2(55)SE3 (IP 베이스)

구성 요소	하드웨어	테스트한 기능	소프트웨어 릴리스
	Cisco Catalyst 3750-X Series	MAB, LWA, CWA, 802.1X 인증 및 CoA를 포함한 Basic Identity 기능.  SNMP, RADIUS, DHCP 릴레이, URL 리디렉션 및 Device Sensor를 포함한 프로파일링 지원 서비스.	Cisco IOS Software Release 15.0(1)SE2 (IP 베이스)
Cisco Catalyst 6000 Series 스위치	Cisco Catalyst 6500 Series Supervisor Engine 720 Policy Feature Card 3A(PFC3A)	Cisco NetFlow 버전 5 및 버전 9 내보내기, DHCP 릴레이 및 SPAN(Switched Port Analyzer)/RSPAN(Remote Switched Port Analyzer)을 포함한 프로파일링 지원 서비스.	Cisco IOS Software Release 12.2(33)SXJ2(고급 IP 서비스)
Cisco WLC(Wireless LAN Controller)	Cisco 5508 Wireless LAN Controller	MAB, LWA, CWA, 802.1X 인증 및 CoA를 포함한 Basic Identity 기능.  SNMP, RADIUS, DHCP 릴레이 및 URL 리디렉션을 포함한 프로파일링 지원 서비스.	Cisco Unified Wireless Network Software Release 7.2.103.0
Cisco Wireless Access Point	Cisco Aironet® Lightweight Access Point 1142N	프로파일 특성에 따라 MAB 및 권한 부여 정책을 사용하여 인증된 엔드포인트	Cisco Lightweight Access Point Software Release 12.4(25e)JA
Cisco IP Phone	Cisco Unified IP Phone 7960	프로파일 특성에 따라 MAB 및 권한 부여 정책을 사용하여 인증된 엔드포인트	Cisco IP Phone 7940 및 7960 펌웨어 릴리스 8.1(1.0)
워크스테이션	VMware 게스트	프로파일 특성에 따라 MAB, LWA, CWA와 802.1X 및 권한 부여 정책을 사용하여 인증된 엔드포인트.	Windows 7



구성 요소	하드웨어	테스트한 기능	소프트웨어 릴리스
태블릿	Apple iPad(G1)	프로파일 특성에 따라 MAB, LWA, CWA와 802.1X 및 권한 부여 정책을 사용하여 인증된 엔드포인트.	iOS 5.0.1
스마트폰	Motorola DROIDX	프로파일 특성에 따라 MAB, LWA, CWA와 802.1X 및 권한 부여 정책을 사용하여 인증된 엔드포인트.	Android 2.3.4

참고: Cisco ISE 프로파일링 서비스는 이 가이드에서 확인된 주요 기능입니다. 기타 Cisco TrustSec 기능은 주로 프로파일링 서비스의 컨피그레이션 및 테스트를 지원하기 위해 구축되었습니다.

표에 나타난 디바이스와 버전은 특히 가이드 테스트 및 문서화 프로세스 중에 사용된 것으로, TrustSec 및 ISE 프로파일링 서비스를 지원하는 모든 디바이스를 반영하지는 않습니다. TrustSec 지원 디바이스 및 권장 버전이 나와 있는 포괄적인 목록을 보려면 <http://www.cisco.com/go/trustsec>으로 이동하십시오.

# 프로파일링 서비스 요구 사항

## 라이선싱

ISE 프로파일링을 사용하려면 다음 라이선스 중 하나를 PAN(정책 관리 노드)에 설치해야 합니다.

고급 엔드포인트 라이선스(유선 또는 무선 배포용)

무선 전용 라이선스(무선 전용 배포용)

네트워크에 능동적으로 인증되는 각 엔드포인트에 대해 권한 부여 정책을 결정하는 데 프로파일링 데이터가 사용되는 경우 하나의 고급 엔드포인트 라이선스가 필요합니다. 고급 엔드포인트 라이선스가 필요할 수 있는 포스터 평가와 같은 다른 서비스를 고려하지 않는다면, 프로파일에 정적으로 할당된 엔드포인트에서 고급 라이선스가 사용되지 않습니다. 여러 엔드포인트를 프로파일링하여 연결된 디바이스 및 해당 분류에 대한 가시성을 확보할 수 있으며, 엔드포인트를 인증하는 데 프로파일 정보가 사용되지 않을 경우 각 엔드포인트에 대해 고급 엔드포인트 라이선스가 필요하지 않습니다. 최소 고급 엔드포인트 또는 무선 전용 라이선스 개수는 100입니다.

## 어플라이언스 요구 사항

ISE 프로파일링 서비스는 정책 서비스 페르소나용으로 구성된 ISE 어플라이언스에서만 실행될 수 있습니다. 표 2에는 정책 서비스 전용 어플라이언스에서 프로파일링될 수 있는 활성 엔드포인트 수에 대한 일반적인 지침이 나와 있습니다. VMware 기반 어플라이언스의 크기는 하드웨어 기반 어플라이언스에 상응하는 사양에 맞게 결정되거나 그 이상으로 결정됩니다.

표 2. ISE 어플라이언스 크기 조정

ISE 어플라이언스	최대 엔드포인트	프로파일링되는 EPS(기존 엔드포인트 프로파일링)	저장되는 EPS (새 엔드포인트 프로파일링)
ACS1121/NAC3315/ISE3315	3000	43	33
NAC3355/ISE3355	6000	사용할 수 없음	사용할 수 없음
NAC3395/ISE3395	10,000	100	5
VMWare	3000/6000/10,000	VMware 컨피그레이션에 종속적	VMware 컨피그레이션에 종속적

또한 각 어플라이언스는 EPS(new events per second)를 처리할 수 있는 비율로 제한됩니다. 이 값은 수신된 프로파일링 데이터가 새로 검색된 엔드포인트에 사용되는지, 아니면 기존 엔드포인트에 사용되는지에 따라 달라집니다. 기존 엔드포인트의 프로파일링 비율은 표 2의 프로파일링되는 EPS 열에 나와 있습니다. 새로 검색된 엔드포인트가 데이터베이스에 추가되고 프로파일링되는 비율은 저장되는 EPS 열에 나와 있습니다.

ISE 프로파일링 서비스는 여러 ISE 어플라이언스 간에 서비스를 분배하여 확장할 수 있습니다. 프로파일링 서비스를 실행하는 ISE 정책 서비스 노드는 로드 밸런서 뒤에서 정책 서비스를 클러스터링하는 데 사용되는 노드 그룹의 멤버일 수도 있습니다.

## 네트워크 요구 사항

ISE 프로파일링 서비스는 다양한 컬렉터 또는 프로브를 사용하여 연결된 엔드포인트에 대한 특성을 수집합니다. 이러한 프로브 중 일부에는 네트워크 인프라, 액세스 디바이스 또는 엔드포인트의 특정 지원이 필요할 수 있습니다. 이러한 요구 사항은 특정 프로브를 다루는 섹션에서 자세히 설명하겠지만 네트워크 또는 엔드포인트에서 적절한 데이터가 제공되지 않을 경우 일부 프로브는 사용하지 못할 수 있습니다.

# 프로파일링 서비스 전역 컨피그레이션

## ISE 프로파일링 전역 컨피그레이션

이 섹션에서는 정책 서비스 노드에서 전역적으로 ISE 프로파일링 서비스를 활성화하고 전역 프로파일링 매개변수를 구성하기 위한 프로세스에 대해 살펴봅니다.

### 전역 프로파일링 설정 구성

#### 정책 관리 노드에서 전역 프로파일링 설정 구성

- Step 1** 지원되는 웹 브라우저 및 관리자 자격 증명([https://<ISE\\_PAN\\_FQDN\\_또는\\_IP>](https://<ISE_PAN_FQDN_또는_IP>))을 사용하여 기본 PAN(정책 관리 노드)의 ISE 관리 인터페이스에 액세스합니다.
- Step 2** Administration(관리) → System(시스템) → Settings(설정)으로 이동합니다. LHS(왼쪽) 창에서 Profiling(프로파일링)을 선택합니다.
- Step 3** RHS(오른쪽) 창에서 프로파일링 전환 및 예외 작업(그림 5)에 사용할 기본 CoA 유형을 선택합니다.

목표가 가시성에 국한되어 있다면 기본값인 No CoA(CoA 없음)를 그대로 사용하십시오. 그렇지 않으면 Port Bounce(포트 바운스)를 선택합니다. 이렇게 하면 클라이언트리스 엔드포인트에서 필요한 경우 IP 주소 새로 고침을 포함하여 전체 다시 권한 부여 프로세스를 진행하게 됩니다. 스위치 포트에서 여러 엔드포인트가 탐지될 경우 ISE는 연결된 다른 디바이스의 서비스 중단을 방지하기 위해 Reauth(재인증) 옵션을 사용하도록 되돌아갑니다.

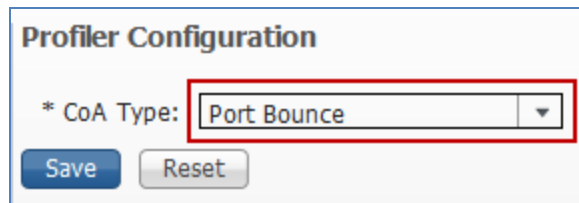


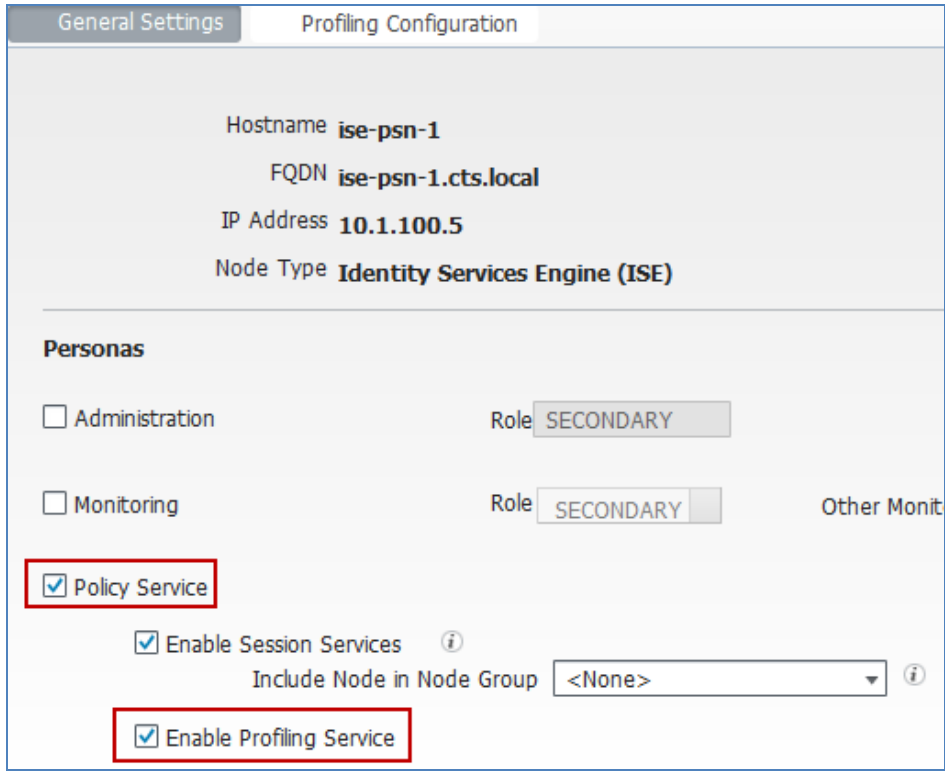
그림 3. 전역 프로파일링 설정: CoA 컨피그레이션

## ISE 프로파일링 서비스 활성화

#### 정책 서비스 노드에서 프로파일링 서비스 활성화

- Step 1** Administration(관리)→System(시스템)→Deployment(구축)로 이동하고 RHS 창의 구축된 노드 목록에서 프로파일링을 수행할 정책 서비스 노드를 선택합니다.
- Step 2** General Settings(일반 설정) 탭에서 정책 서비스라고 하는 노드 페르소나가 선택되어 있고 Enable Profiling Service(프로파일링 서비스 활성화)도 선택되어 있는지 확인합니다(그림 6).

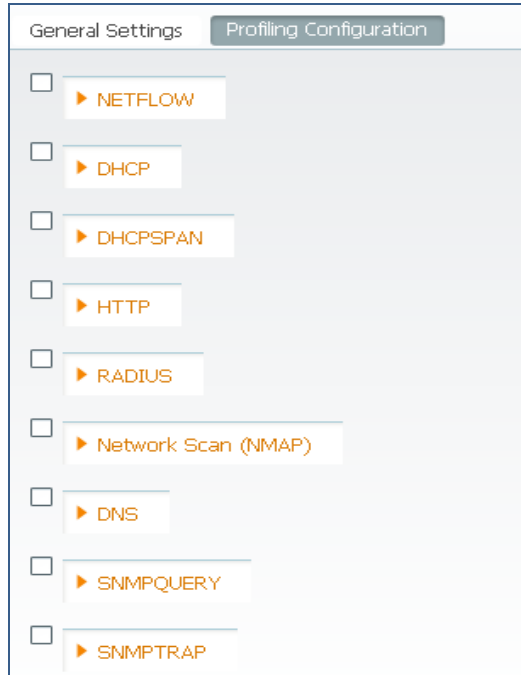
그림 1 정책 서비스 노드의 프로파일링 서비스 활성화



### 프로파일링 컨피그레이션 페이지 액세스 및 보기

**Step 3** Profiling Configuration(프로파일링 컨피그레이션) 탭을 클릭합니다. 해당 확인란을 선택하고 선택적 프로브 매개변수를 선택하여 활성화 및 구성된 다양한 프로브를 봅니다(그림 7).

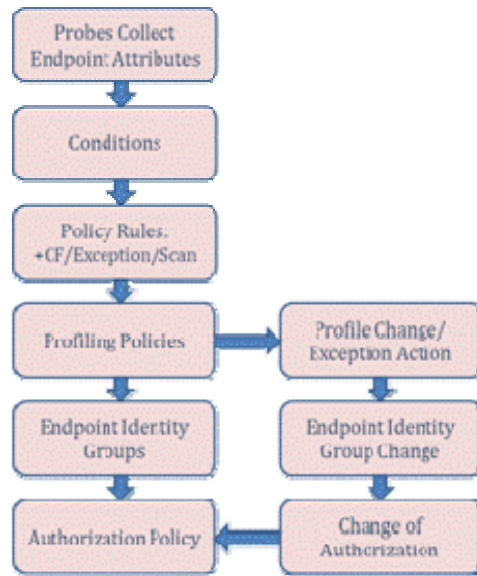
그림 2 프로브 컨피그레이션



**Step 4** 프로파일링 컨피그레이션을 변경할 때마다 페이지 하단의 Save(저장)를 클릭하여 변경 사항을 커밋합니다.

# 프로브 구성

그림 3: 컨피그레이션 흐름: 프로브 및 특성 수집



## 프로브 개요

ISE 프로브는 엔드포인트 특성을 수집하는 ISE 프로파일링 서비스 구성 요소입니다. 각 프로브는 서로 다른 수집 방법을 사용하며 엔드포인트에 대한 고유한 정보를 수집할 수 있습니다. 결과적으로 일부 프로브는 특정 디바이스 유형을 분류하는 데 다른 프로브보다 더 적합하거나 특정 환경에 따라 선호될 수 있습니다.

ISE는 다음과 같은 프로브를 지원합니다.

- RADIUS
- SNMP 트랩
- SNMP 쿼리
- DHCP
- DHCP SPAN
- DNS
- HTTP
- NetFlow
- 네트워크 검사(NMAP)

예를 들어 DHCP 및 DHCP SPAN과 같은 일부 프로브는 그 이름으로 알 수 있듯이 특정 특성을 수집할 수 있는 고유한 프로브입니다(이 예에서는 DHCP 패킷의 DHCP 특성 및 관련 옵션 필드). 특정 네트워크 환경에서 ISE 정책 서비스 노드에 대한 DHCP 트래픽 릴레이를 지원하는지 여부에 따라, 또는 네트워크 토폴로지 및 인프라 기능을 위해 SPAN(Switch Port Analyzer) 방법을 사용하는 것이 더 적합한지에 따라 DHCP와 DHCP SPAN 중에서 선택합니다. 이 가이드에는 각 프로브의 개별 섹션에서 프로브 선택을 위한 자세한 지침이 포함되어 있습니다.

각 프로브 유형은 활성화할 수 있는 난이도가 서로 다릅니다. 각 프로브 유형에서 사용되는 프로토콜 및 구축 방식에 따라 네트워크 또는 엔드포인트에 미치는 영향에도 차이가 있습니다. 마지막으로, 각 프로브에서 생성되는 데이터 값과 네트워크에 관련된 특정 엔드포인트 분류에 대한 적용 가능성도 서로 다릅니다. 이 가이드에서는 각 프로브 구성 및 구축 방식에 대해 살펴보고, 구축 유형에 따른 각 프로브의 구축 난이도, 네트워크 영향 및 상대 프로파일링 값에 대한 전반적인 정보를 제공합니다.

## 프로브 컨피그레이션

ISE 프로브는 프로파일링 서비스용으로 구성된 ISE 정책 서비스 노드에서 활성화됩니다. 이 섹션에서는 여러 엔드포인트 특성을 수집하도록 다양한 ISE 프로브를 활성화하는 단계를 살펴봅니다. 인프라와 ISE 관리 인터페이스 모두에서 예상되는 출력과 함께 네트워크 인프라를 지원하는 컨피그레이션 예도 제공됩니다.

### RADIUS 프로브를 사용한 프로파일링

RADIUS 프로브는 RADIUS 클라이언트(유선 액세스 스위치 및 무선 컨트롤러 포함)에서 RADIUS 서버(세션 서비스를 실행하는 ISE 정책 서비스 노드)로 보내는 RADIUS 특성을 수집합니다. 표준 RADIUS 포트에는 인증 및 권한 부여를 위한 UDP/1645 또는 UDP/1812와, RADIUS 계정 관리를 위한 UDP/1646 및 UDP/1813 포트가 있습니다.

**참고:** RADIUS 프로브는 RADIUS 트래픽을 직접 수신 대기하지 않으며, 그 대신 기본 UDP 포트 20514에서 모니터링 노드로 전송된 syslog의 RADIUS 특성을 수신 대기하고 구문 분석합니다. 그런 다음 캡처된 RADIUS 프로파일 특성은 기본 UDP 포트 30514에서 내부 로거로 전달됩니다.

RADIUS 프로브는 Device Sensor 기능을 사용하여 RADIUS 계정 관리 패킷으로 전송된 CDP(Cisco Discovery Protocol), LLDP(Link Layer Discovery Protocol) 및 DHCP 특성도 수집합니다. 이 기능은 뒷부분에 자세히 설명되어 있습니다([Device Sensor](#) 섹션 참고). 그림 9에서는 RADIUS 프로브 예에 대한 토폴로지를 보여줍니다.

그림 4 RADIUS 프로브 예

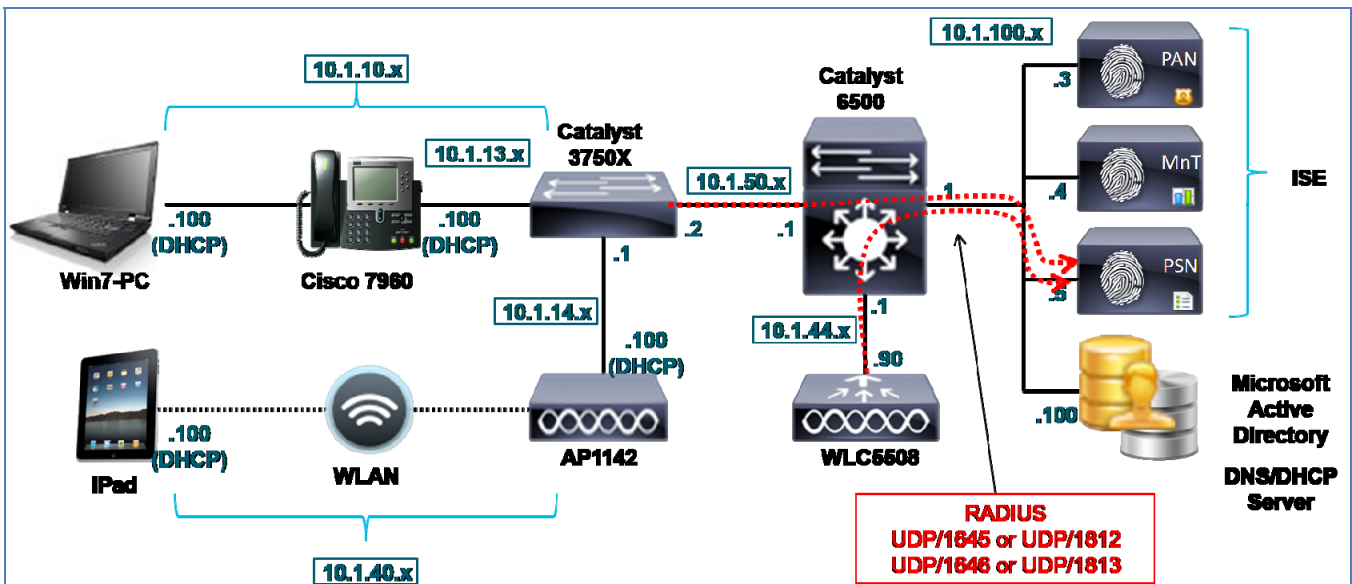




표 3에서는 RADIUS 프로브를 사용하여 수집되는 공통 특성을 보여줍니다.

표 1: 샘플 RADIUS 특성

User-Name	NAS-IP-Address	NAS-Port	Framed-IP-Address
Calling-Station-Id	Acct-Session-Id	Acct-Session-Time	Acct-Terminate-Cause

액세스 디바이스 컨피그레이션에 따라 다르긴 하지만 Calling-Station-ID는 일반적으로 연결하는 엔드포인트의 MAC 주소입니다. 이 특성은 네트워크에 연결하여 인증할 때 MAC 주소를 기초로 고유한 엔드포인트를 빠르게 식별하는 경우에 즉각적인 이점을 제공합니다. 또한 MAC 주소의 처음 세 바이트에서 가져온 OUI(Organizationally Unique Identifier)를 기초로 공급업체 네트워크 어댑터 관련 정보를 제공합니다.

RADIUS 계정 관리 패킷에 있는 Framed-IP-Address는 연결하는 엔드포인트의 IP 주소를 제공합니다. 이 특성은 Calling-Station-ID와 함께 IP 주소(예: DNS, HTTP, Cisco NetFlow 및 NMAP)를 사용하는 다른 프로브를 지원하는데 필요한 중요 IP-MAC 바인딩을 ISE에 제공합니다.

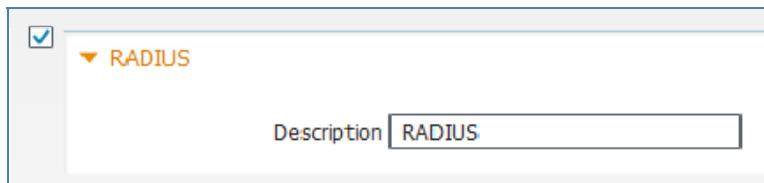
## RADIUS 프로브 구성

RADIUS 프로브는 네트워크 인증 및 권한 부여를 위한 세션 서비스를 실행하는 ISE 정책 서비스 노드로 RADIUS 패킷을 전송하도록 네트워크 액세스 디바이스가 이미 구성된 이후에 활성화 및 구축할 수 있는 가장 단순한 프로브 중 하나입니다.

### ISE에서 RADIUS 프로브 활성화

- Step 1** Administration(관리) → System(시스템) → Deployment(구축)로 이동합니다. RHS 창에 구축된 노드 목록에서 프로파일링을 수행할 정책 서비스 노드를 선택합니다.
- Step 2** Profiling Configuration(프로파일링 컨피그레이션) 탭을 선택하고 RADIUS 프로브를 활성화하기 위한 확인란을 선택합니다. RADIUS 서비스용으로 구성된 인터페이스에서 프로브가 자동으로 활성화됩니다(그림 10).

그림 5 RADIUS 프로브 컨피그레이션



- Step 3** Save(저장)를 클릭하여 변경 사항을 커밋합니다.
- Step 4** 프로파일링 서비스를 사용하여 구성된 다른 모든 정책 서비스 노드에 대해 이 절차의 단계를 반복합니다.

### ISE에서 액세스 디바이스가 구성되어 있는지 확인

이 가이드에서는 Administration(관리) → Network Resources(네트워크 리소스) → Network Devices(네트워크 디바이스)에서 표준 RADIUS 통신을 위한 네트워크 액세스 디바이스가 이미 ISE에 구성되어 있는 것으로 가정합니다.

### RADIUS를 ISE PSN으로 전송하도록 액세스 디바이스가 구성되어 있는지 확인

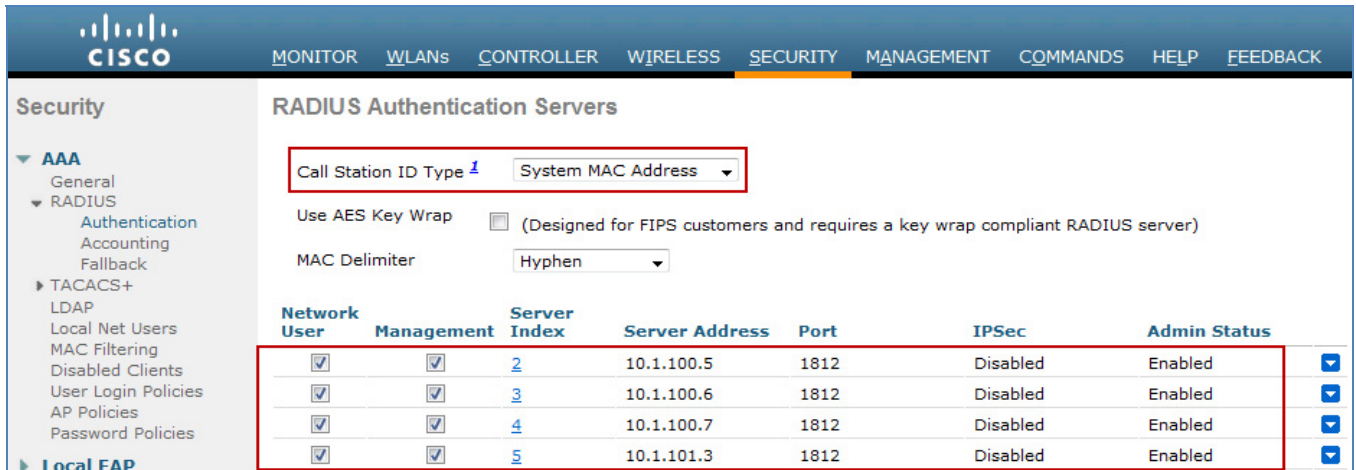
이 가이드에서는 ISE PSN(정책 서비스 노드)에 대해 RADIUS AAA(인증, 권한 부여 및 계정 관리)를 사용하도록 네트워크 액세스 디바이스가 이미 구성되어 있는 것으로 가정합니다. 다음은 유선 스위치를 위한 샘플 RADIUS 컨피그레이션입니다.

```

aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
ip radius source-interface <Interface>
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server host <ISE_PSN_Address> auth-port 1812 acct-port 1813 key xxx
radius-server vsa send accounting
radius-server vsa send authentication
    
```

그림 11은 무선 컨트롤러를 위한 샘플 RADIUS 서버 컨피그레이션을 보여 줍니다. 이 컨피그레이션 페이지에 액세스하려면 WLC 웹 관리 인터페이스에서 Security(보안) → AAA → RADIUS → Authentication(인증)으로 이동합니다.

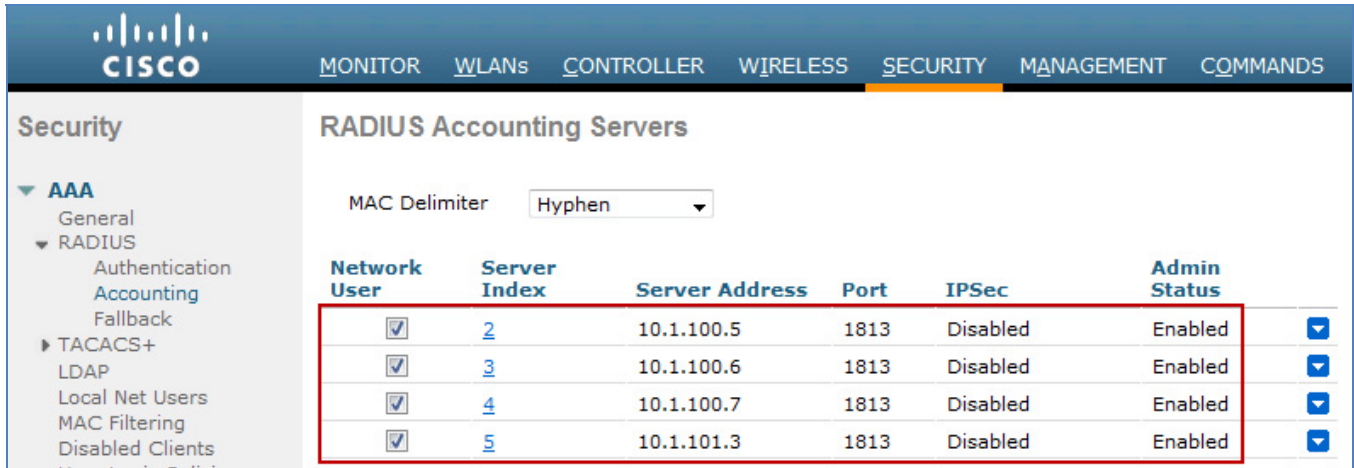
그림 6 무선 컨트롤러를 위한 전역 RADIUS 서버 컨피그레이션 예



**Cisco 모범 사례:** 그림 11과 같이 비 802.1X 클라이언트의 프로파일링을 허용하려면 Call Station ID Type(통화 스테이션 ID 유형)을 System MAC Address(시스템 MAC 주소)로 설정해야 합니다. 이렇게 하면 ISE가 엔드포인트를 데이터베이스에 추가하고 수신된 다른 프로파일 데이터를 알려진 MAC 주소를 기반으로 동일한 엔드포인트에 연결할 수 있게 됩니다.

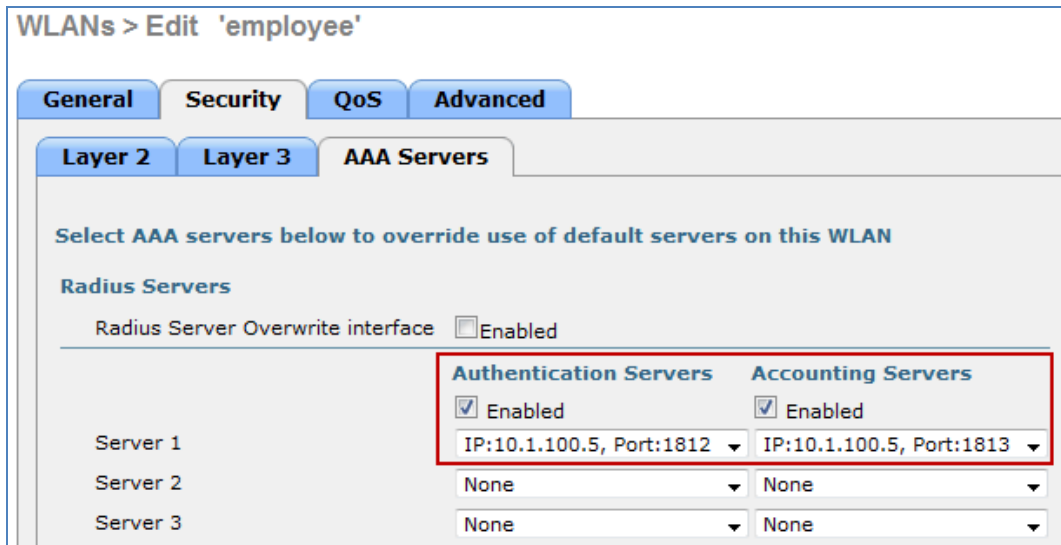
무선 컨트롤러를 위한 RADIUS 계정 관리 컨피그레이션 아래에 유사한 항목이 있어야 합니다(그림 12).

그림 7 무선 컨트롤러를 위한 전역 RADIUS 계정 관리 컨피그레이션 예



각 WLAN은 또한 해당 ISE 정책 서비스 노드를 지정하도록 구성되어야 합니다(그림 13).

그림 8 무선 컨트롤러를 위한 WLAN RADIUS 컨피그레이션 예



### RADIUS 프로브 데이터 확인

- Step 1 네트워크에 새 엔드포인트를 인증합니다.
- Step 2 ISE 정책 관리 노드로 이동하고 Administration(관리) → Identity Management(ID 관리) → Identities(ID)로 이동합니다.
- Step 3 LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 4 새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 RADIUS 프로브에서 캡처한 특성을 표시합니다.
- Step 5 수많은 특성이 캡처될 수 있습니다. 그림 14의 샘플 출력에는 4가지 특성, 즉 **Calling-Station-ID**, **EndPointSource**, **Framed-IP-Address** 및 **OUI**만 나와 있습니다.

그림 9 RADIUS 프로브 특성 예

**Endpoint**

\* MAC Address **00:1A:70:38:B6:66**

\* Policy Assignment **Cisco-Device**

Static Assignment

\* Identity Group Assignment **Profiled**

Static Group Assignment

**Attribute List**

ADDomain	cts.local
AcsSessionID	ise-psn-1/123830140/32632
Airespace-Wlan-Id	1
AuthState	Authenticated
AuthenticationIdentityStore	AD1
AuthenticationMethod	MSCHAPV2
AuthorizationPolicyMatchedRule	Employee_NoPosture
CPMSessionID	0a012c5a00005954f98e8cc
Called-Station-ID	cc-ef-48-0c-99-a0
Calling-Station-ID	00-1a-70-38-b6-66
DestinationIPAddress	10.1.100.5
DestinationPort	1812
Device IP Address	10.1.44.90
Device Type	Device Type#All Device Types#Wireless
EapAuthentication	EAP-MSCHAPV2
Eap Tunnel	PEAP
EndPointMACAddress	00-1A-70-38-B6-66
EndPointMatchedProfile	Cisco-Device
EndPointPolicy	Cisco-Device
EndPointProfilerServer	ise-psn-1
EndPointSource	RADIUS Probe
ExternalGroups	cts.local/users/employees\,cts.local/users/domain users\,cts.local/builtin/users
Framed-IP-Address	10.1.40.100
IdentityAccessRestricted	false
IdentityGroup	Profiled
IdentityPolicyMatchedRule	Default
Location	Location#All Locations#North_America#RTP
MACAddress	00:1A:70:38:B6:66
MatchedPolicy	Cisco-Device
MessageCode	3000
NAS-IP-Address	10.1.44.90
NAS-Identifier	Cisco_0c99:a4
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
NetworkDeviceGroups	Device Type#All Device Types#Wireless, Location#All Locations#North_America#RTP
NetworkDeviceName	wlc5508
OUI	Cisco-Linksys, LLC
PolicyVersion	22
PostureAssessmentStatus	NotApplicable
RequestLatency	1
Response	{User-Name=CTS\employee1; State=ReauthSession:0a012c5a00005954f98e8cc; Class=CACS:0a012c5a00005954f98e8cc; ise-psn-1/123830140/32632; Termination-Action=RADIUS-Request; cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-JP-PERMIT_ALL_TRAFFIC-4f57e406; MS-MPPE-Send-Key=7d:90:04:93:07:bc:92:1e:e5:4d:97:6f:39:51:02:6e:eb:39:46:35:4f:e4:76:06:27:58:96:98:b4:bf:51:cb; MS-MPPE-Recv-Key=ac:0e:b6:a9:6f:c7:72:5d:cf:fe:9d:8b:9d:95:7a:8c:c6:2c:a7:54:1f:ee:3e:40:ed:53:48:d8:68:76:38:e8; Airespace-ACL-Name=PERMIT_ALL_TRAFFIC; }
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	AD1, Internal Users
SelectedAuthorizationProfiles	Employee
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	20
Total Certainty Factor	20
User-Name	CTS\employee1
attribute-52	00:00:00:00
attribute-53	00:00:00:00
cisco-av-pair	audit-session-id=0a012c5a00005954f98e8cc
ip	10.1.40.100

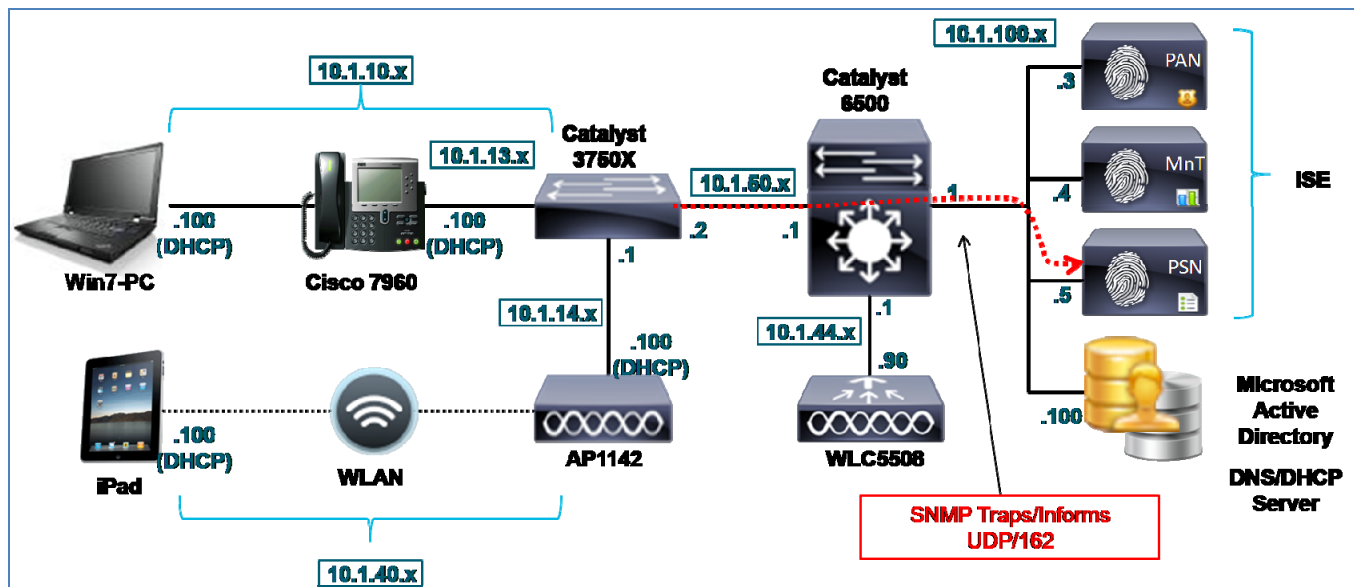
- Step 6** Calling-Station-ID는 **MACaddress** 특성으로 채워집니다. 또한 네트워크 어댑터의 공급업체 OUI는 **Cisco-Linksys**인 것으로 확인됩니다. 이 예에서 네트워크 어댑터는 **Linksys Wireless USB** 어댑터입니다. OUI와 일치하는 조건은 프로파일링 정책 규칙에서 공통된 항목입니다. 그러한 조건은 경우에 따라(예: Nintendo 또는 Sony 게임 콘솔) 엔드포인트를 분류하는 데 필요한 전부일 수 있습니다.
- Step 7** Framed-IP-Address 값은 **ip** 특성으로 채워집니다. 이제 이 엔드포인트에 대한 IP-MAC 주소 바인딩이 생성되었습니다.
- Step 8** **EndPointSource** 특성은 마지막 프로파일 특성 업데이트의 소스를 지정합니다. 이 경우에는 이 엔드포인트 레코드에 대한 마지막 업데이트를 제공하는 **RADIUS** 프로브입니다.
- Step 9** 프로파일링에 추가 **RADIUS** 특성을 사용할 수 있지만 그러한 특성 대부분은 정책 조건 및 규칙을 생성하기 위한 권한 부여 정책에 직접 사용할 수 있으므로 위에 언급된 항목에만 초점을 맞춥니다.

### SNMP 트랩 프로브를 사용한 프로파일링

SNMP 트랩 프로브는 ISE 프로파일링 서비스에 네트워크 엔드포인트의 현재 상태(연결 또는 연결 해제)에 대한 알림을 제공하고 SNMP 쿼리 프로브를 트리거하는 데 사용됩니다.

SNMP 트랩 프로브를 사용하려면 엔드포인트가 연결되는 액세스 디바이스를 프로파일링 서비스용으로 구성된 ISE 정책 서비스 노드에 SNMP 트랩을 보내도록 구성해야 합니다. 그림 15에서는 SNMP 트랩 프로브 예에 대한 토폴로지를 보여줍니다.

그림 10 SNMP 트랩 프로브 예



RADIUS 프로브가 이미 활성화되어 있는 경우 RADIUS 계정 관리 시작 메시지도 SNMP 쿼리 프로브를 트리거할 수 있으므로 SNMP 트랩 프로브가 필요하지 않을 수 있습니다. 이 프로브의 기본 활용 사례는 네트워크 인증을 위한 RADIUS가 아직 구성되지 않은 사전 구축 검색 단계와 관련이 있습니다. 또 다른 활용 사례는 Cisco NAC Appliance Release 4.9 이상과 같이 RADIUS를 사용하지 않는 환경을 통합하는 것입니다.

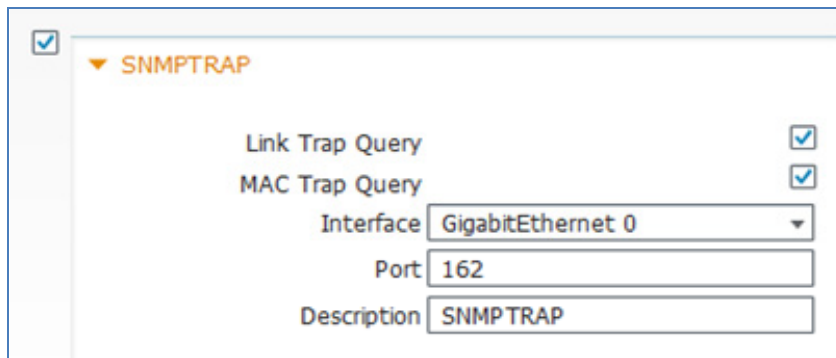
## SNMP 트랩 프로브 구성

SNMP 트랩 프로브를 사용하려면 먼저 ISE에서 활성화해야 합니다. 앞서 언급한 것처럼 엔드포인트가 연결되는 액세스 디바이스를 프로파일링 서비스용으로 구성된 ISE 정책 서비스 노드에 SNMP 트랩을 보내도록 구성해야 합니다. ISE는 또한 이러한 네트워크 액세스 디바이스에서 보내는 트랩을 수락하고 처리하도록 구성해야 합니다.

### ISE에서 SNMP 트랩 프로브 활성화

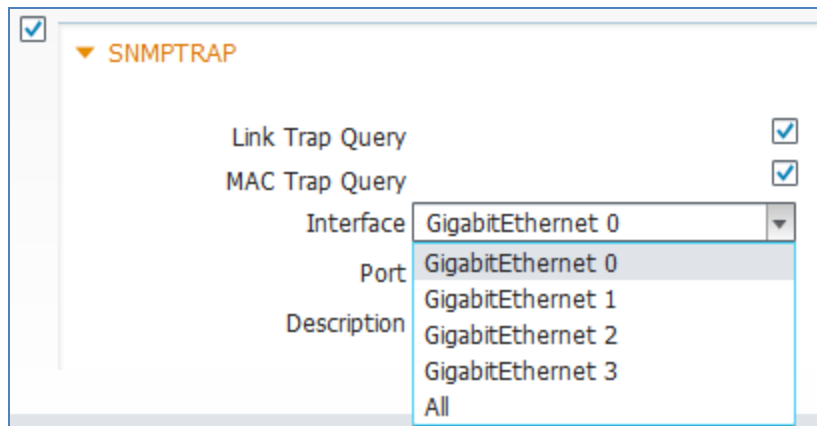
- Step 1** Administration(관리)→System(시스템)→Deployment(구축)로 이동하고 RHS 창의 구축된 노드 목록에서 프로파일링을 수행할 정책 서비스 노드를 선택합니다.
- Step 2** Profiling Configuration(프로파일링 컨피그레이션) 탭을 선택하고 SNMP 트랩 프로브를 활성화하기 위한 확인란을 선택합니다(그림 16).

그림 11 SNMPTRAP 프로브 컨피그레이션



- Step 3** Link Trap Query(링크 트랩 쿼리) 및 MAC Trap Query(MAC 트랩 쿼리)라는 확인란을 선택하여 프로브가 각 트랩 유형에 응답할 수 있도록 합니다.
- Step 4** 트랩을 수신하는 데 ISE PSN 인터페이스가 사용되는지 확인합니다. 다른 인터페이스에서 수신된 트랩을 처리하거나 All interfaces(모든 인터페이스)를 선택할 수 있지만 대부분의 경우 이 인터페이스가 기본 GigabitEthernet 0 인터페이스가 됩니다.

그림 12: SNMP 트랩 프로브 - 인터페이스 컨피그레이션



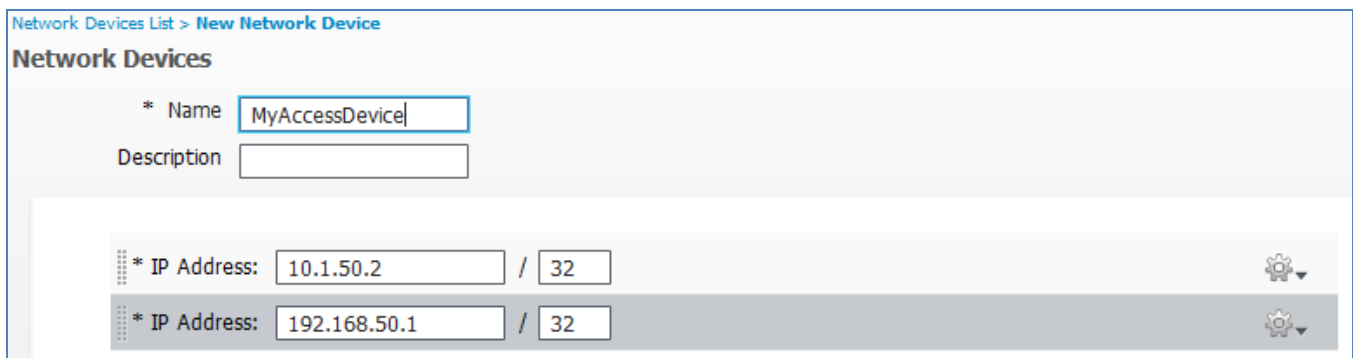
- Step 5** 다른 인터페이스에서 트랩을 처리하려는 경우 그러한 인터페이스가 활성화되고 IP 주소가 할당되었는지 확인하십시오. 이러한 주소는 SNMP 호스트 트랩 대상의 액세스 디바이스에서 구성해야 합니다.
- Step 6** Save(저장)를 클릭하여 변경 사항을 커밋합니다.
- Step 7** 프로파일링 서비스를 사용하여 구성된 다른 모든 정책 서비스 노드에 대해 이 절차의 단계를 반복합니다.

### ISE에 네트워크 액세스 디바이스 추가

일반적으로 RADIUS를 통해 엔드포인트를 인증하는 모든 네트워크 액세스 디바이스는 ISE에서 구성되지만, SNMP 트랩 프로브를 사용하는 것은 대개 RADIUS용으로 아직 액세스 디바이스가 구성되지 않았음을 나타냅니다. 이러한 액세스 디바이스가 아직 구성되지 않은 경우 SNMP 트랩을 ISE로 보내는 액세스 디바이스를 추가해야 합니다.

- Step 1** Administration(관리) → Network Resources(네트워크 리소스) → Network Devices(네트워크 디바이스)로 이동하고 RHS 창에서 Add(추가)를 클릭합니다.
- Step 2** 디바이스 이름 및 IP 주소 정보를 입력합니다(그림 18). IP 주소는 SNMP 트랩을 제공하는 IP 주소를 포함해야 합니다. 간단한 컨피그레이션에서는 하나의 관리 IP 주소만 스위치에 있을 수 있습니다. 다른 경우 여러 IP 주소가 있을 수 있으며 기본적으로 SNMP는 일반적으로 이그레스(egress) 인터페이스의 IP 주소를 사용합니다. 필요한 경우, 액세스 디바이스가 SNMP 패킷을 제공하는 데 사용할 수 있는 가능한 모든 IP 주소를 입력합니다.

그림 13 네트워크 디바이스 컨피그레이션



**모범 사례:** 액세스 디바이스에서 지원하는 경우 관리 트래픽에 루프백 인터페이스를 사용하십시오. **source-interface**와 같은 옵션을 사용하여 관리 트래픽을 제공하는 IP 주소 및 특정 인터페이스를 설정해야 합니다. 이렇게 하면 모든 관리 트래픽에 균일한 주소를 제공할 수 있을 뿐 아니라 특정 인터페이스가 중단된 경우 연결 실패를 방지할 수 있습니다.

- Step 3** SNMP Settings(SNMP 설정) 확인란을 선택합니다.
- Step 4** 액세스 디바이스에 사용되는 SNMP 버전을 지정하고 SNMP 버전 1 및 2c의 SNMP RO 커뮤니티 문자열을 입력합니다. 아니면 액세스 디바이스에 해당하는 SNMPv3 자격 증명 및 컨피그레이션을 입력합니다(그림 19).
- Step 5** Link Trap Query(링크 트랩 쿼리) 및 MAC Trap Query(MAC 트랩 쿼리) 확인란이 선택되어 있는지 확인합니다. 이러한 설정을 통해 ISE는 특정 액세스 디바이스에서 수신되는 SNMP 트랩을 허용하거나 무시할 수 있습니다. 또는 특정 트랩 유형만 허용할 수도 있습니다.

그림 14 네트워크 디바이스 컨피그레이션 - SNMP 트랩

SNMP Settings

- \* SNMP Version: 2c
- \* SNMP RO Community: ciscoro
- SNMP Username: [Empty]
- Security Level: [Empty]
- Auth Protocol: [Empty]
- Auth Password: [Empty] Show
- Privacy Protocol: [Empty]
- Privacy Password: [Empty] Show
- \* Polling Interval: 3,600 seconds (Valid Range 600 to 86400)
- Link Trap Query:
- MAC Trap Query:
- Originating Policy Services Node: None

Step 6 완료되면 변경 사항을 저장합니다.

Step 7 SNMP 트랩을 ISE 정책 서비스 노드로 전송하는 각 액세스 디바이스에 대해 위 단계를 반복합니다.

### SNMP 트랩을 ISE 정책 서비스 노드로 전송하도록 액세스 디바이스 구성

Step 1 액세스 디바이스의 관리 콘솔로 이동하고 액세스 디바이스가 프로파일링 서비스를 실행하는 ISE 정책 서비스 노드로 SNMP 트랩을 전송하도록 구성되고 SNMP 트랩 프로브와 함께 활성화되어 있는지 확인합니다.

Step 2 다음은 Cisco IOS를 실행하는 Catalyst 스위치에서 SNMP LinkUp/LinkDown 트랩과 함께 MAC Notification 트랩을 보내도록 구성한 예입니다.

```
interface <Endpoint_Interface>
snmp trap mac-notification added
snmp trap mac-notification removed
!
mac address-table notification change
mac address-table notification mac-move
!
snmp-server trap-source <Interface>
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host <ISE_PSN_IP_address> version 2c ciscoro
```

참고: Cisco ISE는 현재 Wireless LAN Controller에서 들어오는 SNMP 트랩을 지원하지 않습니다.



### SNMP 트랩 프로브 데이터 확인

SNMP 트랩에는 연결된 MAC 주소가 없으므로 LinkUp 또는 LinkDown 트랩만 기준으로 SNMP 트랩 프로브를 엔드포인트 특성으로 채울 수 없습니다. 그러한 트랩은 기본적으로 인터페이스에 설정되었거나 끊어진 링크에 대해 알려줍니다. 그러나 MAC Notification 트랩은 엔드포인트의 MAC 주소를 포함하므로 ISE 내부 엔드포인트 데이터베이스에 대한 업데이트를 제공할 수 있습니다.

- Step 1** Administration(관리) → Identity Management(ID 관리) → Identities(ID) → Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 2** SNMP 트랩을 위해 구성된 액세스 스위치에서 유선 클라이언트의 연결을 해제했다가 다시 연결합니다.
- Step 3** ISE 정책 관리 노드로 이동하고 Administration(관리) → Identity Management(ID 관리) → Identities(ID)로 이동합니다.
- Step 4** LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 5** 새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 SNMP 트랩 프로브에서 캡처한 특성을 표시합니다(그림 20).

그림 15 SNMP 트랩 프로브 특성 예

**Endpoint**

\* MAC Address **00:50:56:A0:0B:3A**

\* Policy Assignment VMWare-Device

Static Assignment

\* Identity Group Assignment Profiled

Static Group Assignment

**Attribute List**

EndPointPolicy	VMWare-Device		
EndPointProfilerServer	ise-psn-1		
<b>EndPointSource</b>	<b>SNMPTrap Probe</b>	→	<b>EndPointSource</b> <b>SNMPTrap Probe</b>
IdentityGroup	Profiled		
<b>MACAddress</b>	<b>00:50:56:A0:0B:3A</b>	→	<b>MACAddress</b> <b>00:50:56:A0:0B:3A</b>
MacStatus	02		
MatchedPolicy	VMWare-Device		
NADAddress	10.1.50.2		
<b>OUI</b>	<b>VMware, Inc.</b>	→	<b>OUI</b> <b>VMware, Inc.</b>
PolicyVersion	22		
StaticAssignment	false		
StaticGroupAssignment	false		
TimeToProfile	19		
Timestamp	58963997		
Total Certainty Factor	10		
Vlan	10		
dot1dBasePort	1		

강조 표시된 키 특성에는 **EndPointSource**, **MACAddress** 및 **OUI**가 있습니다.

**EndPointSource**를 통해 SNMP 트랩 프로브가 정보의 소스임을 확인할 수 있습니다.

참고: 그림 20에 표시된 예에서는 다른 모든 프로브가 비활성화되었으며 테스트를 실행하기 전에 ISE 데이터베이스에서 엔드포인트가 삭제되었습니다.

**MACAddress**는 MAC Notification 트랩 정보에서 학습되고, 공급업체 OUI는 ISE의 OUI 데이터베이스를 기준으로 상호 연결하여 확인되었습니다. 이 예에서는 클라이언트에서 가상 네트워크 어댑터를 사용하는 VMware가 실행되고 있음을 알 수 있습니다.

SNMP 트랩이 액세스 스위치에서 전송되고 있는지 확인하기 위한 옵션으로 전송된 **SNMP Link** 및 **MAC Notification** 트랩을 볼 수 있도록 디버그 로깅을 활성화할 수 있습니다. 아래의 출력은 다음 디버그가 활성화되어 있는 Catalyst 스위치의 출력입니다.

- debug snmp packets
- debug mac-notification

다음 예에서 Cisco IP Phone에 연결된 스위치 포트 및 해당 전화기에 연결된 Windows 7 PC를 활성화하면 전화기와 PC 모두에 대해 **SNMP LinkUp** 트랩이 ISE PSN으로 전송되고 그 후에는 둘 모두에 대해 **MAC Notification** 트랩이 전송됩니다. MAC 주소 00:50:56:A0:0B:3A를 사용하는 PC와 관련된 트랩만 강조 표시되어 있습니다.

```
Apr 26 16:53:06.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Apr 26 16:53:06.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan13, changed state to up
Apr 26 16:53:06.743: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:06.743: SNMP: V2 Trap, reqid 296, errstat 0, erridx 0
sysUpTime.0 = 58970958
snmpTrapOID.0 = snmpTraps.4
ifIndex.10 = 10
ifDescr.10 = Vlan10
ifType.10 = 53
lifEntry.20.10 = up

Apr 26 16:53:06.861: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:06.861: SNMP: V2 Trap, reqid 299, errstat 0, erridx 0
sysUpTime.0 = 58970970
snmpTrapOID.0 = snmpTraps.4
ifIndex.13 = 13
ifDescr.13 = Vlan13
ifType.13 = 53
lifEntry.20.13 = up
Apr 26 16:53:06.995: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:07.246: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:08.706: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
Apr 26 16:53:09.713: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
Apr 26 16:53:09.713: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:09.713: SNMP: V2 Trap, reqid 302, errstat 0, erridx 0
sysUpTime.0 = 58971255
snmpTrapOID.0 = snmpTraps.4
ifIndex.10101 = 10101
ifDescr.10101 = GigabitEthernet1/0/1
ifType.10101 = 6
lifEntry.20.10101 = up
```

```

Apr 26 16:53:09.964: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:12.280: MN: Enqueue MAC 0050.56a0.0b3a on port 1 vlan 10
MN: New Shadow entry..

Apr 26 16:53:12.280: MN : MAC Notify event for 0050.56a0.0b3a on port 1 vlan 10

Apr 26 16:53:12.456: MN: Enqueue MAC 0030.94c4.528a on port 1 vlan 10
MN: Got the last shadow entry..Index 11

Apr 26 16:53:12.456: MN : MAC Notify event for 0030.94c4.528a on port 1 vlan 10
MN: Shadow entry for Despatch..
Despatching trap for Index 2 Time: 58971575
MN: Wrapping history queue..

Apr 26 16:53:12.925: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:12.925: SNMP: V2 Trap, reqid 305, errstat 0, erridx 0
sysUpTime.0 = 58971577
snmpTrapOID.0 = cmnMacChangedNotification
cmnHistMacChangedMsg.1 =
01 00 0A 00 50 56 A0 0B 3A 00 01 01 00 0A 00 30
94 C4 52 8A 00 01 00
cmnHistTimestamp.1 = 58971575
Apr 26 16:53:13.177: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:23.587: MN: Enqueue MAC 0030.94c4.528a on port 1 vlan 13
MN: New Shadow entry..

Apr 26 16:53:23.604: MN : MAC Notify event for 0030.94c4.528a on port 1 vlan 13
MN: Shadow entry for Despatch..
Despatching trap for Index 2 Time: 58972696
MN: Wrapping history queue..

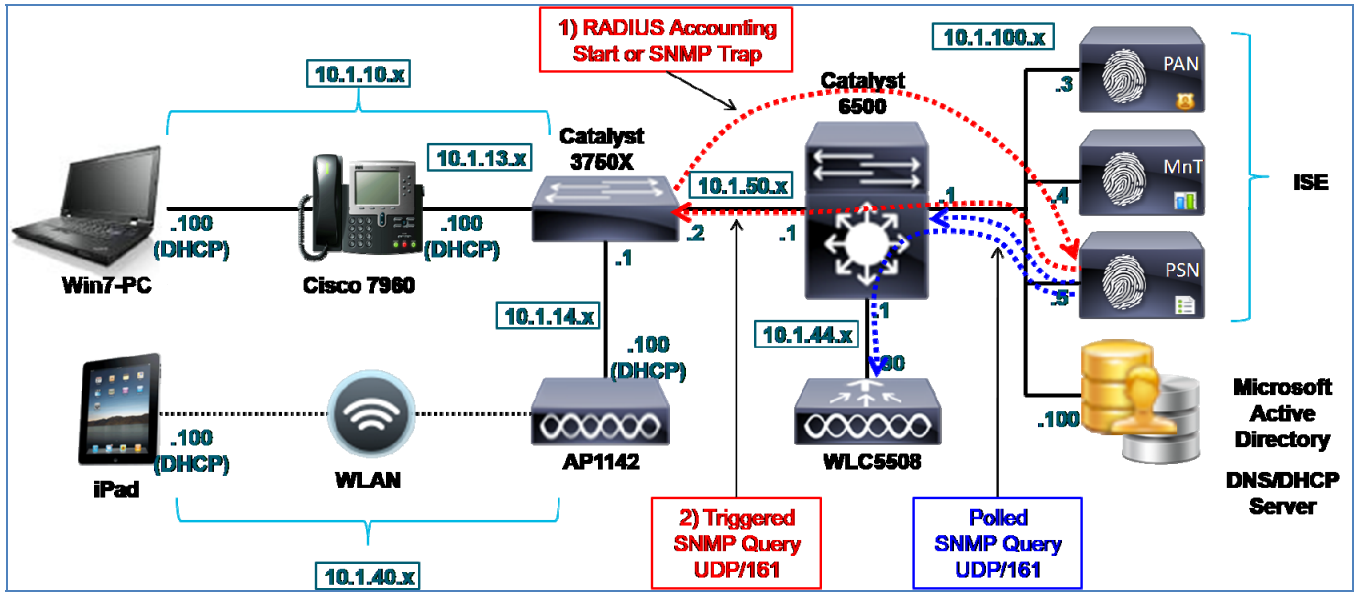
Apr 26 16:53:24.132: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:24.132: SNMP: V2 Trap, reqid 308, errstat 0, erridx 0
sysUpTime.0 = 58972697
snmpTrapOID.0 = cmnMacChangedNotification
cmnHistMacChangedMsg.1 =
01 00 0D 00 30 94 C4 52 8A 00 01 00
cmnHistTimestamp.1 = 58972696
Apr 26 16:53:24.384: SNMP: Packet sent via UDP to 10.1.100.5
    
```

ISE는 참조를 위해 액세스 디바이스에서 사용 가능한 디버그 로깅 외에 고유한 디버그 로깅도 지원합니다. ISE에 수신되는 정보를 검증할 수 있는 대체 방법은 Operations(운영) → Troubleshoot(문제 해결) → Diagnostic Tools(진단 도구) → General Tools(일반 도구)에 있는 내장형 TCP 덤프 유틸리티를 사용하는 것이지만 디버깅은 이 가이드의 범위를 벗어납니다. 해당 도구를 사용하면 액세스 디바이스에서 지정된 ISE 정책 서비스 노드 인터페이스(SNMP 트랩 프로브와 함께 활성화된 항목)로 전달되는 SNMP 트래픽을 캡처할 수 있습니다. 그런 다음 이 정보를 다운로드하여 사람이 읽을 수 있는 형식으로 표시할 수 있습니다. 아니면 Wireshark와 같은 일반 패킷 분석기로 가져올 수 있도록 표준 패킷 캡처 형식으로 표시할 수도 있습니다.

**SNMP 쿼리 프로브를 사용한 프로파일링**

- Step 1** SNMP 쿼리 프로브는 쿼리(또는 SNMP Get 요청)를 액세스 디바이스로 보내고, 선택적으로 다른 인프라 디바이스로 보내 SNMP MIB에 저장된 관련 엔드포인트 데이터를 수집하는 데 사용됩니다. ISE 정책 서비스 노드에서 수행하는 일반적인 SNMP 쿼리 유형으로는 다음 2가지가 있습니다.
- Step 2** 시스템 쿼리(폴링됨)
- Step 3** 인터페이스 쿼리(트리거됨)
- Step 4** 그림 21에는 시스템 쿼리 프로브를 사용하는 토폴로지 예가 나와 있습니다.

그림 16 SNMP 쿼리 프로브 예



### 시스템 쿼리

시스템 쿼리는 ISE의 NAD 컨피그레이션에 설정된 폴링 간격에 따라 주기적으로 수행됩니다. 폴링되는 MIB는 다음과 같습니다.

- IF-MIB
- SNMPv2-MIB
- IP-MIB
- CISCO-CDP-MIB
- CISCO-VTP-MIB
- CISCO-STACK-MIB
- BRIDGE-MIB
- OLD-CISCO-INTERFACE-MIB
- CISCO-LWAPP-AP-MIB
- CISCO-LWAPP-DOT11-CLIENT-MIB
- CISCO-AUTH-FRAMEWORK-MIB
- EEE8021-PAE-MIB: RFC IEEE 802.1X
- HOST-RESOURCES-MIB
- LLDP-MIB

수집되는 키 특성에는 다음과 같은 항목이 있습니다.

- Bridge, IP(ARP)
- **cdpCacheEntry**(유선만 해당)
- lldpLocalSystemData(유선만 해당)
- lldpRemoteSystemsData(유선만 해당)
- **cLApEntry**(WLC만 해당)
- cldcClientEntry(WLC만 해당)

여러 정책 서비스 노드에서 SNMP 쿼리가 활성화되어 있는 경우, 지정된 네트워크 디바이스를 폴링하도록 특정 PSN이 구성되어 있지 않다면 네트워크 디바이스의 SNMP 폴링이 사용 가능한 모든 PSN 간에 분산됩니다.

이와 같이 폴링되는 쿼리 중에 ISE에서 IP-MAC ARP 캐시 표를 작성할 수 있도록 ARP(Address Resolution Protocol) 표 정보도 수집됩니다. 엔드포인트가 레이어 2 전용 스위치 포트에 연결된 환경에서는 엔드포인트에 대한 ARP 표 정보가 포함되어 있는 경우 업스트림 레이어 3 디바이스(예: 브랜치 라우터 또는 레이어 3 분산 스위치)를 ISE 네트워크 액세스 디바이스로 구성하는 것이 좋습니다. DHCP 프로브가 IP-MAC 바인딩 데이터를 수집할 수 없는 경우 또는 액세스 디바이스에 RADIUS가 구성되어 있지 않은 구축 환경에서는 IP-MAC 바인딩 정보를 제공해야 할 수 있습니다. 토폴로지 예(그림 21)에서는 무선 클라이언트 또는 다운스트림 레이어 2 스위치(표시되지 않음)를 위한 ARP 정보를 확보하기 위해 Cisco Catalyst 6500 Series 스위치가 폴링될 수 있습니다.

### 인터페이스 쿼리

인터페이스 쿼리는 RADIUS 계정 관리 시작 패킷(RADIUS 프로브 필요) 또는 SNMP LinkUp/MAC Notification 트랩(SNMP 트랩 프로브 필요)에 의해 트리거됩니다.

**모범 사례:** 구축을 간소화하고 SNMP 트랩으로 인한 트래픽 오버헤드를 줄이기 위해서는 가능하면 RADIUS 프로브를 사용하여 RADIUS 계정 관리 시작 메시지를 기반으로 SNMP 쿼리를 트리거하십시오.

시스템 쿼리에서는 액세스 디바이스 MIB를 읽는 반면, 인터페이스 쿼리에서는 MIB 또는 트랩을 수신하는 특정 인터페이스만 관련된 MIB 부분을 요청합니다. 이와 같이 트리거되는 쿼리는 액세스 디바이스에서 다음 데이터를 검색합니다.

- 인터페이스 데이터(ifIndex, ifDesc 등)
- 포트 및 VLAN 데이터
- 세션 데이터(인터페이스 유형이 이더넷인 경우)
- CDP 데이터(Cisco 디바이스)
- LLDP 데이터

트리거되는 인터페이스 쿼리 중에 수집되는 주요 프로파일링 특성에는 CDP(Cisco Discovery Protocol) 및 LLDP(Link Layer Discovery Protocol) 표가 있습니다. CDP 및 LLDP는 스위치가 연결된 엔드포인트의 특성을 동적으로 학습하도록 허용하는 링크 프로토콜입니다. IP 비디오 장비, 네트워크 인프라 및 Cisco 어플라이언스를 비롯한 다양한 디바이스에서 이러한 프로토콜을 지원합니다. 대부분의 주요 IP 전화기 제조업체는 CDP 또는 LLDP를 지원합니다. 따라서 이 정보 자체만을 기준으로 다수의 엔드포인트를 분류할 수 있습니다. 또한 광범위한 클라이언트 운영 체제에서 최소한의 비용이나 무상으로 사용할 수 있는 CDP/LLDP 에이전트가 많이 있습니다.

다음 출력에서는 연결된 엔드포인트에 대한 CDP 데이터를 수집하는 SNMP 쿼리를 사용하여 수집할 수 있는 정보 유형 샘플을 보여줍니다.

```

cat3750x#show cdp neighbor detail
-----
Device ID: APc471.fe34.197a
Entry address(es):
  IP address: 10.1.14.100
Platform: cisco AIR-LAP1142N-A-K9 , Capabilities: Trans-Bridge
Interface: GigabitEthernet1/0/2, Port ID (outgoing port): GigabitEthernet0
Holdtime : 123 sec

Version :
Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 27-Jan-12 21:45 by prod_rel_team

advertisement version: 2
Duplex: full
Power drawn: 15.400 Watts
Power request id: 1358, Power management id: 2
Power request levels are:15400 14500 0 0 0
Management address(es):

-----
Device ID: SEP003094C4528A
Entry address(es):
  IP address: 10.1.13.100
Platform: Cisco IP Phone 7960, Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1, Port ID (outgoing port): Port 1
Holdtime : 162 sec
Second Port Status: Up

Version :
P00308010100

advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Management address(es):

-----
    
```

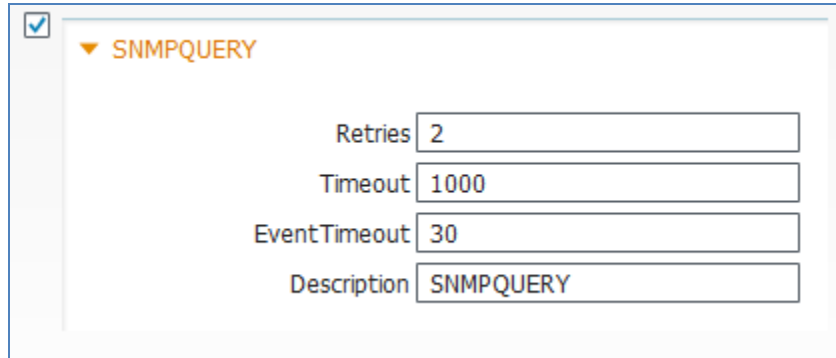
## SNMP 쿼리 프로브 구성

SNMP 쿼리 프로브를 사용하려면 읽기 전용(RO) 커뮤니티를 사용하여 ISE 정책 서비스 노드에서 SNMP 요청을 수락하도록 네트워크 디바이스를 구성해야 합니다. 또한 ISE에서 해당하는 SNMP 커뮤니티 문자열과 함께 네트워크 디바이스로 SNMP 디바이스를 구성해야 합니다. 트리거된 쿼리가 발생하려면 RADIUS 프로브 또는 SNMP 트랩 프로브를 활성화해야 하며 연관된 구성 요소를 적절히 구성해야 합니다. 마지막으로 CDP 또는 LLDP 정보를 검색하려면 엔드포인트가 CDP 또는 LLDP를 지원해야 하며, 이러한 프로토콜 중 하나 또는 둘 모두가 액세스 스위치에서 활성화되어 있어야 합니다.

### ISE에서 SNMP 쿼리 프로브 활성화

- Step 1** Administration(관리)→System(시스템)→Deployment(구축)로 이동하고 RHS 창의 구축된 노드 목록에서 프로파일링을 수행할 정책 서비스 노드를 선택합니다.
- Step 2** Profiling Configuration(프로파일링 컨피그레이션) 탭을 선택하고 SNMP 쿼리 프로브를 활성화하기 위한 확인란을 선택합니다(그림 22).

그림 17 SNMP 쿼리 프로브 컨피그레이션



참고: SNMP 쿼리 프로브를 위한 인터페이스는 구성할 필요가 없습니다. 어플라이언스 라우팅 표에 따라 액세스 디바이스로 SNMP 쿼리가 전송됩니다.

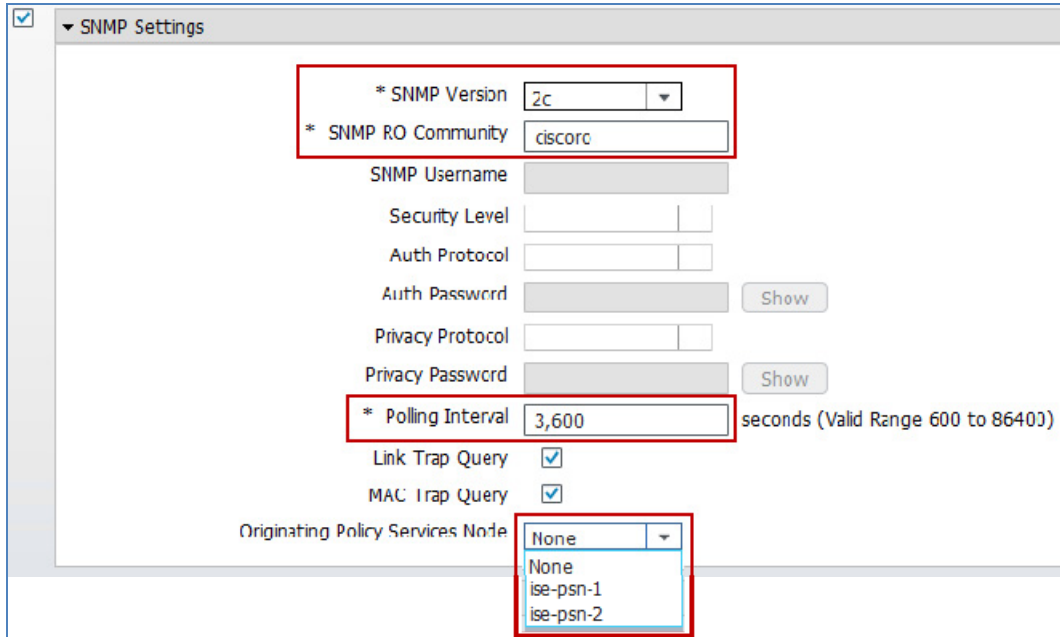
- Step 3** Retries(재시도 횟수), Timeout(시간 제한) 및 Event Timeout(이벤트 시간 제한)에 대해 기본값을 그대로 사용합니다.
- Step 4** Timeout(시간 제한)(밀리초)에서는 SNMP 응답을 대기하는 시간을 지정합니다.
- Step 5** Retries(재시도 횟수)에서는 정책 서비스 노드가 초기에 실패한 시도 이후에 SNMP 세션 설정을 위해 시도하는 횟수를 지정합니다.
- Step 6** EventTimeout(이벤트 시간 제한)(초)에서는 RADIUS 계정 관리 시작 또는 SNMP 트랩 트리거 이후에 일괄 처리된 쿼리를 액세스 디바이스에 전송하기 전까지 기다리는 시간을 지정합니다.
- Step 7** 트리거된 인터페이스 쿼리의 경우 RADIUS 프로브가 활성화되어 있는지 확인합니다. RADIUS가 네트워크 액세스 디바이스에 구성되지 않은 경우 SNMP 트랩 프로브가 활성화되어 있는지 확인합니다.
- Step 8** Save(저장)를 클릭하여 변경 사항을 커밋합니다.
- Step 9** 프로파일링 서비스를 사용하여 구성된 다른 모든 정책 서비스 노드에 대해 이 절차의 단계를 반복합니다.

### ISE(네트워크 리소스)에서 네트워크 디바이스 구성

일반적으로 RADIUS를 통해 엔드포인트를 인증하는 모든 네트워크 액세스 디바이스는 ISE에서 구성되므로 각 액세스 디바이스에 대해 SNMP 설정만 확인하면 됩니다. RADIUS 인증이 구축되지 않은 네트워크에 대해 SNMP 쿼리 프로브를 구성하는 경우 각 액세스 디바이스를 ISE 네트워크 디바이스 목록에 추가하고 선택적으로 레이어 3 디바이스(ARP 정보의 경우)를 선택해야 합니다.

- Step 1** Administration(관리) → Network Resources(네트워크 리소스) → Network Devices(네트워크 디바이스)로 이동합니다. SNMP를 사용하여 쿼리할 디바이스가 이미 있는 경우 목록에서 디바이스를 선택하기만 하면 됩니다. 그렇지 않으면 RHS 창에서 Add(추가)를 클릭합니다.
- Step 2** 새 디바이스의 경우 디바이스 이름 및 IP 주소 정보를 입력합니다.
- Step 3** SNMP Settings(SNMP 설정) 확인란에서 액세스 디바이스에 사용되는 SNMP 버전을 지정하고 SNMP 버전 1 및 2c의 SNMP RO 커뮤니티 문자열을 입력합니다. 아니면 액세스 디바이스에 해당하는 SNMPv3 자격 증명 및 컨피그레이션을 입력합니다(그림 23).

그림 18 네트워크 액세스 디바이스 컨피그레이션: SNMP 쿼리



- Step 4** 시스템(폴링) 쿼리의 경우 Polling Interval(폴링 간격) 및 Originating Policy Services Node(발신 정책 서비스 노드)를 설정합니다.
- Step 5** **Polling Interval(폴링 간격):** 일반적으로 RADIUS 또는 DHCP 프로브가 구축되어 있는 네트워크에서는 ARP 정보에 대한 의존도가 감소하므로 폴링 간격이 길수록 좋습니다.
- Step 6** **Originating Policy Services Node(발신 정책 서비스 노드):** SNMP 쿼리 프로브가 설정되어 있는 각 PSN이 목록에 나타납니다. 네트워크 디바이스의 주기적 폴링을 수행하기 위한 최적의 정책 서비스 노드를 선택합니다. 이는 일반적으로 네트워크 대역폭 측면에서 네트워크 디바이스에 가장 가까운 PSN이 됩니다.
- Step 7** SNMP 트랩을 사용하는 인터페이스(트리거) 쿼리의 경우 트랩 쿼리 옵션 중 하나 또는 둘 모두가 설정되어야 합니다.

**참고:** Originating Policy Services Node(발신 정책 서비스 노드) 설정은 인터페이스 쿼리에 적용되지 않는데 이러한 쿼리는 RADIUS 계정 관리 시작 또는 SNMP 트랩 메시지와 같은 트리거를 수신한 PSN에서 항상 전송되기 때문입니다.

- Step 8** 완료되면 변경 사항을 저장합니다.
- Step 9** ISE 정책 서비스 노드에서 SNMP를 사용하여 쿼리해야 하는 각 액세스 디바이스에 대해 위 단계를 반복합니다.

### ISE PSN에서 SNMP 쿼리를 수락하도록 유선 액세스 디바이스 구성

유선 액세스 디바이스의 관리 콘솔로 이동하고 SNMP 쿼리 프로브가 활성화되어 있는 ISE 정책 서비스 노드에서의 SNMP 읽기 전용 요청을 지원하도록 해당 액세스 디바이스가 구성되어 있는지 확인합니다.



다음은 IOS를 실행하는 Cisco Catalyst 스위치에서 읽기 전용 커뮤니티 문자열 **ciscoro**를 사용하여 ISE PSN의 SNMPv2c 쿼리를 지원하도록 구성한 예입니다.

```
snmp-server community ciscoro RO
snmp-server community ciscorw RW
```

### ISE PSN에서 SNMP 쿼리를 수락하도록 무선 액세스 디바이스 구성

Wireless LAN Controller의 웹 관리 인터페이스로 이동하고 이 컨트롤러가 SNMP 쿼리 프로브가 활성화되어 있는 ISE 정책 서비스 노드에서의 SNMP 읽기 전용 요청을 지원하도록 구성되어 있는지 확인합니다.

- Step 1** Management(관리) → SNMP → Communities(커뮤니티) → SNMP v1/v2c Community(SNMP v1/v2c 커뮤니티)로 이동하고 이 디바이스를 쿼리할 수 있는 ISE 정책 서비스 노드에 사용되는 하나 이상의 읽기 전용 커뮤니티 문자열을 구성합니다.
- Step 2** 다음 그림에서는 읽기 전용 커뮤니티 문자열 **ciscoro**를 사용하여 ISE PSN의 SNMPv2c 쿼리를 지원하도록 구성된 WLC의 컨피그레이션 예를 보여줍니다.

그림 19 무선 컨트롤러를 위한 SNMP 컨피그레이션 예

Management		SNMP v1 / v2c Community				
Summary		Community Name	IP Address	IP Mask	Access Mode	Status
▼ SNMP						
General		<a href="#">public</a>	0.0.0.0	0.0.0.0	Read-Only	Enable
SNMP V3 Users		<a href="#">private</a>	0.0.0.0	0.0.0.0	Read-Write	Enable
Communities		<b><a href="#">ciscoro</a></b>	10.1.0.0	255.255.0.0	Read-Only	Enable
Trap Receivers		<a href="#">ciscorw</a>	10.1.0.0	255.255.0.0	Read-Write	Enable
Trap Controls						
Trap Logs						

SNMPv3이 구축된 경우 Management(관리) → SNMP → SNMP V3 Users(SNMP V3 사용자)에서 적절한 설정을 구성해야 합니다.

### CDP 및 LLDP를 지원하도록 액세스 디바이스 구성

연결된 호스트에서 CDP 및 LLDP 정보를 검색하려면 스위치 포트에서 이러한 프로토콜을 수신하도록 액세스 디바이스가 구성되어 있는지 확인합니다. Cisco 디바이스에서는 대개 기본적으로 CDP가 활성화되어 있지만 LLDP는 활성화되어 있지 않습니다. 그러므로 SNMP 쿼리 프로브를 사용하여 이러한 정보를 수집하려면 전역적으로 LLDP를 활성화해야 합니다.

```
cdp run
interface <Endpoint_Interface>
  cdp enable
!
lldp run
interface <Endpoint_Interface>
  lldp receive
  lldp transmit
```

참고: Wireless LAN Controller는 무선 클라이언트에 대해 CDP/LLDP를 지원하지 않습니다.

### SNMP 쿼리 프로브 데이터 확인

- Step 1** Administration(관리) → Identity Management(ID 관리) → Identities(ID) → Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 2** ISE에서 SNMP 액세스에 대해 구성된 액세스 디바이스에서 엔드포인트의 연결을 해제했다가 다시 연결합니다.
- Step 3** ISE 정책 관리 노드로 이동하고 Administration(관리) → Identity Management(ID 관리) → Identities(ID)로 이동합니다.
- Step 4** LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 5** 새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 SNMP 쿼리 프로브에서 캡처한 특성을 표시합니다.

그림 25에 나타난 예는 SNMP 트랩 및 SNMP 쿼리 프로브만 사용하여 작성되었으며 SNMP 쿼리를 사용하여 수집된 특성이 강조 표시되어 있습니다. 강조 표시된 키 특성에는 **EndPointSource**, **cdpCacheAddress** 및 **cdpCachePlatform**이 있습니다.

- **EndPointSource**는 마지막 프로파일링 업데이트가 SNMP 쿼리 프로브에서 발생했음을 알려줍니다.
- **cdpCacheAddress**는 IP 주소를 제공하며 IP와 MAC 주소 간의 바인딩을 허용합니다.
- **cdpCachePlatform** 특성은 연결된 엔드포인트(이 예에서는 Cisco Aironet 1142N 무선 액세스 포인트에 해당하는 Cisco AIR-LAP1142N-A-K9)에 대한 자세한 설명을 제공합니다.

그림 20 SNMP 쿼리 프로브 특성 예

**Endpoint**

\* MAC Address **C4:71:FE:34:19:7A**

\* Policy Assignment **Cisco-Access-Point**

Static Assignment

\* Identity Group Assignment **Cisco-Access-Point**

Static Group Assignment

**Attribute List**

EndPointPolicy	Cisco-Access-Point
EndPointProfilerServer	ise-psn-1
EndPointSource	SNMPQuery Probe
IdentityGroup	Cisco-Access-Point
MACAddress	C4:71:FE:34:19:7A
MatchedPolicy	Cisco-Access-Point
NADAddress	10.1.50.2
OUI	Cisco Systems
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	24
Total Certainty Factor	20
Vlan	14
VlanName	WIRELESS
cdpCacheAddress	10.1.14.100
cdpCacheCapabilities	T
cdpCacheDeviceId	APc471.fe34.197a
cdpCachePlatform	cisco AIR-LAP1142N-A-K9
cdpCacheVersion	Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE SOFTWARE Copyright (c) 1986-2012 by Cisco Systems, Inc. Compiled Fri 27-Jan-12 21:45 by prod_rel_team
dot1xAuthAuthControlledPortControl	3
dot1xAuthAuthControlledPortStatus	2
ifDescr	GigabitEthernet1/0/2
ifIndex	10102
ifOperStatus	1
ip	10.1.14.100
port	2

**Step 6** 예상되는 특성 데이터를 확인하려면 액세스 스위치 콘솔에서 다음 명령을 사용하십시오.

```
switch# show cdp neighbor detail
switch# show lldp neighbor detail
```

### DHCP 및 DHCP SPAN 프로브를 사용한 프로파일링

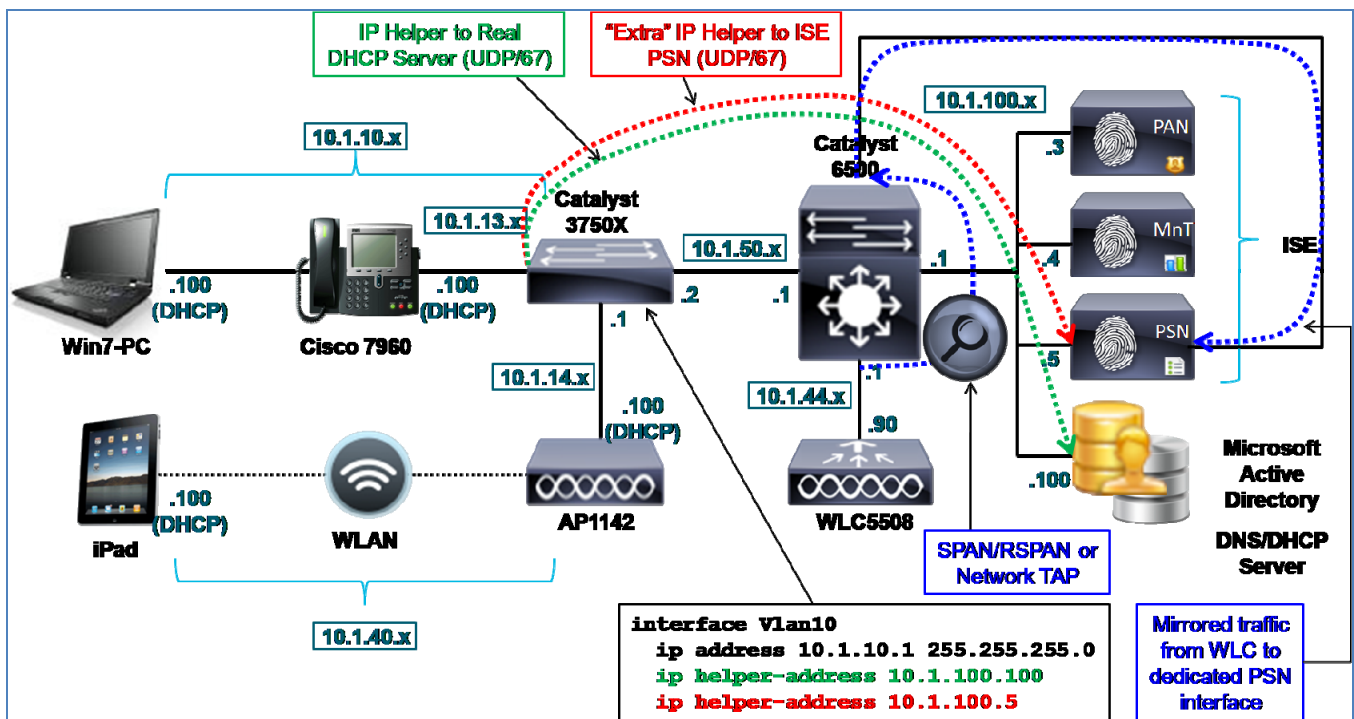
이름에서 알 수 있듯이 DHCP 프로브는 DHCP 패킷에서 특성을 수집합니다. DHCP 특성은 다음 중 하나 또는 둘 모두를 사용하여 수집할 수 있습니다.

- DHCP 프로브
- DHCP SPAN 프로브

### DHCP 프로브

DHCP 프로브는 예를 들어, 네트워크에서 DHCP 릴레이 기능의 결과로 DHCP 요청이 직접 ISE 정책 서비스 노드로 전송되는 방법에 사용됩니다. Cisco 네트워크의 공통 DHCP 릴레이는 로컬 DHCP 클라이언트용 게이트웨이에 해당하는 레이어 3 인터페이스에 적용되는 `ip helper-address` 명령입니다. 그림 26에는 DHCP 프로브를 사용하는 토폴로지 예가 나와 있습니다.

그림 21 DHCP 프로브 예



이 다이어그램의 Cisco Catalyst 3750-X에는 Employee Data VLAN 10과 Voice VLAN 13 모두가 있습니다. 각 SVI(Switched Virtual Interface)의 인터페이스 컨피그레이션에는 로컬 DHCP 브로드캐스트 패킷을 10.1.100.100의 실제 DHCP 서버로 전달하는 `ip helper-address` 명령이 있습니다(그림 26에서 녹색으로 강조 표시됨). 이는 DHCP 요청에 응답하는 서버입니다. 동일한 인터페이스에는 DHCP 프로브와 함께 활성화된 ISE PSN 인터페이스를 가리키도록 또 다른 `ip helper-address` 명령이 구성되어 있습니다(빨간색으로 강조 표시됨). ISE 정책 서비스 노드는 이러한 패킷에 응답하지 않지만 목표는 DHCP 특성을 구문 분석할 수 있도록 요청 사본을 ISE로 보내는 것입니다.

여러 ISE 정책 서비스 노드가 DHCP 요청 사본을 수신할 수 있도록 Cisco 디바이스에서 여러 IP Helper 대상을 구성할 수 있습니다.

**참고:** ISE DHCP 프로브는 DHCP 릴레이와 DHCP 프록시 모두에서 발생하는 트래픽을 구문 분석할 수 있습니다. 이러한 두 방법의 주요 차이점은 ip helper-address 명령을 통한 DHCP 릴레이는 트래픽을 여러 대상에 보낼 수 있다는 것입니다. 따라서 여러 개의 실제 DHCP 서버 및 ISE 정책 서비스 노드에서 DHCP 요청 사본을 수신할 수 있습니다. 반면, DHCP 프록시는 요청을 기본 DHCP 서버에만 보내며 올바른 응답을 받지 못할 경우 구성된 다른 DHCP 대상으로 폴백됩니다. ISE 노드를 실제 DHCP 서버로의 폴백을 허용하는 첫 번째 항목으로 구성할 수 있지만 그러한 구현에서는 엔드포인트에서 IP 주소를 얻는 데 필요한 시간이 지연됩니다. 이는 사용자 환경에 영향을 미칠 수 있지만 응답을 기다리는 클라이언트 시간이 초과될 수도 있습니다.

### DHCP SPAN 프로브

DHCP SPAN 프로브는 트래픽이 SPAN(Switch Port Analyzer), RSPAN(Remote SPAN) 또는 Network TAP과 같은 방법을 사용하여 ISE 정책 서비스 노드의 인터페이스에 미러링되는 경우에 사용하도록 설계되었습니다. 이 방법은 기본적으로 DHCP 릴레이를 활용하는 기본 DHCP 프로브가 제공되지 않거나 사용할 수 없는 경우에 사용됩니다.

**모범 사례:** 지정된 DHCP 트래픽 흐름에 대해 해당 트래픽에서 특성을 수집할 때 하나의 프로브만 선택해야 합니다. DHCP(IP Helper) 및 DHCP SPAN 프로브 모두를 사용하여 같은 DHCP 트래픽에서 특성을 수집하는 경우 값이 제한됩니다.

사용 가능한 경우, DHCP SPAN 프로브 대신 DHCP 프로브를 사용하는 것이 좋습니다. DHCP 릴레이를 통해 DHCP 패킷만 전송하면 DHCP 패킷에서 특성을 검사하고 구문 분석하기 위한 ISE 정책 서비스 노드의 전반적인 트래픽 부하가 줄어듭니다.

DHCP SPAN 프로브는 또한 로컬 서브넷 브로드캐스트에서 DHCP 트래픽을 캡처하는 데에도 사용할 수 있는 반면, DHCP 프로브를 사용하면 업스트림 게이트웨이에서 릴레이되는 DHCP 트래픽만 캡처할 수 있습니다. 이는 레이어 3 게이트웨이가 로컬 클라이언트의 DHCP 서버에도 해당하는 경우에 필요할 수 있습니다. Cisco IOS DHCP 서버는 서브넷에 대한 DHCP를 지원하도록 구성된 경우 세그먼트에 대해 DHCP를 릴레이하지 않습니다.

샘플 토폴로지에서는 SPAN 또는 Network TAP을 사용하여 WLC에 연결된 무선 클라이언트에서 정책 서비스 노드의 전용 인터페이스로 패킷을 복사하는 방법을 보여줍니다(그림 26에서 파란색으로 강조 표시됨). SPAN 대상 포트에는 PSN으로 이동하는 정상적인 트래픽의 송수신을 제한하는 특정한 속성이 있을 수 있으므로 전용 인터페이스가 필요합니다. 또한 미러링되는 트래픽은 RADIUS와 같은 PSN의 다른 중요한 인터페이스에서 혼잡을 유발하므로 권장되지 않습니다. SPAN 방식을 사용하면 SPAN 포트가 처리할 수 있는 것보다 더 많은 데이터를 SPAN 포트에 보내므로 패킷이 삭제되거나 중요한 트래픽이 지연될 수 있습니다.

### DHCP 특성

DHCP 및 DHCP SPAN 프로브는 모두 동일한 주요 프로파일링 특성을 ISE에 전달합니다. 그러한 특성의 일부는 다음과 같습니다.

- dhcp-class-identifier
- dhcp-user-class-id
- dhcp-client-identifier
- dhcp-message-type
- dhcp-parameter-request-list
- dhcp-requested-address

- host-name
- domain-name
- client-fqdn

DHCP는 MAC 주소(**dhcp-client-identifier**)와 IP 주소(**dhcp-requested-address**)를 모두 제공하므로 ISE ARP 캐시 표에 대한 IP-MAC 주소 바인딩도 설정할 수 있습니다. 이는 MAC 주소 대신 IP 주소를 사용하는 다른 프로브를 지원하는 데 유용합니다. 특정 엔드포인트에 대해 제공하는 특성을 적용하고 ISE 데이터베이스에 저장하려면 IP 주소를 MAC 주소에 따라 특정 엔드포인트와 상호 연결해야 합니다.

**dhcp-client-identifier** 및 **dhcp-requested-address** 외에 다른 키 특성에는 **dhcp-class-identifier**, **dhcp-user-class-id** 및 **dhcp-parameters-request-list**가 있습니다. 클래스 식별자는 주로 플랫폼 또는 OS 정보를 전달하는 데 사용됩니다. 클래스 식별자 및 사용자 클래스 ID는 각각 Mac OS 및 Microsoft Windows와 같은 일부 클라이언트 운영 체제에서 프로파일링을 위한 고유한 기업 식별자로 사용되거나 DHCP 서버에서 고유한 범위 값을 반환하도록 사용자 지정할 수 있습니다.

**dhcp-parameters-request-list**는 디바이스 유형에 대해 잠재적으로 고유한 표시기를 제공합니다. 요청된 매개변수의 값과 시퀀스는 대개 단일 또는 제한된 디바이스 유형 집합에 고유합니다. 예를 들어 **dhcp-parameters-request-list** 값인 1, 3, 6, 15, 119, 252는 iPad, iPod 또는 iPhone과 같은 Apple iOS 디바이스를 나타냅니다.

표준 호스트 이름, 도메인 이름 또는 FQDN(정규화된 도메인 이름) 명명 규칙이 특정 엔드포인트에 구축된 경우 이들 특성은 그러한 항목을 분류하는 데 사용될 수 있습니다. 예를 들어 모든 Windows XP 클라이언트에 **jsmith-winxp**와 같은 이름이 할당된 경우 Windows XP 엔드포인트를 분류하기 위한 조건에서 **host-name** 특성 또는 **client-fqdn** 특성을 사용할 수 있습니다. 마찬가지로, **jsmith-corp-dept**와 같이 기업 엔드포인트의 **host-name**을 채우는 규칙이 있는 경우 이 특성을 사용하여 기업 자산을 검증할 수 있습니다.

프로파일 특성을 ID와 혼동하지 않도록 주의해야 합니다. 특성에서 엔드포인트가 특정 유형임을 나타내는 특정 신뢰도 레벨을 추가할 수 있습니다. 예를 들어 프로파일링에 권한 부여 정책을 사용하여 직원에 대한 전체 액세스 권한을 거부할 수 있습니다. 이 경우 PC의 **host-name** 특성(일치하는 엔드포인트 ID 그룹으로 표시됨)에 예상 값이 포함되지 않습니다.

일반적으로 DHCP는 다양한 프로파일링 이점을 제공하며, 대부분의 엔드포인트는 자세한 플랫폼 정보와 함께 DHCP“지문”을 제공하므로 특정 환경에서 상당 부분의 엔드포인트를 분류하기 위한 토대가 됩니다.

## DHCP 및 DHCP SPAN 프로브 구성

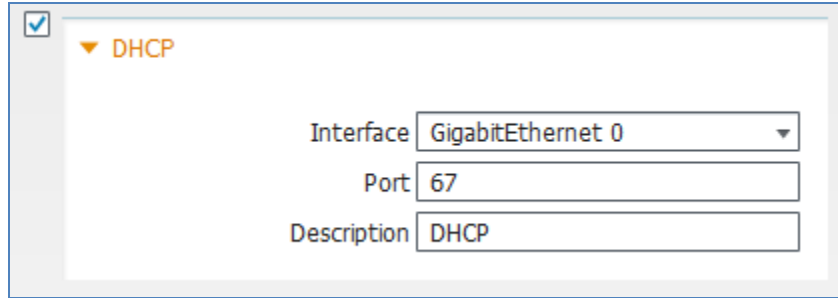
DHCP 프로브를 사용하려면 DHCP 릴레이 또는 DHCP 프록시 패킷을 프로파일링 서비스용으로 구성된 ISE PSN으로 전송하도록 액세스 디바이스(또는 레이어 2 전용 액세스 디바이스의 다음 홉 게이트웨이)를 구성해야 합니다. DHCP SPAN 프로브를 사용하려면 네트워크에서 전용 인터페이스를 통해 네트워크 트래픽(DHCP만 포함하도록 필터링된 트래픽 하위 집합이 선호됨) 사본을 ISE PSN으로 전송해야 합니다.

DHCP 기반 프로브를 효과적으로 사용하기 위한 또 다른 요구 사항은 대상 엔드포인트가 DHCP를 사용하여 IP 주소를 가져와야 한다는 것입니다. 이는 당연한 것으로 보일 수 있지만, 다수의 고객은 고정 IP 주소가 할당되어 있는 클라이언트리스 디바이스를 보유하고 있을 수 있습니다. 이 경우 엔드포인트에서 특정 IP 주소를 유지할 수 있도록 정적 DHCP 예약 항목을 구축할 수 있으며, 그와 동시에 DHCP를 통해 IP 주소를 중앙 집중식으로 관리하고 ISE 프로파일링을 지원할 수 있습니다.

### ISE에서 DHCP 프로브 활성화

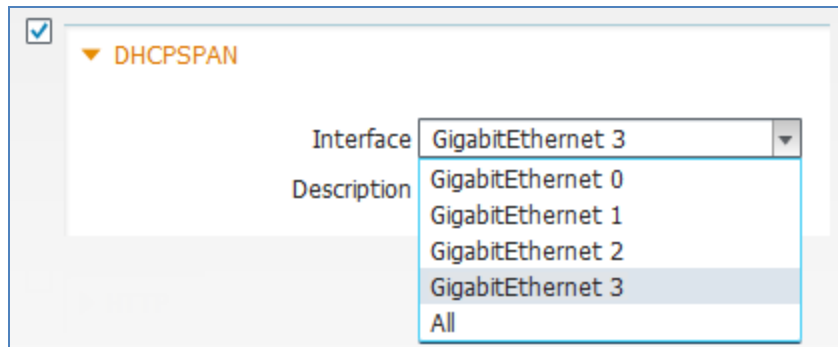
- Step 1** Administration(관리) → System(시스템) → Deployment(구축)로 이동하고 RHS 창의 구축된 노드 목록에서 프로파일링을 수행할 정책 서비스 노드를 선택합니다.
- Step 2** Profiling Configuration(프로파일링 컨피그레이션) 탭을 선택합니다.
- Step 3** DHCP 프로브에 대한 지원을 추가하려면(예: IP Helper에 사용) 그림 27의 왼쪽 상단 모서리에 표시된 것처럼 DHCP라는 확인란을 선택합니다.

그림 22 DHCP 프로브 컨피그레이션



- Step 4** DHCP SPAN 프로브에 대한 지원을 추가하려면(SPAN 또는 다른 포트 미러링 솔루션에 사용) DHCPSPAN이라는 확인란을 선택합니다(그림 28).

그림 23 DHCP 프로브 컨피그레이션 - 인터페이스



- Step 5** DHCP 트래픽 수집에 사용할 인터페이스를 선택합니다.

IP Helper(DHCP 릴레이)에 사용되는 경우 인터페이스에는 주로 세션 서비스에 사용되는 기본 인터페이스가 사용됩니다. 그러나 더 많은 양의 DHCP 트래픽이 예상되는 대규모 환경에서는 전용 인터페이스(예: GigabitEthernet 1, 2 또는 3)를 사용해야 할 수 있습니다.

미러링되는 트래픽(SPAN/RSPAN/TAP)에 사용되는 경우 이는 전용 인터페이스여야 합니다.

- Step 6** Save(저장)를 클릭하여 변경 사항을 커밋합니다.
- Step 7** 프로파일링 서비스를 사용하여 구성된 다른 모든 정책 서비스 노드에 대해 이 절차의 단계를 반복합니다.

**참고:** 트래픽 미러링에 대한 요구 사항으로 인해 SPAN을 수신하도록 여러 정책 서비스 노드를 구성하는 것이 불가능하거나 실행 가능하지 않을 수 있습니다. 동일한 트래픽 흐름을 미러링하는 경우 동일한 트래픽을 여러 정책 서비스 노드에 전달하는 것은 적합하지 않을 수 있습니다. 일부 이중화를 추가하더라도, 이렇게 하면 ISE 노드에 대한 부하가 크게 가중될 수 있으며 다른 노드에서 상호 연결되고 동기화되어야 하는 불필요한 프로파일링 데이터 중복이 발생할 수 있습니다.

**ISE(네트워크 리소스)에 네트워크 디바이스 추가**

RADIUS 또는 SNMP를 지원하는 액세스 디바이스가 이미 ISE 네트워크 디바이스 목록에 추가(Administration(관리) → Network Resources(네트워크 리소스) → Network Devices(네트워크 디바이스) 아래)되어 있을 수 있지만 DHCP를 DHCP 프로브 또는 DHCP SPAN 프로브로 전달하기 위한 목적으로만 네트워크 디바이스를 ISE에 추가할 필요는 없습니다.

**DHCP 릴레이 패킷을 수신하도록 ISE 정책 서비스 노드 인터페이스 구성 (DHCP 프로브만 해당)**

DHCP 프로브가 기본 GigabitEthernet 0 인터페이스에서 활성화된 경우 이 절차는 완전한 절차입니다. DHCP 릴레이 트래픽을 수신하는 데 또 다른 인터페이스를 사용하는 경우 다음 단계를 완료하십시오.

- Step 1** 원하는 인터페이스를 네트워크 스위치 포트에 물리적으로 연결합니다.
- Step 2** ISE PSN 콘솔(CLI)에 액세스합니다. 해당 인터페이스를 활성화하고 그림 29와 같이 올바른 IP 주소를 할당합니다.

그림 24 액세스 스위치에 대한 DHCP 릴레이 컨피그레이션 예

```
ise-psn-1/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise-psn-1/admin(config)# interface GigabitEthernet 3
ise-psn-1/admin(config-GigabitEthernet)# ip address 10.1.99.100 255.255.255.0

Changing the IP may result in undesired side effects on
any installed application(s).
Are you sure you want to proceed? Y/N [N]: Y
ISE M&T Log Processor is not running.
ISE M&T Log Collector is not running.
ISE M&T Alert Process is not running.
Stopping ISE Application Server...
ISE M&T Session Database is not running.
Stopping ISE Database processes...
Starting ISE Database processes...
ISE M&T Session Database is not running.
Starting ISE Application Server...
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.
ise-psn-1/admin(config-GigabitEthernet)# _
```

- Step 3** 지침에 따라 모든 프로세스가 실행 중인 상태인지 확인합니다.
- Step 4** **show running-config** 명령을 사용하여 새로 구성된 인터페이스의 컨피그레이션을 확인하고 활성화(종료되지 않음)되어 있는지 확인합니다(그림 30).



그림 25 액세스 스위치에 대한 DHCP 릴레이 컨피그레이션 확인 예

```
ise-psn-1/admin# show running-config
Generating configuration...
?
hostname ise-psn-1
?
ip domain-name cts.local
?
interface GigabitEthernet 0
  ip address 10.1.100.5 255.255.255.0
  ipv6 address autoconfig
?
interface GigabitEthernet 1
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 2
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 3
  ip address 10.1.99.100 255.255.255.0
  ipv6 address autoconfig
?
ip name-server 10.1.100.100
--More--
```

- Step 5 DHCP를 릴레이해야 하는 네트워크 디바이스에서 ICMP ping을 전송하여 새 ISE 프로브 인터페이스에 대한 연결을 확인합니다.
- Step 6 CLI 명령 `copy running-config startup-config`를 사용하여 변경 내용을 저장합니다.

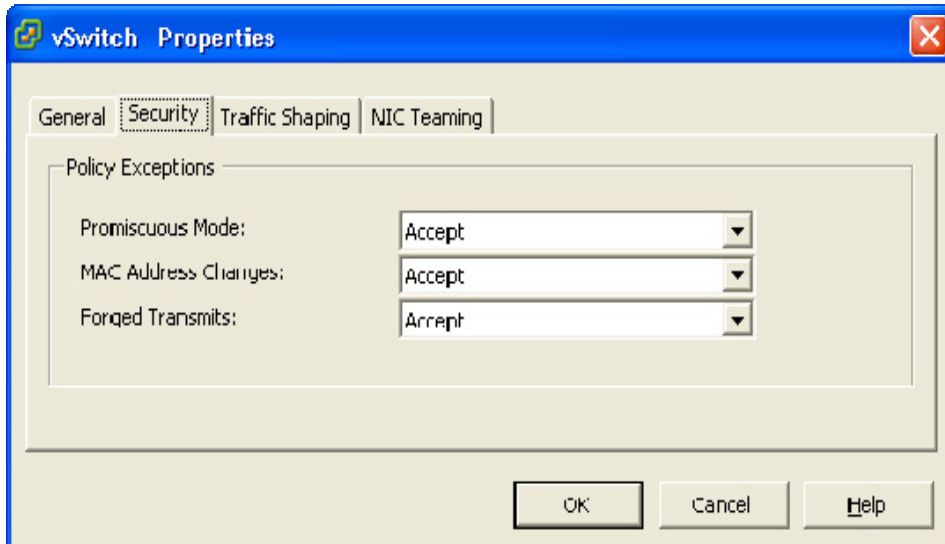
**SPAN 트래픽을 수신하도록 ISE 정책 서비스 노드 인터페이스 구성 (DHCP SPAN 프로브만 해당)**

- Step 1 원하는 인터페이스를 해당 SPAN 대상 포트 또는 Network TAP 인터페이스에 물리적으로 연결합니다.
- Step 2 ISE PSN 콘솔(CLI)에 액세스합니다. 원하는 인터페이스에 대한 컨피그레이션 모드에서 `no shutdown`을 입력하면 해당 인터페이스가 활성화됩니다.
- Step 3 ISE CLI 명령 `copy running-config startup-config`를 사용하여 변경 내용을 저장합니다.

**참고: VMware 어플라이언스에서 실행되는 정책 서비스 노드의 경우**

프로파일링에 전용 인터페이스를 사용하기 위해 가상 어플라이언스에 대한 추가 가상 인터페이스가 구성되어 있는 것으로 가정합니다. 설치 시 완료하지 않은 경우 ISE 노드를 종료하고 필수 인터페이스에 맞게 ESX 어플라이언스의 하드웨어 및 네트워킹 컨피그레이션을 업데이트해야 ISE 컨피그레이션을 계속 진행할 수 있습니다.

또한 ISE DHCP SPAN 인터페이스에서 SPAN/미러 트래픽을 수락하려면 VMware 어플라이언스에서 가상 스위치 인터페이스에 대해 무차별 모드를 설정해야 합니다. 이 모드를 활성화하려면 VMware Host(VMware 호스트) → Configuration(컨피그레이션) → Hardware(하드웨어) → Networking(네트워킹) → vSwitch(스위치) → Security(보안)로 이동하고 다음과 같이 Promiscuous Mode(무차별 모드): Accept(수락)(기본값 = Reject(거부))를 설정합니다.



**DHCP 패킷을 ISE PSN으로 릴레이하도록 유선 액세스 디바이스 구성(DHCP 프로브만 해당)**

Cisco Catalyst 스위치 또는 라우터의 관리 콘솔로 이동합니다. DHCP 트래픽이 발생하는 엔드포인트 서브넷에 연결되는 라우팅된 각 인터페이스에서 다음 명령을 추가하십시오.

```
interface <Endpoint_VLAN>
 ip helper-address <ISE_PSN_address>
```

지정된 주소는 DHCP 프로브가 활성화되어 있는 PSN 인터페이스 주소여야 합니다. 이중화를 위해 DHCP를 다른 정책 서비스 노드로 릴레이하기 위한 IP Helper 명령문을 더 추가할 수 있지만, 각 PSN에서 수신되는 트래픽을 처리하므로 트래픽 중복을 최소화하기 위해 해당 명령문을 최소화하는 것이 좋습니다.

**DHCP 패킷을 ISE PSN으로 릴레이하도록 무선 액세스 디바이스 구성(DHCP 프로브만 해당)**

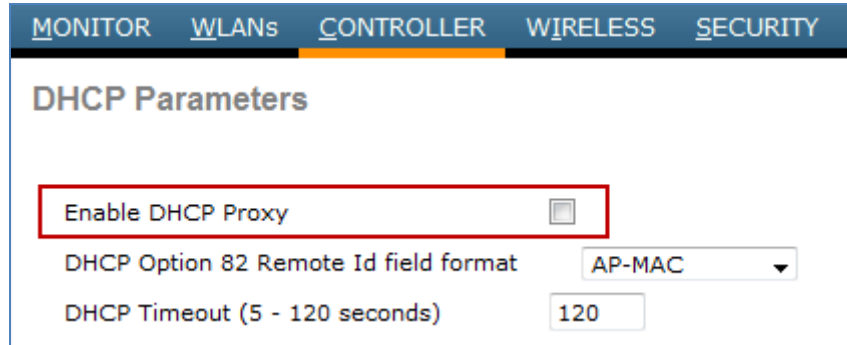
모든 DHCP 패킷이 무선 클라이언트에서 ISE PSN으로 전달되도록 DHCP 프록시 모드가 아닌 DHCP 브리징 모드에서 WLC를 구성하는 것이 좋습니다.

Cisco Wireless LAN Controller 또는 Wireless Services Module의 웹 관리 인터페이스로 이동합니다.

**Step 1** Controller(컨트롤러)→Advanced(고급)→DHCP→DHCP Parameters(DHCP 매개변수)로 이동합니다.

**Step 2** Enable DHCP Proxy(DHCP 프록시 활성화)라는 확인란이 선택되어 있는 경우 선택을 취소합니다(그림 31).

그림 26 무선 컨트롤러를 위한 DHCP 릴레이 컨피그레이션 예



**Step 3** WLC에서 DHCP를 사용하여 구성된 각 WLAN의 경우 이전 절차에 설명된 것처럼 DHCP를 ISE 정책 서비스 노드로 릴레이하도록 업스트림 게이트웨이를 구성해야 합니다.

**DHCP 트래픽 사본을 PSN으로 전송하도록 네트워크 디바이스 구성(DHCP SPAN 프로브만 해당)**  
 트래픽을 ISE 정책 서비스 노드에 미러링하는 방법에는 여러 가지가 있습니다. 이 절차에서는 Cisco Catalyst 스위치에서 기본 SPAN을 사용하는 일반적인 한 방법을 보여줍니다.

DHCP 트래픽의 소스가 되는 인터페이스 또는 VLAN을 확인합니다. WLC의 이그레스(egress) 인터페이스 또는 DHCP 서버에 대한 연결과 같은 특정 검사점은 모든 클라이언트 DHCP 패킷을 캡처하기 위한 이상적인 위치가 될 수 있습니다.

다음 예에서 인터페이스 GigabitEthernet 1/1은 Cisco 5500 Series Wireless LAN Controller에 대한 트렁크 연결입니다. 인터페이스 GigabitEthernet 2/37은 VMware ESXi 4.1을 실행하는 Cisco UCS® 서버에 대한 스위치 포트 연결입니다. ESX 서버는 프로파일링이 활성화되어 있는 정책 서비스 노드로 구성된 ISE 가상 어플라이언스를 호스팅합니다. 인터페이스 GigabitEthernet 2/37은 기가비트 이더넷 3으로 ISE PSN에 연결된 가상 인터페이스 링크입니다.

```
interface GigabitEthernet1/1
description WLC5508 ETH0 (Port 1)
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 40-44
switchport mode trunk

interface GigabitEthernet2/37
description UCS1 SPAN (port 3 of 4)
switchport
```

5500 Series 스위치 연결에서 모든 인바운드 및 아웃바운드 트래픽을 캡처하고 ISE PSN 연결로 전달하도록 SPAN을 구성합니다. 이를 위해 인터페이스 GigabitEthernet 1/1이 SPAN 소스로 설정되어 있으며 대상은 인터페이스 GigabitEthernet 2/37입니다. ISE는 태그가 지정된 패킷을 인식할 필요가 없으므로 802.1Q 트렁킹은 스위치 포트에서 활성화되지 않습니다.

```
cat6500(config)# monitor session 1 source interface gigabitEthernet 1/1 both
cat6500(config)# monitor session 1 destination interface gigabitEthernet 2/37
```

컨피그레이션을 확인하고 저장합니다.

```
cat6500# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
  Both              : Gi1/1
Destination Ports   : Gi2/37

Egress SPAN Replication State:
Operational mode    : Centralized
Configured mode     : Centralized (default)
```

### DHCP 프로브 데이터 확인

- Step 1** Administration(관리) → Identity Management(ID 관리) → Identities(ID) → Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 2** 게이트웨이 인터페이스에 DHCP를 ISE PSN으로 전달하는 IP Helper가 있는 액세스 디바이스에서 엔드포인트의 연결을 해제했다가 다시 연결합니다.
- Step 3** ISE 정책 관리 노드로 이동하고 Administration(관리) → Identity Management(ID 관리) → Identities(ID)로 이동합니다.
- Step 4** LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 5** 새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 DHCP 프로브에서 캡처한 특성을 표시합니다(그림 32). 표시된 예는 DHCP 프로브만 사용하여 작성되었으며 DHCP를 사용하여 수집된 특성이 강조 표시되어 있습니다.

그림 27 DHCP 프로브 특성 예

Endpoint List > 00:30:94:C4:52:8A

### Endpoint

\* MAC Address **00:30:94:C4:52:8A**

\* Policy Assignment

Static Assignment

\* Identity Group Assignment

Static Group Assignment

### Attribute List

EndPointPolicy	Cisco-IP-Phone
EndPointProfilerServer	ise-psn-1
<b>EndPointSource</b>	<b>DHCP Probe</b>
IdentityGroup	Cisco-IP-Phone
MACAddress	00:30:94:C4:52:8A
MatchedPolicy	Cisco-IP-Phone
<b>OUI</b>	<b>Cisco Systems, Inc</b>
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	24
Total Certainty Factor	30
chaddr	00:30:94:c4:52:8a
ciaddr	0.0.0.0
<b>dhcp-class-identifier</b>	<b>Cisco Systems, Inc. IP Phone CP-7960</b>
<b>dhcp-client-identifier</b>	<b>01:00:30:94:c4:52:8a</b>
dhcp-message-type	DHCPDISCOVER
<b>dhcp-parameter-request-list</b>	<b>1, 66, 6, 3, 15, 150, 35</b>
<b>dhcp-requested-address</b>	<b>10.1.13.100</b>
flags	0x8000
giaddr	10.1.13.1
hlen	6
hops	1
host-name	SEP003094C4528A
htype	Ethernet (10Mb)
ip	10.1.13.100
op	BOOTREQUEST
secs	0
yiaddr	0.0.0.0

다음과 같은 키 특성이 강조 표시되어 있습니다.

- EndPointSource
- OUI
- dhcp-class-identifier
- dhcp-client-identifier
- dhcp-parameter-request-list
- dhcp-requested-address

**EndPointSource**는 DHCP 프로브가 마지막 특성 업데이트의 소스임을 표시합니다.

**dhcp-client-identifier**는 일반적으로 MAC 주소를 제공하며, 그에 따라 MAC 주소-OUI 매핑 표에서의 상관 관계를 통해 공급업체 OUI 정보가 제공됩니다.

**dhcp-requested-address**는 엔드포인트에서 요청하는 IP 주소입니다. 이 특성은 **dhcp-client-identifier**와 함께 IP와 MAC 주소 간의 바인딩을 제공합니다.

**dhcp-class-identifier**는 대개 고유한 플랫폼별 특성을 제공하며 경우에 따라 연결된 엔드포인트에 대한 자세한 설명도 제공합니다(이 예에서는 Cisco Systems, Inc. IP Phone CP-7960).

정확한 시퀀스 1, 66, 6, 3, 15, 150, 35, 151은 일반적으로 특정 Cisco IP Phone에만 사용되므로 **dhcp-parameter-request-list**는 또한 엔드포인트가 Cisco IP Phone임을 나타냅니다.

요약하면, 하나 이상의 특성은 DHCP를 사용하여 네트워크 엔드포인트를 분류할 수 있습니다. 이 가이드의 [디바이스 센서](#) 섹션 뒷부분에 설명된 것처럼, Cisco는 디바이스 센서라고 하는 로컬 분류 기술을 사용하여 DHCP 및 다른 정보를 수집할 수 있는 기능을 제공합니다. 이 기능을 통해 IP Helper 또는 SPAN 기술을 통해 DHCP 특성을 수집할 수 없는 경우에도 DHCP 특성을 수집할 수 있습니다. 이 솔루션은 엔드포인트 특성 수집 및 분류를 위한 훨씬 확장성이 뛰어난 접근법을 제공합니다.

## HTTP 프로브를 사용한 프로파일링

웹 브라우저는 일반적으로 특성 식별 문자열을 웹 서버에 제출하는 방식으로 애플리케이션 유형, 운영 체제, 소프트웨어 공급업체 및 소프트웨어 버전을 포함하여 자체 식별합니다. HTTP에서 이러한 정보는 **User-Agent**라고 하는 HTTP 요청 헤더 필드로 전송됩니다.

**User-Agent**는 HTTP 프로브를 사용하여 수집되는 기본 특성입니다. ISE 프로파일링에서는 **User-Agent** 특성뿐 아니라 요청 메시지의 다른 HTTP 특성에서 웹 브라우저 정보를 캡처하여 엔드포인트 특성 목록에 추가합니다. Cisco ISE는 **User-Agent** 특성에 따라 엔드포인트를 식별할 수 있도록 시스템에 내장되어 있는 많은 기본 프로파일을 제공합니다.

HTTP 트래픽을 HTTP 프로브로 전송하는 데 사용되는 두 가지 방법은 다음과 같습니다.

- URL 리디렉션
- SPAN(및 다른 트래픽 미러링 방법)

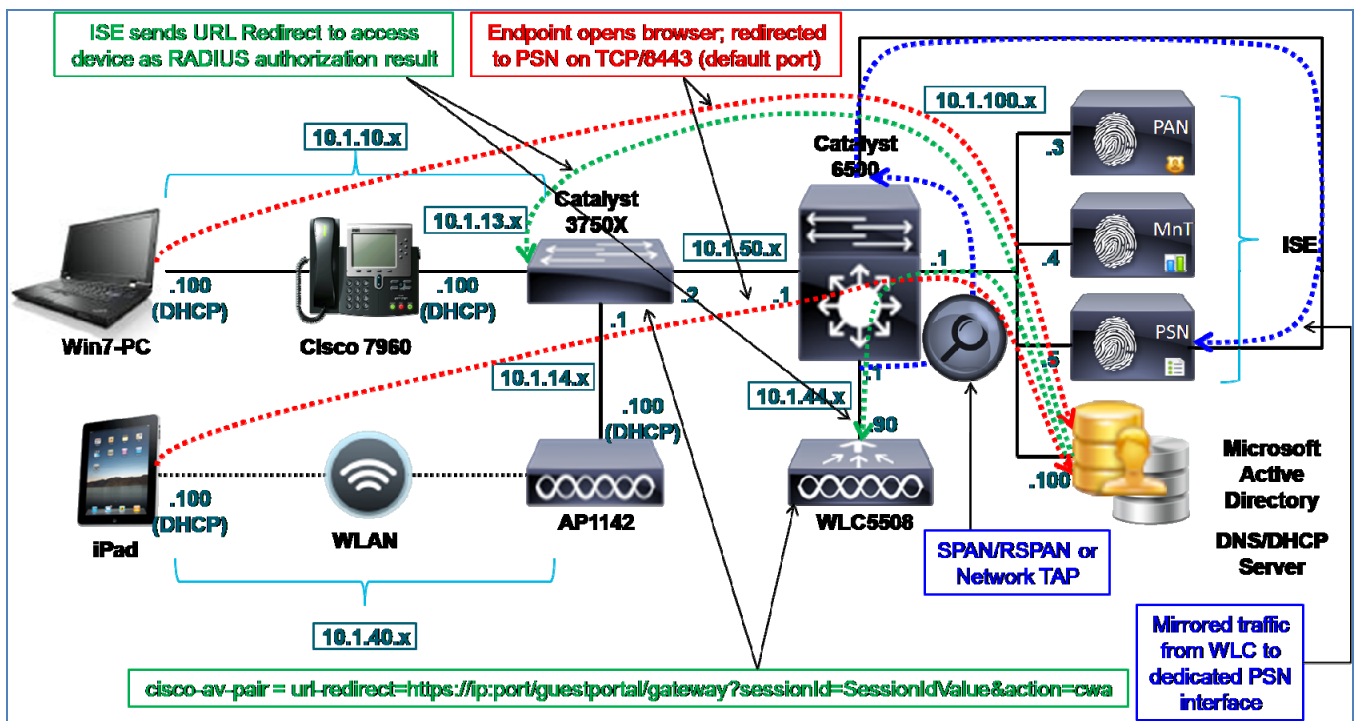
HTTP 프로브는 포트 80과 포트 8080 모두에서 웹 브라우저로부터의 통신을 수신 대기합니다. URL 리디렉션과 SPAN 방식은 모두 **User-Agent** 특성을 HTTP 프로브에 제공합니다.

### URL 리디렉션을 사용한 HTTP 프로브

ISE는 CWA(Central WebAuth), LWA(Local WebAuth), DRW(Device Registration WebAuth), 클라이언트 프로비저닝, Posture 평가 및 NSP(Native Supplicant Provisioning)를 비롯한 다수의 사용자 세션 서비스에 URL 리디렉션을 사용합니다. 이러한 각 활용 사례에서 엔드포인트의 웹 브라우저는 ISE 정책 서비스 노드로 리디렉션됩니다. 이러한 프로세스 중에 ISE에서 **User-Agent** 특성을 캡처할 수 있습니다.

그림 33의 샘플 토폴로지에는 엔드포인트 초기 권한 부여의 일부로 URL 리디렉션을 사용하고 ISE에서 액세스 디바이스로 URL 리디렉션을 전송할 수 있는 방법이 나와 있습니다(그림 33에서 녹색으로 강조 표시됨). 클라이언트에서 웹 브라우저를 열면, Central WebAuth와 같이 지정된 서비스의 정책 서비스 노드(빨간색으로 강조 표시됨)로 리디렉션됩니다.

그림 28 HTTP 프로브 예



URL 리디렉션은 NAD(네트워크 액세스 디바이스)의 기능일 수 있습니다. NAD로 시작된 리디렉션의 예에는 Local WebAuth가 있습니다. 이를 통해 무선 스위치 또는 무선 컨트롤러는 웹 인증 페이지를 제공하는 ISE Guest 포털로 클라이언트의 브라우저를 리디렉션합니다.

또한 ISE에서 네트워크 액세스 디바이스로의 RADIUS 권한 부여로 URL 리디렉션을 시작할 수 있습니다. RADIUS 권한 부여로 트리거되는 URL 리디렉션의 예에는 Central WebAuth가 있으며, 이를 통해 액세스 디바이스는 리디렉션을 더 효율적으로 진행할 수 있습니다. 그러나 실제 세션은 클라이언트와 ISE 정책 서비스 노드 간에 설정되며 고유한 세션 ID를 통해 추적됩니다.

## SPAN을 사용한 HTTP 프로브

URL 리디렉션 없이 HTTP 프로브를 사용하기 위한 선택적 방법은 SPAN, RSPAN 또는 Network TAP과 같은 방법을 사용하여 웹 트래픽을 ISE 정책 서비스 노드의 인터페이스로 복사하거나 미러링하는 것입니다. 이 방법은 URL 리디렉션이 불가능하거나 실행 가능하지 않을 때 기본적으로 사용됩니다.

**모범 사례:** RADIUS 기반 환경에서와 같이 적용 가능한 경우, URL 리디렉션은 HTTP SPAN보다 선호되는 방법입니다. 리디렉션 중에 키 **User-Agent** 특성만 캡처하면 HTTP 패킷에서 특성을 검사하고 구문 분석하기 위한 ISE 정책 서비스 노드의 전반적인 트래픽 부하가 줄어듭니다.

RADIUS 기반 인증을 사용하지 않는 Cisco NAC Appliance 구축 환경이나 RADIUS가 아직 액세스 디바이스에 구축되지 않은 엔드포인트 검색 단계에서와 같이 URL 리디렉션이 적용되지 않는 경우 기본 방법은 SPAN입니다. 그 이유는 요구 사항으로 RADIUS 또는 URL 리디렉션 없이도 **User-Agent**를 캡처할 수 있기 때문입니다.

그림 33의 샘플 토폴로지에서는 SPAN 또는 Network TAP을 사용하여 WLC에 연결된 무선 클라이언트에서 정책 서비스 노드의 전용 인터페이스로 패킷을 복사하는 방법을 보여줍니다(파란색으로 강조 표시됨). SPAN 대상 포트에는 PSN으로 이동하는 정상적인 트래픽의 송수신을 제한하는 특정한 속성이 있을 수 있으므로 전용 인터페이스가 필요합니다. 또한 미러링되는 트래픽은 RADIUS와 같은 PSN의 다른 중요한 인터페이스에서 혼잡을 유발하므로 권장되지 않습니다. SPAN 방식을 사용하면 SPAN 포트가 처리할 수 있는 것보다 더 많은 데이터를 SPAN 포트에 보내므로 패킷이 삭제되거나 중요한 트래픽이 지연될 수 있습니다.

## HTTP 프로브 및 IP-MAC 주소 바인딩 요구 사항

HTTP 트래픽은 엔드포인트의 MAC 주소를 포함하지 않으므로, HTTP 프로브로 전송되는 데이터를 적절히 상호 연결하기 위해서는 ISE 정책 서비스 노드의 ARP 캐시 표에 이미 엔드포인트에 대한 IP-MAC 주소 바인딩이 있어야 합니다. 즉, 엔드포인트가 해당 MAC 주소로 ISE에 알려지지 않은 경우 또는 연결된 IP 주소가 없는 경우에는 학습된 **User-Agent** 특성을 적용할 수 있는 엔드포인트가 없으므로 HTTP 프로브에서 학습된 프로파일링 데이터가 삭제됩니다. 따라서 HTTP 데이터를 수집하기 전에 다른 프로브를 통해 IP-MAC 주소 바인딩을 학습해야 합니다. 이 정보를 제공하는 데 사용할 수 있는 프로브는 다음과 같습니다.

- RADIUS(**Framed-IP-Address** 특성을 통해)
- DHCP(**dhcp-requested-address** 특성을 통해)
- SNMP 쿼리(SNMP 폴링을 통해)

IP-MAC 바인딩 요구 사항에 대한 예외를 제공하는 특정한 HTTP 프로파일링 시나리오가 있습니다. 예를 들면 다음과 같습니다.

- 클라이언트 프로비저닝을 사용한 URL 리디렉션
- Central WebAuth를 사용한 URL 리디렉션

## 클라이언트 프로비저닝을 사용한 URL 리디렉션

CP(클라이언트 프로비저닝)는 Posture 에이전트 및 NSP(Native Supplicant Provisioning) 서비스를 활성화할 수 있도록 에이전트 및 컨피그레이션 파일을 엔드포인트로 동적으로 다운로드하는 ISE 세션 서비스입니다. 클라이언트 프로비저닝에서는 URL 리디렉션을 사용합니다. CP 프로세스 중에 정책 서비스 노드는 사용자 에이전트를 통해 적용할 프로비저닝 정책을 파악하기 위한 클라이언트 OS를 판단해야 합니다. 예를 들어 엔드포인트가 Windows 클라이언트로 탐지되는 경우 포스처 지원을 위한 Windows 포스처 에이전트를



선택해야 합니다. 마찬가지로 엔드포인트가 Android 클라이언트로 탐지되는 경우 Android 클라이언트용 Supplicant Provisioning 파일을 엔드포인트에 설치해야 합니다.

클라이언트 프로비저닝 서비스에서 **User-Agent** 특성을 학습하는 경우 ISE는 프로파일링 서비스를 이 정보로 업데이트하여 이 정보를 사용합니다. 또한 클라이언트 프로비저닝은 활성 세션에 포함되므로 ISE는 세션 캐시에서 검색되는 MAC 주소(**Calling-Station-ID**)에 이 정보를 적용할 수 있습니다. 이 프로세스만 사용해도 다수의 여러 엔드포인트를 완전히 프로파일링할 수 있습니다.

### Central WebAuth를 사용한 URL 리디렉션

CWA(Central WebAuth)는 URL 리디렉션을 사용합니다. CWA 프로세스 중에 HTTP 프로브는 정책 서비스 노드에서 암호화가 완료된 리디렉션 HTTPS 패킷으로부터 **User-Agent** 특성을 캡처할 수 있습니다. 클라이언트 프로비저닝 서비스와 마찬가지로, 게스트 흐름은 ISE가 세션 캐시에서 MAC 주소(**Calling-Station-ID**)를 검색할 수 있는 활성 세션에 포함됩니다. 이 프로세스에서 HTTP 프로브는 엔드포인트 데이터베이스를 채우는 데 필요한 **User-Agent** 및 관련 MAC 주소를 학습할 수 있습니다.

일반적으로 HTTP 프로브는 **User-Agent**를 통해 클라이언트 OS 유형을 탐지할 수 있는 하이파이(Hi-Fi)를 제공합니다. HTTP 프로브는 운영 체제 기반 정책이 필요한 경우, 특히 엔드포인트가 개인 자산인지, 아니면 기업 자산인지에 따라 고객이 주로 차별화된 액세스를 제공해야 하는 무선 환경에서 권장됩니다.

두 시나리오 모두(CP 사용 URL 리디렉션과 CWA 사용 URL 리디렉션)에서 ISE는 기존의 IP-MAC 주소 바인딩 없이도 **User-Agent** 특성을 MAC 주소에 적용할 수 있습니다. 엔드포인트와 인접한 레이어 2에 해당하는 세그먼트에서 미러링되는 트래픽이 발생하는 경우를 제외하고 HTTP SPAN 방식을 사용하려면 항상 기존의 IP-MAC 바인딩 항목이 필요합니다. 이러한 특정한 경우 패킷 소스 MAC 주소는 실제 엔드포인트이며 그에 따라 엔드포인트 데이터베이스를 업데이트하는 데 사용할 수 있습니다.

**모범 사례:** **User-Agent**를 얻으려면 CWA 활용 사례에서 HTTP 프로브와 URL 리디렉션을 사용하십시오. Posture 에이전트 또는 Native Supplicant Provisioning 서비스가 필요한 경우 클라이언트 프로비저닝에서 URL 리디렉션을 사용한 프로파일링이 자동으로 수행됩니다. 그러나 경우에 따라 Posture 또는 Supplicant Provisioning이 필요하지 않은 경우에도 의도적으로 CP를 트리거하는 것이 적합할 수 있습니다. 이를 위해서는 엔드포인트 프로파일이 Unknown(알 수 없음) 또는 Incomplete(불완전)으로 설정된 경우 CWA(Posture 에이전트를 활성화함) 또는 CPP(Client Provisioning and Posture) 서비스(Posture Discovery)로 리디렉션하면 됩니다. 목표는 프로세스에서 **User-Agent**를 캡처하여 결과 Posture 상태에서 CoA(Change of Authorization)를 트리거하도록 허용하는 것입니다. 다시 연결될 경우 보다 구체적인 프로파일 일치 항목에 따라 새로운 권한 부여 정책 규칙을 할당할 수 있습니다.

앞서 언급한 것처럼, URL 리디렉션은 정책 서비스 노드에서 **User-Agent** 특성을 가져올 때 패킷 미러링 방법에 비해 트래픽 부하를 최소화할 수 있으므로 일반적으로 HTTP SPAN보다 권장됩니다. 일부 특수한 경우 ARP 캐시를 먼저 채우지 않고 프로파일링할 수 있습니다. 또한 RADIUS 권한 부여에 기반한 URL 리디렉션은 항상 RADIUS 트래픽이 종료되는 동일한 PSN으로 보내지므로 이러한 리디렉션은 고가용성 시나리오를 간소화합니다.

그러나 액세스 디바이스와 같이 RADIUS가 구축되지 않은 몇 가지 시나리오에서는 SPAN 방식이 실행 가능한 유일한 옵션일 수 있습니다.

### HTTP 프로브 구성

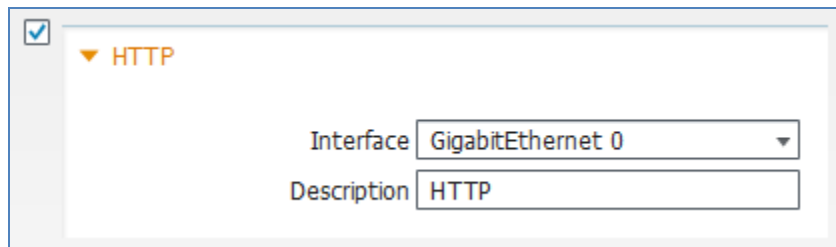
리디렉션된 트래픽에 HTTP 프로브를 사용하려면 액세스 디바이스는 HTTP 트래픽을 ISE로 직접 리디렉션(예: Local WebAuth를 통해)하거나 RADIUS 권한 부여를 통해 리디렉션할 수 있어야 합니다. RADIUS 기반 리디렉션의 경우 권한 부여 결과로 **url-redirect**의 Cisco AVP(특성 값 쌍)를 반환하는 권한 부여 정책 규칙을 사용하여 ISE를 구성해야 합니다.

SPAN에 HTTP 프로브를 사용하려면 네트워크에서 전용 인터페이스를 통해 네트워크 트래픽(HTTP만 포함하도록 필터링된 트래픽 하위 집합이 권장됨) 사본을 ISE PSN으로 전송해야 합니다.

### ISE에서 HTTP 프로브 활성화

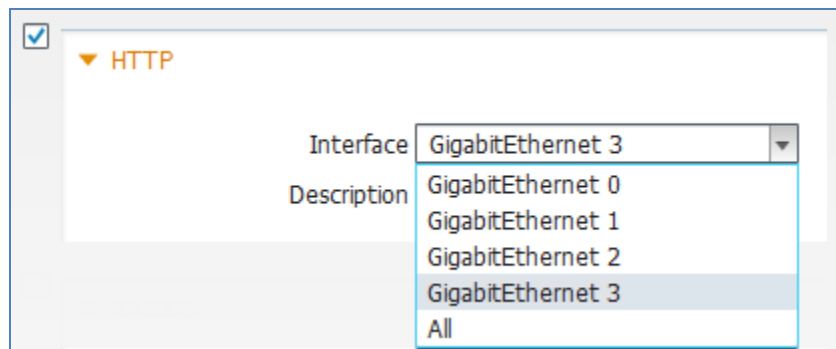
- Step 1** Administration(관리)→System(시스템)→Deployment(구축)로 이동하고 RHS 창의 구축된 노드 목록에서 프로파일링을 수행할 정책 서비스 노드를 선택합니다.
- Step 2** Profiling Configuration(프로파일링 컨피그레이션) 탭을 선택합니다. HTTP 프로브에 대한 지원을 추가하려면 HTTP라는 확인란을 선택합니다(그림 34).

그림 29: HTTP 프로브 컨피그레이션



- Step 3** HTTP 트래픽 수집에 사용할 인터페이스를 선택합니다.
- Step 4** URL 리디렉션에 사용하려면 세션 서비스(예: RADIUS, 웹 인증, Posture 등)에 사용되는 것과 동일한 인터페이스인 GigabitEthernet 0이 인터페이스로 사용되어야 합니다.
- Step 5** 미러링되는 트래픽(SPAN/RSPAN/TAP)에 사용하기 위해서는 전용 인터페이스여야 합니다(그림 35).

그림 30 HTTP 프로브 컨피그레이션 - 인터페이스



- Step 6** Save(저장)를 클릭하여 변경 사항을 커밋합니다.
- Step 7** 프로파일링 서비스를 사용하여 구성된 다른 모든 정책 서비스 노드에 대해 이 절차의 단계를 반복합니다.

**참고:** 트래픽 미러링을 위한 요구 사항으로 인해 SPAN을 수신하도록 여러 정책 서비스 노드를 구성하는 것이 불가능하거나 실행 가능하지 않을 수 있습니다. 동일한 트래픽 흐름을 미러링하는 경우 동일한 트래픽을 여러 정책 서비스 노드에 전달하는 것은 적합하지 않을 수 있습니다. 일부 이중화를 추가하더라도, 이렇게 하면 ISE 노드에 대한 부하가 크게 가중될 수 있으며 다른 노드에서 상호 연결되고 동기화되어야 하는 불필요한 프로파일링 데이터 중복이 발생할 수 있습니다.

## ISE(네트워크 리소스)에 네트워크 디바이스 추가

HTTP 데이터를 캡처하는 방법으로 URL 리디렉션을 사용하는 경우 RADIUS 기반 인증을 지원하도록 네트워크 액세스 디바이스가 이미 구성되어 있어야 합니다. 그러한 경우 네트워크 액세스 디바이스를 추가하거나 편집해야 하는 추가적인 단계가 필요하지 않습니다.

HTTP 데이터를 캡처하는 방법으로 SPAN을 사용하는 경우 RADIUS 기반 인증을 수행하지 않으면 액세스 디바이스를 ISE에 추가해야 한다는 특정 요구 사항이 없습니다.

### 리디렉션된 HTTP 트래픽을 수신하도록 ISE 정책 서비스 노드 인터페이스 구성

URL 리디렉션을 사용하는 경우 기본 GigabitEthernet 0 인터페이스에서 HTTP 프로브를 활성화해야 합니다. 그러므로 추가적인 인터페이스 컨피그레이션이 필요하지 않습니다.

### HTTP SPAN 트래픽을 수신하도록 ISE 정책 서비스 노드 인터페이스 구성

SPAN을 사용하는 경우 전용 SPAN 인터페이스에서 HTTP 트래픽을 수신하도록 HTTP 프로브를 구성해야 합니다. ISE에서 전용 SPAN 인터페이스를 구성하려면 다음 단계를 완료하십시오.

- Step 1** 원하는 인터페이스를 해당 SPAN 대상 포트 또는 Network TAP 인터페이스에 물리적으로 연결합니다.
- Step 2** ISE PSN 콘솔(CLI)에 액세스합니다. 원하는 인터페이스에 대한 컨피그레이션 모드에서 **no shutdown**을 입력하면 해당 인터페이스가 활성화됩니다.
- Step 3** ISE CLI 명령 **copy running-config startup-config**를 사용하여 변경 내용을 저장합니다.

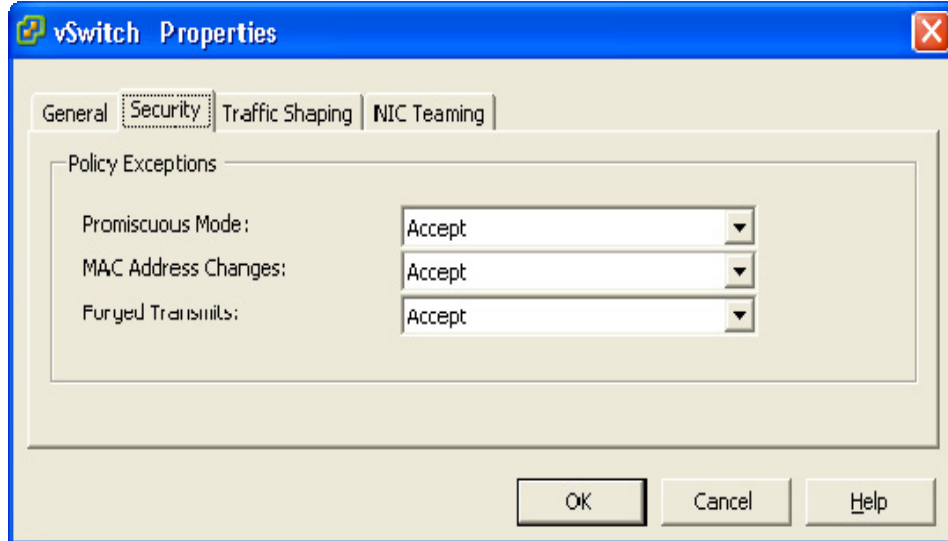
---

#### 참고: VMware 어플라이언스에서 실행되는 정책 서비스 노드의 경우

프로파일링에 전용 인터페이스를 사용하기 위해 가상 어플라이언스에 대한 추가 가상 인터페이스가 구성되어 있는 것으로 가정합니다. 설치 시 완료하지 않은 경우 ISE 노드를 종료하고 필수 인터페이스에 맞게 ESX 어플라이언스의 하드웨어 및 네트워킹 컨피그레이션을 업데이트해야 ISE 컨피그레이션을 계속 진행할 수 있습니다.

또한 ISE DHCP SPAN 인터페이스에서 SPAN/미러 트래픽을 수락하려면 VMware 어플라이언스에서 가상 스위치 또는 인터페이스에 대해 무차별 모드를 설정해야 합니다. 이 모드를 활성화하려면 VMware Host(VMware 호스트) → Configuration(컨피그레이션) → Hardware(하드웨어) → Networking(네트워킹) → vSwitch(스위치) → Security(보안)로 이동하고 다음과 같이 Promiscuous Mode(무차별 모드): Accept(수락)(기본값 = Reject(거부))를 설정합니다.

---



### HTTP 패킷을 ISE PSN으로 리디렉션하도록 유선 액세스 디바이스 구성

CWA, Posture 또는 Supplicant Provisioning을 포함한 특정 서비스에 대해 URL 리디렉션을 지원하는 액세스 디바이스 컨피그레이션은 이 가이드의 범위에 속하지 않습니다. 요약하면, Cisco Catalyst 스위치를 사용하여 RADIUS 권한 부여에 따라 리디렉션을 지원하는 데 필요한 명령은 다음과 유사합니다.

- 전역 컨피그레이션 모드에서 HTTP를 활성화하고 선택적으로 HTTPS 서버를 활성화합니다.
- ISE RADIUS 권한 부여에서 리디렉션에 적합한 트래픽을 지정하기 위해 참조되는 리디렉션 ACL을 구성합니다.

```
ip http server
ip http secure-server
ip access-list extended REDIRECT-ACL
deny tcp any any <PSN_IP_address>
permit tcp any any eq http
permit tcp any any eq https
```

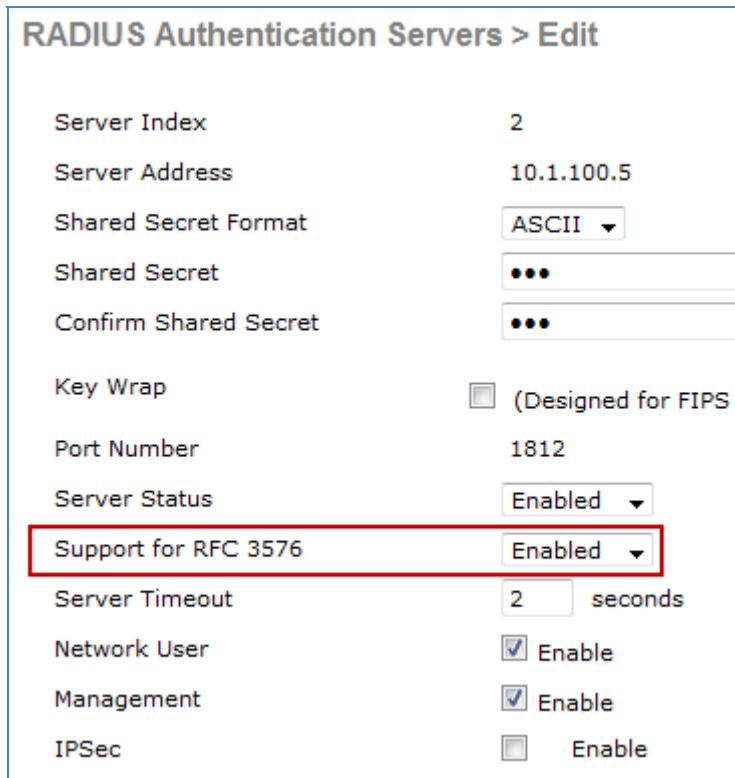
클라이언트에서 시작된 트래픽의 경우 Catalyst 스위치는 HTTP 및 HTTPS 트래픽 모두의 리디렉션을 지원할 수 있습니다. ISE로 리디렉션되는 트래픽은 항상 HTTPS입니다.

### HTTP 패킷을 ISE PSN으로 리디렉션하도록 무선 액세스 디바이스 구성

CWA, Posture 또는 Supplicant Provisioning을 포함한 특정 서비스에 대해 URL 리디렉션을 지원하는 액세스 디바이스 컨피그레이션은 이 가이드의 범위에 속하지 않습니다. 요약하면, Wireless LAN Controller를 사용하여 RADIUS 권한 부여에 따라 리디렉션을 지원하기 위한 필수 단계는 다음 예와 유사합니다.

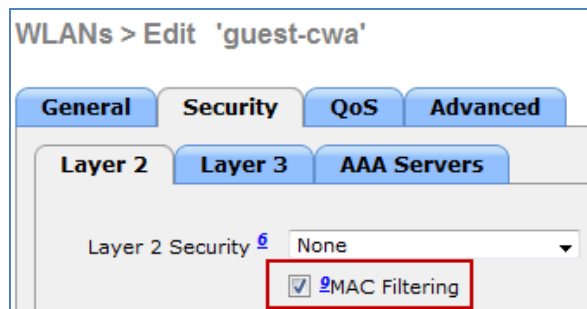
**Step 1** Security(보안)→AAA→RADIUS→Authentication(인증)→(RADIUS Server)(RADIUS 서버)→Edit(편집)에서 Support for RFC 3576(RFC 3576 지원)이 Enabled(사용)로 설정되어 있는지 확인합니다(그림 36).

그림 31 무선 컨트롤러를 위한 CoA 컨피그레이션 예



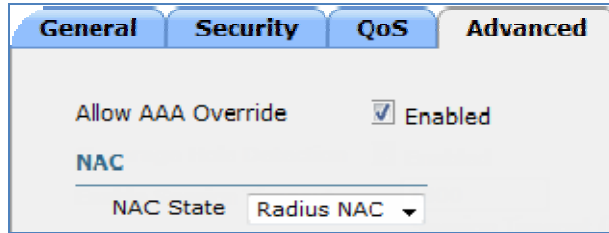
**Step 2** WLAN→Edit (WLAN)(편집(WLAN))→Security(보안)→Layer 2(레이어 2)에서 MAC Filtering(MAC 필터링)에 대해 WLAN을 구성합니다. Layer 2 Security(레이어 2 보안) 및 Layer 3 Security(레이어 3 보안)는 None(없음)으로 설정되어야 합니다(그림 37).

그림 32 무선 컨트롤러를 위한 MAC 필터링 컨피그레이션 예



**Step 3** Advanced(고급) 탭에서 Allow AAA Override(AAA 재정의 허용)를 선택하고 NAC State(NAC 상태)를 RADIUS NAC로 설정합니다(그림 38).

그림 33 무선 컨트롤러에 대한 RADIUS 권한 부여 컨피그레이션 예



클라이언트에서 시작된 트래픽의 경우 Cisco Wireless LAN Controller는 HTTP 트래픽 리디렉션만 지원합니다. HTTPS 트래픽 리디렉션은 지원하지 않습니다. ISE로 리디렉션되는 트래픽은 항상 HTTPS입니다.

**RADIUS 권한 부여로 URL 리디렉션을 수행하도록 ISE 구성**

CWA, Posture 또는 Supplicant Provisioning을 포함한 특정 서비스에 대해 URL 리디렉션을 지원하는 ISE 컨피그레이션은 이 가이드의 범위에 속하지 않습니다. 요약하면, ISE 권한 부여 정책의 RADIUS 권한 부여에 따라 리디렉션을 지원하기 위한 필수 단계는 다음 예와 유사합니다.

- Step 1** ISE 관리 인터페이스에서 Policy(정책)→Policy Elements(정책 요소)→Results(결과)로 이동합니다.
- Step 2** LHS 창에서 Authorization(권한 부여)→Authorization Profiles(권한 부여 프로파일)를 선택한 다음 RHS 창에서 Add(추가)를 클릭하여 그림 39와 같이 **Posture\_Remediation**이라는 새 권한 부여 프로파일을 추가합니다.

그림 34 URL 리디렉션 컨피그레이션의 권한 부여 프로파일 예

Authorization Profiles > Posture\_Remediation

### Authorization Profile

\* Name: Posture\_Remediation

Description: [Empty]

\* Access Type: ACCESS\_ACCEPT

▼ Common Tasks

DACL Name: POSTURE\_REMEDIATION

VLAN

Voice Domain Permission

Web Authentication: Posture Discovery, ACL: ACL-POSTURE-REDIRECT

Auto Smart Port

▼ Advanced Attributes Settings

Select an item = [Empty] - +

▼ Attributes Details

```

Access Type = ACCESS_ACCEPT
DACL = POSTURE_REMEDIATION
cisco-av-pair = url-redirect-acl=ACL-POSTURE-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cpp
    
```

그림 39에 표시된 예에서는 특정 리디렉션이 Posture Discovery로 선택된 상태로 Web Authentication이라는 레이블이 지정된 공통 작업이 선택되어 있습니다. 그러면 엔드포인트가 Client Provisioning and Posture 서비스, 즉 CPP로 리디렉션됩니다. 리디렉션 ACL은 ACL-POSTURE-REDIRECT이며 액세스 디바이스에서 미리 구성되어 있어야 합니다. 그에 따른 결과 RADIUS 권한 부여가 파란색으로 강조 표시되어 있습니다.

**Step 1** Policy(정책) → Authorization(권한 부여)으로 이동하고 **Employee\_PreCompliant**라는 권한 부여 정책 규칙을 추가합니다. 이 규칙의 경우 사용되는 디바이스 유형이 워크스테이션도 아니고 Apple iPad도 아닌 직원에 새 권한 부여 프로파일을 사용합니다(그림 40 참고).

그림 35 URL 리디렉션에 대한 권한 부여 정책 규칙 예

<input checked="" type="checkbox"/>	Employee-Workstation	if Workstation AND Employee	then Employee AND SGT_Employee
<input checked="" type="checkbox"/>	Employee-iPad	if Apple-iPad AND Employee	then Employee_iPad AND SGT_Guest
<input checked="" type="checkbox"/>	Employee_PreCompliant	if (Employee AND Session:PostureStatus NOT_EQUALS Compliant )	then Posture_Remediation

그림 40 예에서는 직원이 네트워크에 연결된 상태에서 디바이스 유형이 워크스테이션 또는 Apple-iPad와 동일한 명시적 엔드포인트 ID 그룹 중 하나와 일치하지 않은 경우에만 일치하도록 하기 위해

**Employee\_PreCompliant**라는 레이블이 지정된 규칙이 이전 규칙 **다음에** 의도적으로 배치되었습니다. 인증된 직원이 **Posture\_Redirection** 규칙과 일치하는 경우 Posture\_Redirection이라는 권한 부여 프로파일의 할당됩니다. 그러면 RADIUS 권한 부여가 액세스 디바이스로 반환되어 Client Provisioning and Posture 서비스에 대한 URL 리디렉션이 수행됩니다.

### HTTP 트래픽 사본을 ISE PSN으로 전송하도록 네트워크 디바이스 구성

트래픽을 ISE 정책 서비스 노드에 미러링하는 방법에는 여러 가지가 있습니다. 이 절차에서는 Cisco Catalyst 스위치에서 VACL Capture를 사용하는 일반적인 한 가지 방법을 보여줍니다. 이 방법을 통해 일부 관심 트래픽만 ISE 정책 서비스 노드로 전달할 수도 있습니다.

**모범 사례:** 사용 가능한 경우, 필요한 트래픽만 ISE 프로브로 보낼 수 있는 필터와 함께 확장 가능한 트래픽 미러링을 지원하는 지능형 TAP 시스템을 활용합니다. 여기에는 SPAN 방식을 사용하여 프로파일링 데이터를 확보하는 DHCP SPAN 및 HTTP 프로브가 포함됩니다. 고급 TAP 시스템에서는 미러링되는 트래픽에 대한 고가용성을 지원합니다.

또는 인프라에서 지원하는 경우, 네트워크 트래픽의 선택적 캡처를 허용하도록 RSPAN과 함께 지능형 SPAN 기술(예: 로컬 스위치의 VACL Capture 또는 VACL Capture/Redirect)을 활용합니다.

DHCP 트래픽의 소스가 되는 인터페이스 또는 VLAN을 확인합니다. WLC의 이그레스(egress) 인터페이스 또는 DHCP 서버에 대한 연결과 같은 특정 검사점은 모든 클라이언트 DHCP 패킷을 캡처하기 위한 이상적인 위치가 될 수 있습니다.

다음 예에서 VLAN 40-44는 Cisco Wireless LAN Controller 5500 Series로 트렁크됩니다. GigabitEthernet 2/37은 VMware ESXi 4.1을 실행하는 Cisco UCS 서버에 대한 스위치 포트 연결입니다. ESX 서버는 프로파일링이 활성화되어 있는 정책 서비스 노드로 구성된 ISE 가상 어플라이언스를 호스팅합니다. 인터페이스 GigabitEthernet 2/37은 기가비트 이더넷 3으로 ISE PSN에 연결된 가상 인터페이스 링크입니다.

```
interface GigabitEthernet1/1
description WLC5508 ETH0 (Port 1)
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 40-44
switchport mode trunk

interface GigabitEthernet2/37
description UCS1 SPAN (port 3 of 4)
switchport
```

**Step 2** VLAN 40-44의 모든 HTTP 트래픽을 일치시키고 ISE PSN 연결로 전달하도록 VACL Capture를 구성합니다.

**Step 3** 다음과 같이 HTTP 트래픽만 일치시키는 한 ACL과 함께 모든 IP 트래픽을 일치시키는 또 다른 ACL을 구성합니다.

```
cat6500(config)# ip access-list extended HTTP_TRAFFIC
cat6500(config-ext-nacl)# permit tcp any any eq www

cat6500(config)# ip access-list extended ALL_TRAFFIC
cat6500(config-ext-nacl)# permit ip any any
```



**Step 4** HTTP\_TRAFFIC ACL과 일치하는 트래픽에 캡처 비트를 설정하는 시퀀스를 사용하여 VLAN 액세스 맵을 구성합니다. 동일한 VLAN 액세스 맵에서 다른 모든 트래픽(ALL\_TRAFFIC ACL과 일치)을 전달하는 또 다른 시퀀스를 구성합니다.

```
cat6500(config)# vlan access-map HTTP_MAP 10
cat6500(config-access-map)# match ip address HTTP_TRAFFIC
cat6500(config-access-map)# action forward capture

cat6500(config)# vlan access-map HTTP_MAP 20
cat6500(config-access-map)# match ip address ALL_TRAFFIC
cat6500(config-access-map)# action forward
```

**Step 5** 다음과 같이 VLAN 액세스 맵을 VLAN 40, 41, 42 및 43에 적용하는 VLAN 필터를 구성합니다.

```
cat6500(config)# vlan filter HTTP_MAP vlan-list 40-43
```

**Step 6** 다음과 같이 업스트림 VLAN 100으로 라우팅되는 트래픽을 포함하여 VLAN 40, 41, 42 및 43의 일치하는 모든 트래픽을 포함하도록 캡처 포트(Gi2/37)를 구성합니다.

```
cat6500(config)# int Gi2/37
cat6500(config-if)# switchport capture allowed vlan 40-43,100
cat6500(config-if)# switchport capture
```

**URL 리디렉션을 사용하여 HTTP 프로브 데이터 확인(CWA 예)**

- Step 1** Administration(관리)→Identity Management(ID 관리)→Identities(ID)→Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 2** ISE PSN에 대한 HTTP 리디렉션을 지원하도록 구성된 액세스 디바이스에서 엔드포인트의 연결을 해제했다가 다시 연결합니다.
- Step 3** 엔드포인트에서 웹 인증을 사용하여 로그인합니다.
- Step 4** ISE 정책 관리 노드로 이동하고 Administration(관리)→Identity Management(ID 관리) → Identities(ID)로 이동합니다.
- Step 5** LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 6** 새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 HTTP 프로브에서 캡처한 특성을 표시합니다.

그림 41의 예에는 HTTP 프로브만 사용하여 URL 리디렉션을 통해 수집된 특성이 강조 표시되어 나타나 있습니다.

그림 36 URL 리디렉션을 사용한 HTTP 프로브 특성 - CWA 예

* MAC Address	00:50:56:A0:0B:3A
* Policy Assignment	Windows7-Workstation
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Microsoft-Workstation
Static Group Assignment	<input type="checkbox"/>
<b>Attribute List</b>	
EndPointPolicy	Windows7-Workstation
EndPointSource	HTTP Probe
IdentityGroup	Microsoft-Workstation
MACAddress	00:50:56:A0:0B:3A
MatchedPolicy	Windows7-Workstation
OUI	VMware, Inc.
PolicyVersion	20
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	60
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:11.0) Gecko/20100101 Firefox/11.0

다음과 같은 키 특성이 강조 표시되어 있습니다.

- EndPointSource
- MACAddress
- OUI
- User-Agent

표시된 예에는 HTTP 프로브만 사용하여 URL 리디렉션을 통해 수집된 특성이 강조되어 나타나 있습니다. 이러한 특정 시나리오에서는 IP-MAC 주소 바인딩이 없는 경우에도 엔드포인트가 내부 엔드포인트 데이터베이스에 추가될 수 있습니다.

**EndPointSource**에서는 HTTP 프로브가 특성 업데이트의 최신 소스임을 보여줍니다.

**MACAddress**는 세션 캐시에서 가져온 값입니다.

**OUI**는 **MACAddress** 값에서 파생됩니다.

**User-Agent**는 이 VMware 기반 클라이언트에서 Windows 7 운영 체제가 실행 중임을 표시하는 중요한 데이터 포인트입니다.

### URL 리디렉션을 사용하여 HTTP 프로브 데이터 확인(클라이언트 프로비저닝 예)

- Step 1** Administration(관리)→Identity Management(ID 관리)→Identities(ID)→Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 2** ISE PSN에 대한 HTTP 리디렉션을 지원하도록 구성된 액세스 디바이스에서 엔드포인트의 연결을 해제했다가 다시 연결합니다.

- Step 3**    엔드포인트에서 로그인을 시도합니다.
- Step 4**    Administration(관리)→Identity Management(ID 관리)→Identities(ID)로 이동하고 LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 5**    새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 클라이언트 프로비저닝 서비스에서 캡처한 특성을 표시합니다.
- Step 6**    그림 42에 표시된 예에서는 프로브가 활성화되지 않은 채 클라이언트 프로비저닝에서 URL 리디렉션을 사용하여 수집된 특성이 강조 표시되어 있습니다.

그림 37 URL 리디렉션을 사용한 HTTP 프로브 특성 - 클라이언트 프로비저닝 예

* MAC Address	7C:6D:62:E3:D5:05
* Policy Assignment	Apple-iPad
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Apple-iPad
Static Group Assignment	<input type="checkbox"/>
<b>Attribute List</b>	
EndPointPolicy	Apple-iPad
EndPointProfilerServer	ise-psn-1
EndPointSource	CP
IdentityGroup	Apple-iPad
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iPad
OUI	Apple, Inc
PolicyVersion	20
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	26
Total Certainty Factor	30
User-Agent	Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3

- Step 7**    강조 표시된 키 특성은 CP(클라이언트 프로비저닝)로 설정된 EndPointSource를 제외하고 이전 예와 유사합니다.

**SPAN을 사용하여 HTTP 프로브 데이터 확인**

- Step 1**    Administration(관리)→Identity Management(ID 관리)→Identities(ID)→Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 2**    구성된 액세스 디바이스에서 엔드포인트의 연결을 해제했다가 다시 연결합니다.
- Step 3**    엔드포인트에서 웹 브라우저를 열고 웹 사이트에 대한 http 액세스를 시도합니다.
- Step 4**    Administration(관리)→Identity Management(ID 관리)→Identities(ID)로 이동하고 LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 5**    새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 HTTP 프로브에서 캡처한 특성을 표시합니다.
- Step 6**    그림 43에는 HTTP 프로브만 활성화된 채 SPAN을 사용하여 수집된 특성이 강조 표시되어 있습니다.

그림 38 SPAN을 사용한 HTTP 프로브 특성 예

Endpoint List > 7C:6D:62:E3:D5:05	
<b>Endpoint</b>	
* MAC Address	7C:6D:62:E3:D5:05
** Policy Assignment	Apple-iPad
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Apple-iPad
Static Group Assignment	<input type="checkbox"/>
<b>Attribute List</b>	
Cookie	NID=59=eFjUh-KeyMvY3sJa6yMES3u3I1LDRpolvqVVdInBu30HDIVTz PREF=ID=1425<f19b36df761:U=9b71d718247b1acd:FF=0:TM=1333
EndPointPolicy	Apple-iPad
EndPointProfilerServer	ise-psn-1
EndPointSource	HTTP Probe
Host	www.google.com
IcentityGroup	Apple-iPad
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iPad
OUI	Apple, Inc
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TmeTcProfile	21
Total Certainty Factor	30
User-Agent	Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3
ip	10.1.41.101

이전 예와 동일한 키 특성에는 일부 새로운 특성도 포함되어 있습니다.

- 쿠키(표시를 위해 잘림)
- 호스트

초기 CWA 프로세스가 완료된 이후의 출력은 URL 리디렉션을 사용한 출력과 유사합니다. 이러한 추가적인 특성은 일반적인 클라이언트 검색 작업으로 수집된 추가 HTTP 헤더 정보의 캡처를 나타냅니다. 이러한 특성의 변경에 따라 ISE가 지속적으로 업데이트됩니다. 사용되지 않을 수 있는 특성에 대한 이러한 수많은 업데이트는 데이터베이스 업데이트 및 동기화 프로세스에 훨씬 큰 영향을 미칠 수 있습니다. 여기에서는 URL 리디렉션과 함께 HTTP 프로브를 사용한 **User-Agent**의 캡처가 SPAN 방식에 비해 얼마나 더 효율적일 수 있는지 다시 한 번 강조하여 보여줍니다.

요약하면 엔드포인트는 **User-Agent** 특성에 의해 결정되는 운영 체제를 기반으로 분류될 수 있습니다. 이러한 특성은 HTTP 프로브를 통해 수집될 수 있으며 특정한 경우에는 클라이언트 프로비저닝 서비스를 통해 수집될 수 있습니다. HTTP 트래픽을 수집하기 위한 2가지 일반적인 방법에는 URL 리디렉션과 SPAN 기술이 있습니다. 일반적으로, RADIUS 인증이 비활성화된 환경에서 프로파일링이 필요한 경우에는 SPAN이 유일한 옵션일 수 있지만 URL 리디렉션이 훨씬 더 효율적입니다.

## DNS 프로브를 사용한 프로파일링

기존 엔드포인트의 IP 주소가 학습된 경우 DNS 프로브는 ISE 정책 서비스 노드에서 역방향 DNS 조회를 기반으로 DNS FQDN(정규화된 도메인 이름)을 얻는 데 사용됩니다. 그러므로 DNS 프로브는 IP 주소가 알려진 경우 이외에는 작동되지 않습니다.

엔드포인트의 IP 주소를 확인하는 데 사용할 수 있는 프로브는 다음과 같습니다.

- Framed-IP-Address를 통한 RADIUS 프로브
- cdpCacheAddress를 통한 SNMP 프로브
- SourceIP를 통한 HTTP 프로브
- dhcp-requested-address를 통한 DHCP 프로브

알려진 IP 주소 외에, 역방향 DNS 조회가 작동하기 위한 다른 요구 사항에는 여러 가지가 있습니다.

- DNS의 각 엔드포인트에는 주소 또는 **A** 레코드(호스트 이름) 및 포인터 또는 **PTR** 레코드(IP 주소)가 필요합니다.
- 엔드포인트에서 DHCP를 사용한다고 가정할 때 DHCP 서버에 DDNS(동적 DNS)를 구성해야 합니다.
- DHCP 서버 컨피그레이션에 따라 엔드포인트에는 동적 업데이트를 요청하는 컨피그레이션이 필요할 수 있습니다.
- 동적으로 업데이트되는 DNS 서버에서 주소를 확인하도록 ISE 정책 서비스 노드를 구성해야 합니다.
- DDNS가 구성되어 적절히 작동하고 있다고 가정할 때 DNS 프로브는 FQDN을 검색할 수 있습니다. 그렇지 않으면 역방향 조회가 실패할 경우 특성이 추가되지 않습니다.

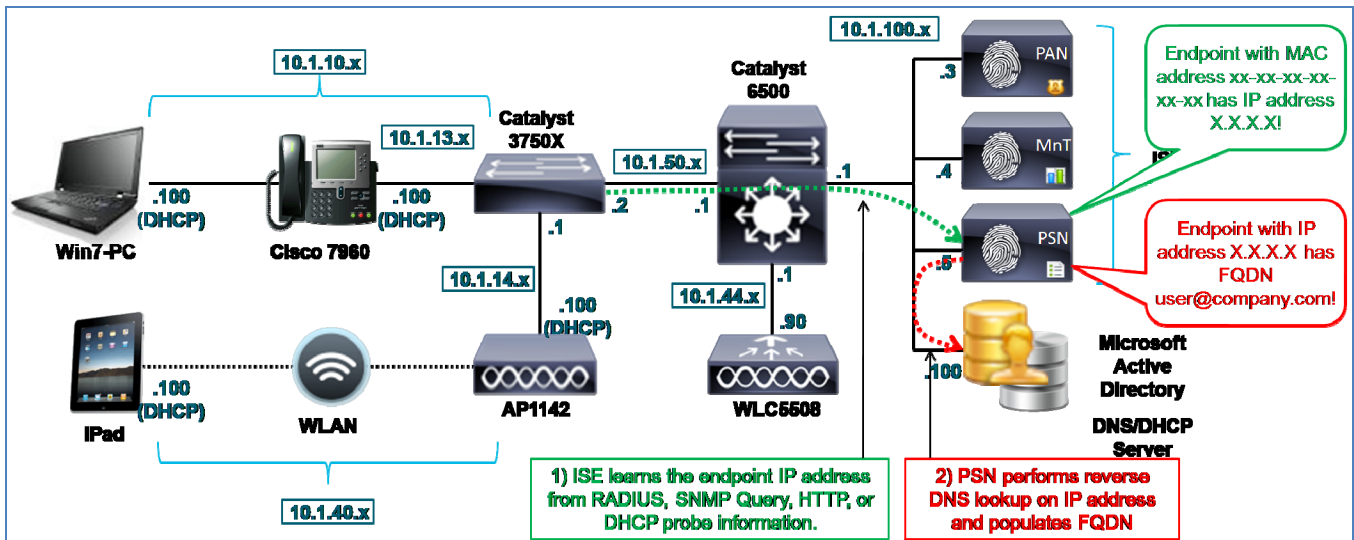
표준 호스트 이름, 도메인 이름 또는 FQDN 명명 규칙이 특정 엔드포인트에 구축된 경우 이들 특성은 그러한 항목을 분류하는 데 사용될 수 있습니다. 예를 들어 모든 Windows CP 클라이언트에 **jsmith-winxp**와 같은 이름이 할당된 경우 Windows XP 엔드포인트를 분류하기 위한 조건에서 **host-name** 특성 또는 **client-fqdn** 특성을 사용할 수 있습니다. 마찬가지로 규칙에 따라 기업 엔드포인트의 호스트 이름을 **jsmith-corp-dept**와 같은 특성으로 채워야 할 경우 기업 자산을 검증하는 데 그러한 특성을 사용할 수 있습니다.

프로파일 특성을 ID와 혼동하지 않도록 주의해야 합니다. 특성에서 엔드포인트가 특정 유형임을 나타내는 특정 신뢰도 레벨을 추가할 수 있습니다. 예를 들어 프로파일링에 권한 부여 정책을 사용하여 직원에 대한 전체 액세스 권한을 거부할 수 있습니다. 이 경우 PC의 **host-name** 특성(일치하는 엔드포인트 ID 그룹으로 표시됨)에 예상 값이 포함되지 **않습니다**. 참고: 이 가이드의 뒷부분에서는 프로파일과 엔드포인트 ID 그룹의 관계에 대해 설명합니다.

여기에 설명된 것처럼 다른 프로브를 사용하여 FQDN 또는 해당 구성 요소를 수집할 수 있습니다. 그러므로 다른 수단을 통해 FQDN의 일부 또는 동일한 FQDN 정보를 이미 사용할 수 있는 경우에는 DNS 프로브를 사용할 필요가 없을 수 있습니다. 그러나 DHCP 클라이언트 패킷을 통해 해당 정보를 검색될 수 있게 하여 DDNS를 보다 안전하게 구성할 수 있습니다. 이 방법은 신뢰할 수 있는 DNS 서버에 대한 역방향 조회에 비해 신뢰성이 떨어집니다.

그림 44에서는 DNS 프로브를 사용한 샘플 토폴로지를 보여줍니다. 그림에 나타난 것처럼 ISE 정책 서비스 노드는 여러 가지 방법 중 한 가지를 사용하여 엔드포인트의 IP 주소를 학습합니다. 그런 다음 PSN은 IP 주소에 대한 역방향 조회를 시작합니다. 응답이 수신되면 ISE 프로파일링 서비스는 엔드포인트 레코드를 FQDN 특성으로 업데이트합니다.

그림 39 DNS 프로브 예



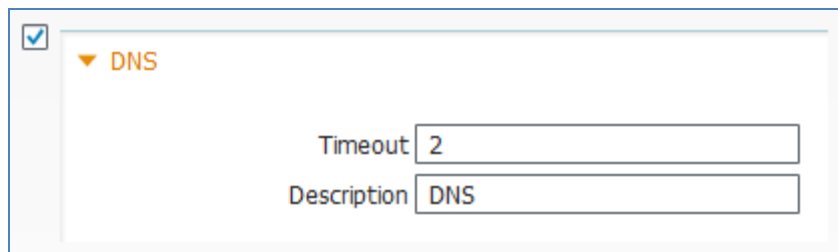
## DNS 프로브 구성

DNS 프로브를 사용하려면 ISE 정책 서비스 노드에 참조되는 DNS를 수동으로 또는 DDNS를 사용하여 동적으로 구성해야 합니다. 이 경우 FQDN을 검색할 각 엔드포인트에 대한 호스트 및 역방향 포인터 레코드를 포함하도록 구성해야 합니다.

### ISE에서 DNS 프로브 활성화

- Step 1** Administration(관리)→System(시스템)→Deployment(구축)로 이동하고 RHS 창의 구축된 노드 목록에서 프로파일링을 수행할 정책 서비스 노드를 선택합니다.
- Step 2** Profiling Configuration(프로파일링 컨피그레이션) 탭을 선택합니다.
- Step 3** DNS 프로브에 대한 지원을 추가하려면 DNS라는 확인란을 선택합니다.

그림 40: SPAN을 사용한 HTTP 프로브 특성 예



모든 프로브 쿼리는 ISE 정책 서비스 노드에서 로컬로 구성된 DNS 서버에 대한 역방향 조회용 전역 라우팅 표를 사용하여 시작되므로 DNS 프로브에서는 인터페이스가 선택되지 않습니다.

- Step 4** 시간 초과와 기본값을 그대로 사용합니다. 이 값은 PSN이 역방향 조회 응답을 기다리는 시간(초)을 지정합니다.
- Step 5** Save(저장)를 클릭하여 변경 사항을 커밋합니다.
- Step 6** 프로파일링 서비스를 사용하여 구성된 다른 모든 정책 서비스 노드에 대해 이 절차의 단계를 반복합니다.

### 엔드포인트 IP 주소를 가져오도록 프로브 구성

**참고:** 엔드포인트 IP 주소를 가져오도록 프로브를 구성하십시오. DNS 프로브에서 FQDN에 대한 역방향 DNS 조회를 수행하려면 먼저 SNMP 쿼리, DHCP, DHCP SPAN, HTTP 또는 RADIUS 프로브에서 엔드포인트의 IP 주소를 학습해야 합니다. 이러한 프로브의 컨피그레이션에 대한 자세한 내용은 이 가이드의 해당 섹션을 참고하십시오.

### DNS 서버에서 역방향 주소 조회를 수행하도록 ISE 구성

ISE 어플라이언스를 처음 설치한 경우 필요한 컨피그레이션 단계는 하나 이상의 도메인 이름 서버를 구성하는 것입니다.

필요한 경우, 그림 46에 표시된 것처럼 전역 컨피그레이션 모드에서 ISE CLI 명령 **ip name-server**를 사용하여 프로파일링 서비스를 실행하는 ISE 정책 서비스 노드에 사용되는 DNS 서버 목록을 업데이트하십시오.

그림 41 ISE 정책 서비스 노드 DNS 서버 컨피그레이션 예

```
ise-pan-1/admin(config)# ip name-server ?
<A.B.C.D> Primary DNS server IP address
<A.B.C.D> DNS server 2 IP address
<A.B.C.D> DNS server 3 IP address
```

- Step 7** 항목을 제거하려면 **no name-server** 명령을 사용합니다.
- Step 8** 변경 내용을 저장하려면 전역 컨피그레이션 모드를 종료하고 **copy running-config startup-config** 명령을 입력합니다.
- Step 9** 프로파일링 서비스를 실행하는 나머지 정책 서비스 노드에 대해 필요한 대로 위 단계를 반복합니다.

### DNS 프로브 데이터 확인

- Step 1** Administration(관리)→Identity Management(ID 관리)→Identities(ID)→Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 2** ISE PSN에 대한 HTTP 리디렉션을 지원하도록 구성된 액세스 디바이스에서 엔드포인트의 연결을 해제했다가 다시 연결합니다.
- Step 3** ISE 정책 관리 노드로 이동하고 Administration(관리)→Identity Management(ID 관리) → Identities(ID)로 이동합니다.
- Step 4** LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 5** 새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 HTTP 프로브에서 캡처한 특성을 표시합니다.

그림 47의 예에서는 RADIUS, DHCP(IP Helper) 및 DNS 프로브만 활성화되어 있음을 보여줍니다. RADIUS 및 DHCP는 MAC 주소와 엔드포인트의 IP 주소를 모두 가져오기 위한 방법으로 활성화되어 있습니다. 이러한 프로브는 또한 다양한 프로브를 사용하여 수집할 수 있는 유사 데이터를 비교하기 위해 선택되어 있습니다.

해시 표시는 표시 목적으로 출력이 잘린 섹션을 나타냅니다.

그림 42 DNS 프로브 특성 예

Endpoint List > 00:50:56:A0:0B:3A

**Endpoint**

\* MAC Address **00:50:56:A0:0B:3A**

\* Policy Assignment **Microsoft Workstation**

Static Assignment

\* Identity Group Assignment **Microsoft-Workstation**

Static Group Assignment

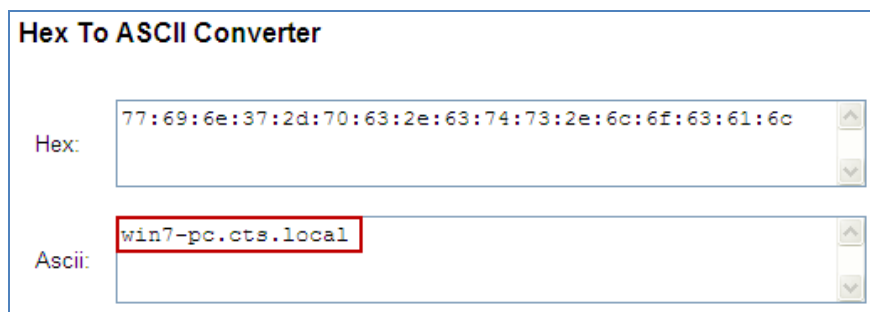
**Attribute List**

ADDomain	cts.local
AccsSessionID	be-psn-1/124936089/19986
EndPointMACAddress	00-50-56-A0-0B-3A
EndPointMatchedProfile	VMWare-Device
EndPointPolicy	Microsoft-Workstation
EndPointProfilerServer	be-psn-1
EndPointSource	DNS Probe
ExternalGroups	cts.local/users/employees\,cts.local/users/domain users\,cts.local/builtin/users
FQDN	win7-pc.cts.local.
Framed-IP-Address	10.1.10.100
GroupsOrAttributesProcessFailure	true
IdentityGroup	Microsoft-Workstation
chaddr	00:50:56:a0:0b:3a
ciaddr	0.0.0.0
cisco-zv-pair	audit-session-id=0A0132020000032046FD998, disc-cause-ext=No Reason, connect-pro
client-fqdn	00:00:00:77:69:6e:37:2d:7c:63:2e:63:74:73:2e:6c:6f:63:61:6c
dhcp-class-identifier	MSFT 5.0
dhcp-client-identifier	01:00:50:56:a0:0b:3a
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43
dhcp-requested-address	10.1.10.100
flags	0x8000
giaddr	10.1.10.1
hlen	6
hops	1
huser-name	win7-pc
htype	Ethernet (10Mb)
ip	10.1.10.100
op	BOOTREQUEST
secs	0
yiaddr	0.0.0.0



- Step 6** 빨간색으로 강조 표시된 키 특성에는 다음과 같은 항목이 있습니다.
- Step 7** EndPointSource = DNS 프로브
- Step 8** FQDN = win7-pc.cts.local
- Step 9** ip = 10.1.10.100
- Step 10** EndPointSource는 엔드포인트 특성의 마지막 소스를 반영합니다.
- Step 11** FQDN 값은 DNS 프로브를 사용한 DNS 서버에 대한 성공적인 역방향 조회의 결과입니다.
- Step 12** ip 특성은 DNS 프로브가 작동하기 위해서는 이 특성을 가져와야 한다는 요구 사항을 강조하는 중요한 요소입니다. 이 예의 RADIUS 또는 DHCP 프로브에서는 이 값이 업데이트되었을 수 있습니다.
- Step 13** 주황색으로 강조 표시된 보조 특성에는 다음과 같은 항목이 있습니다.
- Step 14** ADDomain = cts.local
- Step 15** client-fqdn = 00:00:00:77:69:6e:37:2d:70:63:2e:63:74:73:2e:6c:6f:63:61:6c
- Step 16** host-name = win7-pc
- Step 17** ADDomain 값은 RADIUS 프로브를 사용하여 RADIUS 특성에서 학습된 도메인 이름입니다.
- Step 18** client-fqdn 특성은 DHCP 프로브에서 학습된 엔드포인트의 정규화된 도메인 이름이며 HEX 형식으로 표시됩니다(그림 48).

그림 43 16진수-ASCII 변환 예



- Step 19** host-name 특성은 DHCP 프로브에서 학습된 엔드포인트의 간단한 호스트 이름입니다.
- Step 20** 이 예에서는 서로 다른 프로브 특성이 유사한 정보를 제공할 수 있음을 보여줍니다. 따라서, 정책 관리자는 프로파일링 엔드포인트에 가장 유용한 특성과 함께 이러한 정보를 가장 효과적으로 얻을 수 있는 프로브를 선택해야 합니다. 프로브 및 프로파일링의 방법의 비교에 대해서는 이 가이드의 뒷부분에 설명되어 있습니다.

### NetFlow 프로브를 사용한 프로파일링

Cisco NetFlow는 Cisco IOS Software 기반 라우터 및 레이어 3 스위치에서 내보낸 텔레메트리의 한 형식입니다. NetFlow는 각 NetFlow 지원 라우터 또는 스위치를 통해 전달되거나 해당 라우터 또는 스위치로 직접 전달되는 트래픽 관련 정보를 제공합니다. NetFlow 지원 디바이스는 네트워크 흐름 데이터를 수집하여 지정된 UDP 포트(기본 UDP/9996)의 수집기로 내보냅니다. 흐름은 지정된 소스와 대상 사이의 단방향 패킷 스트림으로 다음과 같은 키 필드 조합으로 고유하게 식별됩니다.

소스 IP 주소

대상 IP 주소

소스 포트 번호

대상 포트 번호

레이어 3 프로토콜 유형

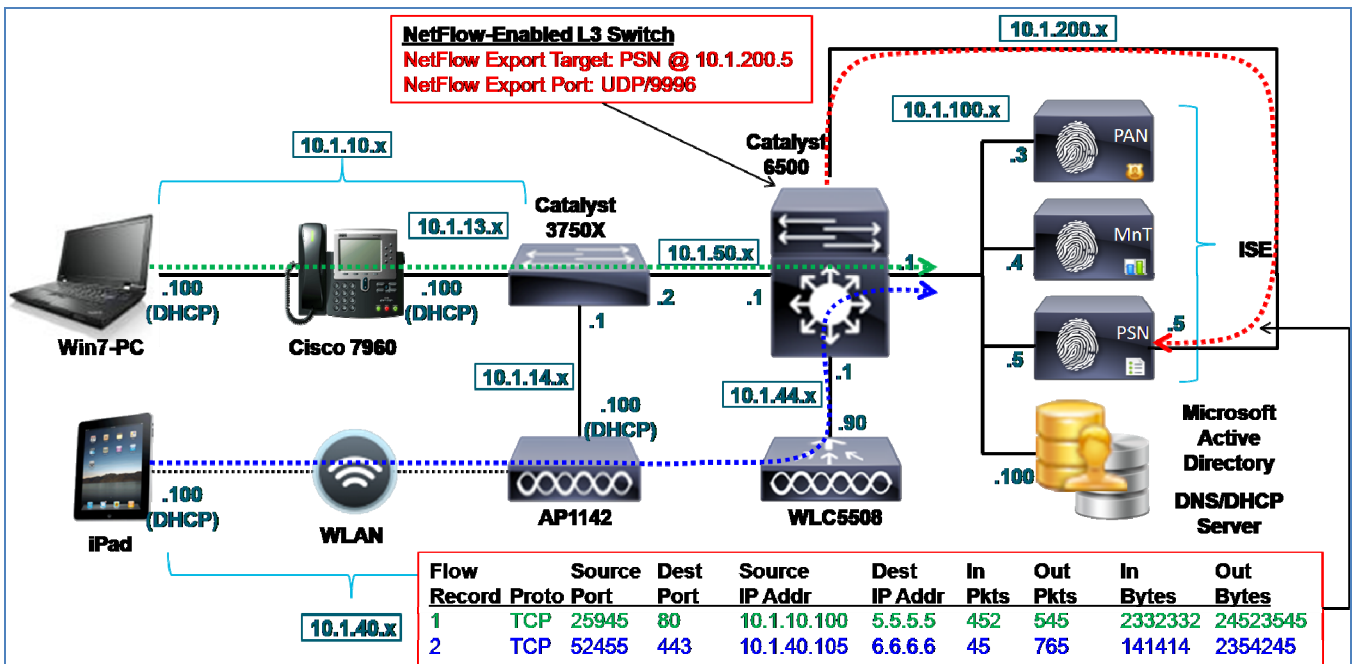
ToS 바이트

논리적 인터페이스 입력(ifIndex)

ISE NetFlow 프로브는 프로파일링 용도로 중요한 정보를 구문 분석할 수 있도록 NetFlow 버전 5 및 버전 9 지원 디바이스에서 흐름 레코드를 수신할 수 있습니다.

그림 49의 샘플 토폴로지에서는 NetFlow 지원 스위치(Cisco Catalyst 6500 Series)를 통해 트래픽 흐름을 설정한 2가지 서로 다른 엔드포인트를 보여줍니다. 6500 Series는 UDP/9996에서 IP 주소로 10.1.200.5를 사용하는 전용 인터페이스의 ISE 정책 서비스 노드로 흐름을 내보내도록 구성되었습니다. 이 인터페이스는 RADIUS 및 웹 인증과 같이 사용자 세션 서비스를 종료하는 인터페이스와는 구분됩니다.

그림 44: NetFlow 프로브 예



토폴로지에 나와 있는 것처럼 NetFlow는 관련 트래픽 경로에 있는 라우터 또는 스위치에서 활성화해야 합니다. 예를 들어 원격 분기 내에서 세그먼트 간의 트래픽 흐름을 수집해야 하는 경우 허브 또는 중앙 위치에 구축된 NetFlow는 필요한 가시성을 제공하지 않습니다. 또한 특정 트래픽 흐름을 수집하려면 먼저 네트워크에서 해당 트래픽을 허용해야 합니다. 그러므로 네트워크 액세스가 NetFlow 데이터를 사용하는 프로파일링에 종속적인 경우 프로파일링을 완료하는 데 필요한 트래픽을 계속 허용하면서 액세스를 가장 효과적으로 제한하는 방법을 결정해야 합니다.

## NetFlow 특성

표 4에는 NetFlow 프로브를 통해 수집되는 일부 특성이 나와 있습니다.

표 2 NetFlow 프로브 특성

IN_BYTES	IN_PKTS	FLows
PROTOCOL	SRC_TOS	TCP_FLAGS
L4_SRC_PORT	IPV4_SRC_ADDR	SRC_MASK
L4_DST_PORT	IPV4_DST_ADDR	DST_MASK
IPV4_NEXT_HOP	LAST_SWITCHED	FIRST_SWITCHED
OUT_BYTES	OUT_PKTS	IPV6_SRC_ADDR
IPV6_DST_ADDR	IPV6_SRC_MASK	IPV6_DST_MASK
IPV6_FLOW_LABEL	ICMP_TYPE	DST_TOS
IN_SRC_MAC	OUT_DST_MAC	SRC_VLAN
DST_VLAN	IP_PROTOCOL_VERSION	DIRECTION

ISE 프로파일링 서비스에서 NetFlow는 일반적으로 생성되는 트래픽을 기반으로 엔드포인트를 식별하는 데 사용됩니다. 반면에, 특정 엔드포인트가 해당 엔드포인트의 특성에 해당하지 않는 트래픽을 생성하는 것처럼 보이는 경우 비정상적인 동작 표시기를 제공할 수 있습니다. 예를 들어 IP 전화기가 NetFlow 특성에 반영된 것처럼 443번 포트의 원격 대상과 갑자기 통신을 시작할 때 엔드포인트가 초기에 프로파일링된 경우 비정상적인 조건 및 잠재적인 스푸핑 공격용 악성코드를 나타냅니다. 그러나 ISE 프로파일링 서비스는 NetFlow와 함께 사용할 경우 안티 스푸핑 기능 또는 솔루션 역할을 하지 못한다는 점에 유의하십시오.

엔드포인트의 명확한 분류에 초점을 맞추는 경우 NetFlow는 범용 하드웨어가 미션별 기능에 가장 유용하게 사용될 수 있습니다. 그에 따라 엔드포인트를 고유하게 분류하는 유일한 정보가 트래픽과 관련이 있습니다. 이러한 디바이스 유형의 예에는 제조 또는 의료 업계에 사용되는 디바이스가 있습니다. 예를 들어 병원의 심장 모니터는 표준 하드웨어 기술을 이용하는 내장형 Windows OS 또는 강화된 Linux 커널을 사용할 수 있지만, 매우 특정한 프로토콜, 포트 및 대상에서 통신하는 애플리케이션을 실행할 수 있습니다. 이러한 엔드포인트 유형의 경우 NetFlow가 실행 가능한 유일한 옵션일 수 있습니다.

**Step 21** 일반적으로 무작위로 NetFlow를 활성화하거나 NetFlow 프로브를 범용 프로파일링 방법으로 사용하는 것은 권장되지 않습니다. NetFlow는 사용되는 플랫폼은 물론 NetFlow 컨피그레이션 및 트래픽 양에 따라 디바이스 리소스에 부정적인 영향을 미칠 수 있으므로 구축 시 주의해야 합니다. 또한 하나 이상의 소스에서 대량의 트래픽을 지속적으로 전송할 경우 NetFlow는 ISE 정책 서비스 노드에 과부하를 야기할 수도 있습니다. 다른 ISE 프로브와 달리, NetFlow 프로브는 데이터 수집 및 데이터베이스 효율성을 최적화하는 특성 필터를 지원하지 않습니다.

**Step 22** 네트워크 디바이스에서 사용하는 경우 NetFlow를 ISE 정책 서비스 노드로 내보내려면 NetFlow 버전 5보다 버전 9가 권장됩니다. 버전 9는 Flexible NetFlow는 물론 수집되어 NetFlow 프로브로 내보내지는 흐름 데이터를 필터링할 수 있는 수많은 개선 사항을 지원합니다. 샘플링된 NetFlow는 전반적인 트래픽 양을 줄일 수 있지만, 일부 시나리오에서는 NetFlow 프로브가 모든 흐름을 인식해야 하므로 샘플링으로는 모든 프로파일링 요구 사항을 충족하지 못할 수 있습니다.

## NetFlow 프로브 및 IP-MAC 주소 바인딩 요구 사항

- Step 23** NetFlow 레코드는 소스 및 대상 IP 주소 간의 통신을 기반으로 합니다. NetFlow 트래픽은 소스 또는 대상 엔드포인트의 MAC 주소를 포함하지 않으므로 전송되는 데이터를 NetFlow 프로브와 적절히 상호 연결하려면 ISE 정책 서비스 노드의 ARP 캐시 표에 IP-MAC 주소 바인딩이 있어야 합니다. 즉, 엔드포인트가 해당 MAC 주소로 ISE에 알려지지 않은 경우 또는 연결된 IP 주소가 없는 경우에는 학습된 흐름 특성을 적용할 수 있는 엔드포인트가 없으므로 NetFlow 프로브에서 학습된 프로파일링 데이터가 삭제됩니다. 따라서 NetFlow 데이터를 수집하기 전에 다른 프로브를 통해 IP-MAC 주소 바인딩을 학습해야 합니다. 이 정보를 제공하는 데 사용할 수 있는 프로브는 다음과 같습니다.
- Step 24** RADIUS(Framed-IP-Address를 통해)
- Step 25** DHCP(dhcp-requested-address를 통해)
- Step 26** SNMP 쿼리(SNMP 폴링을 통해)
- Step 27** NetFlow 버전 9는 흐름 레코드 안에 소스 및 대상 MAC 주소를 포함할 수 있는 옵션을 지원하지만 버전 5는 그렇지 않습니다. 그러나 이와 같이 보고된 MAC 주소는 경로에서 두 홉 이상 떨어져 있는 엔드포인트의 MAC 주소가 아니라 인접한 노드(일반적으로 레이어 3 라우터 및 스위치)의 주소입니다. 엔드 시스템이 직접 NetFlow 디바이스에 연결된 경우를 제외하고 이 기능의 값은 매우 작습니다.

**모범 사례:** 프로파일링에 NetFlow를 사용하면 구문 분석을 위해 잠재적으로 막대한 양의 데이터가 ISE로 전송될 수 있습니다. 다른 프로브로 불충분한 경우에만 NetFlow를 사용하십시오. 필요한 경우 Flexible NetFlow에서 개선된 필터링 기능을 활용하려면 NetFlow 버전 9를 사용하는 것이 좋습니다. ISE에서 기본 인터페이스를 사용할 수 있지만 NetFlow를 NetFlow 프로브 전용 ISE PSN 인터페이스로 내보내는 것이 좋습니다.

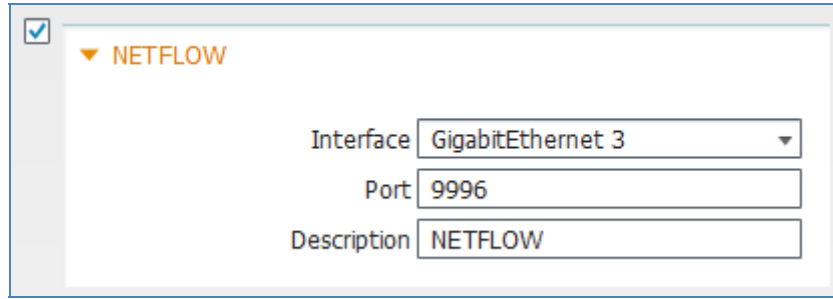
## NetFlow 프로브 구성

- Step 28** NetFlow 프로브를 사용하려면 해당 트래픽 흐름에 부합하는 네트워크 디바이스는 NetFlow를 지원하고 NetFlow 버전 5 또는 버전 9를 지원해야 합니다. NetFlow 데이터의 대상이 되는 각 ISE PSN에서 전용 인터페이스를 사용해야 합니다.

### ISE에서 NetFlow 프로브 활성화

- Step 1** Administration(관리)→System(시스템)→Deployment(구축)로 이동하고 RHS 창의 구축된 노드 목록에서 프로파일링을 수행할 정책 서비스 노드를 선택합니다.
- Step 2** Profiling Configuration(프로파일링 컨피그레이션) 탭을 선택하고 NetFlow 프로브를 활성화하기 위한 확인란을 선택합니다(그림 50).
- Step 3** NetFlow 트래픽 수집에 사용할 인터페이스를 선택합니다. 이는 라우팅 가능한 IP 주소를 사용하는 전용 인터페이스여야 합니다(그림 50).

그림 45 NetFlow 프로브 컨피그레이션



- Step 4**    내보낸 NetFlow를 수신 대기할 UDP 포트를 선택합니다. 이 값은 NetFlow 내보내기 디바이스에 구성된 값과 동일해야 합니다. 기본 포트는 UDP/9996입니다.
- Step 5**    Save(저장)를 클릭하여 변경 사항을 커밋합니다.
- Step 6**    프로파일링 서비스를 사용하여 구성된 다른 모든 정책 서비스 노드에 대해 이 절차의 단계를 반복합니다.

**참고:** 대다수의 NetFlow 지원 라우터 및 스위치는 NetFlow 내보내기를 위한 단일 대상만 지원합니다. 그러므로 고가용성을 고려해야 합니다. 또한 지정된 엔드포인트의 모든 프로파일 데이터는 동일한 정책 서비스 노드에서 수신하는 것이 좋습니다. 그러나 네트워크 컨피그레이션 및 기타 제한 사항으로 인해 불가능한 경우가 있을 수 있습니다.

**ISE(네트워크 리소스)에 네트워크 디바이스 추가**

액세스 디바이스도 NetFlow를 지원할 수 있지만, NetFlow를 NetFlow 프로브로 전송할 수 있는 다른 네트워크 디바이스를 ISE에서 네트워크 디바이스로 구성해야 한다는 특정 요구 사항은 없습니다.

**NetFlow 트래픽을 수신하도록 ISE 정책 서비스 노드 인터페이스 구성**

전용 인터페이스에서 NetFlow 트래픽을 수신하도록 NetFlow 프로브를 구성해야 합니다. ISE에서 전용 NetFlow 인터페이스를 구성하려면 다음 단계를 완료하십시오.

- Step 1**    원하는 인터페이스를 네트워크 스위치 포트에 물리적으로 연결합니다.
- Step 2**    ISE PSN 콘솔(CLI)에 액세스합니다. 해당 인터페이스를 활성화하고 그림 51과 같이 올바른 IP 주소를 할당합니다.

그림 46 ISE 프로브 전용 인터페이스 컨피그레이션 예

```

ise-psn-1/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise-psn-1/admin(config)# interface GigabitEthernet 3
ise-psn-1/admin(config-GigabitEthernet)# ip address 10.1.99.100 255.255.255.0

Changing the IP may result in undesired side effects on
any installed application(s).
Are you sure you want to proceed? Y/N [N]: Y
ISE M&T Log Processor is not running.
ISE M&T Log Collector is not running.
ISE M&T Alert Process is not running.
Stopping ISE Application Server...
ISE M&T Session Database is not running.
Stopping ISE Database processes...
Starting ISE Database processes...
ISE M&T Session Database is not running.
Starting ISE Application Server...
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.
ise-psn-1/admin(config-GigabitEthernet)# _
    
```

- Step 3** 지침에 따라 모든 프로세스가 실행 중인 상태인지 확인합니다.
- Step 4** **show running-config** 명령을 사용하여 새로 구성된 인터페이스의 컨피그레이션을 확인하고 활성화(종료되지 않음)되어 있는지 확인합니다(그림 52).

그림 47 ISE 프로브 전용 인터페이스 확인 예

```

ise-psn-1/admin# show running-config
Generating configuration...
?
hostname ise-psn-1
?
ip domain-name cts.local
?
interface GigabitEthernet 0
  ip address 10.1.100.5 255.255.255.0
  ipv6 address autoconfig
?
interface GigabitEthernet 1
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 2
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 3
  ip address 10.1.99.100 255.255.255.0
  ipv6 address autoconfig
?
ip name-server 10.1.100.100
--More--
    
```

- Step 5** NetFlow 데이터를 내보내야 하는 네트워크 디바이스에서 ICMP ping을 전송하여 새 프로브 인터페이스에 대한 연결을 확인합니다.
- Step 6** CLI 명령 `copy running-config startup-config`를 사용하여 변경 내용을 저장합니다.
- Step 7** 원하는 인터페이스를 해당 SPAN 대상 포트 또는 Network TAP 인터페이스에 물리적으로 연결합니다.

**참고:** VMware 어플라이언스에서 실행되는 정책 서비스 노드의 경우

프로파일링에 전용 인터페이스를 사용하기 위해 가상 어플라이언스에 대한 추가 가상 인터페이스가 구성되어 있는 것으로 가정합니다. 설치 시 완료하지 않았다면, ISE 노드를 종료하고 필수 인터페이스에 맞게 ESX 어플라이언스의 하드웨어 및 네트워킹 컨피그레이션을 업데이트해야 ISE 컨피그레이션을 계속 진행할 수 있습니다.

**NetFlow를 ISE PSN으로 내보내도록 NetFlow 지원 스위치/라우터 구성**

NetFlow 컨피그레이션은 NetFlow 지원 디바이스에 따라 다릅니다. 이 절차에는 Catalyst 6500 Series 스위치의 컨피그레이션 예가 포함되어 있습니다.

- Step 1** 전역 컨피그레이션 모드에서 NetFlow를 활성화하고 NetFlow 버전 9 지원, NetFlow 데이터를 공급할 인터페이스 IP 주소 및 데이터를 내보낼 정책 서비스 노드를 구성합니다. UDP 9996의 ISE 기본 포트 사양을 확인합니다.

```

mls netflow interface
mls flow ip interface-full
mls nde sender
mls nde interface
ip flow-cache timeout active 1
ip flow-export source Vlan100
ip flow-export version 9
ip flow-export destination 10.1.100.5 9996

```

**참고:** 위 예에서 Catalyst 6500 Series 스위치에는 Supervisor 720이 있습니다. 여기서는 PFC(Policy Feature Card)가 하드웨어 기반 NetFlow를 실행하고 MSFC(Multilayer Switch Feature Card)로 펀트되는 흐름이 소프트웨어에서 진행됩니다. `mls nde sender` 명령을 사용하여 NDE(NetFlow Data Export)를 수행하도록 PFC를 구성해야 합니다.

**Step 2** 선택적으로 다음과 같이 캡처 필터를 구성합니다.

```

ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture ip-id
ip flow-capture mac-addresses

```

**Step 3** 인그레스 인터페이스(엔드포인트측 인터페이스)에서 다음과 같이 NetFlow를 활성화합니다.

```

interface GigabitEthernet 2/47
description To cat3750x
ip address 10.1.50.1 255.255.255.0
ip flow ingress
!
interface Vlan40
description EMPLOYEE
ip address 10.1.40.1 255.255.255.0
ip helper-address 10.1.100.100
ip helper-address 10.1.100.5
ip flow ingress
!
interface Vlan41
description GUEST
ip address 10.1.41.1 255.255.255.0
ip helper-address 10.1.100.100
ip helper-address 10.1.100.5
ip flow ingress

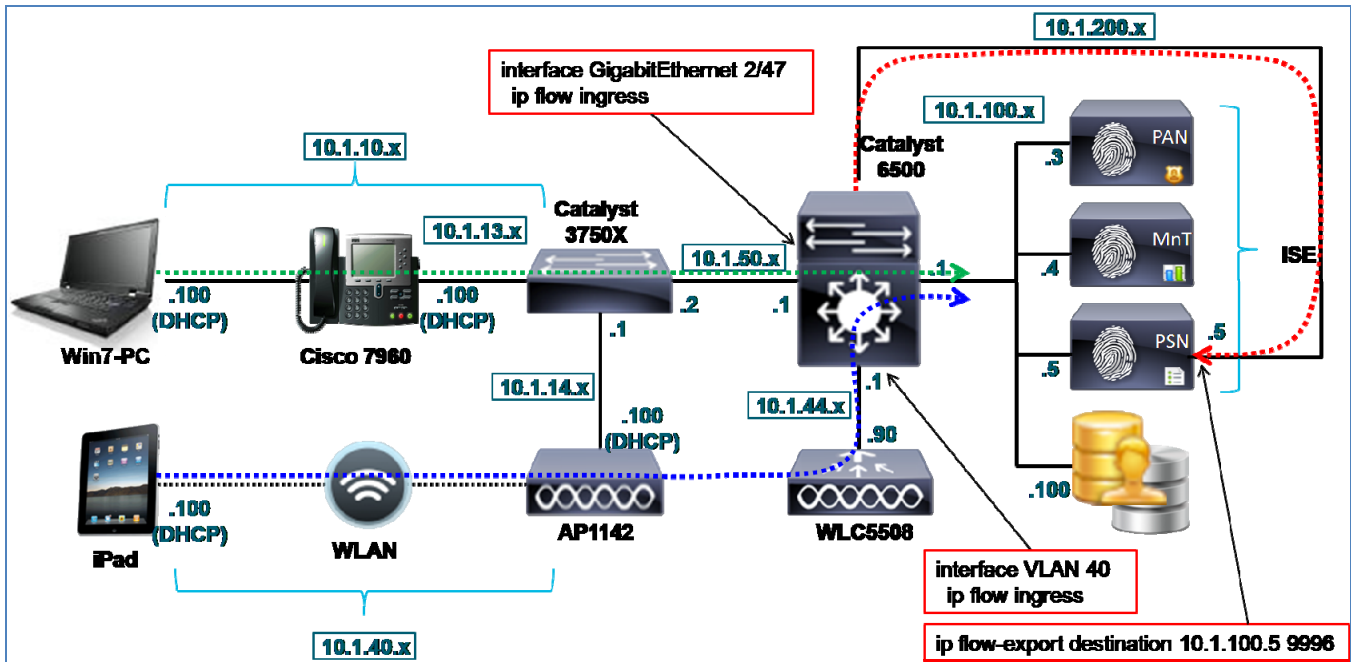
```

DHCP 프로브를 지원하는 컨피그레이션을 강조하기 위한 IP Helper 명령도 나와 있습니다. DHCP 프로브는 IP-MAC 주소 바인딩 정보를 가져오는 데 사용됩니다. 이를 통해 NetFlow 프로브는 일치하는 IP 특성을 기반으로 특성을 적용할 수 있습니다.

그림 53에서는 NetFlow가 적용되는 인터페이스와 NDE(NetFlow Data Export)의 대상을 보여줍니다. 목표는 Cisco Catalyst 3750-X Series 스위치를 통해 연결되는 유선 엔드포인트 및 Cisco 5500 Series Wireless LAN Controller를 통해 연결되는 무선 엔드포인트에서 트래픽을 캡처하는 것입니다.



그림 48 NetFlow 내보내기 예



**NetFlow 프로브 데이터 확인**

- Step 1 Administration(관리)→Identity Management(ID 관리)→Identities(ID)→Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 2 액세스 디바이스에서 엔드포인트의 연결을 해제했다가 다시 연결합니다.
- Step 3 엔드포인트에서 로그인하고 브라우저를 사용하여 웹 액세스를 시도하는 등 샘플 트래픽을 생성해 봅니다.
- Step 4 ISE 정책 관리 노드로 이동하고 Administration(관리)→Identity Management(ID 관리)→Identities(ID)로 이동합니다.
- Step 5 LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 6 새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 NetFlow 프로브에서 캡처한 특성을 표시합니다(그림 54).
- Step 7 그림 54의 예에는 NetFlow 내보내기를 사용하여 수집된 특성이 강조 표시되어 있습니다. 또한 NetFlow 프로브를 지원하기 위한 IP-MAC 바인딩을 구현할 수 있도록 RADIUS 및 DHCP 프로브가 활성화되었습니다.

그림 49 NetFlow 특성 예

Endpoint List > 00:50:56:A0:0B:3A

**Endpoint**

\* MAC Address **00:50:56:A0:0B:3A**

\* Policy Assignment

Static Assignment

\* Identity Group Assignment

Static Group Assignment

**Attribute List**

EndPointProfilerServer	ise-psr-1
EndPointSource	NETFLOW Probe
ExternalGroups	cts.local/users/contractors\,cts.local/users/domain users\,cts.local/builtin/users
FIRST_SWITCHED	137839523
FLOW_SAMPLER_ID	0
FQDN	win7-pc.cts.local
FragmentOffset	0
FrameID-IP-Address	10.1.10.100
GroupsOrAttributesProcessFailure	true
INPUT_SNMP	49
IN_BYTES	1869
IN_PKTS	6
IPV4_DST_ADDR	173.37.144.208
IPV4_NEXT_HOP	172.16.1.1
IPV4_SRC_ADDR	10.1.10.100
IdentityGroup	Microsoft-Workstation
IdentityPolicyMatchedRule	Default
L4_DST_PORT	80
L4_SRC_PORT	53149
LAST_SWITCHED	137839715
Location	Location#All Locations#North_America#RTP
MACAddress	00:50:56:A0:0B:3A
MatchedPolicy	Windows7-Workstation
MessageCode	3002
NAS-IP-Address	10.1.50.2
NAS-Port	50101
NAS-Port-Id	GigabitEthernet1/0/1
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device Type#All Device Types#Wired, Location#All Locations#North_America#RTP
NetworkDeviceName	cat3750x
OUI	VMware, Inc.
OUTPUT_SNMP	52
PROTOCOL	6

빨간색으로 강조 표시된 키 특성에는 다음과 같은 항목이 있습니다.

- EndPointSource = NetFlow 프로브
- IPV4\_DST\_ADDR = 173.37.144.208(cisco.com)
- IPV4\_SRC\_ADDR = 10.1.10.100(win7-pc)
- L4\_DST\_PORT = 80(HTTP)
- L4\_SRC\_PORT = 53149
- PROTOCOL = 6(TCP)

flow capture 문을 사용하는 경우 다음과 같은 추가 특성을 확인할 수 있습니다.

- DST\_VLAN/SRC\_VLAN
- IN\_SRC\_MAC/OUT\_DST\_MAC
- MAX\_TTL/MIN\_TTL

NetFlow 데이터가 수집되고 있는지 확인하려면 **show ip cache flow** 및 **show mls netflow ip** 명령을 사용할 수 있습니다. 다음 예에서는 **show ip cache flow** 명령을 사용합니다.

```

cat6503#show ip cache flow
-----
Displaying software-switched flow entries on the MSFC in Module 1:

IP packet size distribution (348128 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .548 .342 .077 .005 .000 .000 .000 .000 .000 .000 .015 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
    .000 .000 .007 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 15760 added
  251284 aged polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  6 active, 1018 inactive, 47280 added, 15760 added to flow
  0 alloc failures, 2775 force free
  1 chunk, 24 chunks added
  last clearing of statistics never

Protocol      Total      Flows      Packets Bytes   Packets Active(Sec) Idle(Sec)
-----
              Flows      /Sec       /Flow  /Pkt   /Sec    /Flow    /Flow
TCP-Telnet    44         0.0        91     42     0.0     14.4     7.8
TCP-WWW       1361      0.0        22     45     0.0     0.0      14.2
TCP-other     1602      0.0        25     51     0.0     0.1      13.6
UDP-DNS       128       0.0        1      70     0.0     0.0      15.4
UDP-NTP       1375      0.0        1      76     0.0     0.0      15.5
UDP-other     2880      0.0        3     338    0.0     3.8      15.4
ICMP          6985      0.0        34     30     0.0     0.4      13.4
IP-other      1383      0.0        13     65     0.0     58.3     2.0
Total:        15758     0.0        22     46     0.0     6.0      13.0

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
-----
Gi2/47     10.1.50.2    Null       224.0.0.10    58 0000 0000   4
Gi2/47     10.1.13.1    Null       10.1.100.7    11 0043 0043   3
    
```

```

Displaying hardware-switched flow entries in the PFC (Active) Module 1:
SrcIf          SrcIPAddress    DstIf          DstIPAddress    Pr  SrcP  DstP  Pkts
-----
Gi2/47         10.1.50.1       Gi2/47         10.1.50.2       58 0000 0000    0
Gi2/47         10.1.50.2       ---           10.1.100.1      11 007B 007B    0
Gi2/47         10.1.50.2       ---           10.1.50.1       58 0000 0000    0
Gi2/47         10.1.100.1      Gi2/47         10.1.50.2       11 007B 007B    0
Gi2/47         10.1.50.2       V1100         10.1.100.5      11 CC9B 00A2   15
Gi2/47         10.1.13.1       V1100         10.1.100.100    11 0043 0043  124
Gi2/47         10.1.13.1       V1100         10.1.100.5      11 0043 0043  124
Gi2/47         10.1.13.1       V1100         10.1.100.6      11 0043 0043  124
Gi2/47         10.1.50.2       ---           224.0.0.10     58 0000 0000   84
V140          10.1.40.1       ---           224.0.0.10     58 0000 0000    0
Gi2/47         10.1.50.2       V1100         10.1.100.4      11 C8D5 5022   30
Gi2/47         10.1.13.1       ---           10.1.100.7      11 0043 0043    0
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 CA72 0035    1
Gi2/47         10.1.50.2       V1100         10.1.100.5      11 066E 0715  128
V141          10.1.41.1       ---           224.0.0.10     58 0000 0000    0
Gi2/47         10.1.50.2       V1100         10.1.100.5      11 06A4 7195    2
Gi2/47         10.1.50.2       V1100         10.1.100.6      11 E6D7 00A2   15
Gi2/47         10.1.50.2       ---           10.1.100.7      11 C748 00A2    0
Gi2/47         10.1.50.2       V1100         10.1.100.5      11 066D 0714    6
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 E5CC 0035    1
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 DA8B 0035    1
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 C114 0035    1
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 FC03 0035    1
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 D295 0035    1
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 ED48 0035    1
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 E7E8 0035    1
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 D770 0035    1
Gi2/47         10.1.10.100     V1100         10.1.100.100    11 D5AB 0035    1
--           0.0.0.0         ---           0.0.0.0         00 0000 0000  31K
    
```

**Step 8** 다음 예에서는 `show mls netflow ip`를 사용합니다.

```

at6503#show mls netflow ip
Displaying Netflow entries in Active Supervisor EARL in module 1
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f          :AdjPtrPkts      Bytes
Age   LastSeen  Attributes
-----
10.1.50.2      10.1.100.1    udp :ntp      :ntp             Gi2/47           :0x00             0
43   20:26:48  L2 - Dynamic
10.1.44.90     10.1.14.100   udp :16792    :5246            Gi2/47           :0x03             359
35   20:27:26  L3 - Dynamic
10.1.100.100  10.1.13.1     udp :67        :67              Gi2/47           :0x04             1846
32   20:27:30  L3 - Dynamic
10.1.100.5    10.1.50.2     udp :52379    :162             Gi2/47           :0x015            2734
335  20:23:02  L3 - Dynamic
10.1.100.4    10.1.50.2     udp :51413    :20514           Gi2/47           :0x030            5286
334  20:23:58  L3 - Dynamic
10.1.100.5    10.1.50.2     udp :1646     :1813            Gi2/47           :0x04             2680
32   20:27:30  L3 - Dynamic
10.1.100.100  10.1.10.100   udp :51826    :dns             Gi2/47           :0x01             61
211  20:24:00  L3 - Dynamic
10.1.44.90     10.1.14.100   udp :16792    :5247            Gi2/47           :0x06             901
30   20:27:30  L3 - Dynamic
224.0.0.10    10.1.41.1     88  :0            :0               V141             :0x00             0
426  20:27:27  Multicast
10.1.100.5    10.1.50.2     udp :1700     :29077           Gi2/47           :0x02             132
335  20:23:56  L3 - Dynamic
    
```

10.1.100.6	10.1.50.2	udp	:59095	:162	Gi2/47	:0x015	2734
335	20:23:02	L3 - Dynamic					
10.1.100.7	10.1.50.2	udp	:51016	:162	Gi2/47	:0x00	0
335	20:23:02	L3 - Dynamic					
10.1.100.5	10.1.50.2	udp	:1645	:1812	Gi2/47	:0x06	1365
270	20:23:56	L3 - Dynamic					
10.1.100.100	10.1.10.100	udp	:54699	:dns	Gi2/47	:0x01	64
211	20:24:00	L3 - Dynamic					
10.1.100.1	10.1.50.2	udp	:ntp	:ntp	Gi2/47	:0x00	0
43	20:26:48	L3 - Dynamic					
17.172.232.209	10.1.40.101	tcp	:61858	:443	V140	:0x02	173
17	20:27:14	L3 - Dynamic					
17.172.232.209	10.1.40.101	tcp	:61858	:443	V140	:0x00	0
17	20:27:14	L2 - Dynamic					
10.1.40.101	17.172.232.209	tcp	:443	:61858	V140	:0x00	0
17	20:27:14	L2 - Dynamic					
0.0.0.0	0.0.0.0	0	:0	:0	--	:0x032283	20941051
1573	20:27:31	L3 - Dynamic					

**Step 9** NetFlow 내보내기 컨피그레이션과 함께 흐름이 ISE 정책 서비스 노드로 전송되고 있는지 확인하려면 다음과 같이 **show ip flow export** 명령을 사용합니다.

```

cat6503# sh ip flow export
Flow export v9 is enabled for main cache
Export source and destination details :
VRF ID : Default
Source(1)      10.1.100.1 (Vlan100)
Destination(1) 10.1.99.5 (9996)
Version 9 flow records
20408 flows exported in 7635 udp datagrams
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
0 export packets were dropped enqueueing for the RP
0 export packets were dropped due to IPC rate limiting
0 export packets were dropped due to Card not being able to export
    
```

### 네트워크 검사(NMAP) 프로브를 사용한 프로파일링

네트워크 검사 프로브는 내장된 버전의 오픈 소스 Network Mapper 유틸리티를 기반으로 합니다. NMAP(Network Mapper)는 대규모 네트워크에 연결된 엔드포인트가 있는지 검사한 다음 개별 호스트에 대한 검사를 수행하여 OS(운영 체제), OS 버전 및 서비스(애플리케이션 이름 및 버전)를 탐지하도록 설계되었습니다.

다른 ISE 프로브는 직접 엔드포인트를 조사하는 대신 디바이스에서 생성된 데이터 또는 다른 네트워크 디바이스에서 생성된 데이터를 구문 분석하는 등 간접적인 데이터 수집 방법을 사용한다는 측면에서 “수동” 프로브로 간주됩니다. 네트워크 검사 프로브는 엔드포인트와 직접 통신하여 소스의 정보를 가져오므로 “활성” 평가 메커니즘으로 간주됩니다.

## NMAP 프로브 검사 작업

NMAP 프로브가 검사를 수행하는 경우 다음 NMAP 작업 중 하나 이상을 수행할 수 있습니다.

- 운영 체제 검사
- SNMP 포트 검사
- 공통 포트 검사

OS(운영 체제) 검사는 OS 및 엔드포인트 버전을 탐지하는 데 사용됩니다. 이는 집약적인 작업입니다.

SNMP 포트 검사에서는 UDP 포트 161(SNMP 데몬) 및 162(SNMP 트랩)가 열려 있는지 탐지합니다. 열려 있는 경우 **public** 커뮤니티 문자열을 사용하여 엔드포인트를 대상으로 SNMP 쿼리를 시작하여 시스템 MIB 및 기타 소스에서 엔드포인트 관련 추가 정보를 수집합니다. 이 프로브는 기본적으로 SNMP가 활성화되어 있으며 기본 커뮤니티 문자열 **public**을 포함하는 네트워크 프린터와 같은 엔드포인트에서 특히 유용한 것으로 검증되었습니다.

참고: NMAP 프로브는 직접 엔드포인트를 쿼리하는 데 기본 커뮤니티 문자열 **public**만 사용할 수 있습니다. 이 값은 현재 구성할 수 없습니다.

엔드포인트가 아닌 네트워크 디바이스를 쿼리하며 네트워크 디바이스 설정에서 SNMP 설정을 구성할 수 있는 SNMP 쿼리 프로브와 이 프로브를 혼동해서는 안 됩니다.

공통 포트 검사에서는 표 5에 표시된 것처럼 15개의 공통 TCP 및 UDP 포트를 검사합니다.

표 3 NMAP 프로브 공통 포트 검사: TCP 및 UDP 포트

TCP 포트		UDP 포트	
포트	서비스	포트	서비스
21/tcp	ftp	53/udp	도메인
22/tcp	ssh	67/udp	dhcps
23/tcp	텔넷	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	도메인	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp

143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3306/tcp	mysql	631/udp	ipp
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

참고: 검사되는 공통 포트 목록은 현재 구성할 수 없습니다.

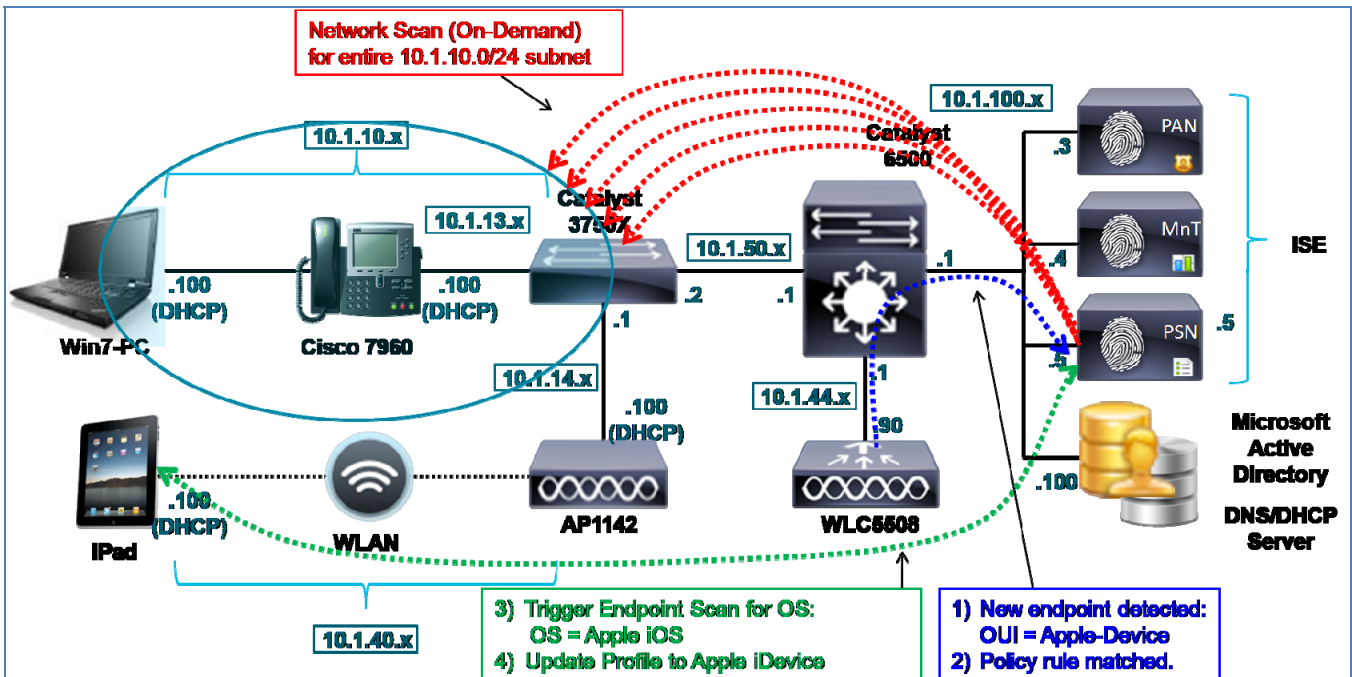
관리자는 실행되는 서비스를 기반으로 엔드포인트를 다르게 분류 및 보호하도록 선택할 수 있습니다. 예를 들어 웹 서비스를 실행하는 Windows 서버의 경우 비 HTTP 요청으로부터 보호하기 위해서는 특정 권한 부여 정책(dACL, VLAN, SGT)을 적용해야 할 수 있습니다. 반면, 웹 서버를 실행하는 Windows 또는 Linux 워크스테이션은 유사한 권한 부여 방법을 통해 액세스가 거부되거나 격리되어야 합니다.

다음 두 가지 방법 중 한 가지를 사용하여 NMAP 프로브를 시작할 수 있습니다.

- 네트워크 검사
- 엔드포인트 검사

그림 55의 샘플 토폴로지에는 10.1.10/24 서브넷에서 시작되는 네트워크 검사(빨간색으로 강조 표시됨)가 나와 있습니다.

그림 50 MAP 프로브 예



## NMAP 프로브 네트워크 검사

네트워크 검사는 하나 또는 여러 네트워크 엔드포인트에 대한 온디맨드 검사로, 관리 사용자가 ISE 관리 노드에서 수동으로 시작할 수 있습니다. 이 프로브는 수동 네트워크 검사를 실행하기 위해 정책 서비스 노드에서 활성화할 필요가 없습니다. 관리 사용자는 검사할 IP 서브넷을 지정하고 **Run Scan(검사 실행)** 버튼을 클릭하기만 하면 됩니다.

네트워크 검사는 SNMP 포트 및 운영 체제 검사를 모두 수행합니다. 대규모 네트워크 검사는 시간이 오래 소요되는 작업으로, 정책 서비스 노드에 부하를 가중시킬 수 있으므로 서브넷 범위를 신중히 선택하는 것이 좋습니다. 검사를 시작한 후에 관리 사용자는 링크를 클릭하여 결과가 표시되는 페이지로 이동할 수 있습니다.

## NMAP 프로브 엔드포인트 검사

엔드포인트 검사는 단일 엔드포인트에서 트리거되는 검사입니다. 이 검사는 프로파일링 정책의 일치 규칙을 기반으로 자동으로 시작됩니다. 트리거된 검사를 수행하려면 엔드포인트는 프로파일 정책은 물론 네트워크 검사 작업이 할당된 지정 조건과 일치해야 합니다. 네트워크 검사 작업은 프로파일 규칙에 따라 구성할 수 있으며 수행할 특정 검사 작업에 대해 정의합니다.

기본적으로 일치하는 프로파일 조건에 대한 응답으로 할당할 수 있는 NMAP 작업에는 3가지가 있습니다.

- **CommonPortsAndOS-scan**(공통 포트 + OS 검사)
- **OS-scan**(OS 검사만 해당)
- **SNMPPortsAndOS-scan**(SNMP 포트 + OS 검사)

그림 55의 샘플 토폴로지에는 이러한 프로세스가 나와 있습니다. 새 엔드포인트는 최근 프로브 이벤트(파란색으로 표시됨)의 결과로 탐지되었습니다. 엔드포인트는 수집된 프로파일 데이터를 바탕으로 MAC 주소의 OUI에 따라 Apple 디바이스로 인식됩니다. 그러나 엔드포인트가 Mac OS X 워크스테이션, Apple iDevice 또는 다른 Apple 엔드포인트인 경우에는 인식되지 않습니다. 정책 규칙이 일치하여 Apple 디바이스(녹색으로 표시됨)에 대해 지정된 OS 검사가 트리거됩니다. 결과적으로 엔드포인트에서 Apple iOS가 실행 중임을 인식하여 프로파일이 모바일 Apple 디바이스 프로파일로 업데이트됩니다.

알 수 없는 프로파일과 일치하는 엔드포인트가 SNMP 포트 및 OS 검사 모두를 사용하여 자동으로 검사됩니다. 이는 구성 가능한 응답이 아닙니다. 이는 ISE 프로파일링에서 검색되었지만 프로파일링되지 않은 엔드포인트 관련 추가 정보를 신속하게 가져오도록 설계되었습니다.

**참고:** 일부 엔드포인트에는 엔드포인트를 검사하려는 시도를 차단하는 개인 방화벽 또는 다른 에이전트 소프트웨어가 활성화되어 있습니다. 이러한 엔드포인트에서는 NMAP 데이터를 거의 생성하지 않거나 전혀 생성하지 않습니다. 또한 네트워크 액세스가 제한되어 있는 엔드포인트는 NMAP 작업을 수신하거나 NMAP 작업에 응답하지 못할 수 있습니다.



### NMAP 프로브 및 IP-MAC 주소 바인딩 요구 사항

NMAP는 알려진 IP 주소를 기반으로 합니다. NMAP 프로브가 엔드포인트의 특성을 수집하지만 해당 특성을 특정 MAC 주소에 상호 연결할 수 없는 경우 데이터가 삭제됩니다. 정책 서비스 노드가 검사하는 엔드포인트와 동일한 세그먼트에 있는 경우 로컬 ARP 캐시에서 IP-MAC 주소 바인딩을 학습하고 엔드포인트를 직접 내부 엔드포인트 데이터베이스에 추가할 수 있습니다. 따라서 NMAP 프로브 데이터를 수집하기 전에 다른 프로브를 통해 IP-MAC 주소 바인딩을 학습해야 합니다. 이 정보를 제공하는 데 사용할 수 있는 프로브는 다음과 같습니다.

- RADIUS(Framed-IP-Address를 통해)
- DHCP(dhcp-requested-address를 통해)
- SNMP 쿼리(SNMP 폴링을 통해)

**Cisco 모범 사례:** ISE에서 아직 엔드포인트를 인증하지 않은 경우 ISE 구축을 검색하는 단계에서 대규모 네트워크 블록에 대해 네트워크 검사를 실행하여 관련된 OS 및 엔드포인트 정보와 함께 엔드포인트를 검사하고 탐지할 수 있습니다. 이 단계에서는 엔드포인트 ARP 표 정보를 저장하는 모든 네트워크 디바이스에 대해 SNMP 쿼리 프로브도 활성화하는 것이 좋습니다. 이렇게 하면 정적으로 주소가 지정된 엔드포인트를 포함하여 엔드포인트 MAC 및 IP 주소를 검색할 수 있습니다. 그러면 PSN은 이제 네트워크 검사 중에 검색된 각 IP 주소별로 MAC 주소를 가질 수 있으므로 NMAP 프로브 수집을 지원하게 됩니다.

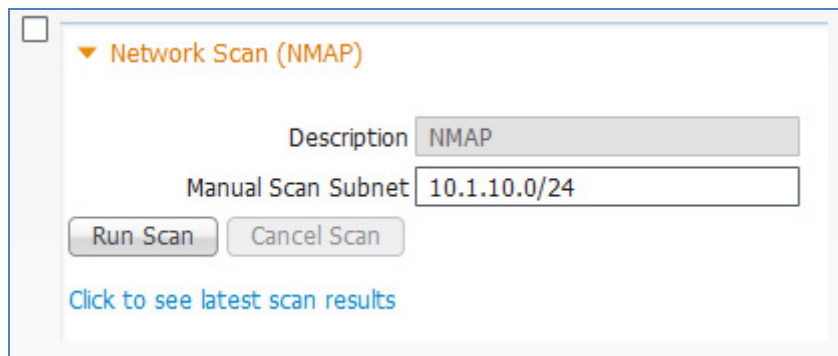
### NMAP 프로브 구성

위에서 설명한 것처럼 NMAP 프로브를 실행하는 방법에는 2가지가 있습니다. 즉, 수동 온디맨드 네트워크 검사와 단일 엔드포인트에 대해 자동으로 트리거되는 검사 이벤트가 있습니다. 각 방법을 사용하는 절차는 개별적으로 다릅니다.

#### 네트워크 검사 실행

- Step 1** Administration(관리)→System(시스템)→Deployment(구축)로 이동하고 RHS 창의 구축된 노드 목록에서 네트워크 검사를 수행할 정책 서비스 노드를 선택합니다.
- Step 2** Profiling Configuration(프로파일링 컨피그레이션) 탭을 선택합니다.
- Step 3** 네트워크 검사를 실행하려면 Network Scan (NMAP)(네트워크 검사(NMAP)) 옵션을 선택하여 해당 내용을 확장합니다(그림 56).


그림 51: NMAP 프로브



참고: 그림 56에서와 같이 프로브를 활성화하는 것은 수동 네트워크 검사를 수행하기 위한 요구 사항이 아닙니다.

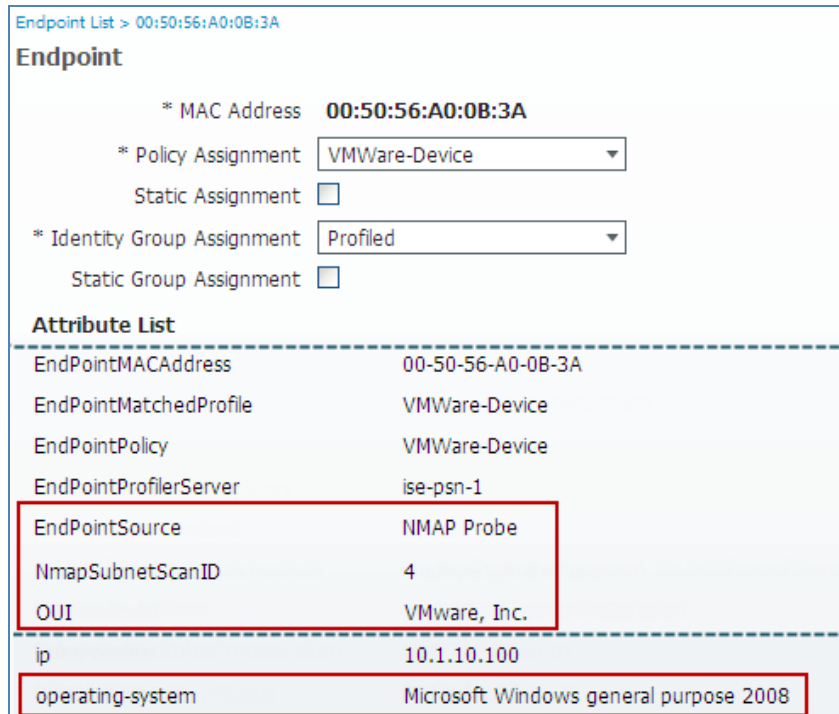
- Step 4** 예에 표시된 형식으로 검사할 IP 서브넷 주소 및 마스크를 입력합니다. 이 예에서는 클래스 C 서브넷에 해당하는 마스크 비트 숫자(24)와 함께 클래스 C 서브넷(10.1.10.0)이 입력되었음을 보여줍니다.
- Step 5** 기타 서브넷 크기를 선택할 수 있지만 검사를 실행하기 위한 전반적인 시간 및 로드를 줄일 수 있도록 선택에 포함할 네트워크 범위 및 엔드포인트 수를 고려해야 합니다.
- Step 6** Run Scan(검사 실행)을 클릭합니다.
- Step 7** 활성 검사를 취소하려면 Cancel Scan(검사 취소)을 클릭합니다. 그렇지 않고 Administration(관리)→Identity Management(ID 관리)→Identities(ID) 페이지로 바로 이동하려면 “Click to see latest scan results”(최신 검사 결과를 보려면 클릭)를 선택합니다. 페이지에서 벗어나 이동한 경우에도 검사는 완료될 때까지 계속 진행됩니다.
- Step 8** Identities(ID) 페이지의 LHS 창에서 **Latest Network Scan Results(최신 네트워크 검사 결과)**를 선택합니다. 검사 진행 상황에 따라 긍정적 검사 결과를 가진 엔드포인트가 RHS 창에 표시됩니다(그림 57).

그림 52 NMAP 네트워크 검사 결과 예

Latest Network Scan Results Endpoints			
 Edit			
<input type="checkbox"/> Endpoint Profile	MAC Address	Profiler Server	Static Assignment
<input type="checkbox"/> Cisco-Device	1C:DF:0F:8F:60:42	ise-psn-1	false
<input type="checkbox"/> <b>VMWare-Device</b>	00:50:56:A0:0B:3A	ise-psn-1	false

- Step 9** MAC 주소별 엔드포인트 항목을 클릭하여 결과를 확인합니다.

그림 53 네트워크 검사의 NMAP 프로브 특성 예



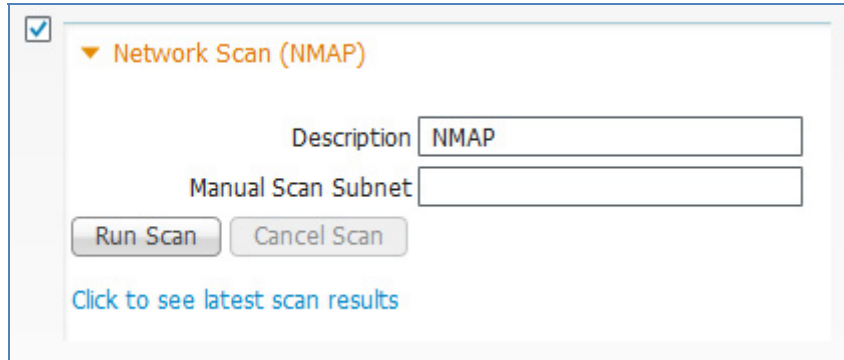
선택된 엔드포인트는 Windows 7 PC입니다. 수동 네트워크 검사 출력에서 볼 수 있는 것처럼 NMAP는 일반 OS 클래스(Windows 7 및 Windows 2008은 공통 코드베이스를 공유함)를 탐지했지만, 현재 VMware 프로파일(OUI 조건과의 일치율 기반)을 벗어나는 엔드포인트를 세부적으로 분류하기에는 사용 가능한 정보가 충분하지 않습니다. EndPointSource는 NMAP 프로브로 표시됩니다. ScanID는 수동 네트워크 검사 이벤트에 할당된 ID를 나타냅니다.

참고: NMAP 프로브에서 성공적으로 검사하기 위해서는 기본 Windows 7 방화벽 설정을 비활성화해야 했습니다.

**엔드포인트 검사를 위한 NMAP 프로브 구성**

- Step 1** Administration(관리)→System(시스템)→Deployment(구축)로 이동하고 RHS 창의 구축된 노드 목록에서 프로파일링을 수행할 정책 서비스 노드를 선택합니다.
- Step 2** Profiling Configuration(프로파일링 컨피그레이션) 탭을 선택하고 Network Scan (NMAP)(네트워크 검사(NMAP))이라는 확인란을 선택합니다(그림 59).

그림 54 NMAP 프로브 컨피그레이션



- Step 3 Save(저장)를 클릭하여 변경 사항을 커밋합니다.
- Step 4 프로파일링 서비스를 사용하여 구성된 다른 모든 정책 서비스 노드에 대해 이 절차의 단계를 반복합니다.

### 네트워크 검사(NMAP) 작업 검토

- Step 1 Policy(정책)→Policy Elements(정책 요소)→Results(결과)로 이동하고 LHS 창에서 Profiling(프로파일링)→Network Scan (NMAP) Actions(네트워크 검사(NMAP) 작업)를 선택합니다.
- Step 2 기본 NMAP 작업을 검토합니다(그림 60).

그림 55 NMAP 검사 작업

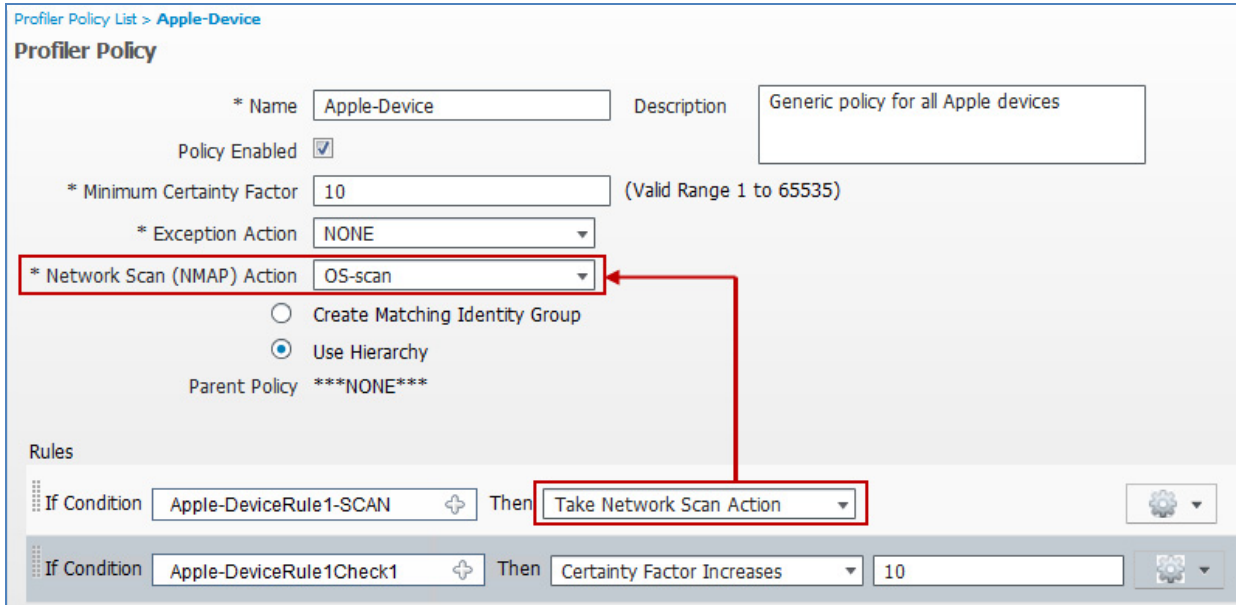
Network Scan Actions	
<span>Edit</span> <span>+ Add</span> <span>X Delete</span>	
<input type="checkbox"/> Network Scan (NMAP) Action Name	Description
<input type="checkbox"/> CommonPortsAndOS-scan	Perform operating system and common ports detection (not SNMP).
<input type="checkbox"/> OS-scan	Perform operating system detection.
<input type="checkbox"/> SNMPPortsAndOS-scan	Perform operating system and SNMP ports detection. Used for 'Unknown' endpoints.

- Step 3 가장 일반적인 옵션이 구성되었지만 필요한 경우 추가 NMAP 작업을 정의할 수 있습니다. 예를 들어 트리거된 응답의 일부로서만 공통 포트 또는 SNMP 포트를 검사하는 **CommonPorts** 또는 **SNMPPorts**라는 새 검사 작업을 생성할 수 있습니다.

### NMAP 작업을 프로파일링 정책 조건에 할당하는 컨피그레이션 검토

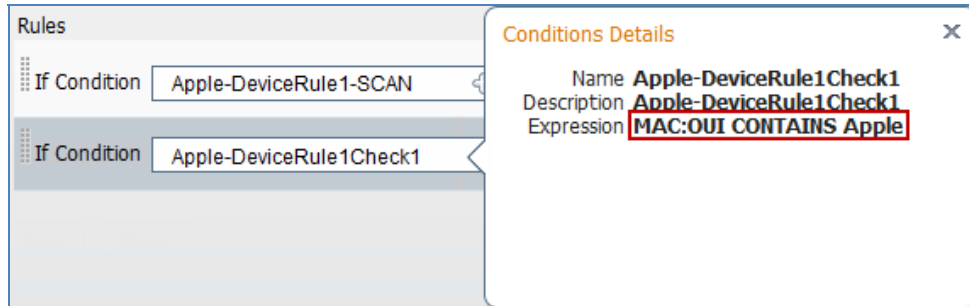
- Step 1 Policy(정책)→Profiling(프로파일링)으로 이동하고 RHS 창 목록에서 Apple-디바이스 프로파일을 선택합니다(그림 61).

그림 56 NMAP 검사 작업을 사용하는 프로파일링 정책 예



**Step 2** Apple-디바이스 프로파일에는 2가지 조건이 있습니다. 두 번째 조건 이름의 오른쪽을 클릭하여 규칙 항목의 내용을 검토합니다(그림 62).

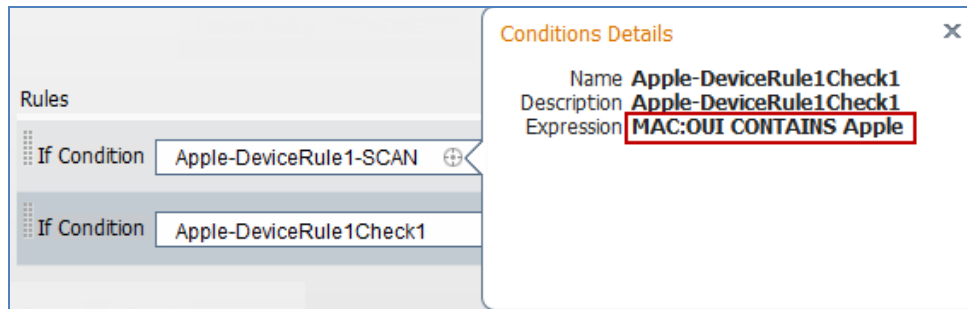
그림 57 NMAP 검사에 대한 프로파일링 정책 규칙 예 1



이 규칙은 확실성 요인(CF)을 증가시켜 엔드포인트를 이 프로파일에 일치시키는 데 사용됩니다. MAC 주소의 OUI가 “Apple”과 일치하는 경우 조건이 일치합니다.

**Step 3** 첫 번째 조건 이름의 오른쪽을 클릭하여 해당 내용을 검토합니다(그림 63).

그림 58 NMAP 검사에 대한 프로파일링 정책 규칙 예 2



이 규칙은 엔드포인트 검사를 트리거하는 데 사용됩니다. 첫 번째 조건은 두 번째 규칙에 사용된 조건과 동일합니다. 그러므로 두 번째 조건을 기반으로 이 프로파일과 일치하는 엔드포인트는 자동으로 첫 번째 조건과 일치하게 되며 선택된 네트워크 검사 작업(OS-scan)을 트리거합니다.

개별 규칙 항목을 추가하거나 제거하려면 기존 규칙 표 오른쪽에 있는 기어 아이콘을 클릭하면 됩니다.

**Step 4** 검토 또는 변경을 완료한 경우 페이지 하단의 Save(저장)를 클릭하여 변경 사항을 커밋합니다.

이 절차의 목적은 일치 조건을 기반으로 네트워크 검사 작업이 프로파일에 적용되는 방식을 검토하는 것입니다. 프로파일링 정책 컨피그레이션에 대해서는 [프로파일링 정책 구성](#) 섹션에서 자세히 다뤄집니다.

**트리거된 엔드포인트 검사 작업을 기반으로 NMAP 프로브 데이터 확인**

- Step 1** Administration(관리)→Identity Management(ID 관리)→Identities(ID)→Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 2** NMAP 프로브를 사용하여 프로파일링을 지원하도록 구성된 액세스 디바이스에서 엔드포인트의 연결을 해제했다가 다시 연결합니다.
- Step 3** ISE 정책 관리 노드로 이동하고 Administration(관리)→Identity Management(ID 관리)→Identities(ID)로 이동합니다.
- Step 4** LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 5** 새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 HTTP 프로브에서 캡처한 특성을 표시합니다.
- Step 6** 이 예에서는 NMAP 프로브 외에 RADIUS 및 DHCP(IP Helper) 프로브만 활성화되었습니다. 이와 같은 추가 프로브는 새 엔드포인트를 검색하고 이를 적절한 MAC 주소 및 IP 주소 정보와 함께 내부 엔드포인트 데이터베이스에 추가하는 데 사용됩니다. 이렇게 하면 NMAP 프로브 데이터를 적절히 적용하고 해당 데이터가 삭제되지 않도록 하는 데 도움이 됩니다.

그림 59 엔드포인트 검사의 NMAP 프로브 특성 예 1

Endpoint List > 7C:6D:62:E3:D5:05

**Endpoint**

- \* MAC Address **7C:6D:62:E3:D5:05**
- \* Policy Assignment Apple-Device
- Static Assignment
- \* Identity Group Assignment Profiled
- Static Group Assignment

**Attribute List**

MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-Device
MessageCode	3001
NAS-IP-Address	10.1.44.90
NAS-Identifier	Cisco_0c:99:a4
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
NetworkDeviceGroups	Device Type#All Device Types#Wireless, Location#All Locations#I
NetworkDeviceName	wlc5508
NmapScanCount	1
OUI	Apple, Inc

잘린 출력에서는 이 엔드포인트(NmapScanCount)에 대해 초기 검사가 실행되었지만 Apple에 대한 프로파일 할당은 여전히 OUI를 기반으로 하고 있음을 표시합니다. 검사는 Apple-디바이스에 대해 일치하는 프로파일 조건을 기반으로 트리거됩니다.

OS 검사는 단기간 내에 완료되어야 합니다. 검사를 종료하고 동일한 엔드포인트를 다시 선택하여 업데이트된 프로파일링 특성을 검토합니다(그림 65).

다음과 같은 키 특성이 강조 표시되어 있습니다.

- EndPointPolicy
- LastNmapScanTime
- NmapScanCount
- OUI
- operating-system

그림 60 엔드포인트 검사의 NMAP 프로브 특성 예 2

Endpoint List > 7C:6D:62:E3:D5:05

**Endpoint**

\* MAC Address **7C:6D:62:E3:D5:05**

\* Policy Assignment

Static Assignment

\* Identity Group Assignment

Static Group Assignment

**Attribute List**

EndPointMACAddress	7C-6D-62-E3-D5-05
EndPointMatchedProfile	Apple-iDevice
EndPointPolicy	Apple-iDevice
EndPointProfilerServer	ise-psn-1
EndPointSource	RADIUS Probe
ExternalGroups	cts.local/users/employees\,cts.local/users/domain users\
Framed-IP-Address	10.1.40.101
IdentityAccessRestricted	false
IdentityGroup	Apple-iDevice
IdentityPolicyMatchedRule	Default
LastNmapScanTime	2012-May-03 05:59:56 UTC
Location	Location#All Locations#North_America#RTP
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iDevice
NAS-Port-Type	Wireless - IEEE 802.11
NetworkDeviceGroups	Device Type#All Device Types#Wireless, Location#All L
NetworkDeviceName	wlc5508
NmapScanCount	2
OUI	Apple, Inc
PolicyVersion	22
PostureAssessmentStatus	NotApplicable
host-name	Apple-1pad
htype	Ethernet (10Mb)
ip	10.1.40.101
op	BOOTREQUEST
operating-system	Apple iOS general purpose 4.X (accuracy 93%)
secs	0

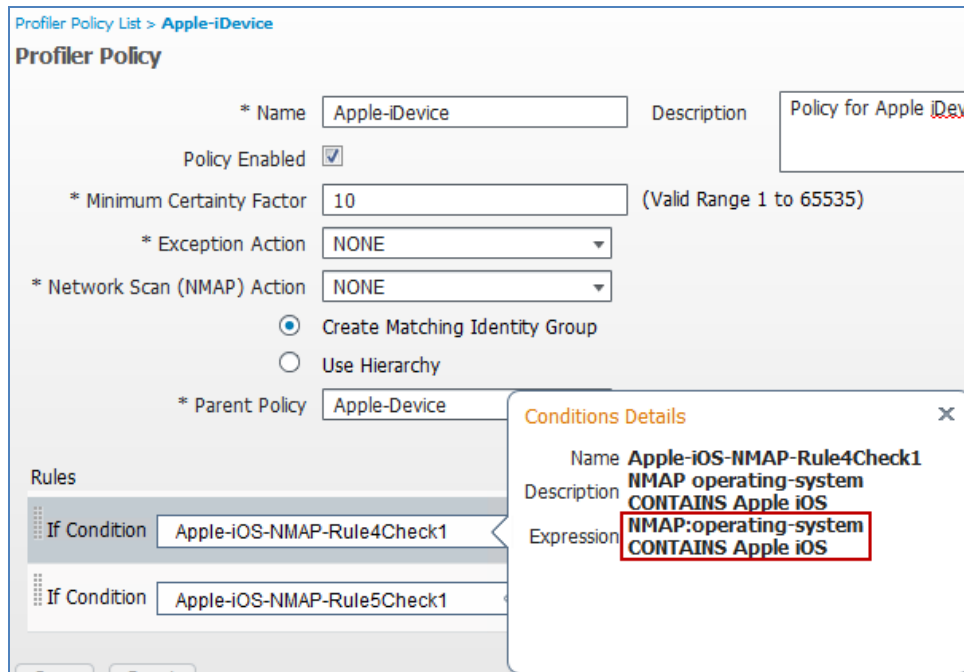


이 예에서는 NMAP 검사가 완료되었음을 명확히 알 수 있습니다. **EndPointSource** 특성은 RADIUS에서 마지막 업데이트가 수행되었음을 나타냅니다. 이는 여러 소스에서 프로파일링 데이터를 제공하면서 값이 지속적으로 변경되기 때문에 가능합니다.

**LastNmapScanTime** 및 **NmapScanCount** 특성은 디바이스 분류에 있어 실제로는 중요하지 않지만 NMAP 프로브에서 추가한 특성을 보여주기 위해 강조 표시되어 있습니다.

**OUI** 특성은 Apple이지만 이제 할당된 프로파일은 보다 일반적인 Apple-디바이스가 아니라 Apple-iDevice의 프로파일입니다. 이는 트리거된 NMAP 검사 결과에서 일치하기 때문이며, 해당 결과에 따르면 엔드포인트 OS가 Apple iOS인 것으로 나타났습니다. Policy(정책)→Profiling(프로파일링)에서 Apple-iDevice 프로파일의 내용을 검토하면 이 프로파일이 NMAP OS 검사 결과에 따라 두 조건 중 하나와 일치한다는 것을 알 수 있습니다(그림 66).

그림 61 Apple-iDevice에 대한 프로파일링 정책



**Step 7** NMAP 검사에서 Apple iOS 또는 Apple iPhone OS가 포함된 **operating-system** 특성 값을 반환하는 경우 이 프로파일은 일치합니다. 이 예에서는 Apple iOS에 일치합니다.

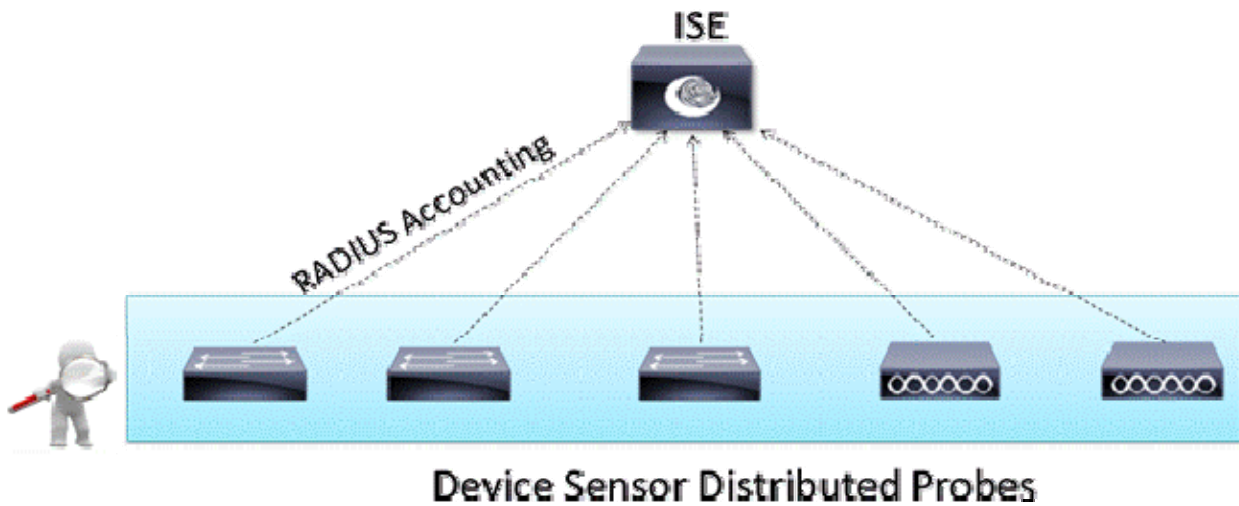
**Step 8** 요약하면 NMAP 프로브는 운영 체제 검사 결과에 따라 운영 체제를 기반으로 엔드포인트를 분류하는 데 유용할 수 있습니다. 대다수의 클라이언트리스 디바이스는 디바이스 분류를 위해 쿼리될 수 있는 SNMP 에이전트를 지원합니다. 기타 디바이스는 오픈 포트를 기반으로 분류될 수 있으며, 정책에 따라 특정 서비스를 실행하는 특정 디바이스에 더 제한적이거나 덜 제한적인 권한이 부여되도록 제어할 수 있습니다. 권한 부여 정책 할당에 상관없이 각 프로브는 전체 네트워크의 운영 및 보안 관리에 유용할 수 있는 추가적인 가시성 레벨을 제공합니다.

# Device Sensor

## Device Sensor 개요

Device Sensor는 현재 Cisco 액세스 스위치 및 무선 컨트롤러(예: Cisco Catalyst 3650 및 3750 Series, 4500 Series Switches)에서 지원되는 액세스 디바이스 기능입니다. Device Sensor는 CDP(Cisco Discovery Protocol), LLDP(Link Layer Discovery Protocol) 및 DHCP(Dynamic Host Configuration Protocol)와 같은 프로토콜을 통해 연결된 엔드포인트에서 네트워크 정보를 수집하고 이 정보를 RADIUS 계정 관리 패킷의 ISE PSN에 전달합니다(그림 67). ISE는 RADIUS 프로브만 사용하여 프로파일링 데이터를 수집하고 구문 분석할 수 있습니다.

그림 62 Device Sensor 개요



## Device Sensor 세부사항

Device Sensor는 네트워크 디바이스에서 원시 엔드포인트 데이터를 수집합니다. 수집된 엔드포인트 정보는 스위치의 프로파일링 기능을 완성하는 데 도움이 됩니다. 액세스 디바이스의 프로파일링 기능은 두 부분으로 구성됩니다.

수집기 - 네트워크 디바이스에서 엔드포인트 데이터를 수집합니다.

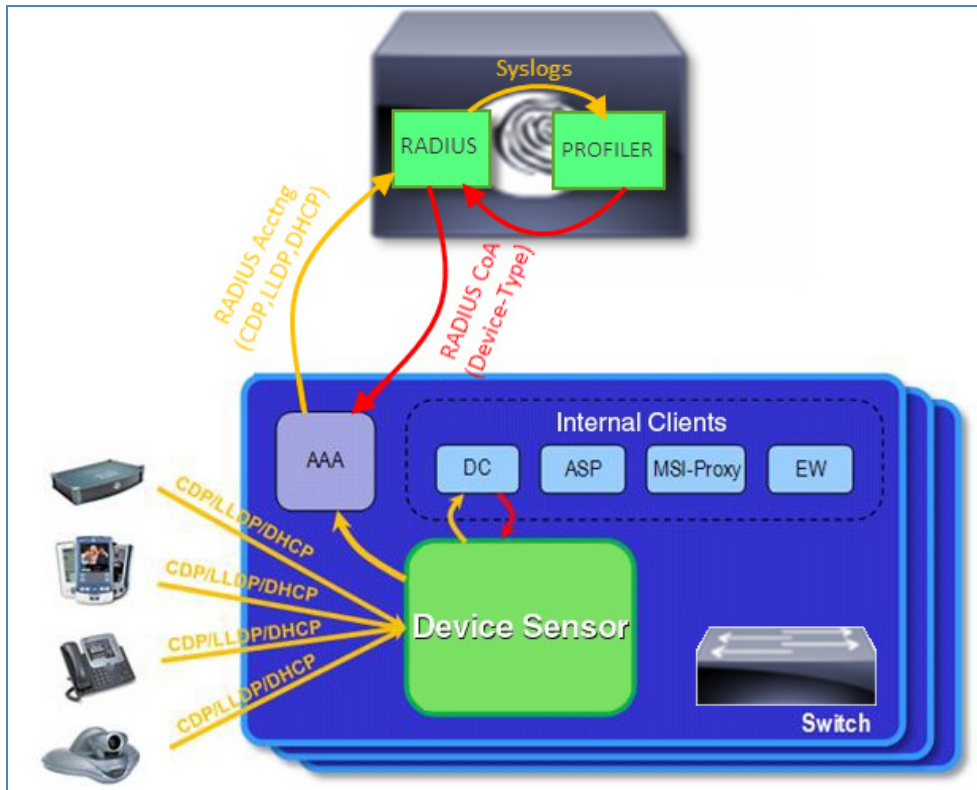
애널리라이저 - 데이터를 수집하고 디바이스 유형을 확인합니다.

Device Sensor는 Cisco Catalyst 스위치, Cisco Wireless LAN Controller 등 액세스 디바이스에 내장된 수집기 기능을 나타냅니다. 그림 68에는 프로파일링 시스템 측면에서의 Device Sensor가 나와 있으며 센서 데이터의 다른 가능한 소비자도 보여줍니다.

센서 기능이 있는 스위치 또는 무선 컨트롤러는 네트워크 디바이스에서 CDP, LLDP 및 DHCP와 같은 프로토콜을 사용하여 엔드포인트 정보를 수집하고, 정적으로 구성된 필터에 따라 액세스 세션 맥락에서 이 정보를 등록된 클라이언트에 제공합니다. 액세스 세션은 네트워크 디바이스에 대한 엔드포인트의 연결을 나타냅니다.

Device Sensor에는 내부 및 외부 클라이언트가 있습니다. 내부 클라이언트에는 내장형 Device Classifier(DC 또는 로컬 애널리저), Cisco ASP(Auto SmartPorts), MSI-Proxy 및 Cisco EW(EnergyWise™)와 같은 구성 요소가 포함됩니다. Device Sensor는 RADIUS 계정 관리를 사용하여 ISE(Identity Services Engine) 프로파일링 “애널리저”와 같은 외부 클라이언트로 데이터를 전송합니다.

그림 63 Device Sensor 운영 예



세션 이벤트 및 다른 세션 관련 데이터(예: AC 주소 및 인그레스 포트 데이터)와 함께 프로파일링 데이터가 포함된 클라이언트 알림 및 계정 관리 메시지가 생성되어 내부 및 외부 클라이언트(ISE)로 전송됩니다. 기본적으로 지원되는 각 피어 프로토콜마다 지정된 세션 맥락에서 이전에 수신되지 않은 프로파일링 특성 또는 TLV(type-length 값)가 수신 패킷에 포함된 경우에만 클라이언트 알림 및 계정 관리 이벤트가 생성됩니다. 새 TLV가 수신되었거나 이전에 수신된 TLV가 CLI 명령을 사용하여 다른 값으로 수신되는 모든 TLV 변경 사항에 대해 클라이언트 알림 및 계정 관리 이벤트를 사용하도록 설정할 수 있습니다.

센서는 최대 디바이스 모니터링 세션을 포트(액세스 포트 및 트렁크 포트)당 32개로 제한합니다. 즉, 포트당 최대 32개의 엔드포인트를 모니터링할 수 있습니다. 비활성 타이머는 12시간을 초과하는 세션을 삭제합니다.

## Device Sensor 요구 사항

표 6에는 액세스 디바이스 및 버전에 따른 Device Sensor 프로토콜 지원 정보가 요약되어 있습니다.

표 4 Device Sensor 요구 사항

플랫폼	CDP	LLDP	DHCP	HTTP	mDNS
Catalyst 3560/3750 Series Switches	15.0(1)SE1	15.0(1)SE1	15.0(1)SE1	-	-
Catalyst 4500 Series Switch	15.1(1)SG IOS-XE 3.3.0SG	15.1(1)SG IOS-XE 3.3.0SG	15.1(1)SG IOS-XE 3.3.0SG	-	15.1(1)SG IOS-XE 3.3.0SG
WLC/WiSM2 Wireless Controllers	-	-	7.2.110.0	7.3	-

참고: 소프트웨어 버전 및 기능 지원을 확인하려면 사용 중인 플랫폼에 해당하는 릴리스 정보를 참조하십시오. 예를 들어 Cisco IOS Software Release 15.0(1)SE1 및 Device Sensor 기능의 요구 사항을 충족하지 않는 다수의 Catalyst 3560 및 3750 스위치가 있습니다.

Catalyst 3560-C 및 3560-CG Series Switches에 대한 Device Sensor 기능 지원은 Cisco IOS Software Release 15.0(2)SE에서 제공됩니다.

Device Sensor가 Cisco Wireless Controller에 구축된 경우 감지용으로 구성된 WLAN에 가입하는 모든 클라이언트에 대해 DHCP 프로파일링이 활성화됩니다. 클라이언트 DHCP 요청의 경우 DHCP 프록시 및 브리지 모드가 모두 지원됩니다. 7.2MR1의 제한 사항은 다음과 같습니다.

독립형 액세스 포인트는 지원되지 않습니다.

로컬 스위칭을 사용한 로컬 인증은 지원되지 않습니다.

요약하면, Device Sensor는 ISE 프로파일링 서비스의 데이터 수집을 확장할 때 상당한 이점을 제공합니다. Device Sensor를 사용하는 경우 데이터 수집은 엔드포인트 및 데이터 소스에 가장 가까운 지점인 액세스 레이어에서 광범위하게 분산됩니다. 그런 다음 정보는 원본 위치에서 선택적으로 필터링된 후 RADIUS 계정 관리 패킷에서 분석 및 분류를 위해 중앙 집중식 정책 서비스 노드로 전송됩니다. 이렇게 하면 기존 ISE 프로브를 사용하여 이와 동일한 데이터를 캡처하기 위한 다수의 설계 과제 및 인프라 요구 사항을 완화할 수 있습니다.

## ISE 프로파일링에 맞게 Device Sensor 구성

Device Classifier는 MAC-OUI의 정보 및 프로토콜(예: CDP, LLDP 및 DHCP)을 수집하여 디바이스를 식별합니다. CDP 및 LLDP 정보를 수집하려면 Catalyst 스위치에서 CDP 및 LLDP를 활성화해야 합니다. DHCP 옵션 정보를 DC에 제공하려면 스위치에서 DHCP 스누핑 기능을 활성화해야 합니다. Cisco Wireless LAN Controller는 현재 DHCP 데이터만 지원합니다. 그런 다음 애널리저(ISE)에 전송할 특정한 특성 및 옵션을 지정하는 필터를 정의할 수 있습니다. 센서 데이터를 ISE에 전송하려면 액세스 디바이스에서 RADIUS 계정 관리가 활성화되어 있어야 합니다. ISE에서 RADIUS 프로브가 활성화되고 적절히 구성되어 있어야 합니다.

**참고:** 센서 데이터를 ISE에 전달하려면 RADIUS 계정 관리가 필요합니다. 그러나 센서 데이터를 수집하여 ISE에 전송하기 위해 RADIUS 인증 및 권한 부여가 필요하지는 않습니다. 그러므로 모니터 모드에서도 조직이 아직 RADIUS 인증을 활성화할 준비가 되어 있지 않으면 네트워크 검색 단계에서 사전 ISE 구축에 Device Sensor를 사용할 수 있습니다. 이는 Cisco NAC Appliance와 함께 ISE 프로파일링 서비스를 사용하는 구축 환경(RADIUS 액세스 제어가 구축되어 있지 않음)으로 확장 지원됩니다.

### ISE에서 RADIUS 프로브 활성화

- Step 9** RADIUS 프로브 활성화 단계는 [RADIUS 프로브 구성](#) 섹션에 자세히 설명되어 있습니다. RADIUS 프로브를 적절히 활성화하고 구성하는 방법은 해당 섹션을 참조하십시오.
- Step 10** 해당 섹션에 제공된 지침에 대한 한 가지 예외는 RADIUS 기반 인증 및 권한 부여를 사용하지 않는 구축 환경에서 Device Sensor를 사용하는 것과 관련이 있습니다. 이 시나리오에서는 액세스 디바이스가 ISE에 추가되지 않았습니다. 그러나 RADIUS 계정 관리가 ISE와 통신해야 하므로 Administration(관리)→Network Resources(네트워크 리소스)→Network Devices(네트워크 디바이스)에서 Device Sensor를 지원하는 모든 액세스 디바이스를 추가해야 합니다.
- Step 11** ISE에 입력한 IP 주소는 RADIUS 전송을 위해 액세스 디바이스에서 제공하는 값과 일치해야 합니다. 또한 RADIUS 공유 키는 액세스 디바이스에 구성된 값과 일치해야 합니다. 이러한 단계는 Device Sensor에서 RADIUS 계정 관리 패킷을 수신할 수 있도록 지원하는 데 필요합니다.

### Cisco 유선 스위치에서 프로파일링 프로토콜 활성화

엔드포인트에서 CDP, LLDP 또는 DHCP 특성을 수집하려면 액세스 스위치에서 연결된 특성을 읽고 수집할 수 있도록 이러한 프로토콜을 활성화해야 합니다.

- Step 12** Device Sensor가 지원되는 액세스 스위치의 명령 콘솔에 액세스합니다.
- Step 13** CDP를 지원하기 위한 스위치를 활성화합니다.
- Step 14** CDP는 기본적으로 Cisco 스위치에서 전역적으로 활성화되어 있습니다. 비활성화되어 있는 경우 다음 전역 명령을 사용하여 활성화하십시오.

```
cat3750x(config)# cdp run
```

- Step 15** CDP는 기본적으로 각 스위치 포트에서 활성화되어 있습니다. 비활성화되어 있는 경우 다음 인터페이스 명령을 사용하여 활성화하십시오.

```
cat3750x(config-if)# cdp enable
```

**Step 16** 다음과 같이 `show cdp neighbors` 명령을 사용하여 CDP가 스위치에서 작동하고 있는지 확인합니다.

```

cat3750x# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
APc471.fe34.197a Gig 1/0/2       137        T            AIR-LAP11  Gig 0
SEP003094C4528A Gig 1/0/1       150        H P M        IP Phone   Port 1
cat6503.cts.local
                  Gig 1/0/24     140        R S I        WS-C6503  Gig 2/47
    
```

자세한 보기는 다음과 같습니다.

```

cat3750x# show cdp neighbors detail
-----
Device ID: APc471.fe34.197a
Entry address(es):
  IP address: 10.1.14.100
Platform: cisco AIR-LAP1142N-A-K9 , Capabilities: Trans-Bridge
Interface: GigabitEthernet1/0/2, Port ID (outgoing port): GigabitEthernet0
Holdtime : 133 sec

Version :
Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 27-Jan-12 21:45 by prod_rel_team

advertisement version: 2
Duplex: full
Power drawn: 15.400 Watts
Power request id: 21756, Power management id: 2
Power request levels are:15400 14500 0 0 0
Management address(es):
-----
Device ID: SEP003094C4528A
Entry address(es):
  IP address: 10.1.13.100
Platform: Cisco IP Phone 7960, Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1, Port ID (outgoing port): Port 1
Holdtime : 147 sec
Second Port Status: Up

Version :
P00308010100

advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Management address(es):
-----
Device ID: cat6503.cts.local
Entry address(es):
  IP address: 10.1.50.1
Platform: cisco WS-C6503, Capabilities: Router Switch IGMP
Interface: GigabitEthernet1/0/24, Port ID (outgoing port): GigabitEthernet2/47
Holdtime : 136 sec
    
```

```
Version :
Cisco IOS Software, s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Versio
n 12.2(33)SXJ2, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Wed 14-Dec-11 19:51 by prod_rel_team

advertisement version: 2
VTP Management Domain: 'cts'
Duplex: full
Management address(es):
  IP address: 10.1.50.1
```

**Step 17** LLDP를 지원하기 위한 스위치를 활성화합니다.

**Step 18** LLDP는 기본적으로 Cisco 스위치에서 전역적으로 비활성화되어 있습니다. 활성화하려면 다음 전역 명령을 입력합니다.

```
cat3750x(config)# lldp run
```

**Step 19** LLDP는 기본적으로 각 스위치 포트에서 활성화되어 있습니다. 비활성화되어 있는 경우 다음 인터페이스 명령을 사용하여 활성화하십시오.

```
cat3750x(config-if)# lldp receive
```

**Step 20** 다음과 같이 **show lldp neighbors** 명령을 사용하여 스위치에서 LLDP가 작동하고 있는지 확인합니다.

```
cat3750x# show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID Local Intf Hold-time Capability Port ID
AVA4FF00E Gi1/0/9 120 B 0004.0d4f.f00e
AVAEC8C79 Gi1/0/10 120 B 0004.0dec.8c79
AVAF694AC Gi1/0/15 120 B 0004.0df6.94ac
AVAEC8C79 Gi1/0/17 120 B 0004.0dec.8c79

Total entries displayed: 4
```

자세한 보기는 다음과 같습니다.

```

cat3750x# show lldp neighbors detail
-----
Chassis id: 10.6.104.29
Port id: 0004.0d4f.f00e
Port Description - not advertised
System Name: AVA4FF00E
System Description - not advertised

Time remaining: 106 seconds
System Capabilities: B,T
Enabled Capabilities: B
Management Addresses:
IP: 10.X.104.29
OID:
1.3.6.1.4.1.6889.1.69.1.5.
Auto Negotiation - supported, enabled
Physical media capabilities:
Symm Pause (FD)
Pause (FD)
100base-TX (FD)
100base-TX (HD)
10base-T (FD)
10base-T (HD)
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:

MED Codes:
(NP) Network Policy, (LI) Location Identification
(PS) Power Source Entity, (PD) Power Device
(IN) Inventory

H/W revision: 4620D01B
F/W revision: b20d01b2_9_1.bin
S/W revision: a20d01b2_9_1.bin
Serial number: 051606020284
Manufacturer: Avaya
Model: 4620
Capabilities: NP, IN
Device type: Endpoint Class III
Network Policy(Voice): VLAN dot1p, tagged, Layer-2 priority: 6, DSCP: 46
Power requirements - not advertised
Location - not advertised

----<snip>----

Total entries displayed: 4
    
```

**Step 21** DHCP를 스누핑하기 위한 스위치를 활성화합니다. 전역 컨피그레이션 모드에서 다음 명령을 입력하여 선택한 액세스 VLAN에서 DHCP 스누핑을 활성화합니다.

```

cat3750x(config)# ip dhcp snooping
cat3750x(config)# ip dhcp snooping vlan <VLANs>
    
```



- Step 22** 최소한, 프로파일링할 엔드포인트를 연결하는 액세스 VLAN이 목록에 포함되어야 합니다.
- Step 23** 신뢰할 수 있는 DHCP 서버에 직접 또는 간접적으로 연결된 인터페이스에서 전송된 DHCP 정보를 신뢰하려면 다음 인터페이스 컨피그레이션 명령을 사용합니다.

```
cat3750x(config)# interface <interface_to_DHCP_Server>
cat3750x(config-if)# ip dhcp relay information trusted
```

- Step 24** 다음과 같이 **show ip dhcp snooping** 명령을 사용하여 스위치에서 DHCP 스누핑이 활성화되어 있는지 확인합니다.

```
cat3750x# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10-14
DHCP snooping is operational on following VLANs:
10-14
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: lcdf.0f8f.6000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface          Trusted    Allow option    Rate limit (pps)
-----

```

- Step 25** 다음과 같이 **show ip dhcp snooping binding** 명령을 사용하여 스위치에서 DHCP 스누핑이 작동하고 있는지 확인(DHCP 클라이언트를 위한 바인딩 표가 생성됨)합니다.

```
cat3750x# show ip dhcp snooping binding
-----
MacAddress          IPAddress          Lease (sec)      Type              VLAN  Interface
-----
00:30:94:C4:52:8A   10.1.13.100       691187           dhcp-snooping     13    GigabitEthernet1/0/1
00:50:56:A0:0B:3A   10.1.10.100       653260           dhcp-snooping     10    GigabitEthernet1/0/1
C4:71:FE:34:19:7A   10.1.14.100       653068           dhcp-snooping     14    GigabitEthernet1/0/2
Total number of bindings: 3
```

- Step 26** 스위치 컨피그레이션 변경 사항을 저장합니다.

**Cisco 유선 스위치에 Device Sensor 구성**

- Step 27** 데이터 수집에 포함하거나 데이터 수집에서 제외할 CDP, LLDP 또는 DHCP 특성을 선택하는 필터를 정의합니다.
- Step 28** 전역 컨피그레이션 모드에서 시작하여 CDP 특성에 대한 필터를 정의합니다.

```

cat3750x(config)# device-sensor filter-list cdp list <my_cdp_list>
cat3750x(config-sensor-cdplist)# tlv name device-name
cat3750x(config-sensor-cdplist)# tlv name address-type
cat3750x(config-sensor-cdplist)# tlv name capabilities-type
cat3750x(config-sensor-cdplist)# tlv name platform-type
cat3750x(config)# device-sensor filter-spec cdp include list <my_cdp_list>
    
```

**Step 29** 이름 또는 번호로 CDP TLV 값을 입력할 수 있습니다. CDP TLV 이름은 다음과 같습니다.

address-type	주소 유형
capabilities-type	기능 유형
cos-type	COS 유형
device-name	디바이스 이름
duplex-type	이중 유형
external-port-id-type	외부 포트 ID 유형
ipprefix-type	IP 접두사 유형
mgmt-address-type	관리 주소 유형
mtu-type	MTU 유형
native-vlan-type	기본 VLAN 유형
platform-type	플랫폼 유형
port-id-type	포트 ID 유형
power-available-type	가용 전력 유형
power-request-type	외부 포트 ID 유형
power-type	전원 유형
protocol-hello-type	프로토콜 Hello 유형
trigger-type	트리거 유형
trust-type	신뢰 유형
twoway-connectivity-type	양방향 연결 유형
unidirectional-mode-type	단방향 모드 유형
version-type	버전 유형

vtp-mgmt-domain-type	VTP 관리 도메인 유형
vvid-type	VVID 유형

**Step 30** 전역 컨피그레이션 모드에서 시작하여 다음과 같이 LLDP 특성에 대한 필터를 정의합니다.

```
cat3750x(config)# device-sensor filter-list lldp list <my_lldp_list>
cat3750x(config-sensor-lddplist)# tlv name system-name
cat3750x(config-sensor-lddplist)# tlv name system-description
cat3750x(config)# device-sensor filter-spec lldp include list <my_lldp_list>
```

**Step 31** 이름 또는 번호로 LLDP TLV 값을 입력할 수 있습니다. LLDP TLV 이름은 다음과 같습니다.

chassis-id	새시 ID	새시 Id
end-of-lldpdu	LLDP의 끝	
management-address	관리 주소	
port-description	포트 설명	
port-id	포트 ID	
system-capabilities	시스템 기능	
system-description	시스템 설명	
system-name	시스템 이름	
time-to-live	TTL(Time To Live)	

**Step 32** 전역 컨피그레이션 모드에서 시작하여 다음과 같이 DHCP 특성에 대한 필터를 정의합니다.

```
cat3750x(config)# device-sensor filter-list dhcp list my_dhcp_list
cat3750x(config-sensor-dhcplist)# option name host-name
cat3750x(config-sensor-dhcplist)# option name default-ip-ttl
cat3750x(config-sensor-dhcplist)# option name requested-address
cat3750x(config-sensor-dhcplist)# option name parameter-request-list
cat3750x(config-sensor-dhcplist)# option name class-identifier
cat3750x(config-sensor-dhcplist)# option name client-identifier
cat3750x(config)# device-sensor filter-spec dhcp include list my_dhcp_list
```

**Step 33** 이름 또는 번호로 DHCP 옵션을 입력할 수 있습니다. 몇 가지 주요한 일반 옵션은 다음과 같습니다.

class-identifier	클래스 식별자
client-fqdn	클라이언트 FQDN
client-identifier	클라이언트 식별자
default-ip-ttl	기본 IP TTL(Time To Live)

domain-name	도메인 이름
host-name	호스트 이름
server-identifier	서버 ID
user-class-id	사용자 클래스 ID
...	

**모범 사례:** CDP, LLDP 및 DHCP에 대해 표시된 샘플 필터는 대부분의 활용 사례에서 합리적인 선택입니다. 사용 가능한 특성을 이해하려면 CDP 및 LLDP에 대해 show 명령을 사용하여 네트워크의 엔드포인트가 제공하는 TLV를 보고 특정 특성이 엔드포인트를 고유하게 분류하는 데 도움이 되는지 판단합니다. Device Sensor도 필터 없이 초기에 구축하여 Administration(관리)→Identity Management(ID 관리)→Identities(ID)에서 ISE에 제공되는 특성을 확인할 수 있습니다. 고객 엔드포인트의 프로파일링 조건과 일치하는 데 필요하다고 판단되는 특성을 기준으로 적절한 필터를 적용할 수 있습니다.

**참고:** 특정 TLV 또는 옵션 값을 입력하는 것이 엔드포인트에서 이 정보를 전송한다는 의미는 아닙니다. 엔드포인트가 스위치 또는 네트워크에 제공하는 특성에 따라 필터가 적용됩니다. 예를 들어 필터에 포함되는 DHCP 옵션으로 client-fqdn이 선택되었지만 DHCP 클라이언트에서 해당 옵션을 요청하지 않으면 해당 옵션에 대한 정보가 Device Sensor 또는 ISE에 제공되지 않습니다.

**Step 34** 다음과 같이 RADIUS 계정 관리에서 모든 변경 사항을 포함한 센서 데이터가 전송되도록 합니다.

```
cat3750x(config)# device-sensor accounting
cat3750x(config)# device-sensor notify all-changes
```

**Step 35** 로컬 애널라이저를 비활성화하여 중복된 업데이트가 ISE로 전송되지 않도록 합니다.

```
cat3750x(config)# no macro auto monitor
cat3750x(config)# access-session template monitor
```

내장형 Device Classifier는 기본적으로 Cisco 스위치에서 활성화되어 있으며 이 경우 Device Sensor는 프로그래밍 방식으로 활성화됩니다. 그러므로 Device Sensor도 기본적으로 활성화되어 있습니다. 센서 데이터를 ISE로 보내도록 RADIUS 인증 및 계정 관리가 활성화되어 있는 경우 TLV 변경이 발생할 때마다 중복 RADIUS 계정 관리 패킷이 전송될 수 있습니다. 이는 로컬 애널라이저에 의한 세션 모니터링 때문입니다. 중복 계정 관리 메시지가 발생하지 않게 하려면 로컬 애널라이저를 비활성화해야 합니다.

RADIUS 인증이 비활성화된 경우(예: 사전 ISE 구축/검색 단계에 있거나 Cisco NAC Appliance와 함께 ISE 프로파일링 서비스가 구현된 네트워크) 로컬 애널라이저가 비활성화되어 있으면 센서 데이터가 전송되지 않습니다. 로컬 애널라이저와 상관없이 센서 데이터가 전송되도록 하려면 **access-session template monitor** 명령을 사용하십시오.

**Step 36** RADIUS 계정 관리를 사용하여 세션 계정 관리 정보를 ISE에 전송하도록 스위치를 구성합니다.

**Step 37** RADIUS 인증 및 권한 부여가 구성되어 있는 경우 이 단계는 이미 완료된 것입니다. ISE와의 RADIUS 통신을 위해 스위치를 구성하는 방법에 대한 추가 세부사항은 [RADIUS 프로브 구성](#) 섹션을 참조하십시오.

**Step 38** RADIUS/802.1X가 아직 구축되어 있지 않은 경우 스위치 컨피그레이션에 다음 명령을 포함해야 합니다.

```
cat3750x(config)# aaa new-model
cat3750x(config)# aaa accounting dot1x default start-stop group radius
cat3750x(config)# radius-server host <PSN_ip> auth-port <port> acct-port <port> key <shared-secret>
cat3750x(config)# radius-server vsa send accounting
```

**Step 39** Device Sensor가 프로파일링 정보를 수집하고 있는지 확인합니다.

다음과 같이 **show device-sensor cache** 명령을 사용하여 Device Sensor가 제대로 작동하고 있는지 확인합니다.

```
cat3750x# show device-sensor cache all
Device: 0050.56a0.0b3a on port GigabitEthernet1/0/1
-----
Proto Type:Name                               Len Value
dhcp  55:parameter-request-list              14 37 0C 01 0F 03 06 2C 2E 2F 1F 21 79 F9 2B
dhcp  60:class-identifier                       10 3C 08 4D 53 46 54 20 35 2E 30
dhcp  12:host-name                              9 0C 07 77 69 6E 37 2D 70 63
dhcp  50:requested-address                      6 32 04 0A 01 0A 64
dhcp  61:client-identifier                      9 3D 07 01 00 50 56 A0 0B 3A

Device: 0012.d9e3.427e on port GigabitEthernet1/0/24
-----
Proto Type:Name                               Len Value
cdp   4:capabilities-type                       8 00 04 00 08 00 00 00 29
cdp   2:address-type                           17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 32 01
cdp   6:platform-type                          18 00 06 00 12 63 69 73 63 6F 20 57 53 2D 43 36 35 30 33
cdp   1:device-name                            21 00 01 00 15 63 61 74 36 35 30 33 2E 63 74 73 2E
      6C 6F 63 61 6C

Device: c471.fe34.197a on port GigabitEthernet1/0/2
-----
Proto Type:Name                               Len Value
cdp   4:capabilities-type                       8 00 04 00 08 00 00 00 02
cdp   2:address-type                           17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 0E 64
cdp   6:platform-type                          30 00 06 00 1E 63 69 73 63 6F 20 41 49 52 2D 4C 41
      50 31 31 34 32 4E 2D 41 2D 4B 39 20 20 20
cdp   1:device-name                            20 00 01 00 14 41 50 63 34 37 31 2E 66 65 33 34 2E 31 39 37 61
dhcp  50:requested-address                      6 32 04 0A 01 0E 64
dhcp  60:class-identifier                       16 3C 0E 43 69 73 63 6F 20 41 50 20 63 31 31 34 30
dhcp  55:parameter-request-list              10 37 08 01 06 0F 2C 03 21 96 2B
dhcp  12:host-name                              18 0C 10 41 50 63 34 37 31 2E 66 65 33 34 2E 31 39 37 61
dhcp  61:client-identifier                      9 3D 07 01 C4 71 FE 34 19 7A

Device: 0030.94c4.528a on port GigabitEthernet1/0/1
-----
Proto Type:Name                               Len Value
cdp   2:address-type                           17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 0D 64
cdp   6:platform-type                          23 00 06 00 17 43 69 73 63 6F 20 49 50 20 50 68 6F
      6E 65 20 37 39 36 30
cdp   4:capabilities-type                       8 00 04 00 08 00 00 04 90
cdp   1:device-name                            19 00 01 00 13 53 45 50 30 30 33 30 39 34 43 34 35 32 38 41
dhcp  50:requested-address                      6 32 04 0A 01 0D 64
dhcp  55:parameter-request-list              9 37 07 01 42 06 03 0F 96 23
dhcp  60:class-identifier                       39 3C 25 43 69 73 63 6F 20 53 79 73 74 65 6D 73 2C
      20 49 6E 63 2E 20 49 50 20 50 68 6F 6E 65 20 43
      50 2D 37 39 36 30 00
dhcp  12:host-name                              18 0C 10 53 45 50 30 30 33 30 39 34 43 34 35 32 38 41 00
dhcp  61:client-identifier                      9 3D 07 01 00 30 94 C4 52 8A
```

## Cisco Wireless Controller에 Device Sensor 구성

지원되는 무선 컨트롤러에서 CLI 또는 웹 관리 인터페이스를 사용하여 DHCP용 Device Sensor를 활성화할 수 있습니다.

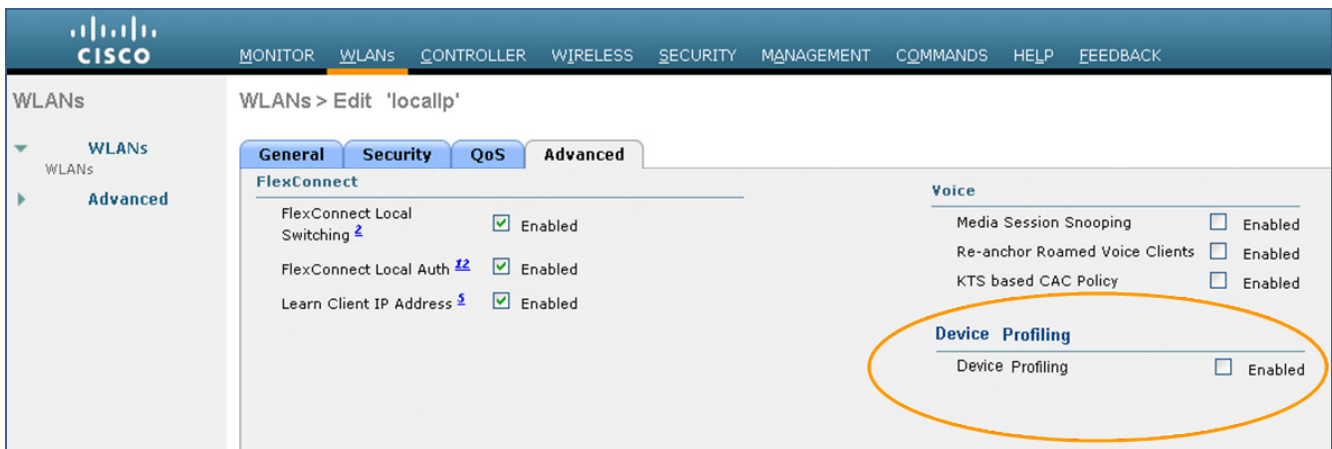
**Step 40** Cisco Wireless Controller에서 CLI를 통해 Device Sensor를 구성하려면 다음 명령을 입력합니다.

```
> config wlan profiling radius enable <wlan-id>
```

Device Sensor는 지정된 WLAN의 모든 무선 클라이언트에 대해 활성화됩니다.

- Step 41** RADIUS 계정 관리를 사용하여 세션 계정 관리 정보를 ISE에 전송하도록 무선 컨트롤러를 구성합니다.
- Step 42** RADIUS 인증 및 권한 부여가 구성되어 있는 경우 이 단계는 이미 완료된 것입니다.
- Step 43** ISE와의 RADIUS 통신을 위해 무선 컨트롤러를 구성하는 방법에 대한 추가 세부사항은 [RADIUS 프로브 구성](#) 섹션을 참고하십시오.
- Step 44** WLC 웹 인터페이스에서 WLANs(WLAN)→(WLAN-id)→Edit(편집)로 이동합니다. 그림 69의 화면에는 Device Sensor를 활성화하는 위치가 나와 있습니다.

그림 64 무선 컨트롤러에 대한 Device Sensor 컨피그레이션 예



### Device Sensor를 사용한 프로파일링 확인

- Step 45** Administration(관리)→Identity Management(ID 관리)→Identities(ID)→Endpoints(엔드포인트)에서 엔드포인트를 삭제합니다.
- Step 46** NMAP 프로브를 사용하여 프로파일링을 지원하도록 구성된 액세스 디바이스에서 엔드포인트의 연결을 해제했다가 다시 연결합니다.
- Step 47** ISE 정책 관리 노드로 이동하고 Administration(관리)→Identity Management(ID 관리)→Identities(ID)로 이동합니다.
- Step 48** LHS 창에서 Endpoints(엔드포인트)를 선택합니다.
- Step 49** 새로 연결된 엔드포인트의 MAC 주소를 찾아 선택하여 HTTP 프로브에서 캡처한 특성을 표시합니다.

그림 70의 ISE 정책 서비스 노드에는 RADIUS 프로브만 활성화되어 있습니다. 다음과 같은 키 특성이 강조 표시되어 있습니다.

EndPointPolicy

EndPointSource

OUI

CDP 특성(cdpCacheAddressType, cdpCacheCapabilities, cdpCacheId, cdpCachePlatform)

DHCP 특성(dhcp-class-identifier, dhcp-client-identitifier, dhcp-parameter-request-list, dhcp-requested-address, host-name)

그림 65 Device Sensor 특성 예

**Endpoint**

\* MAC Address **00:30:94:C4:52:8A**

\* Policy Assignment **Cisco-IP-Phone-7960**

Static Assignment

\* Identity Group Assignment **Cisco-IP-Phone**

Static Group Assignment

**Attribute List**

AcsSessionID	ise-psn-1/125323864/12755
AuthState	Authenticated
CPMSessionID	0A010A01000000900036DFC
Called-Station-ID	1C-DF-0F-8F-60-01
Calling-Station-ID	00-30-94-C4-52-8A
Device IP Address	10.1.50.2
Device Type	Device Type#All Device Types#Wired
EndPointPolicy	Cisco-IP-Phone-7960
EndPointProfilerServer	ise-psn-1
EndPointSource	RADIUS Probe
Framed-IP-Address	10.1.13.100
IdentityGroup	Cisco-IP-Phone
Location	Location#All Locations#North_America#RTP
MACAddress	00:30:94:C4:52:8A
MatchedPolicy	Cisco-IP-Phone-7960
MessageCode	3002
NAS-IP-Address	10.1.50.2
NAS-Port	50101
NAS-Port-Id	GigabitEthernet1/0/1
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device Type#All Device Types#Wired, Location#All Locations#North_America#RTP
NetworkDeviceName	cat3750x
OUI	Cisco Systems, Inc.
PolicyVersion	22
RequestLatency	12
SelectedAccessService	Default Network Access
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	24
Total Certainty Factor	145
attribute-151	A4117E8D
cdpCacheAddressType	00:00:00:01:01:01:cc:00:04:0a:01:0d:64
cdpCacheCapabilities	H;P;M
cdpCacheDeviceId	SEP003094C4528A
cdpCachePlatform	Cisco IP Phone 7960
audit-session-id=0A010A01000000900036DFC, connect-progress=Call Up, cdp-tlv=cdpCacheAddressType=00:00:00:01:01:01:cc:00:04:0a:01:0d:64, cdp-tlv=cdpCachePlatform=Cisco IP Phone 7960, cdp-tlv=cdpCacheCapabilities=00:00:04:90, cdp-tlv=cdpCacheDeviceId=SEP003094C4528A, dhcp-address=10.1.13.100, dhcp-option=dhcp-parameter-request-list=1, 66, 6, 3, 15, 150, 35, dhcp-option=dhcp-class-identifier=Cisco Systems, Inc. IP Phone CP-7960, dhcp-option=dhcp-client-identifier=01:00:30:94:c4:52:8a	
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7960
dhcp-client-identifier	01:00:30:94:c4:52:8a
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.1.13.100
host-name	SEP003094C4528A
ip	10.1.13.100



**EndPointSource**를 RADIUS 프로브로 설정한 상태로 Device Sensor 자체만 사용하는 경우 **EndPointPolicy**가 Cisco-IP-Phone-7960과 적절히 일치한다는 것을 알 수 있습니다. Device Sensor에서 수신된 프로파일링 특성 중 프로파일 일치에 기여하는 특성에는 **OUI = Cisco Systems, Inc.**, **cdpCachePlatform = Cisco IP Phone 7960** 및 **dhcp-class-identifier = Cisco Systems, Inc, IP Phone CP-7960**이 있습니다.

CDP 및 DHCP 특성은 필터에 지정된 항목만 포함하며 이는 데이터 수집이 최적화되는 방식을 보여줍니다. ISE 구축의 모든 관리 및 정책 서비스 노드에서 불필요한 특성을 구문 분석하고 동기화하는 데 정책 서비스 노드가 필요하지 않았습니다. Device Sensor 컨피그레이션에 따라 변경 사항이 발생할 경우에만 업데이트가 수신됩니다. 반면에, SNMP 쿼리 및 DHCP 프로브는 쿼리 또는 DHCP 갱신이 발생할 때마다 항상 특성을 업데이트합니다.

---

**모범 사례:** 확장성을 크게 높이고 전반적인 관리 및 프로파일링 컨피그레이션을 간소화할 수 있는 경우 Device Sensor를 사용하여 ISE 프로파일링을 구축합니다. Device Sensor는 RADIUS 인증 환경 및 다른 구축 유형(예: 사전 ISE 검색 단계 또는 NAC Appliance와의 통합) 모두를 위해 유선 액세스 스위치 및 무선 컨트롤러에 구축할 수 있습니다.

---

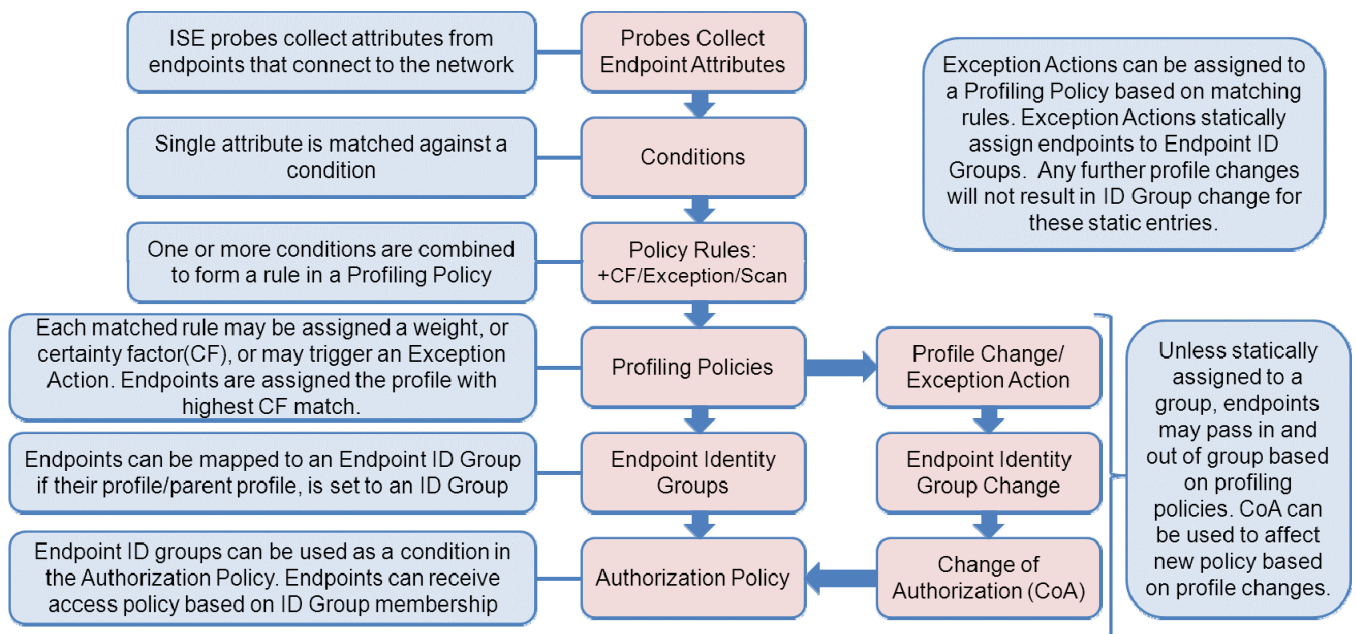
# 프로파일링 정책 구성

## 프로파일링 정책 컨피그레이션 개요

이 가이드의 앞부분에서 그림 71과 같은 ISE 프로파일링 서비스의 대략적인 아키텍처에 대해 소개했습니다. 이는 또한 ISE 프로파일링 컨피그레이션 및 전반적인 프로세스 흐름에 대한 일반적인 지침으로 사용할 수도 있습니다.

앞서, 흐름의 첫 번째 구성 요소, 즉 엔드포인트 특성을 수집하는 프로브 컨피그레이션을 완료했습니다. 이 섹션에서는 계속해서 고객 프로파일링 요구 사항을 지원할 수 있도록 프로파일링 정책 및 권한 부여 정책을 구성하는 나머지 구성 요소에 대해 설명합니다.

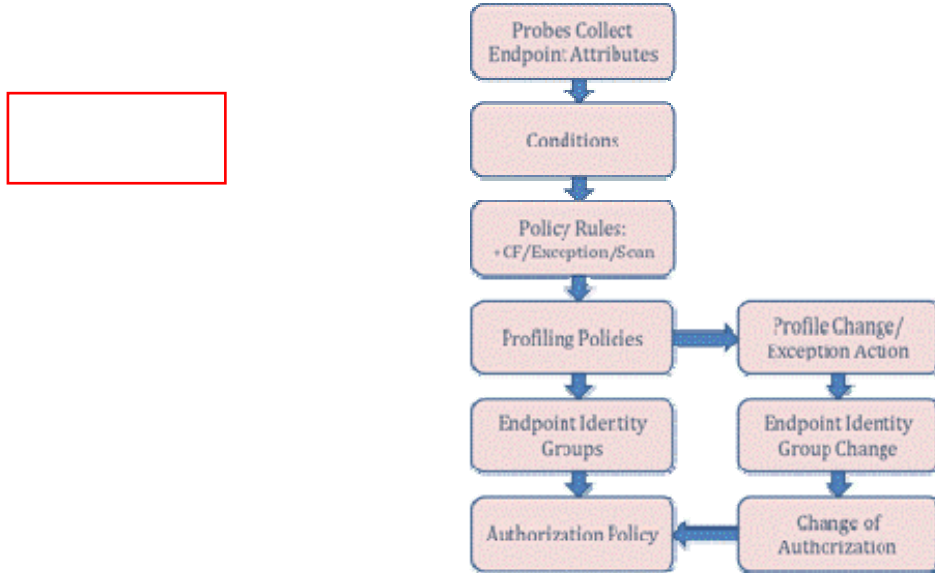
그림 66: ISE 프로파일링 정책 컨피그레이션 흐름



## 프로파일링 조건

다양한 ISE 프로브를 통해 다수의 프로파일링 특성을 수집할 수 있습니다. ISE 정책 서비스 노드에서 특성이 수집된 경우 프로파일링 프로세스의 다음 단계는 이러한 특성을 프로파일링 조건과 일치시키는 것입니다(그림 72). 각 조건은 Policy(정책)→Policy Elements(정책 요소)→Dictionary(사전) 아래 System Dictionary(시스템 사전)에 나열된 지원되는 특성과의 일치를 나타냅니다.

그림 67 컨피그레이션 흐름: 프로파일링 조건



사전 특성

표 7에는 Policy(정책)→Policy Elements(정책 요소)→Dictionary(사전) 아래 System Dictionary(시스템 사전)에 나열된 특성이 나와 있습니다. 이러한 특성은 Policy(정책)→Policy Elements(정책 요소)→Conditions(조건)→Profiling(프로파일링)에서 프로파일링 조건이 생성되거나 수정된 경우에 선택할 수 있습니다.

표 5 사전 특성

RADIUS	MAC	SNMP	CDP	NetFlow	NMAP
Acct-Authentic	MACAddress	cafSessionAuthorizedBy	cdpCacheAddress	MAX_PKT_LENGTH	110-tcp
Acct-Delay-Time	OUI	cafSessionAuthUserName	cdpCacheCapabilities	MAX_TTL	123-udp
Acct-Input-Octets		cafSessionAuthVlan	cdpCacheDeviceId	MIN_PKT_LENGTH	135-tcp
Acct-Input-Packets		cafSessionClientMacAddress	cdpCachePlatform	MIN_TTL	135-udp
Acct-Interim-Interval		cafSessionDomain	cdpCacheVersion	nexthop	137-udp
Acct-Link-Count		cafSessionStatus		OUT_BYTES	138-udp
Acct-Multi-Session-Id	<b>IP</b>	clApIfMacAddress	<b>LLDP</b>	OUT_PKTS	139-tcp
Acct-Output-Octets		clApName		OUTPUT_SNMP	139-udp
Acct-Output-Packets	EndpointSource	clApNameServerAddress	lldpCacheCapabilities	prot	143-tcp
Acct-Session-Id	FQDN	clApNameServerAddressType	lldpCapabilitiesMapSupported	PROTOCOL	1434-udp
Acct-Session-Time	Host	clApSshEnable	lldpChassisId	sampling_interval	161-udp
Acct-Status-Type	ip	clApSysMacAddress	lldpManAddress	source_id	162-udp
Acct-Terminate-Cause	mask	clApTelnetEnable	lldpPortDescription	src_as	1900-udp
Acct-Tunnel-Connection	PortalUser	clApTertiaryControllerAddress	lldpPortId	SRC_MAC	21-tcp
Acct-Tunnel-Packets-Lost	User-Agent	clApTertiaryControllerAddress	lldpSystemCapabilitiesMapEnabled	SRC_MASK	22-tcp
Callback-ID	<b>DHCP</b>	clApUpTime	lldpSystemDescription	SRC_TOS	23-tcp
Callback-Number			lldpSystemName	SRC_VLAN	25-tcp

boot-file client-fqdn client-identifier device-class dhcp-class-identifier dhcp-client-identifier dhcp-message-type dhcp-parameter-request-list dhcp-requested-address dhcp-user-class-id domain-name host-name name-servers pxe-client-arch pxe-client-machine-id pxe-client-network-id server-identifier vendor-class				
--	--	--	--	--

### 프로파일링 조건 구성

Cisco ISE는 프로파일링 정책에서 대규모 프로파일 라이브러리를 작성하는 데 사용되는 사전 구성된 프로파일링 조건의 광범위한 목록과 함께 패키지로 제공됩니다. 새 사용자 지정 조건을 생성하거나 특정 엔드포인트 집합 및 특정 환경에 맞게 기존 조건을 수정해야 하는 경우가 있습니다.

사용자 지정(사용자 정의) 프로파일링 조건을 구성합니다.

- Step 50** Policy(정책)→Policy Elements(정책 요소)→Conditions(조건)로 이동하고 LHS 창에서 Profiling(프로파일링)을 선택합니다. 조건 목록을 스크롤하여 조건(예: **OUI, dhcp-class-identifier, host-name, User-Agent**) 및 SNMP MIB 데이터(예: **cdpCachePlatform, lldpSystemDescription** 및 **hrDeviceDescr**)를 생성하는 데 사용되는 공통 특성을 파악합니다.
- Step 51** 사용자 지정 프로파일링 조건을 생성하는 프로세스를 보여주기 위해 실제 예가 사용됩니다. Endpoints(엔드포인트)→Identities(ID) 목록에는 다음을 표시하는 엔드포인트가 있습니다(그림 73).

그림 68 알 수 없는 엔드포인트 예

Endpoints		
Endpoint Profile	MAC Address	Static Assignment
<input type="checkbox"/> Unknown	00:C0:B7:65:1F:BC	false
<input type="checkbox"/> Unknown	00:C0:B7:68:31:E1	false

**Step 52** 다이어그램의 두 항목에는 모두 Unknown(알 수 없음) 프로파일이 나타나 있으며 동일한 MAC 접두사를 공유합니다. 첫 번째 엔드포인트에 대한 자세한 특성을 살펴보면 다음을 확인할 수 있습니다(그림 74).

그림 69 엔드포인트 검사의 NMAP 프로브 특성 예 1

MACAddress	00:C0:B7:65:1F:BC
MatchedPolicy	Unknown
MessageCode	3000
NAS-IP-Address	10.1.50.2
NAS-Port	50108
NAS-Port-Id	GigabitEthernet1/0/8
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device#All Device Types#Wired, Location#All Locations#North_America#RTP
NetworkDeviceName	cat3750x
OUI	AMERICAN POWER CONVERSION CORP

**Step 53** GigabitEthernet1/0/8에 연결된 엔드포인트를 검사하거나 OUI(American Power Conversion Corp)에서 간단하게 추론해 보면 이러한 엔드포인트는 실습 데이터 센터에 설치된 APC UPS(Uninterruptible Power System)에 대한 SNMP 네트워크 관리 연결임을 알 수 있습니다. 라이브러리에 이러한 엔드포인트에 대한 기본 조건이 없으므로 해당 조건을 생성하고 궁극적으로 네트워크 전체에서 이러한 모든 디바이스를 지원하기 위한 새 정책을 만듭니다.

**Step 54** RHS 창에서 Add(추가)를 클릭합니다.

**Step 55** 이 예에서는 공급업체 및 선택 유형을 나타내기 위해 **APC-OUICheck**라는 이름이 사용되었습니다.

**Step 56** 설명을 입력합니다(이 예에서는 **American Power Conversion Corp에 대한 OUI 선택 사용자 지정**). 고유 식별자(이 예에서는 단어“사용자 지정”)를 추가하는 것이 좋습니다. 그러면 생성된 모든 사용자 정의 조건을 빠르게 필터링하여 표시할 수 있습니다.

**Step 57** Type(유형) 아래에는 다양한 범주가 있습니다. 여기서 선택된 Type(유형)은 **Mac**입니다(그림 75).

그림 70 사용자 정의 프로파일러 조건 예

- Step 58**    특성 이름은 **OUI**입니다.
- Step 59**    연산자는 **EQUALS**입니다.
- Step 60**    특성 값은 OUI에 할당된 공급업체 이름입니다. 이 예에서는 **AMERICAN POWER CONVERSION CORP**입니다.

참고: 특성 값 문자열을 지정할 때는 정확한 대/소문자를 사용해야 합니다.

지정된 예에서는 정확한 대/소문자(EQUALS) 대신 특성 값이 “AMERICAN POWER” 또는 “AMERICAN POWER CONVERSION”으로 설정되어 있는 MATCH의 연산자를 선택적으로 사용할 수 있습니다.

OUI 데이터베이스에 특정 MAC 주소 접두사 항목이 없는 경우 다음 설정을 사용하여 알 수 없는 OUI에 대한 조건을 생성할 수 있습니다.

- 유형 = Mac
- 특성 이름 = MACAddress
- 연산자 = CONTAINS
- 특성 값 = XX:XX:XX(MAC 주소의 3바이트 접두사)

**Step 61**    그림 76에서는 사용자 정의 프로파일 조건을 최종 양식을 보여줍니다.

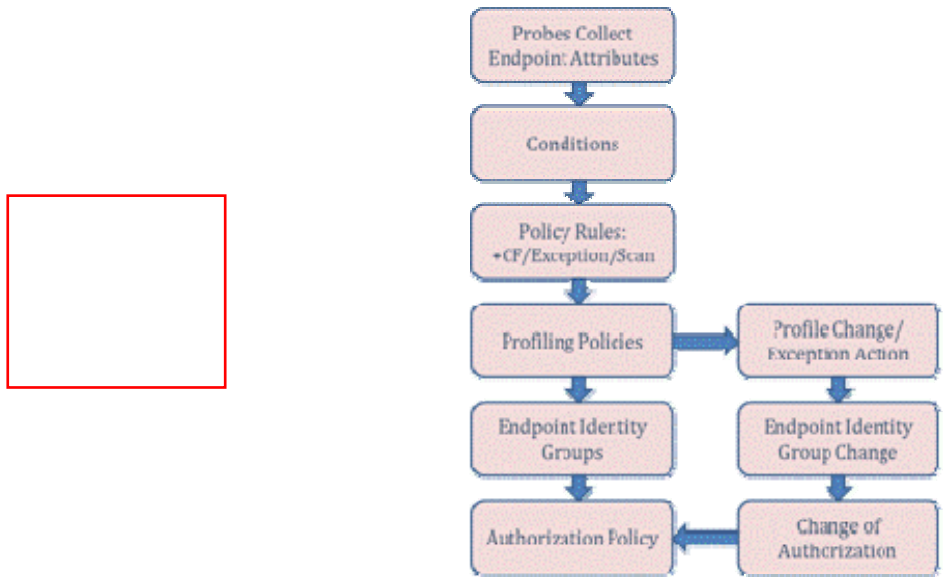
그림 71 사용자 정의 프로파일러 조건 예 2

**Step 62**    Submit(제출) 버튼(또는 연속 편집을 위해서는 Save(저장))을 클릭하여 변경 사항을 커밋합니다.

## 프로파일링 정책 및 규칙

프로파일링 정책 또는 프로파일은 엔드포인트가 프로파일 일치 항목으로 간주되기 위해 일치되어야 하는 정책 규칙을 정의합니다. 정책 규칙에는 하나 이상의 조건이 포함되어 있습니다. 규칙의 모든 조건이 충족(AND 연산자 사용)되거나 규칙의 조건 중 하나가 충족(OR 연산자 사용)되면 지정된 작업이 수행됩니다. 그림 77에는 프로파일링 정책 컨피그레이션 흐름이 나와 있습니다.

그림 72 컨피그레이션 흐름: 프로파일링 정책 및 규칙



**프로파일링 정책 규칙 작업**

지원되는 3가지 프로파일링 정책 규칙 작업은 다음과 같습니다.

확실성 요인 증가 <X>

예외 작업 수행

네트워크 검사 작업 수행

**확실성 요인(CF)**

그림 78에는 Android라는 간단한 프로파일링 정책이 나와 있습니다. 이 정책에는 2가지 규칙이 있습니다. 각 규칙에는 하나의 조건이 있으며, 일치하는 경우 Certainty Factor Increases 30(확실성 요인 증가 30) 작업이 수행됩니다. CF는 일반 가중치 또는 상대 확실성 레벨을 제공하기 위해 사용됩니다(엔드포인트가 일치하는 조건을 기준으로 프로파일과 적절히 일치함).

Android 프로파일에 대한 최소 확실성 요인은 30으로 설정됩니다. 그러므로 한 규칙이 일치할 경우 엔드포인트는 이 프로파일에 할당될 수 있는 후보가 됩니다. 엔드포인트가 여러 조건과 일치하며 결과적으로 여러 프로파일에 동시에 할당될 수 있으므로 일치하는 프로파일마다 누적 CF 값을 계산해야 합니다.

그림 73 프로파일링 정책 예

Profiler Policy List > Android

**Profiler Policy**

\* Name:  Description:

Policy Enabled:

\* Minimum Certainty Factor:  (Valid Range 1 to 65535)

\* Exception Action:

\* Network Scan (NMAP) Action:

Create Matching Identity Group  
 Use Hierarchy

\* Parent Policy:

Rules

If Condition	<input type="text" value="AndroidRule1Check1"/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="30"/>
If Condition	<input type="text" value="AndroidRule1Check2"/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="30"/>

4개의 프로파일링 정책 할당 기준이 있습니다. 다음 조건을 모두 충족하는 경우 엔드포인트가 프로파일에 할당됩니다.

정책을 활성화해야 합니다. (Policy Enabled(정책 사용) 확인란을 선택해야 함)

프로파일의 엔드포인트 누적 CF 값이 최소 확실성 요인을 충족합니다.

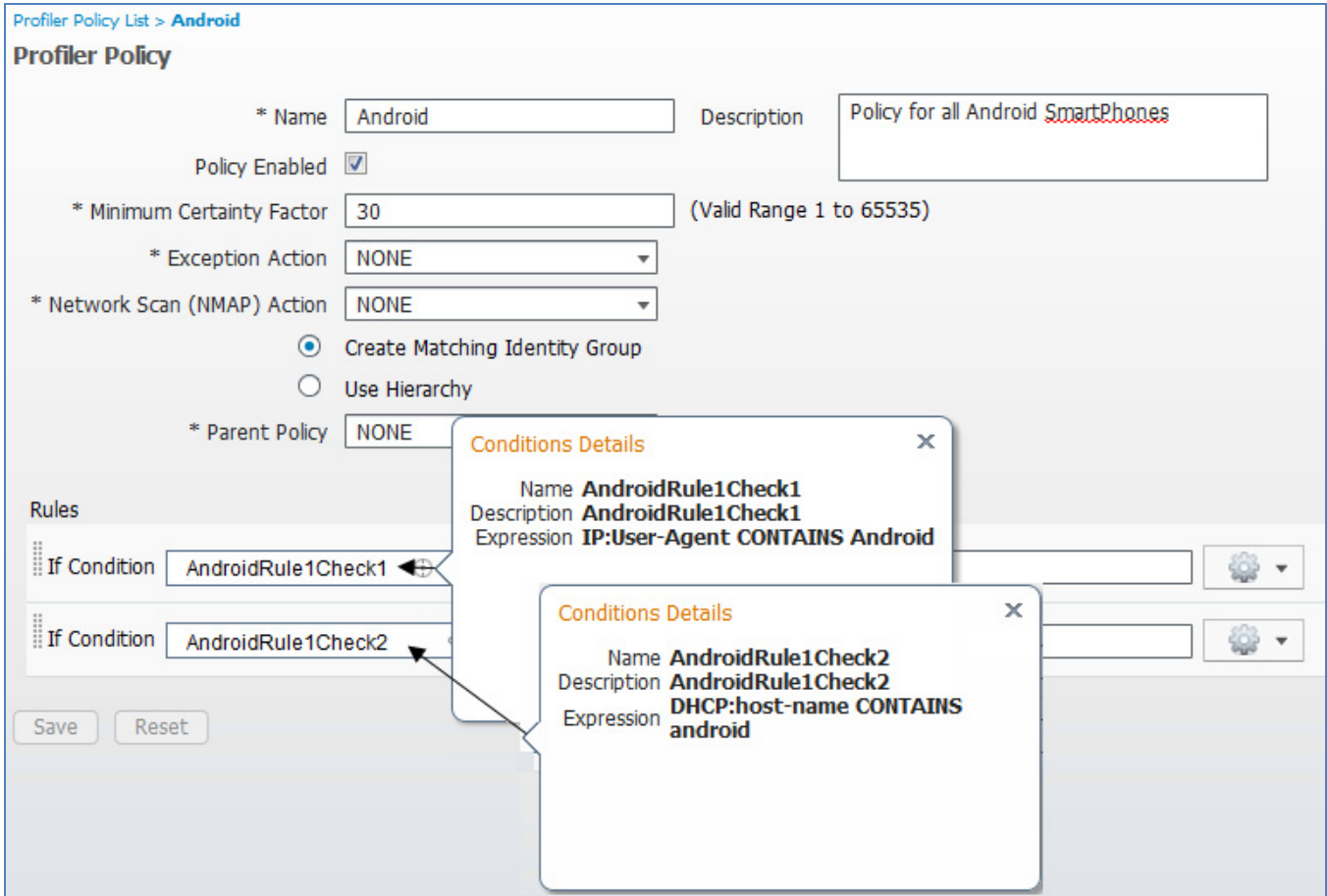
프로파일의 CF 등급은 1과 2도 true에 해당하는 다른 프로파일보다 더 높습니다.

엔드포인트가 상위 프로파일(프로파일이 계층 구조에 포함된 경우)의 최소 CF를 충족합니다.

그림 79에 표시된 Android 정책 예의 첫 번째 조건에 따라 엔드포인트의 **User-Agent**에 “Android” 문자열이 포함된 경우 이 프로파일의 CF는 30으로 증가합니다. 엔드포인트가 두 번째 규칙(DHCP **host-name** 값에 “android” 문자열 포함)과 일치하는 경우에도 이 프로파일의 해당 CF가 30으로 증가합니다. 두 규칙 모두의 조건과 일치하는 경우 CF는 60이 됩니다.



그림 74 프로파일링 정책 규칙 예



CF가 60인 경우에도 기술적으로 엔드포인트는 CF 값이 60보다 큰 다른 정책의 조건과 일치할 수 있습니다. 다른 모든 조건을 충족하는 경우 엔드포인트는 Android 정책의 모든 조건에 부합하더라도 해당 프로파일에 할당됩니다.

일반적으로 미리 정의된 정책의 CF 값은 기본값으로 유지되어야 합니다. 경우에 따라, 네트워크 정책 또는 환경 설정에 따라 특정 정책이 다른 정책보다 우선 적용되도록 기본값을 수정해야 할 수 있습니다. 이 경우 기본 설정 정책에서 적용 가능한 규칙의 CF 값을 원하는 프로파일링 목표를 달성할 수 있는 최소 수준으로 높이십시오.

마찬가지로 새 프로파일을 생성하는 경우 비교적 낮은 설정(즉, 10 또는 20)으로 초기 CF 값을 설정한 다음 정책 할당을 모니터링하여 원하는 결과인지 검증합니다. 초기 값을 너무 높게 설정하면, 한 프로파일에 대한 규칙이 다른 정책에 비해 지나치게 높은 CF 값으로 설정된 경우 CF 계산을 바탕으로 실제 엔드포인트와 더 긴밀하게 연계된 다른 프로파일이 적용되지 못할 수 있습니다.

예를 들어 엔드포인트가 사용자 지정 Profile\_A의 단일 규칙과 일치하는 경우(CF가 100 값으로 증가) 이 엔드포인트는 CF가 각각 20씩만 증가하는 4개의 규칙과 일치하는 Profile\_B에 할당되지 않을 수 있습니다. 심지어 Profile\_A의 규칙이 Profile\_B의 규칙과 동일할 수 있지만 서로 다른 CF 값이 할당됩니다. 그러므로 일반적으로 정책 규칙 전체에서 일관된 CF 등급을 사용하는 것이 좋습니다.

**Cisco 모범 사례:** 일반적으로, CF 값을 기본 설정으로 유지하는 것이 좋습니다. 특정 프로파일 할당을 우선 적용하기 위해 기본 설정을 수정해야 하는 경우 원하는 기본 설정 프로파일의 규칙 값을 원하는 정책 할당을 적용할 수 있는 최솟값으로 높이십시오.

사용자 지정 프로파일을 생성하는 경우 CF의 초기 값을 다른 프로파일에 비해 상대적으로 낮게 유지하거나 다른 프로파일에 설정된 값과 동일하게 유지하십시오.

## 예외 및 NMAP 작업

일치 규칙에 대한 다른 2가지 가능한 작업은 Take Network Scan Action(네트워크 검사 작업 수행)과 Take Exception Action(예외 작업 수행)입니다. Take Network Scan Action(네트워크 검사 작업 수행)을 사용하면 Network Scan (NMAP) Action(네트워크 검사(NMAP) 작업) 필드의 설정에 따라 정책 서비스 노드에서 엔드포인트에 대해 NMAP 검사를 트리거할 수 있습니다. 이 기능은 [네트워크 검사\(NMAP\) 프로브를 사용한 프로파일링](#) 섹션에서 자세히 설명합니다.

Take Exception Action(예외 작업 수행)을 사용하면 ISE에서 Exception Action(예외 작업) 필드의 설정에 따라 엔드포인트를 정책에 정적으로 할당할 수 있습니다. 이 기능은 [예외 작업](#) 섹션에서 자세히 설명합니다.

이러한 작업은 모두 엔드포인트가 정책과 일치하고 지정된 조건과도 일치하는 경우에만 트리거될 수 있습니다. 조건은 일치하지만 엔드포인트가 프로파일 정책과 일치하지 않으면 작업이 수행되지 않습니다.

또한 여러 작업이 수행되도록 정책의 여러 규칙과 일치할 수도 있습니다. 예를 들어 정책도 일치하는 경우 CF가 10만큼 증가하는 규칙과 일치하고, Take Exception Action(예외 작업 수행) 또는 Take Network Scan Action(네트워크 검사 작업 수행)과 같은 다른 규칙과도 일치할 수 있습니다.

## 사용자 지정(사용자 정의) 프로파일링 정책 구성

- Step 63** 이 절차에서는 이전에 구성된 조건을 사용하여 실습용 APC UPS 디바이스를 위한 사용자 지정 프로파일링 정책을 생성합니다.
- Step 64** Policy(정책)→Profiling(프로파일링)으로 이동합니다. RHS 창 메뉴에서 Add(추가)를 클릭합니다.
- Step 65** 프로파일 이름에 APC-UPS를 입력합니다.
- Step 66** 설명에 **Custom profile for APC UPS Network Management module**을 입력합니다. APC 사용자 지정 조건에 대한 설명과 유사하게, **Custom** 키워드를 사용하면 이 문자열을 기준으로 모든 사용자 정의 정책을 간단하게 필터링할 수 있습니다.
- Step 67** 최소 확실성 요인에 대한 설정을 기본값인 10으로 유지합니다.
- Step 68** 기본 설정인 Create Matching Identity Group(일치하는 ID 그룹 생성) 대신 Use Hierarchy(계층 구조 사용) 라디오 버튼을 선택합니다.
- Step 69** Rules(규칙) 아래에서 조건 옆의 + 기호를 클릭하고 Select Existing Condition from Library(라이브러리에서 기존 조건 선택)를 선택합니다.
- Step 70** Condition Name(조건 이름)→Select Condition(조건 선택)에서 APC-OUICheck를 선택합니다.

**참고:** 프로파일링 조건을 먼저 생성한 다음 별도의 작업에서 프로파일링 정책을 생성하는 대신, Create New Condition(새 조건 생성) 옵션(고급 옵션)을 사용하여 프로파일링 정책 자체에서 새 조건을 생성할 수도 있습니다. 생성된 새 조건은 정책 규칙에서 명명된 조건으로 나타납니다.

- Step 71** 기본 규칙 작업인 Certainty Value Increases(확실성 값 증가)를 10 값으로 유지합니다(그림 80).

그림 75 사용자 정의 프로파일링 정책 예

Profiler Policy List > APC-UPS

**Profiler Policy**

\* Name: APC-UPS      Description: Custom profile for APC UPS Network Management module

Policy Enabled:

\* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

\* Exception Action: NONE

\* Network Scan (NMAP) Action: NONE

Create Matching Identity Group  
 Use Hierarchy

\* Parent Policy: NONE

---

Rules

If Condition: APC-OUICheck    Then: Certainty Factor Increases    10

**Step 72** Submit(제출)을 클릭하여 변경 내용을 저장합니다.

**Step 73** Administration(관리)→Identity Management(ID 관리)→Identities(ID)로 이동하고 LHS 창에서 Endpoints(엔드포인트)를 선택합니다. 그림 81과 같이 APC 디바이스는 목록에서 더 이상 Unknown(알 수 없음)으로 표시되지 않으며 일치하는 프로파일링 정책 할당이 새로 추가됩니다.

그림 76 사용자 정의 프로파일을 사용하는 엔드포인트 예

**Endpoints**

Edit Add Delete Import Export

Endpoint Profile	MAC Address	Static Assignment
<input type="checkbox"/> APC-UPS	00:C0:B7:68:31:E1	false
<input type="checkbox"/> APC-UPS	00:C0:B7:65:1F:BC	false

**Step 74** 목록에서 엔드포인트 중 하나에 대해 APC-UPS를 클릭합니다(그림 82).

그림 77 사용자 정의 프로파일을 사용하는 엔드포인트 세부사항 예

Endpoint List > 00:C0:B7:68:31:E1

**Endpoint**

\* MAC Address **00:C0:B7:68:31:E1**

\* Policy Assignment APC-UPS

Static Assignment

\* Identity Group Assignment Unknown

Static Group Assignment

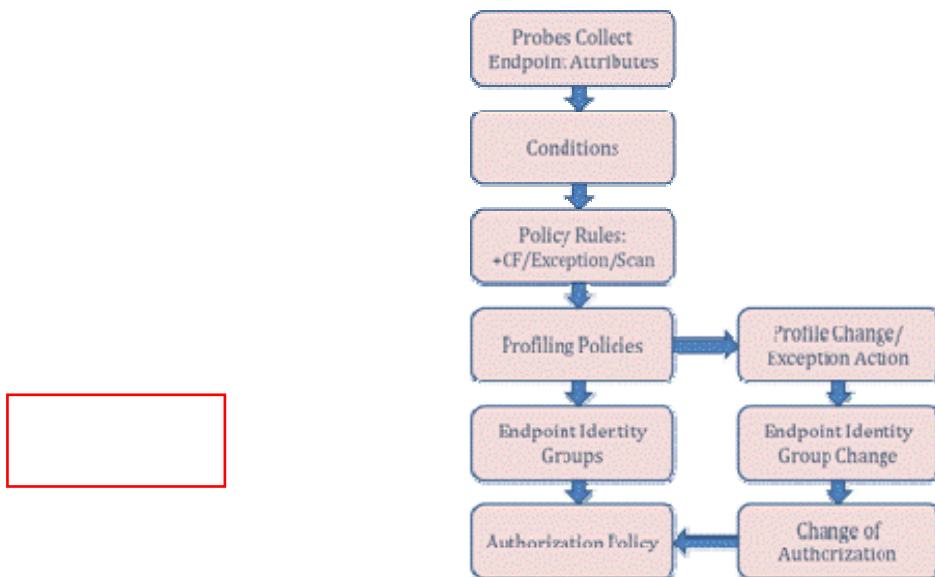
**Step 75** Policy Assignment(정책 할당)는 APC-UPS이지만 Identity Group Assignment(ID 그룹 할당)는 Unknown(알 수 없음)으로 설정되어 있습니다. 이는 프로파일의 기본 설정을 Create Matching Identity Group(일치하는 ID 그룹 생성)에서 User Hierarchy(사용자 계층)로 변경하기로 결정한 결과입니다. 이 옵션은 프로파일링 정책과 엔드포인트 ID 그룹의 관계를 보여주기 위해 의도적으로 선택되었습니다.

## 엔드 포인트 ID 그룹

디바이스 프로파일링은 네트워크 및 보안 관리자가 네트워크에 연결할 디바이스 유형을 더 효과적으로 파악할 수 있는 유용한 도구일 수 있습니다. 단순히 가시성뿐만 아니라, 엔드포인트의 디바이스 분류 또는 프로파일링 정책 할당에 따라 권한 부여 정책을 결정하기 위해서는 프로파일을 엔드포인트 ID 그룹에 연결해야 합니다. ISE 권한 부여 정책에서는 현재 원시 프로파일링 특성 또는 정책 할당을 조건으로 허용하지 않지만 프로파일링 정책 할당에 매핑되는 엔드포인트 ID 그룹을 생성할 수는 있습니다. 이렇게 하면 권한 부여 정책에서 엔드포인트의 프로파일링 정책 할당을 규칙 조건으로 간접적으로 참조할 수 있습니다.

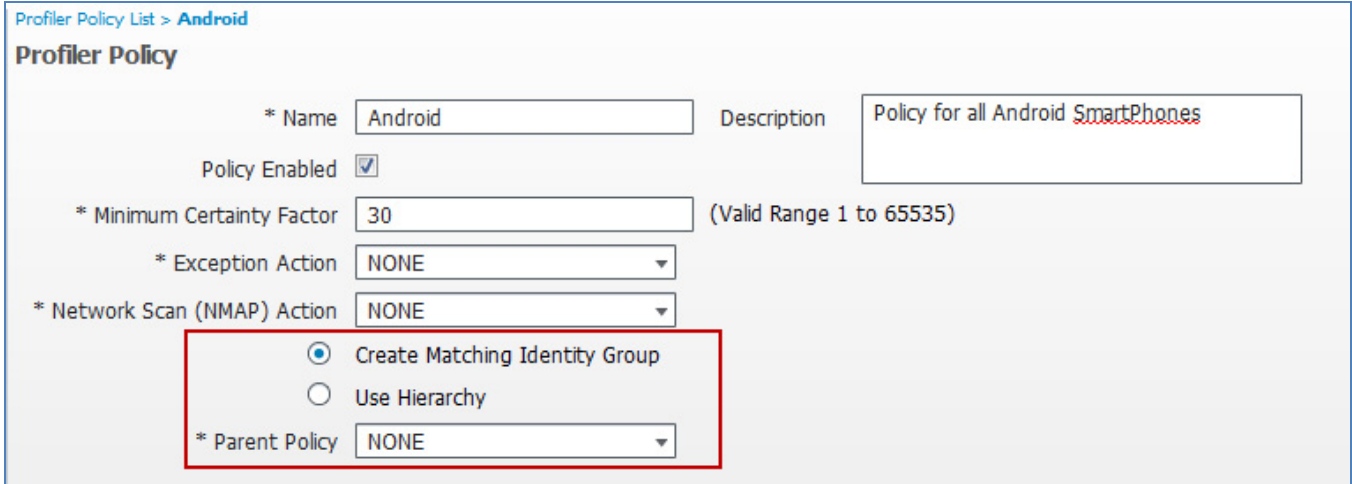
그림 83에서는 엔드포인트 ID 그룹의 컨피그레이션 흐름을 보여줍니다.

그림 78 컨피그레이션 흐름: 엔드포인트 ID 그룹



프로파일링 정책을 엔드포인트 ID 그룹에 매핑하려면 그림 84와 같이 프로파일 아래에서 Create Matching Identity Group(일치하는 ID 그룹 생성)이라는 라디오 버튼을 선택하십시오.

그림 79 프로파일링 정책 - 일치하는 ID 그룹 생성 예

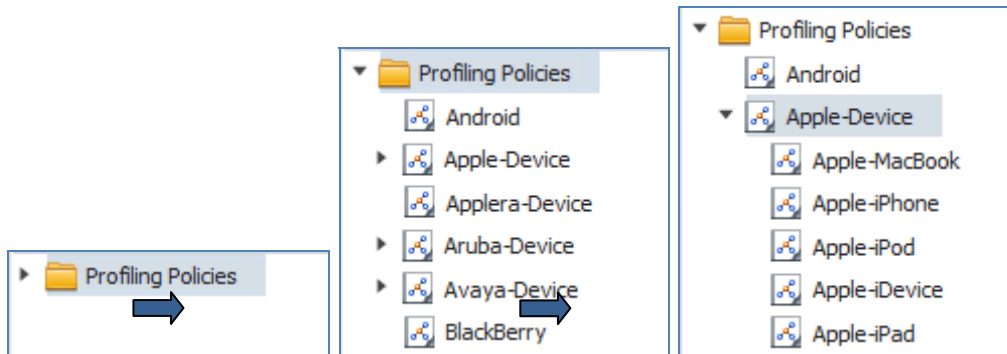


Create Matching Identity Group(일치하는 ID 그룹 생성) 옵션은 대부분의 사전 구성된 프로파일에 대한 기본 선택 사항인 Use Hierarchy(계층 구조 사용) 설정과 함께 사용할 수 없습니다. 그림 84의 Android 정책 예에서 기본 설정은 정책 이름에 따라 엔드포인트 ID 그룹을 생성하도록 변경되었습니다. 사용자 정의 프로파일의 기본 설정은 일치하는 ID 그룹을 생성하는 것입니다.

### 프로파일링 정책 계층

프로파일링 정책을 일치시키기 위한 마지막 기준은 엔드포인트가 상위 정책의 최소 CF를 충족하는 것입니다. 여기에서는 프로파일링 정책의 계층 항목에 대해 설명합니다. Parent Policy(상위 정책)가 NONE으로 설정되어 있는 Android 프로파일과 달리, 그림 84에서와 같이 Apple-iPad 및 Apple-iPhone과 같은 프로파일은 상위 프로파일이 Apple-디바이스인 하위 프로파일입니다. 정책을 계층을 보려면 Policy(정책)→Profiling(프로파일링)으로 이동합니다. LHS 창에서 레이블 앞에 있는 오른쪽 화살표 기호(▶)를 클릭하여 Profiling Policies(프로파일링 정책)를 확장합니다. 그러면 첫 번째 레벨 정책이 모두 표시됩니다 (그림 85).

그림 80 프로파일링 정책 계층



특정 항목 앞에 있는 오른쪽 화살표는 해당 프로파일에 대한 하위 정책이 있음을 나타냅니다. 위 그래픽에 따르면 Android 정책에는 하위 정책이 없는 반면 Apple-디바이스에는 상위 정책이 있습니다. 화살표를 클릭하면 Apple-디바이스의 하위 정책이 표시됩니다.

계층 구조는 화면을 구성하고 정책을 관리하는 데 유용합니다. 하위 정책을 일치시키면 보다 세부적인 규칙에 따라 상위 레벨의 조건을 반복적으로 정의할 필요 없이 상위 정책이 자동으로 일치되도록 여러 하위 정책에 대한 공통 조건 집합을 정의하는 방법도 제공됩니다.

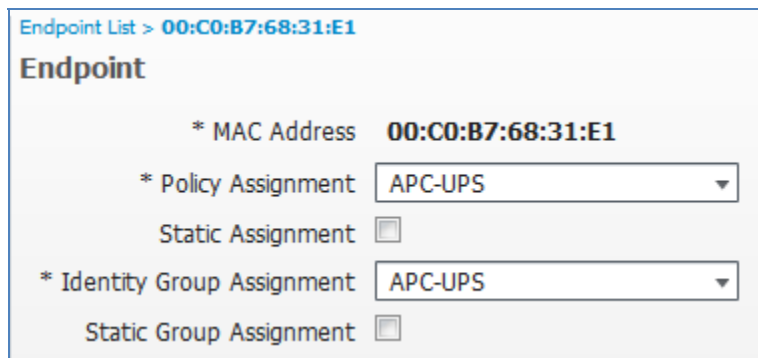
일반적인 계층 사용법은 OUI에 따라 일치시키는 것입니다. 예를 들어 모든 Apple 디바이스는 Apple과 같은 OUI를 갖습니다. 그러므로 iPad, iPod, iPhone 등에 대해 이 조건을 반복 적용할 필요가 없습니다. Apple-iPhone 프로파일을 일치시키려면 해당 엔드포인트에도 Apple OUI도 있어야 합니다. 이것이 바로 다른 브라우저 **User-Agent** 문자열과 유사한 User Agent Switch라는 간단한 Firefox 브라우저 플러그인을 사용해도 Apple iPhone에 대한 프로파일 조건을 통과하지 못하는 이유입니다. Apple MAC 주소가 없으면 상위 조건 테스트에 실패합니다. 이 가이드 앞부분에 설명된 것처럼 프로파일링은 안티 스푸핑 솔루션 역할을 하지는 못하지만 특정 스푸핑 활동을 자연스럽게 차단하는 솔루션 기능이 있습니다.

계층 구조는 ID 그룹 할당을 일치시키는 작업을 간소화하는 데에도 유용합니다. 상위 정책이 ID 그룹에 매핑된 경우 모든 하위 정책을 ID 그룹에 매핑할 필요는 없습니다. 예를 들어 Cisco IP Phone에는 사전 구성된 여러 프로파일이 있습니다. Cisco-IP-Phone(기본 설정)에 대해 일치하는 ID 그룹을 생성하면 이 상위 정책을 기반으로 권한 부여 정책을 생성할 수 있으며 각 하위 정책마다 별도의 ID 그룹이 필요하지 않습니다. 그에 따라 권한 부여 정책의 규칙을 크게 간소화할 수 있습니다. 개별 IP 전화기 모델에 대한 특수한 처리가 필요한 경우가 아니라면 상위 프로파일 및 ID 그룹 할당을 참조하여 일관되게 처리할 수 있습니다.

### 프로파일링 정책에 대해 일치하는 ID 그룹 생성

- Step 76** 이 절차에서는 APC-UPS라는 사용자 정의 프로파일 정책에 대한 ID 그룹을 생성합니다.
- Step 77** Policy(정책)→Profiling(프로파일링)으로 이동하고 프로파일 목록에서 APC-UPS를 선택합니다.
- Step 78** Create Matching Identity Group(일치하는 ID 그룹 생성) 옵션을 선택한 다음 Save(저장)를 클릭하여 변경 사항을 커밋합니다.
- Step 79** Administration(관리)→Identity Management(ID 관리)→Identities(ID)→Endpoints(엔드포인트)에서 내부 엔드포인트(Internal Endpoints) 목록으로 돌아가서 APC-UPS 프로파일에 할당된 엔드포인트 중 하나를 선택합니다(그림 86).

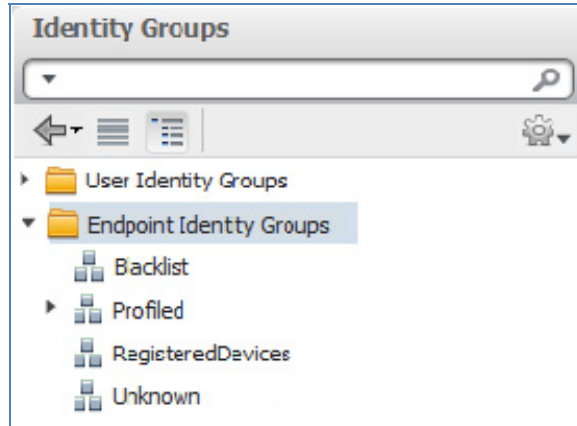
그림 81: 사용자 정의 프로파일에 대한 엔드포인트 ID 그룹 예



참고: Identity Group Assignment(ID 그룹 할당)가 Unknown(알 수 없음)에서 APC-UPS로 변경되었습니다.

**Step 80** Administration(관리)→Identity Management(ID 관리)→Groups(그룹)로 이동하고 LHS 창에서 엔드포인트 ID 그룹 왼쪽에 있는 화살표(▶)를 클릭하여 그림 87에 표시된 것처럼 해당 내용을 확장합니다.

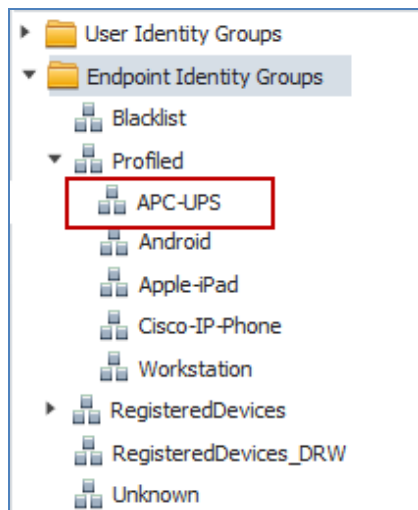
그림 82 엔드포인트 ID 그룹 보기 예 1



**Step 81** 이 목록에는 기본 최상위 ID 그룹이 지정되어 있습니다. 기본적으로, 일치하는 ID 그룹이 없는 프로파일링 정책에 할당된 모든 엔드포인트는 ID 그룹 **Unknown**의 멤버가 됩니다. 일치하는 ID 그룹이 있는 프로파일링 정책에 할당된 모든 엔드포인트는 상위 ID 그룹 **Profiled** 아래에 있는 ID 그룹의 멤버로 표시됩니다. **Blacklist** 및 **RegisteredDevices** 그룹은 특수 그룹입니다. **Blacklist**는 엔드포인트에서 거부된 네트워크 액세스를 식별하는 데 사용됩니다. **RegisteredDevices**는 MyDevicesPortal 및 Native Supplicant Provisioning에서 네트워크 액세스 사용자가 등록한 엔드포인트를 지정하는 데 사용됩니다.

**Step 82** Profiled 왼쪽의 ▶를 클릭하여 해당 내용을 확장합니다(그림 88).

그림 83 엔드포인트 ID 그룹 보기 예 2

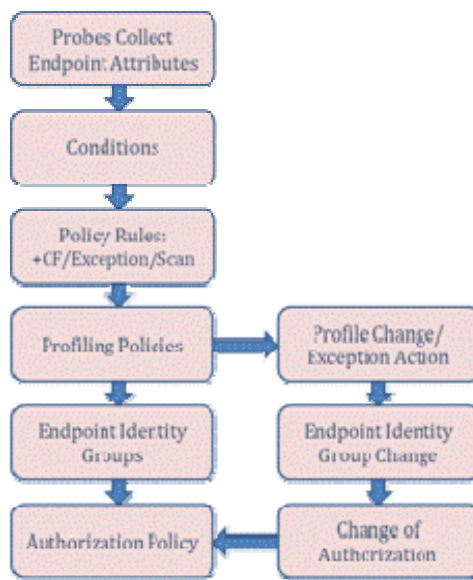


**Step 83** Cisco-IP-Phone 및 워크스테이션을 포함하여 기본적으로 일치하는 ID 그룹이 있는 몇 가지 프로파일링 정책이 있습니다. APC-UPS는 엔드포인트 ID 그룹 목록에도 표시되며 이제 권한 부여 정책 규칙에서 일치 조건으로 선택할 수 있습니다.

## 프로파일링 및 권한 부여 정책

권한 부여 정책은 일치 규칙을 기반으로 네트워크에 연결되는 엔드포인트에 대한 액세스 권한을 정의합니다. 권한 부여 정책 규칙은 지정된 권한이 할당되기 전에 엔드포인트에서 충족되어야 하는 조건을 지정합니다. 프로파일링을 기반으로 정책을 엔드포인트에 할당하려면 일치하는 ID 그룹이 있는 프로파일링 정책에 엔드포인트를 할당해야 합니다. 그림 89에서는 권한 부여 정책의 컨피그레이션 흐름을 보여줍니다.

그림 84 컨피그레이션 흐름: 권한 부여 정책



ISE 프로파일링 서비스를 사용하여 디바이스를 분류하고 ID 그룹에 할당하면 ISE에서 프린터 또는 IP 전화기와 같이 MAB를 사용하여 인증되지 않은 엔드포인트에 서로 다른 정책을 적용하거나, 회사 워크스테이션과 달리 iPad와 같은 개인 디바이스를 사용하여 연결하는 경우 인증된 직원에 다른 정책을 적용할 수 있습니다(그림 90).

그림 85 권한 부여 정책 예

Authorization Policy			
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.			
First Matched Rule Applies			
▶ Exceptions (0)			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones
✓	Employee_Personal_Device	if <b>Android</b> OR <b>Apple-iPad</b> AND Employee	then Guest
✓	Employee_Corp_Device	if <b>Workstation</b> AND Employee	then Employee



- Step 84** 샘플 권한 부여 정책에 나타난 것처럼 Cisco IP Phone으로 프로파일링되는 엔드포인트에 특수 전화기 권한을 할당하는 데 Cisco-IP-Phone이라는 ID 그룹이 사용됩니다. 이러한 엔드포인트는 MAB를 사용하여 인증됩니다. 계층적 정책을 사용하면 특정 IP 전화기 모델에 대한 프로파일 일치에 상관없이 이러한 정책을 Cisco IP Phone에 적용할 수 있습니다.
- Step 85** 또한 권한 부여 정책에서는 프로파일링을 통해 Apple-iPad 또는 Android로 분류된 개인 디바이스를 사용하여 연결하는 직원에게 고유한 인터넷 전용 액세스(게스트 권한) 권한을 부여하고, 그와 동시에 워크스테이션을 통해 연결하는 직원에게는 전체 액세스 권한(직원 권한)을 부여하는 방법도 보여줍니다.

**권한 부여 정책에서 엔드포인트 ID 그룹 사용**

- Step 86** 이 절차에서는 MAB 인증 및 APC-UPS라는 ID 그룹에 대한 권한 부여 정책 규칙에 따라 APC UPS 디바이스로 프로파일링된 엔드포인트에 특수 권한이 할당됩니다.
- Step 87** Policy(정책)→Authorization(권한 부여)으로 이동하고 Profiled Cisco IP Phones 규칙 아래에 Profiled UPS Systems라는 새 규칙을 삽입합니다.
- Step 88** Identity Group(ID 그룹) 조건에서 Endpoint Identity Groups(엔드포인트 ID 그룹)→Profiled(프로파일링됨)로 이동하고 APC-UPS를 선택합니다.
- Step 89** Permissions(권한)에서 UPS와 같은 적절한 Authorization Profile(권한 부여 프로파일)을 선택한 다음 Save(저장)를 클릭하여 변경 사항을 커밋합니다. 그림 91과 같이 정책 규칙이 표시됩니다.

그림 86 권한 부여 정책 컨피그레이션 예 1

Authorization Policy			
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.			
First Matched Rule Applies			
▶ Exceptions (0)			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✔	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✔	Profiled UPS systems	if APC-UPS	then UPS

- Step 90** UPS 디바이스 연결을 해제했다가 다시 연결하거나 해당 인터페이스에서 **shut / no shut** 명령을 실행하여 연결 스위치 포트를 재설정하는 방식으로 권한 부여 정책이 예상대로 작동하는지 확인합니다.
- Step 91** Operations(운영)→Authentications(인증)로 이동하여 실시간 인증 로그를 봅니다. 그림 92의 항목과 유사한 항목이 표시됩니다.

그림 87 권한 부여 정책 컨피그레이션 예 2

Live Authentications								
Add or Remove Columns Refresh							Refresh	
Every 1 minute								
Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Authorization Profiles	Identity Group
May 07,12 06:35:17.230 AM	✔		00:C0:B7:65:1F:BC	00:C0:B7:65:1F:BC	172.16.1.48	cat3750x	UPS	Profiled:APC-UPS
May 07,12 06:35:01.802 AM	✔		#ACSACL#-IP-PERMI			cat3750x		
May 07,12 06:35:01.768 AM	✔		00:C0:B7:68:31:E1	00:C0:B7:68:31:E1	172.16.1.49	cat3750x	UPS	Profiled:APC-UPS

**Step 92** 이 로그를 통해 APC-UPS로 프로파일링된 두 엔드포인트가 UPS라는 권한 부여 프로파일을 사용하여 인증되고 권한이 부여됨을 알 수 있습니다. 이 예에서는 첫 번째 엔드포인트에 권한이 부여된 후에 다운로드 가능한 ACL(dACL)이 스위치로 전송됩니다. 두 번째 엔드포인트에서는 이미 다운로드된 dACL을 재사용하므로 두 번째 dACL은 전송되지 않습니다.

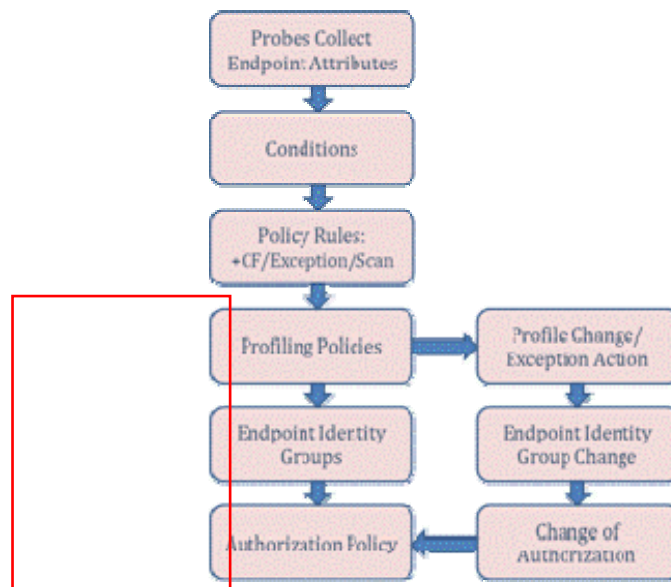
## 프로파일 전환 및 COA(Change of Authorization)

프로파일링 과정을 통해 엔드포인트는 알 수 없는 ID 그룹에서 보다 구체적인 특정 프로파일(예: Apple-디바이스)로 전환될 수 있습니다. 경우에 따라 Apple-iPad 등으로 직접 전환되지만, 네트워크에서 새 프로파일 데이터가 수집되면 그에 맞춰 전환이 발생할 수도 있습니다. 일반적인 경우는 아니지만 엔드포인트에 대한 “네거티브” 프로파일링 데이터의 경우 더 구체적인 프로파일에서 덜 구체적인 상위 프로파일로 전환되거나 모두 완전히 다른 프로파일로 전환되도록 할 수 있습니다.

프로파일 전환 유형에 상관없이 일치하는 엔드포인트가 네트워크에 인증될 때 엔드포인트 ID 그룹 할당에서 다른 권한 부여 정책 규칙을 적용하는 연관된 변경 사항이 있는 경우가 있을 수 있습니다. 문제는 네트워크에 이미 인증되고 권한이 부여된 엔드포인트에 새 권한 부여가 미치는 영향입니다.

그림 93에서는 프로파일 전환 및 CoA(Change of Authorization)의 컨피그레이션 흐름을 보여줍니다.

그림 88 컨피그레이션 흐름: 프로파일 전환 및 CoA



### CoA(Change of Authorization)

CoA는 특정 상태 또는 정책 변경이 발생하는 경우 RADIUS 서버(ISE)가 네트워크 액세스 디바이스(RADIUS 클라이언트)를 대상으로 요청하지 않은 통신을 시작하여 엔드포인트에 대한 액세스 정책을 업데이트하도록 하는 표준 기반 RADIUS 기능(RFC 3576)입니다. 업데이트는 엔드포인트에서 재인증을 시작하지 않아도 발생할 수 있습니다.

ISE 프로파일링 서비스는 다음 2가지 기본 조건에 따라 CoA를 트리거합니다.

프로파일 전환에서 예외 작업이 트리거됩니다.

프로파일 전환으로 인해 권한 부여 정책 규칙에 따라 엔드포인트 액세스가 변경됩니다.

### 예외 작업

기본적으로 미리 정의되고 구성 불가능한 3가지의 예외 작업이 있습니다. Policy(정책)→Policy Elements(정책 요소)→Results(결과)→Profiling(프로파일링)→Exception Action(예외 작업)으로 이동하여 목록을 봅니다 (그림 94).

그림 99 예외 작업

<input type="checkbox"/>	Profiler Action Name ▲	Description
<input type="checkbox"/>	EndpointDelete	When endpoint is deleted or reassigned to the unknown profile.
<input type="checkbox"/>	FirstTimeProfile	When an endpoint profile changes from unknown to known for the first time.
<input type="checkbox"/>	StaticAssignment	When an endpoint has connected to the network and is now statically assigned.

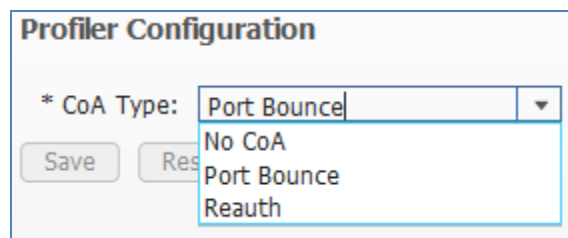
엔드포인트가 삭제되거나 프로파일링된 프로파일에서 알 수 없는 프로파일(프로파일링 정책이 일치하지 않음)로 전환될 경우 **EndpointDelete**에서 CoA를 보냅니다.

엔드포인트가 알 수 없는 프로파일에서 특정 프로파일링 정책 할당으로 전환되면 **FirstTimeProfile**에서 CoA를 생성합니다. 엔드포인트가 알 수 없는 프로파일 간에 전환(예: Apple-디바이스에서 Apple-iPod으로)되는 경우에는 이 예외 작업에서 CoA가 트리거되지 **않습니다**.

엔드포인트가 동적 프로파일 할당에서 정적으로 프로파일에 할당되면 **StaticAssignment**에서 CoA가 발생합니다. 정적 정책 할당에 지정되고 나면 프로파일링 특성에서 정상적으로 전환을 지시하는 경우에도 새 엔드포인트 프로파일링 정책을 할당할 수 없습니다.

각 예외 작업에 대해 전송되는 기본 CoA 유형은 **Administration(관리)→System(시스템)→Settings(설정)→Profiling(프로파일링)**의 전역 설정에서 구성됩니다(그림 95).

그림 90 전역 프로파일러 CoA 컨피그레이션



전역 프로파일링 설정 컨피그레이션은 이 가이드의 [전역 프로파일링 설정 구성](#) 섹션에서 다뤄집니다. 다른 세션의 중단을 최소화하기 위해 동일한 스위치 포트를 통해 여러 세션이 연결된 경우 포트 바운스 설정은 재인증 설정으로 축소됩니다.

시스템 정의 예외 작업은 구성이 불가능하며 프로파일링 정책 아래에 작업으로 할당할 수 없습니다. 이는 정의된 전환에 따라 자동으로 트리거됩니다. 그러나 관리자는 사용자 지정 예외 작업을 정의할 수 있습니다. 사용자 정의 예외는 프로파일링 정책에서 정적 프로파일링 정책 할당을 적용하고 CoA를 전송할지 지정하는 데 사용할 수 있습니다.

### 권한 부여 정책이 변경되는 경우 프로파일 전환에 따른 자동 CoA

Cisco ISE Software Release 1.1.1 이전 버전에서는 예외 작업이 일반적으로 프로파일 간 전환(알려진 한 프로파일에서 알려진 다른 프로파일로)에 CoA를 시행하는 데 사용되었으며, 엔드포인트를 프로파일링 정책에 정적으로 할당하는 경우 예기치 않은 부작용이 발생했습니다. ISE 1.1.1부터는 프로파일 전환으로 인해 권한 부여 정책 규칙에 따라 엔드포인트 액세스가 변경되는 경우 ISE 정책 서비스 노드는 CoA를 실행합니다. 결정 로직은 권한 부여 정책 규칙에서 ID 그룹이 사용되는 엔드포인트 ID 그룹의 변경을 기반으로 합니다. 이 개선된 기능에서는 프로파일 간 전환에 CoA를 전송하는 활용 사례를 처리하는 데 예외 작업을 사용해야 할 필요성을 제거했습니다. 또한 엔드포인트에서 동적 프로파일 할당을 유지할 수 있으므로 프로파일링 특성 및 정책 컨피그레이션에 따라 추가적인 전환이 가능합니다.

사용자 정의 예외 작업은 특정 조건을 충족하는 경우 엔드포인트를 기본 설정 정책 할당에 정적으로 지정하며, 선택적으로 정책 할당 시 CoA가 전송되지 않도록 차단하는 데 적합합니다. 활용 사례의 예로는 제조 시설의 프로세스 제어 엔드포인트 또는 의료 시설의 네트워크 연결 의료 디바이스와 같은 네트워크 디바이스가 있습니다. 이 예에서 관리자는 정책 및 관련 ID 그룹에 엔드포인트를 정적으로 할당해야 할 수 있습니다. 예외를 통한 정적 할당을 사용하면 의사 프로파일 데이터가 엔드포인트의 프로파일을 되돌리고 해당 네트워크 연결에 영향을 미칠 수 있는 위험을 차단할 수 있습니다.

### 사용자 지정(사용자 정의) 예외 작업 구성

**Step 93** 이 절차에서는 지정된 조건과 일치하는 경우 정적 프로파일링 정책에 할당되도록 의료 디바이스에 대한 예외 작업을 구성합니다. 디바이스의 예는 이동식 무선 심장 모니터인 Draeger M300입니다.

주의: 의료 솔루션과 관련된 고유한 규정 준수 요인으로 인해 이 예의 목표는 사용자 지정 예외 작업의 사용을 엄격히 보여주는 것입니다. 의료 디바이스에 대한 네트워크 액세스를 보호하기 위한 방법으로 ISE 프로파일링 서비스가 적절한지 검증하지는 않습니다.

**Step 94** Policy(정책)→Profiling(프로파일링)으로 이동하고 목록에서 Draeger-M300을 선택합니다. 기본적으로 이 프로파일은 예외 작업을 참조하는 규칙을 포함하지 않습니다. 또한 예외 작업은 정의되어 있지 않습니다(그림 96).

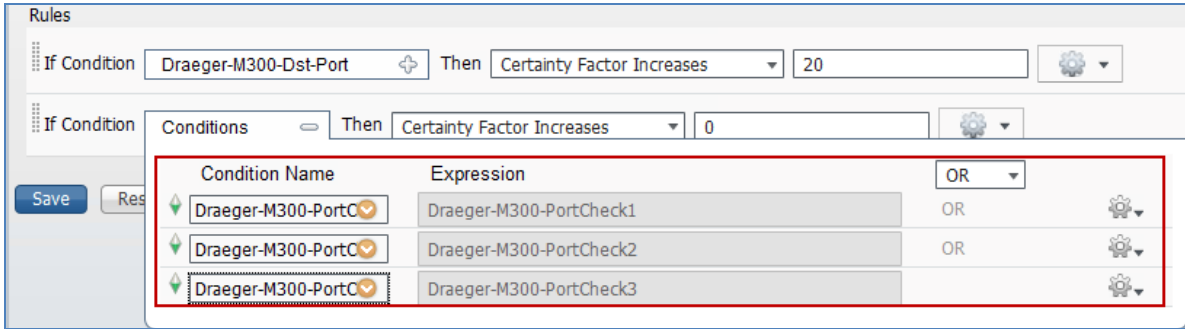
그림 91 Draeger-M300 프로파일링 정책 예

- Step 95 새 예외 작업을 추가합니다.
- Step 96 Policy(정책)→Policy Elements(정책 요소)→Results(결과)로 이동하고 LHS 창의 프로파일링 왼쪽에 있는 화살표(▶)를 클릭하여 해당 내용을 확장합니다.
- Step 97 LHS 창에서 예외 작업을 선택하고 RHS 창의 메뉴에서 Add(추가)를 클릭합니다.
- Step 98 그림 97에 표시된 값을 사용하여 새 예외 작업이 추가되었습니다.

그림 92 사용자 정의 예외 작업 예

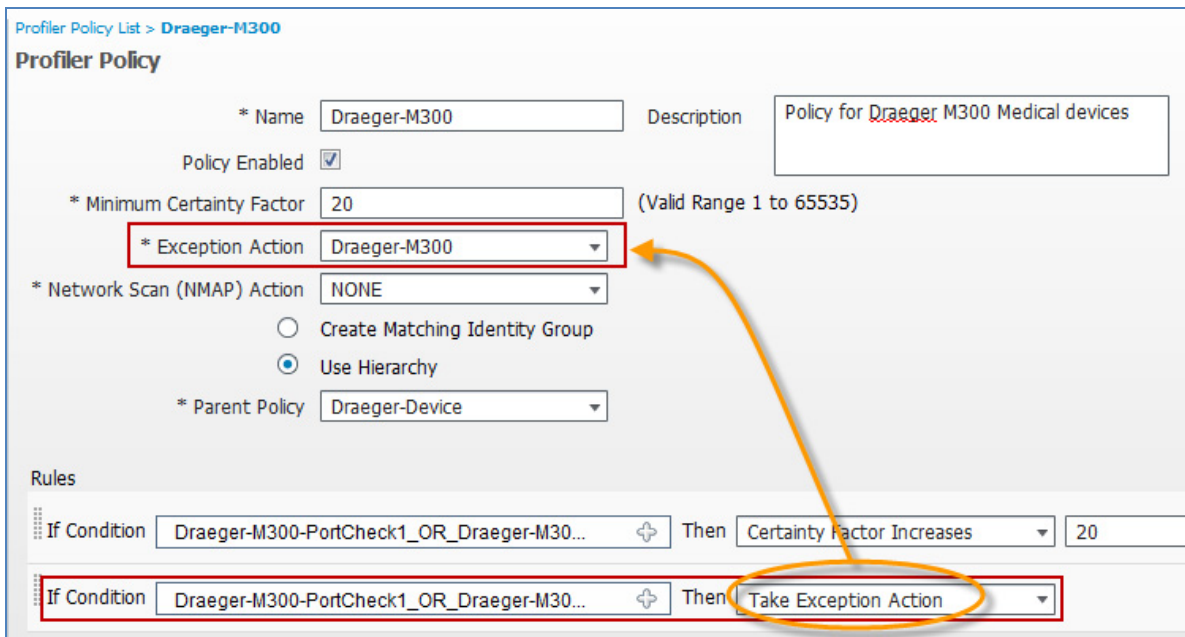
- Step 99 이 예에서는 프로파일 Draeger-M300에 대한 정적 정책 할당에 따라 추가 CoA가 전송되지 않습니다. 이는 앞서 표시된 프로파일과 동일합니다.
- Step 100 Policy(정책)→Profiling(프로파일링) 아래의 Draeger-M300 프로파일링 정책으로 돌아가서 다음 단계를 완료하여 프로파일에 대한 예외 작업을 정의합니다.
- Step 101 예외 작업을 Draeger-M300으로 설정합니다.
- Step 102 프로파일 일치에 사용된 기존 규칙의 조건과 동일하게 새 규칙을 생성합니다(그림 98).

그림 93 사용자 정의 예외 작업을 사용한 프로파일링 정책 규칙 예 1



**Step 103** 작업(Then)을 기본값인 Certainty Factor Increases(확실성 요인 증가)에서 Take Exception Action(예외 작업 수행)으로 변경합니다. 그림 99와 유사하게 결과 프로파일링 정책이 표시됩니다.

그림 94 사용자 정의 예외 작업을 사용한 프로파일링 정책 규칙 예 2



**Step 104** 변경 내용을 저장합니다.

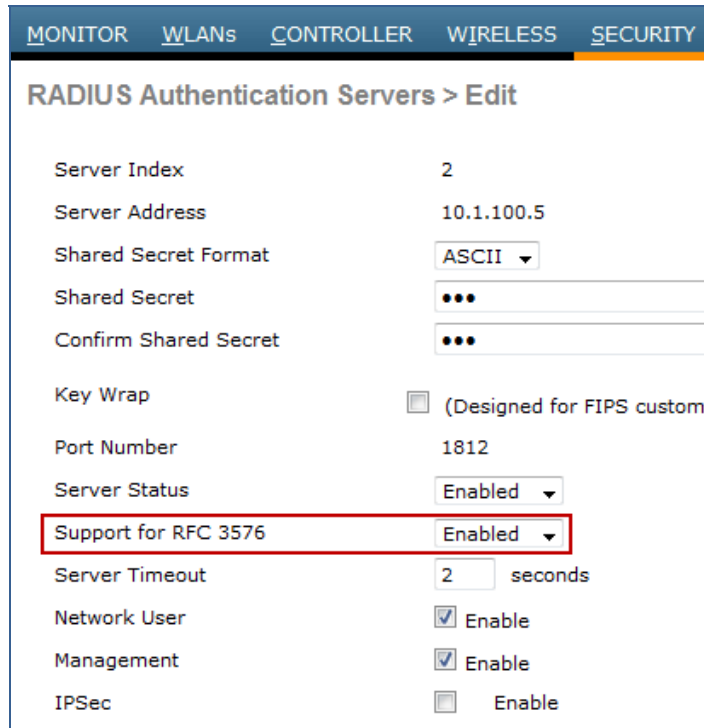
**Step 105** 이 정책 예에서는 정책을 엔드포인트에 할당하고 엔드포인트를 정책에 정적으로 할당하는 데 사용한 것과 동일한 기준을 사용했습니다. 권한 부여 정책에서는 Draeger-디바이스라는 상위 정책에 일치하는 ID 그룹이 있다는 사실을 이용할 수 있습니다. 그렇지 않으면 이 정책에는 ID 그룹이 할당되어 있을 수 있으며 이를 통해 권한 부여 정책에서 이 특정 프로파일을 참조합니다.

**Step 106** CoA를 지원하도록 유선 스위치를 구성합니다. 표시된 것처럼 전역 컨피그레이션 모드에서 **aaa server radius dynamic-author** 명령을 사용합니다.

```
cat3750x(config)# aaa server radius dynamic-author
cat3750x(config-locsvr-da-radius)# client <ISE_PSN_IP_address> server-key <secret-key>
```

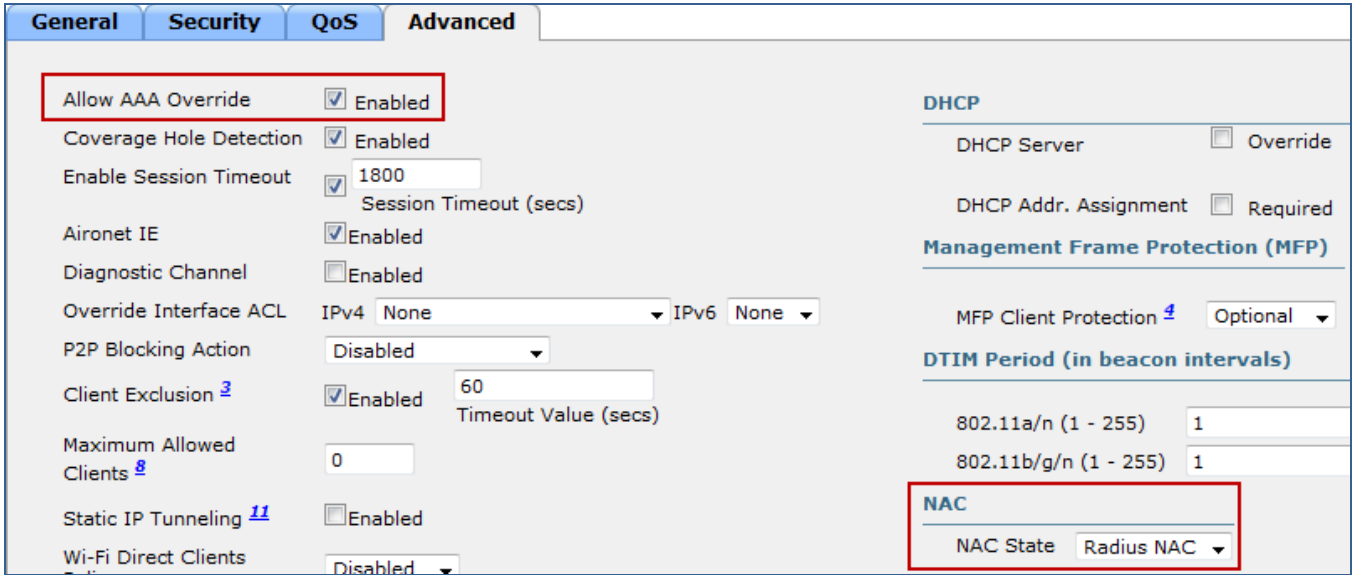
- Step 107** RADIUS를 통해 스위치와 통신하는 각 ISE 정책 서비스 노드마다 별도의 클라이언트 항목을 추가합니다.
- Step 108** CoA를 지원하도록 무선 컨트롤러를 구성합니다.
- Step 109** WLC 웹 관리 인터페이스에서 Security(보안)→AAA→RADIUS→Authentication(인증)으로 이동합니다. RADIUS 서버 정의에서 그림 100과 같이 Support for RFC 3576(RFC 3576 지원)이 활성화되어 있는지 확인합니다.

그림 95 무선 컨트롤러에 대한 CoA 컨피그레이션 예 1



- Step 110** WLANs(WLAN)→(WLAN)→Edit(편집)→Advanced(고급)로 이동합니다. 각 WLAN에서 CoA를 지원하도록 그림 101과 같이 Allow AAA Override(AAA 재정의 허용)를 Enabled(사용)로 설정하고 NAC State(NAC 상태)를 RADIUS NAC로 설정합니다.

그림 96 무선 컨트롤러에 대한 CoA 컨피그레이션 예 2



**Step 111** 각 플랫폼에 대한 변경 내용을 적절히 저장합니다.



## 프로파일링 설계 및 모범 사례

이 섹션에서는 다양한 구축 및 활용 사례에 대한 일반적인 프로파일링 설계 및 모범 사례 권장 사항에 대해 설명합니다.

### 프로파일링 설계 고려 사항

ISE 프로파일링 요구 사항에 대한 계획을 수립하는 경우에는 먼저 네트워크 액세스 정책을 지원하기 위해 분류해야 하는 엔드포인트 유형을 파악해야 합니다. 예를 들어 특정 유형의 네트워크 디바이스 중 다수가 802.1X 또는 웹 기반 인증을 지원하지 않는 경우 디바이스 분류에 따라 MAB 인증과 권한 부여가 요구될 가능성이 높습니다. 네트워크 액세스를 위한 프로파일링이 필요할 수 있는 알려진 디바이스 유형을 모두 나열해야 합니다.

#### 알려진 디바이스 유형 프로파일링

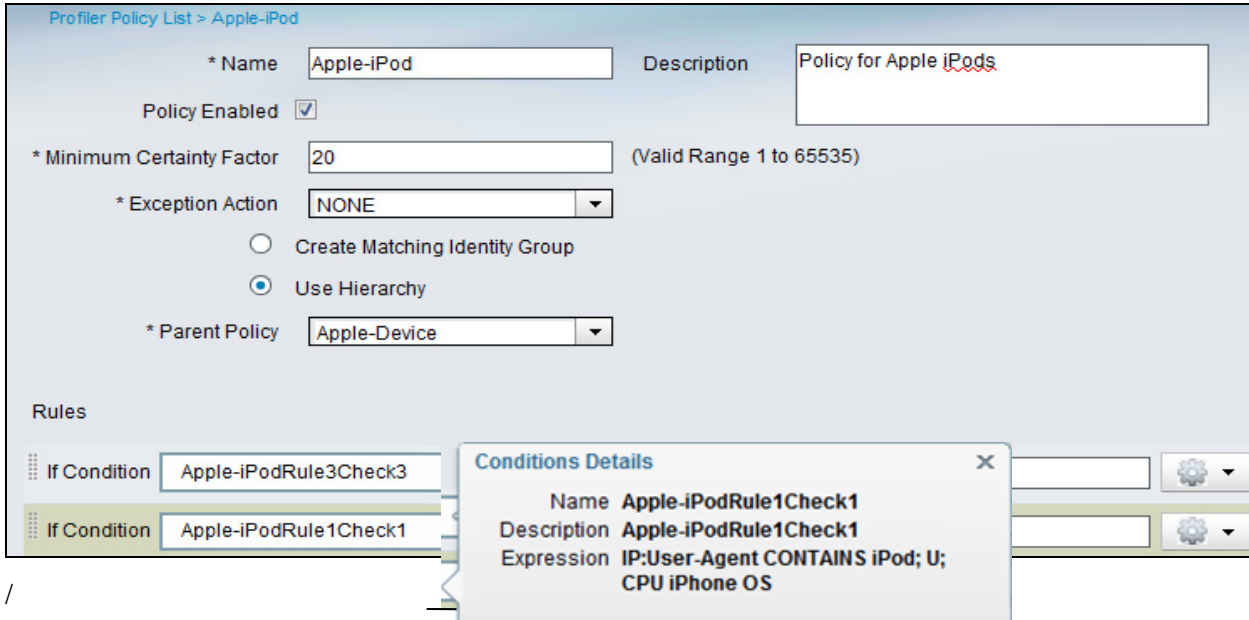
ISE 계획 단계에서 디바이스 분류(프로파일 특성에 따라 권한 부여)가 요구되는 엔드포인트를 식별하고 이러한 엔드포인트를 프로파일링하는 데 필요한 특성을 결정합니다. 권한 부여가 필요한 디바이스가 이미 알려져 있는 경우 다음 단계는 그러한 디바이스를 적절히 프로파일링하는 데 필요한 특성 및 관련 프로브를 결정하는 것입니다.

널리 사용되는 엔드포인트의 경우 ISE 프로파일 라이브러리에 사전 구성된 정책이 있습니다. 이러한 기본 ISE 프로파일을 검토하여 특성 및 프로브 요구 사항을 결정합니다. 예를 들어 프로파일 X에 조건 A, B 및 C가 포함되어 있다는 것을 알면 해당 데이터를 수집하는 데 필요한 특성 및 프로브를 추론할 수 있습니다. 프로파일 라이브러리에 특정 일치 항목이 없으면 유사한 디바이스 유형의 프로파일을 참조합니다. 프로파일링 요구 사항은 유사한 디바이스 유형의 요구 사항과 유사한 경우가 종종 있습니다.

기존 프로파일이 없는 경우 엔드포인트에 대한 특성을 수집하기 위한 프로브를 일시적으로 활성화할 수 있습니다. 관리자는 대개 엔드포인트를 재설정하거나 네트워크 연결을 해제했다가 다시 연결하는 방식으로 정상 시동 시 디바이스에 사용할 수 있는 특성을 캡처할 수 있습니다. ISE에 표시되는 특성은 엔드포인트를 고유하게 분류할 수 있는 관련 특성을 나타내는 경우가 많습니다. 일부 디바이스의 경우 OUI, DHCP 옵션, 사용자 에이전트, TCP/UDP 포트 또는 DNS 이름 지정을 위한 고유한 특성을 결정하기 위해 패킷 캡처를 비롯한 트래픽 분석이 필요할 수 있습니다.

다음 예(그림 102)에서는 Apple iPod 프로파일에 대한 일치에 사용되는 특성을 조회하는 방법을 보여줍니다. 이 프로파일은 DHCP 특성 또는 **User-Agent** 기반임을 알 수 있습니다. 그러므로 Apple iPod을 프로파일링하려면 DHCP 및 HTTP를 사용하는 것이 좋습니다.

그림 97 Apple-iPod에 대한 프로파일링 조건 예



프로파일 라이브러리(Policy(정책)→Profiling(프로파일링) 아래)를 보거나 프로파일러 조건(Policy(정책)→Policy Elements(정책 요소)→Conditions(조건)→Profiling(프로파일링) 아래)(그림 103)을 검토하여 해당 엔드포인트 또는 유사한 엔드포인트를 프로파일링하는 데 필요한 프로브 및 사용되는 특성을 적절히 이해할 수 있습니다.

그림 98: 프로브 및 프로파일러 조건

주요 프로파일링 특성을 파악했으면 사용 가능한 프로브 및 필요한 프로파일 데이터를 수집하기 위한 다른 수집 방법에서 최상의 옵션을 결정합니다. 각 프로브 유형을 지원하기 위한 특정 요구 사항에 대한 자세한 내용은 ISE 프로브 컨피그레이션의 개별 섹션을 참조하십시오. 이 섹션의 끝부분에는 프로브 선택 모범 사례에 대한 추가 권장 사항이 제공되어 있습니다.

### 알 수 없는 디바이스 유형 프로파일링

프로파일링되는 엔드포인트 목록에는 네트워크 연결 프린터, 팩스 기기, 전화기, 카메라, 저장 장치 또는 IP 지원 엔드포인트가 포함될 수 있습니다. 중요한 디바이스 목록이 이미 알려져 있는 경우(예: 대규모 IP 텔레포니 구축 환경 내)도 있습니다. 경우에 따라 알 수 없는 다수의 호스트가 있는 경우도 있으며, 이 경우에는 먼저 엔드포인트를 검색해야 합니다. 단계별 ISE 구축은 모니터 모드에서 시작하는 일반적인 모범 사례입니다. 이 경우 관리자는 네트워크에 연결되는 엔드포인트 및 스위치 포트가 적용 모드로 전환되는 경우 네트워크 액세스가 거부되는 엔드포인트의 유형을 알 수 있습니다.

무선 엔드포인트에는 “모니터 모드”가 없지만 802.1X, 웹 인증 또는 MAC 필터링을 사용하여 연결되는 엔드포인트를 분류하는 데 무선 프로파일링을 계속 사용할 수 있습니다. Cisco Wireless LAN Controller Software Release 7.0.116.0부터 ISE는 무선 802.1X 엔드포인트 프로파일링을 지원합니다. WLC Release 7.2.103.0부터 ISE는 Central WebAuth를 사용하여 인증되는 엔드포인트를 포함하여 MAC 필터링을 사용한 무선 엔드포인트의 프로파일링을 지원합니다. 이는 이러한 WLAN 인증 방법으로 CoA 지원이 도입되었기 때문에 가능합니다.

7.2.103.0 이전 버전에서도 여전히 무선 클라이언트를 프로파일링할 수 있지만 ISE는 프로파일 전환에 CoA를 적용할 수 없습니다. 그러나 인벤토리(가시성) 용도를 위해 엔드포인트를 분류하고 선택적으로 엔드포인트 ID 그룹에 할당할 수 있습니다. 또한 무선 네트워크에 다시 연결할 때 현재 ID 그룹 할당에 따라 권한 부여 정책을 엔드포인트에 적용할 수 있습니다. 활성 세션 중에 프로파일 변경이 발견된 경우에는 권한 부여를 변경할 수 없습니다.

**모범 사례:** 위 그림에 표시된 통화 스테이션 ID 유형이 비 802.1X 클라이언트를 프로파일링할 수 있도록 시스템 MAC 주소로 설정되어 있는지 확인합니다. 이렇게 하면 ISE가 엔드포인트를 데이터베이스에 추가하고 수신된 다른 프로파일 데이터를 알려진 MAC 주소를 기반으로 동일한 엔드포인트에 연결할 수 있게 됩니다.

가능하면 구축 초기 단계에 ISE 프로파일링을 구축합니다. ISE는 검색 프로세스를 시작하기 위한 네트워크 인증 또는 권한 부여 없이 유선 엔드포인트를 프로파일링할 수 있습니다. 이는 네트워크에 연결하려는 엔드포인트를 파악할 수 있는 가시성 측면에서 큰 도움이 됩니다. 이와 같은 초기 단계에서 네트워크 액세스를 위한 프로파일링이 필요한 특정 엔드포인트 유형이 아직 명확하지 않은 경우 ISE 프로파일링 정책은 바뀔 수 있습니다.

### 프로파일링에 미치는 액세스 정책 및 디바이스 컨피그레이션 영향

사용되는 802.1X 구축 모드(공개 인증과 닫힌 모드 비교) 및 액세스 디바이스에 구성된 인증 방법의 순서/우선순위에 따라 프로파일링 결과는 다를 수 있습니다. 예를 들어 포트가 닫힌 모드인 경우 포트에 권한이 부여될 때까지 DHCP 패킷을 전송할 수 없습니다. 특정 트래픽이 전송되지 않으면 프로브는 프로파일링을 결정하는 데 필요한 데이터를 수집할 수 없습니다. 공개 인증(모니터 모드 및 로임팩트 모드)을 사용하면 포트에 권한이 부여되기 전에 특정 트래픽이 통과할 수 있습니다. 어떤 시나리오에서든 프로파일링이 지원되지만 특정 구축 모드가 특성 수집의 시기 및 기능에 미치는 영향을 이해해야 합니다.

유연한 인증(FlexAuth)의 경우 인증 방법의 순서도 특성이 수집되는 시기와 권한 부여 시점에 할당되는 프로파일에 영향을 미칠 수 있습니다. 예를 들어 MAB 인증을 먼저 수행하도록 순서가 설정된 경우 802.1X가 모니터 또는 로임팩트 모드에 있으면 ISE에서 초기 연결 시에 원하는 정책을 할당하기에는 프로파일 데이터가 부족할 수 있습니다. MAB 조회가 수행되는 경우 엔드포인트는 여전히 알려지지 않은 그룹 또는 일반 프로파일링된 ID 그룹에 있을 수 있습니다. 802.1X를 먼저 수행하도록 순서가 설정된 경우 802.1X 시간이 초과되기 전에 DHCP 및 다른 프로파일링 특성을 수집할 수 있습니다. 그러면 초기 연결 중에 수집된 추가 특성에 따라 올바른 프로파일로 MAB 조회가 성공할 수 있습니다.

**참고:** 엔드포인트에 미치는 영향은 일반적으로 네트워크에 대한 첫 번째 연결로 제한됩니다. 엔드포인트가 완전히 프로파일링되면 ISE는 해당 ID 그룹 할당을 사용하여 네트워크에 대한 이후의 재연결 시점에 즉각적인 정책 일치를 수행할 수 있습니다.

또 다른 고려 사항으로는 초기에 포트에 적용되거나 중간 또는 최종 권한 부여 상태에 적용되는 전체 액세스 정책이 있습니다. 예를 들어 엔드포인트가 처음 네트워크에 연결되는 경우 포트 ACL(로임팩트 모드라고 가정) 또는 초기 VLAN에 따라 액세스가 부여될 수 있습니다. 엔드포인트를 알 수 없으며 MAB 조회가 실패하거나 해당 포스처 상태를 알 수 없는 경우에는 Central WebAuth 또는 Posture 상태로 진행할 수 있으며 포트 또는 VLAN 할당 시 새 ACL이 적용됩니다. 성공적인 웹 인증 또는 보안정책 교정에 따라 포트는 새 ACL 또는 VLAN으로 권한이 부여될 수 있습니다. 각 상태마다 서로 다른 레벨의 네트워크 액세스가 있습니다. 프로파일링에서 특정 데이터 수집이 사용되는 경우 해당 액세스가 허용되어야 합니다.

간단한 예는 DHCP입니다. DHCP가 허용되지 않으면 DHCP 프로브의 데이터를 활용하는 프로파일링이 사용되지 않을 수 있습니다. 네트워크 검사가 사용되지만 포트에서 NMAP 프로브에 의해 조사되는 포트에 대한 액세스를 차단할 경우, 다시 말하지만 프로파일링을 결정하는 데 해당 정보를 사용할 수 없습니다. 여기에는 엔드포인트에서 활성화되어 있는 SNMP 포트에 대한 액세스도 포함됩니다. 또한 엔드포인트 자체에서도 트래픽을 허용해야 합니다. 일반적인 예는 NMAP를 사용하여 OS 검사를 수행하는 것입니다. 개인 방화벽에서 엔드포인트 검사 시도를 차단하는 경우 프로브에서 결과가 생성되지 않습니다.

NetFlow 데이터를 수집하도록 네트워크와 통신할 수 있는 액세스 권한이 엔드포인트에 허용되어야 하므로 NetFlow 프로브를 사용하는 것은 특히 어려운 과제일 수 있습니다. 그러므로 엔드포인트에 대한 완전한 네트워크 액세스를 고려하지 않고 정책에서 데이터의 초기 수집을 허용해야 합니다. 한 가지 가능한 솔루션은 VLAN A의 엔드포인트를 프로파일링하는 것입니다. 이 경우 보안 리소스에 대한 액세스를 금지하되 지정된 포트에 대한 일반적인 액세스는 차단하지 않습니다. 일치하는 트래픽에 따라 프로파일링된 경우 엔드포인트는 VLAN B에 대해 다시 권한이 부여될 수 있으며 보안 리소스에 대한 권한 있는 액세스가 허용됩니다.

또 다른 옵션은 초기에 트래픽을 허용하되 비정상적 트래픽이 탐지되면 포트 권한 부여를 변경하는 보다 구체적인 프로파일을 일치시키는 것입니다. 예를 들어 프로세스 제어 엔드포인트가 예기치 않은 포트에서 통신하는 경우 엔드포인트를 격리 ID 그룹 및 정책에 할당하도록 예외 작업을 적용할 수 있습니다. 다시 말하지만, ISE 프로파일링은 안티 스푸핑 솔루션 역할을 하도록 설계되지 않았지만 비정상적인 트래픽 또는 기타 프로파일링 특성을 기반으로 정책을 적용하는 데 사용할 수 있습니다. 중요한 디바이스가 포함된 환경에서 그러한 디바이스는 종종 잠기거나 알려진 엔드포인트 목록으로 액세스가 제한됩니다. 이 경우 특정 프로파일링 정책과 일치하는 모든 엔드포인트에서 이러한 디바이스 유형과 일치하는 특성을 표시하도록 프로파일링 값을 파악할 수 있습니다.

예외 작업은 정적 정책 할당을 수행해야 하는 경우 사용할 수 있는 도구가 될 수 있습니다. 그러나 엔드포인트가 프로파일에 정적으로 할당된 경우에는 관리자만이 해당 할당을 변경할 수 있다는 점에 유의하십시오.

## 프로브 선택 모범 사례

구축마다 각기 다른 프로브를 사용할 수 있습니다. 이 섹션에서는 각 프로브에 따라 사용 가능한 정보를 중점적으로 다루고 구축 유형에 따른 프로브 선택 과정을 안내합니다.

### 프로브 특성

네트워크에서 사용할 프로브를 결정할 때는 각 프로브에서 수집하는 특성을 이해하는 것이 도움이 됩니다. 표 8에는 다양한 프로브, 수집되는 키 특성 및 해당하는 활용 사례가 요약되어 있습니다.

표 6 프로브 및 키 특성

프로브	키 프로파일링 특성	일반적인 엔드포인트 프로파일링 활용 사례
RADIUS	<ul style="list-style-type: none"> <li>• MAC 주소(OUI)</li> <li>• IP 주소</li> </ul>	MAC 주소→OUI = 디바이스 공급업체 표시. 공급업체가 특정 디바이스만 제조한 경우 일부 엔드포인트는 이 특성만 사용하여 프로파일링될 수 있습니다. 예: 서드파티 IP 전화기, 모바일 디바이스, 게임 콘솔, MAC-IP 바인딩 및 프로브 지원
Device Sensor를 사용하는 RADIUS	<ul style="list-style-type: none"> <li>• CDP/LLDP</li> <li>• DHCP</li> </ul>	CDP/LLDP 정보에 대해서는 SNMP 프로브 참고 DHCP 정보에 대해서는 DHCP 프로브 참고
SNMP	<ul style="list-style-type: none"> <li>• MAC 주소/OUI</li> <li>• CDP/LLDP</li> <li>• ARP 표</li> </ul>	CDP/LLDP를 사용하는 공급업체에 유용합니다. 예: Cisco IP Phone, 카메라, 액세스 포인트, 어플라이언스  DHCP(DHCP 프로브 정보 참고)  MAC 주소(RADIUS 프로브 참고)  디바이스 ARP 표를 폴링하면 ISE MAC-IP 바인딩을 채울 수 있습니다.
DHCP	<ul style="list-style-type: none"> <li>• DHCP</li> </ul>	하드웨어 및 소프트웨어에 대한 고유한 공급업체 ID. OS 탐지를 위한 DHCP 지문. 일반 이름 패턴의 호스트 이름/FQDN은 OS 또는 디바이스 유형을 나타낼 수 있습니다. 또한 다른 프로브를 지원할 수 있는 MAC-IP 바인딩을 제공합니다.
NMAP	<ul style="list-style-type: none"> <li>• 운영 체제</li> <li>• 공통 포트</li> <li>• 엔드포인트 SNMP 데이터</li> </ul>	네트워크/클라이언트 FW에 의해 차단되지 않는 운영 체제 탐지 IF 검사.  네트워크 프린터와 같은 SNMP 에이전트를 실행하는 엔드포인트 분류를 제공합니다.  공통 UDP/TCP 포트에서 수신하는 엔드포인트를 탐지하는 데 적합합니다.
DNS	<ul style="list-style-type: none"> <li>• FQDN</li> </ul>	일반 명명 규칙이 호스트 이름/DNS에 사용되는지 여부에 따라 값이 달라집니다.
HTTP	<ul style="list-style-type: none"> <li>• User-Agent</li> </ul>	운영 체제 탐지, Chrome과 같은 일부 브라우저는 실제 OS를 마스킹할 수 있습니다.
NetFlow	<ul style="list-style-type: none"> <li>• 프로토콜</li> <li>• 소스/대상 IP</li> <li>• 소스/대상/포트</li> </ul>	고유한 트래픽 패턴을 가진 미션별 엔드포인트를 탐지하거나 범용 하드웨어/소프트웨어 용도로 적합합니다.  특정 엔드포인트에 대한 비정상적인 트래픽을 탐지할 수 있습니다.

표 9에서는 프로브에 따른 세부적인 키 특성 목록을 제공합니다. 프로브에 따라 다른 특성도 사용할 수 있지만, 다음 목록에는 일반적인 구축에 가장 보편적인 특성 또는 유용한 특성이 나타나 있습니다.

표 7 프로브 및 프로파일링 특성 세부사항

프로브	키 프로파일링 특성
RADIUS	<ul style="list-style-type: none"> <li>• <b>Calling-Station-ID(OUI)</b></li> <li>• <b>Framed-IP-Address</b></li> </ul>
Device Sensor를 사용하는 RADIUS	<ul style="list-style-type: none"> <li>• <b>cdpCachePlatform</b></li> <li>• <b>cdpCacheAddress</b></li> <li>• <b>cdpCacheCapabilities</b></li> <li>• <b>lldpSystemDescription</b></li> <li>• <b>lldpSystemName</b></li> <li>• <b>dhcp-requested-address</b></li> <li>• <b>dhcp-class-identifier</b></li> <li>• <b>dhcp-client-identifier</b></li> <li>• <b>dhcp-parameter-request-list</b></li> <li>• <b>host-name</b></li> <li>• <b>domain-name</b></li> <li>• <b>client-fqdn</b></li> </ul>
SNMP 쿼리	<ul style="list-style-type: none"> <li>• <b>MACAddress(OUI)</b></li> <li>• <b>MAC-IP(ARP)</b></li> <li>• <b>cdpCachePlatform</b></li> <li>• <b>cdpCacheAddress</b></li> <li>• <b>cdpCacheCapabilities</b></li> <li>• <b>lldpSystemDescription</b></li> <li>• <b>lldpSystemName</b></li> </ul>
DHCP	<ul style="list-style-type: none"> <li>• <b>dhcp-requested-address</b></li> <li>• <b>dhcp-class-identifier</b></li> <li>• <b>dhcp-client-identifier</b></li> <li>• <b>dhcp-parameter-request-list</b></li> <li>• <b>host-name</b></li> <li>• <b>domain-name</b></li> <li>• <b>client-fqdn</b></li> </ul>

NMAP	<ul style="list-style-type: none"> <li>• <b>operating-system</b></li> <li>• <b>tcp-x</b></li> <li>• <b>udp-x</b></li> <li>• <b>SNMP 특성</b></li> </ul>
DNS	<ul style="list-style-type: none"> <li>• <b>FQDN</b></li> </ul>
HTTP	<ul style="list-style-type: none"> <li>• <b>User-Agent</b></li> </ul>
NetFlow	<ul style="list-style-type: none"> <li>• <b>IPV4_DST_ADDR</b></li> <li>• <b>IPV4_SRC_ADDR</b></li> <li>• <b>PROTOCOL</b></li> <li>• <b>L4_SRC_PORT</b></li> <li>• <b>L4_DEST_PORT</b></li> <li>• <b>MIN_TTL</b></li> <li>• <b>MAX_TTL</b></li> </ul>
기타	<ul style="list-style-type: none"> <li>• <b>PortalUser</b></li> <li>• <b>EndPointSource</b></li> <li>• <b>DeviceRegistrationStatus</b></li> </ul>

### 프로브 선택을 위한 비공식 가이드

특정 활용 사례에 선택할 프로브를 고려할 때 다음 질문을 처리하는 일반화된 메트릭을 바탕으로 각 프로브를 평가하면 도움이 될 수 있습니다.

구축하기 가장 수월하거나 가장 까다로운 프로브는 무엇입니까?

트래픽 오버헤드, ISE 서버 로드 또는 추가 지원 구성 요소 측면에서 네트워크에 미치는 영향이 가장 크거나 작은 프로브는 무엇입니까?

엔드포인트를 프로파일링할 수 있는 기능에 이 프로브가 부가할 수 있는 일반적인 가치는 무엇입니까?

표 10에는 다양한 활용 사례에서 프로브를 선택하는 데 도움이 되는 메트릭 및 등급 중 표 11, 12 및 13에 사용된 메트릭 및 등급에 대한 범례가 나와 있습니다.

표 8 프로브 등급 범례

메트릭		평가		
이름	설명	1	2	3
DDI	구축 난이도 지수	쉬움	중간	어려움
NII	네트워크 영향 지수	낮은 영향	보통 영향	높은 영향
PVI	프로브 값 지수	높은 값	중간 값	낮은 값



### 검색 단계 - 프로브 모범 사례

표 11에서는 ISE 구축 검색 단계 중에 프로브를 선택하는 데 권장되는 모범 사례 및 지침을 제공합니다. RADIUS 포트 인증 및 권한 부여를 위한 네트워크 액세스 디바이스가 아직 구성되어 있지 않은 것으로 가정합니다. 그러므로 RADIUS 프로브와 같은 주요 프로브는 네트워크 인증과 관련된 데이터를 수집할 수 없습니다.

이러한 권장 사항은 ISE 프로파일링 서비스와의 통합이 필요한 Cisco NAC Appliance 설치와 같이 RADIUS 인증이 사용되지 않는 다른 구축에도 적용됩니다.

표 9: 프로브 선택 - 검색 단계

프로브(방법)	EDI	NII	PVI	키 프로파일링 특성	참고
RADIUS	-	-	-	<ul style="list-style-type: none"> <li>해당 없음</li> </ul>	ISE가 인증 제어 영역에 없으므로 해당되지 않습니다.
Device Sensor를 사용하는 RADIUS	2	1	1	<ul style="list-style-type: none"> <li>CDP/LLDP</li> <li>DHCP</li> </ul>	네트워크에서 Device Sensor를 지원하는 경우 인증 제어 영역에 상관없이 RADIUS 계정 관리를 사용할 수 있습니다.
SNMPTrap	1	1	1	<ul style="list-style-type: none"> <li>LinkUp/Down 트랩</li> <li>MAC Notify 트랩</li> <li>Informs</li> </ul>	엔드포인트 연결 검색/SNMPQuery 프로브 트리거
SNMPQuery	1	2	1	<ul style="list-style-type: none"> <li>MAC 주소(OUI)</li> <li>CDP/LLDP</li> <li>ARP 표</li> </ul>	디바이스 ARP 표를 폴링하면 ISE MA-IP 바인딩을 채울 수 있습니다. 재인증 또는 중간 업데이트로 인한 과도한 RADIUS 계정 관리 업데이트에 의해 트리거되는 높은 SNMP 쿼리 트래픽에 유의하십시오.
DHCP(Helper)	2	1	1	<ul style="list-style-type: none"> <li>DHCP</li> </ul>	MAC-IP 바인딩을 제공합니다. 네트워크에 미치는 영향은 일반적으로 작지만 낮은 DHCP 리스 타이머에 유의하십시오.
DHCP SPAN	2	3	1	<ul style="list-style-type: none"> <li>DHCP</li> </ul>	MAC-IP 바인딩을 제공합니다.
NMAP	1	2	2	<ul style="list-style-type: none"> <li>운영 체제</li> <li>공통 포트</li> <li>엔드포인트 SNMP 데이터</li> </ul>	SNMP 데이터는 UDP/161이 열려 있고 public 문자열이 있다고 가정합니다. NMAP의 상대 값은 고객 네트워크와 함께 유선 액세스 정책에서 OS 탐지가 중요한 요인인지 여부에 따라 달라집니다.

DNS	1	1	2	<ul style="list-style-type: none"> <li>• FQDN</li> </ul>	값은 일반 명명 규칙이 사용되는지 여부에 따라 달라집니다.
HTTP(Redirect)	-	-	-	<ul style="list-style-type: none"> <li>• 해당 없음</li> </ul>	ISE가 인증 제어 영역에 없으므로 해당되지 않습니다.
HTTP(SPAN)	2	3	2	<ul style="list-style-type: none"> <li>• User-Agent</li> </ul>	지능형 SPAN/TAP 솔루션 또는 VACL Capture를 사용하여 서버 또는 인터넷 에지와 같은 주요 HTTP 검사점의 SPAN을 고려해 보십시오.
NetFlow	3	3	2	<ul style="list-style-type: none"> <li>• 프로토콜</li> <li>• 소스/대상 IP</li> <li>• 소스/대상 포트</li> </ul>	일반적인 프로파일링이 아닌 특정 활용 사례에서만 권장됩니다.

유선 네트워크 - 프로브 모범 사례

표 12에서는 유선 네트워크에 구축된 프로브에 대해 권장되는 모범 사례 및 지침을 제공합니다.

표 10 프로브 선택 - 유선 네트워크

프로브(방법)	EDI	NII	PVI	키 프로파일링 특성	참고
RADIUS	1	1	1	<ul style="list-style-type: none"> <li>• MAC 주소(OUI)</li> <li>• IP 주소</li> <li>• User-Name, 기타</li> </ul>	디바이스 탐지 및 다른 프로브 활성화를 위한 기본 프로브.
Device Sensor를 사용하는 RADIUS	2	1	1	<ul style="list-style-type: none"> <li>• CDP/LLDP</li> <li>• DHCP</li> </ul>	Device Sensor가 지원되는 3000 또는 4000 Series 액세스 스위치를 실행하고 있는 경우 이는 선택된 특성을 수집하기 위한 이상적이고 최적화된 방법입니다.
SNMPTrap	1	1	3	<ul style="list-style-type: none"> <li>• LinkUp/Down 트랩</li> <li>• MAC Notify 트랩</li> <li>• Informs</li> </ul>	엔드포인트 연결 검색/SNMP 프로브 트리거
SNMPQuery	1	2	1	<ul style="list-style-type: none"> <li>• MAC 주소(OUI)</li> <li>• CDP/LLDP</li> <li>• ARP 표</li> </ul>	디바이스 ARP 표를 폴링하면 ISE MAC- IP 바인딩을 채울 수 있습니다. 재인증 또는 중간 업데이트로 인한 과도한 RADIUS 계정 관리 업데이트에 의해 트리거되는 높은 SNMP 쿼리 트래픽에 유의하십시오.
DHCP(Helper)	2	1	1	<ul style="list-style-type: none"> <li>• DHCP 특성</li> </ul>	MAC-IP 바인딩을 제공합니다. 낮은 DHCP 리스 타이머에 유의하십시오.
DHCP SPAN	2	3	1	<ul style="list-style-type: none"> <li>• DHCP 특성</li> </ul>	MAC-IP 바인딩을 제공합니다.
NMAP	1	2	2	<ul style="list-style-type: none"> <li>• 운영 체제</li> <li>• 공통 포트</li> <li>• 엔드포인트 SNMP 데이터</li> </ul>	SNMP 데이터는 UDP/161이 열려 있고 public 문자열이 있다고 가정합니다.
DNS	1	1	2	<ul style="list-style-type: none"> <li>• FQDN</li> </ul>	일반 명명 규칙이 사용되는지 여부에 따라 값이 달라집니다.
HTTP(Redirect)	2	1	2	<ul style="list-style-type: none"> <li>• 사용자 에이전트</li> </ul>	유선 액세스에 대한 OS의 상대적 중요도에 따라 값이 달라집니다.

HTTP(SPAN)	2	3	2	<ul style="list-style-type: none"> <li>• 사용자 에이전트</li> </ul>	인터넷 에지와 같은 주요 HTTP 검사점의 SPAN을 고려해 보십시오. 가능한 경우 스마트 SPAN 솔루션 및 VACL Capture를 사용합니다.
NetFlow	3	3	2	<ul style="list-style-type: none"> <li>• 프로토콜</li> <li>• 소스/대상 IP</li> <li>• 소스/대상 포트</li> </ul>	일반적인 프로파일링이 아닌 특정 활용 사례에서만 권장됩니다.

무선 네트워크 - 프로브 모범 사례

표 13에서는 무선 네트워크에 구축된 프로브에 대해 권장되는 모범 사례 및 지침을 제공합니다.

표 11 프로브 선택 - 무선 네트워크

프로브(방법)	EDI	NII	PVI	키 프로파일링 특성	참고
RADIUS	1	1	1	<ul style="list-style-type: none"> <li>• MAC 주소(OUI)</li> <li>• IP 주소</li> <li>• User-Name, 기타</li> </ul>	디바이스 탐지 및 다른 프로브 활성화를 위한 기본 프로브
Device Sensor를 사용하는 RADIUS	2	1	1	<ul style="list-style-type: none"> <li>• CDP/LLDP</li> <li>• DHCP</li> </ul>	Device Sensor가 지원되는 3000 또는 4000 Series 액세스 스위치를 실행하고 있는 경우 이는 선택된 특성을 수집하기 위한 이상적이고 최적화된 방법입니다.
SNMPTrap	1	1	3	<ul style="list-style-type: none"> <li>• LinkUp/Down 트랩</li> <li>• MAC Notify 트랩</li> <li>• Informs</li> </ul>	엔드포인트 연결 검색/SNMPQuery 프로브 트리거
SNMPQuery	1	2	1	<ul style="list-style-type: none"> <li>• MAC 주소(OUI)</li> <li>• CDP/LLDP</li> <li>• ARP 표</li> </ul>	디바이스 ARP 표를 폴링하면 ISE MAC-IP 바인딩을 채울 수 있습니다. 재인증 또는 중간 업데이트로 인한 과도한 RADIUS 계정 관리 업데이트에 의해 트리거되는 높은 SNMP 쿼리 트래픽에 유의하십시오.
DHCP(helper)	2	1	1	<ul style="list-style-type: none"> <li>• DHCP</li> </ul>	MAC-IP 바인딩을 제공합니다. 낮은 DHCP 리스 타이머에 유의하십시오.
DHCP SPAN	2	3	1	<ul style="list-style-type: none"> <li>• DHCP</li> </ul>	MAC-IP 바인딩을 제공합니다.
NMAP	1	2	2	<ul style="list-style-type: none"> <li>• 운영 체제</li> <li>• 공통 포트</li> <li>• 엔드포인트 SNMP 데이터</li> </ul>	SNMP 데이터는 UDP/161이 열려 있고 public 문자열이 있다고 가정합니다.
DNS	1	1	2	<ul style="list-style-type: none"> <li>• FQDN</li> </ul>	일반 명명 규칙이 사용되는지 여부에 따라 값이 달라집니다.
HTTP(Redirect)	2	1	2	<ul style="list-style-type: none"> <li>• 사용자 에이전트</li> </ul>	유선 액세스에 대한 OS의 상대적 중요도에 따라 값이 달라집니다.

HTTP(SPAN)	2	3	2	<ul style="list-style-type: none"> <li>• 사용자 에이전트</li> </ul>	<p>인터넷 에지와 같은 주요 HTTP 검사점의 SPAN을 고려해 보십시오. 가능하면 스마트 SPAN 솔루션 및 VACL Capture를 사용합니다.</p>
NetFlow	3	3	2	<ul style="list-style-type: none"> <li>• 프로토콜</li> <li>• 소스/대상 IP</li> <li>• 소스/대상 포트</li> </ul>	<p>일반적인 프로파일링이 아닌 특정 활용 사례에서만 권장됩니다.</p>

## 프로파일링 계획

디바이스 유형에 따른 가시성 또는 네트워크 액세스를 위해 디바이스 분류를 필요로 하는 다양한 유형의 엔드포인트를 검토하고 필요한 데이터를 수집하기 위한 최상의 프로브에 대해 합의한 이후의 다음 단계는 프로파일링 계획을 문서화하는 것입니다. 최소한, 이 계획에는 프로파일링해야 할 모든 디바이스와 네트워크 액세스 권한을 부여하기 위해 프로파일링 데이터를 사용할 방법이 포함되어야 합니다. 계획에는 각 엔드포인트를 분류하는 데 필요한 고유한 특성 목록, 그러한 특성을 캡처하는 데 사용되는 프로브 또는 방법, 그리고 수집 방법에 대한 세부정보도 포함되어야 합니다. 예를 들어 HTTP를 캡처하는 데 URL 리디렉션 또는 SPAN 중 어떤 것을 사용할지, 데이터를 어디에 캡처할지, 어떤 PSN으로 데이터를 수신할지 등의 정보를 포함해야 합니다. 계획에 대한 또 다른 중요한 측면에는 확장성 및 이중화 구축 방식이 있습니다.

**참고:** 로드 밸런싱을 비롯한 프로파일링 고가용성 및 확장성은 이 문서의 범위를 벗어납니다.

표 14에서는 한 샘플 회사의 기본 프로파일링 계획을 보여줍니다.

표 12 샘플 프로파일링 계획

디바이스 프로파일	인증 정책 규칙에서 사용되는 위치	고유한 특성	사용되는 프로브	수집 방법
Cisco IP Phone	Cisco-IP-Phones(MAB)	OUI	RADIUS	RADIUS 인증
		CDP	SNMP 쿼리	RADIUS 시작에 의해 트리거됨
IP 카메라	Cisco-IP-Cameras(MAB)	OUI	RADIUS	RADIUS 인증
		CDP	SNMP 쿼리	RADIUS 시작에 의해 트리거됨
프린터	프린터(MAB)	OUI	RADIUS	RADIUS 인증
		DHCP 클래스 식별자	DHCP	로컬 레이어 3 스위치 SVI의 IP Helper
PoS(Point of Sale) 스테이션 (고정 IP)	POS(MAB)	MAC 주소	RADIUS(MAC 주소 검색)	RADIUS 인증
		MAC-IP 매핑을 위한 ARP 캐시	SNMP 쿼리	RADIUS 시작에 의해 트리거됨
		DNS 이름	DNS	IP 검색에 의해 트리거됨

Apple iDevice	Employee_Personal (802.1X/CWA)	OUI	RADIUS	RADIUS 인증
		브라우저 사용자 에이전트	HTTP	중앙 정책 서비스 노드 클러스터로 권한 부여 정책 포스처 리디렉션
		DHCP 클래스 식별자 및 MAC-IP 매핑	DHCP	로컬 레이어 3 스위치 SVI의 IP Helper
디바이스 X	Critical_Device_X (MAB)	MAC 주소	RADIUS(MAC 주소 검색)	RADIUS 인증
		MAC-IP 매핑을 위해 요청된 IP 주소	DHCP	로컬 정책 서비스 노드에 대한 DHCP 서버 포트의 RSPAN
		MAC-IP 매핑을 위한 ARP 캐시 확보(선택 사항)	SNMP 쿼리	RADIUS 계정 관리 시작에 의해 트리거됨
		대상 포트/IP에 대한 트래픽	NetFlow	Distribution 6500 스위치에서 중앙 정책 서비스 노드로 NetFlow 내보내기

**프로파일링 모범 사례 및 권장 사항 요약**

다음은 ISE 프로파일링에 대한 모범 사례 및 권장 사항을 요약한 것입니다.

데이터 수집을 최적화할 수 있는 경우 Device Sensor를 사용합니다.

- 가능하면, 지정된 엔드포인트에 대한 프로파일 데이터를 동일한 정책 서비스 노드로 전송해야 합니다. 그렇지 않으면, 엔드포인트 데이터가 과도하게 업데이트되고 여러 PSN의 경합이 발생할 수 있습니다.
- 대부분의 경우 ISE는 이런 상황을 자동으로 처리합니다.
- RADIUS 계정 관리 시작 또는 SNMP 트랩 패킷을 수신하는 동일한 PSN에 의해 SNMP 쿼리가 실행됩니다.
- URL 리디렉션으로 발생하는 HTTP 트래픽은 RADIUS 세션을 처리하는 PSN으로 전송됩니다.
- DHCP Helper는 여러 PSN으로 보내질 수 있으므로 특정 액세스 디바이스를 위해 RADIUS용으로 구성된 동일 PSN으로 보내는 것이 좋습니다.
- DNS 쿼리는 IP 주소를 학습하는 동일 PSN을 통해 전송됩니다. 이 PSN은 일반적으로 RADIUS 세션을 처리하고, RADIUS 계정 관리의 Framed-IP-Address, DHCP의 dhcp-requested-address 또는 cdpCacheAddress의 트리거된 SNMP 쿼리 중 하나에서 IP 주소를 수신하는 PSN입니다.
- 트리거된 NMAP 검사는 프로파일링 데이터를 수신하여 정책 규칙을 일치하게 하는 동일 PSN을 통해 제공됩니다. 예를 들어 NMAP 작업이 OUI 일치에 따라 프로파일 규칙 조건에 할당된 경우 RADIUS, DHCP 또는 다른 프로브를 통해 엔드포인트 MAC 주소를 수신하는 첫 번째 PSN은 NMAP 검사를 제공하는 PSN이 됩니다.



- 한편 DHCP, SPAN, HTTP SPAN 또는 NetFlow 프로브를 사용하는 경우와 같이 트래픽은 분산형 구축 환경에서 동일 PSN에 도달하지 못할 수도 있습니다.

HTTP 프로브:

- SPAN 대신 URL 리디렉션을 사용하여 수집을 중앙 집중화하고 SPAN/RSPAN과 관련된 트래픽 부하를 줄이십시오.
- 일반적으로 HTTP SPAN(사용하는 경우)을 사용하여 데이터를 수집하지 않도록 하십시오. 사용하는 경우,
- 인터넷 에지 또는 무선 컨트롤러 연결과 같은 주요 트래픽 검사점을 찾습니다.
- 지능형 SPAN/TAP 옵션 또는 VACL Capture를 사용하여 IS로 전송되는 데이터의 양을 제한합니다.
- 지능형 Network TAP 인프라 없이는 SPAN에 대한 고가용성을 제공하기 어려울 수 있습니다.

DHCP 프로브:

- 가능한 경우 DHCP 릴레이(IP Helper)를 사용하십시오.
- 일반적으로 DHCP SPAN을 사용하여 데이터를 수집하지 않도록 하십시오. 사용하는 경우, 프로브가 중앙 DHCP 서버로 향하는 트래픽을 캡처하도록 하십시오.
- DHCP에 서비스를 제공하는 레이어 3 디바이스가 동일한 네트워크에 대해 DHCP를 릴레이하지 않도록 하십시오.
- 지능형 Network TAP 인프라 없이는 SPAN에 대한 고가용성을 제공하기 어려울 수 있습니다.
- SNMP 프로브:
- 과도한 재인증(낮은 세션/재인증 타이머) 또는 빈번한 중간 계정 관리 업데이트에 의해 트리거된 RADIUS 계정 관리 업데이트로 인해 발생하는 높은 SNMP 쿼리 트래픽에 유의하십시오.
- 폴링된 쿼리의 경우 폴링 간격을 너무 낮게 설정하지 않도록 주의하십시오. ISE 네트워크 디바이스 컨피그레이션에서 폴링을 위해 최적화된 PSN을 설정해야 합니다.
- SNMP 트랩은 RADIUS 기반 인증 및 권한 부여를 사용하는 네트워크가 아닌 NAC Appliance와의 통합과 같은 비 RADIUS 구축에 유용합니다.
- NetFlow: 특정 활용 사례에만 사용하십시오. NetFlow는 네트워크 디바이스 및 PSN에 높은 로드를 초래할 수 있습니다.

## 부록 A: 참조

---

### Cisco TrustSec System:

<http://www.cisco.com/go/trustsec>

[http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing\\_DesignZone\\_TrustSec.html](http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html)

### 디바이스 컨피그레이션 가이드:

Cisco Identity Services Engine 사용 가이드:

[http://www.cisco.com/en/US/products/ps11640/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html)

Cisco IOS Software, Cisco IOS XE Software, Cisco NX-OS Software 릴리스에 대한 자세한 내용은 다음 URL을 참고하십시오.

Cisco Catalyst 2900 Series 스위치:

[http://www.cisco.com/en/US/products/ps6406/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html)

Cisco Catalyst 3000 Series 스위치:

[http://www.cisco.com/en/US/products/ps7077/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html)

Cisco Catalyst 3000-X Series 스위치:

[http://www.cisco.com/en/US/products/ps10745/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html)

Cisco Catalyst 4500 Series 스위치:

[http://www.cisco.com/en/US/products/hw/switches/ps4324/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html)

Cisco Catalyst 6500 Series 스위치:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)

Cisco ASR 1000 Series 라우터:

[http://www.cisco.com/en/US/products/ps9343/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html)

Cisco Wireless LAN Controller:

[http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc\\_cg70MR1.html](http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html)