

ISE 3.3의 엔드포인트 분류를 위한 Wifi 분석 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[WLC의 구성](#)

[1단계. 전역적으로 장치 분류 기능 활성화](#)

[2단계. TLV 캐싱 및 RADIUS 프로파일링 활성화](#)

[ISE의 컨피그레이션](#)

[1단계. 구축의 PSN에서 프로파일링 서비스 활성화](#)

[2단계. ISE PSN에서 RADIUS 프로파일링 프로브 활성화](#)

[3단계. CoA 유형 및 엔드포인트 특성 필터 설정](#)

[4단계. Wifi 분석 데이터 특성을 사용하여 권한 부여 정책 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[1단계. 계정 관리 패키지가 ISE에 도달함](#)

[2단계. ISE는 엔드포인트 특성을 사용하여 어카운팅 패키지를 구문 분석합니다](#)

[3단계. 엔드포인트 특성이 업데이트되고 엔드포인트가 분류됨](#)

[4단계. CoA 및 재인증](#)

[관련 정보](#)

소개

이 문서에서는 WiFi Analytics for Endpoint Classification의 작동 방식을 설명합니다. 또한 구성, 확인 및 문제 해결 방법에 대해서도 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 9800 WLC(Wireless LAN Controller) 컨피그레이션
- ISE(Identity Services Engine) 컨피그레이션
- RADIUS 인증. AAA(Authorization and Accounting) 패키지 흐름 및 용어

이 문서에서는 ISE를 RADIUS 서버로 사용하는 작동하는 WLAN 인증 클라이언트가 이미 있다고 가정합니다.

이 기능이 작동하려면 최소한 다음 항목이 있어야 합니다.

- 9800 WLC Cisco IOS® XE Dublin 17.10.1
- Services Engine v3.3을 식별합니다.
- 802.11ac Wave2 또는 802.11ax(Wi-Fi 6/6E) 액세스 포인트

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800 WLC Cisco IOSXE v17.12.x
- ISE(Identity Services Engine) v3.3
- Android 13 장치

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

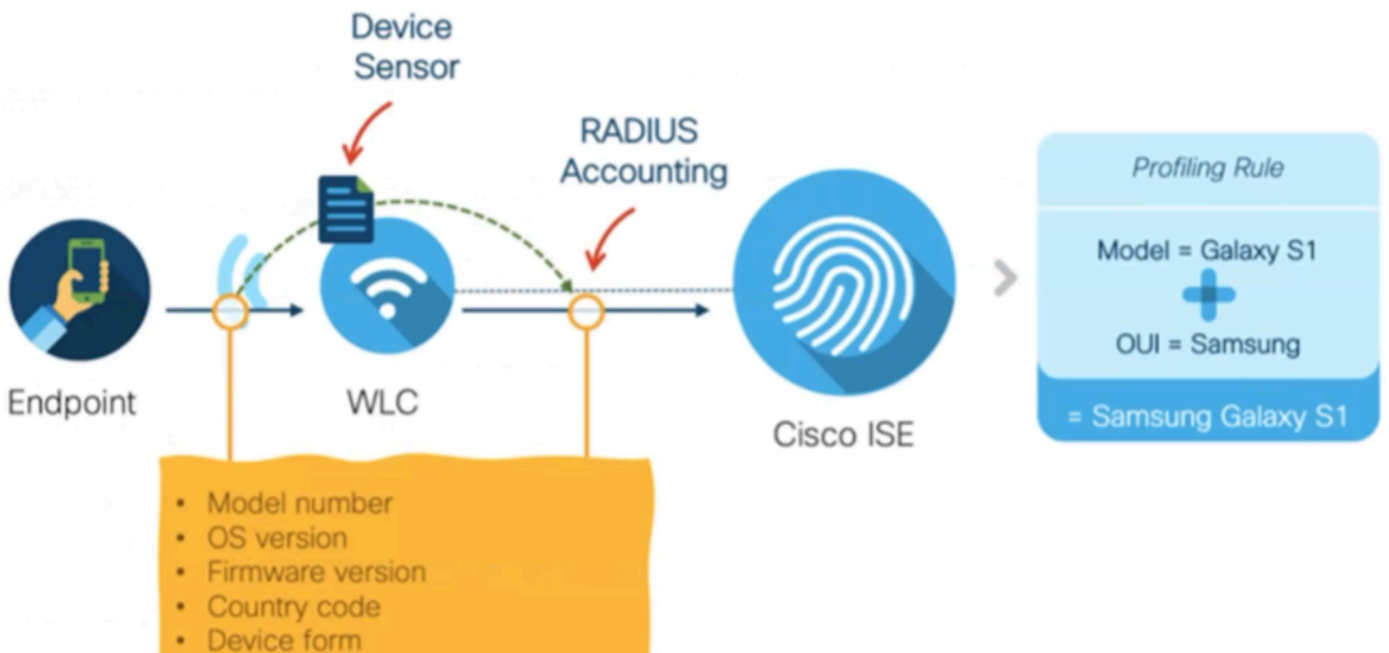
배경 정보

Cisco 9800 WLC는 WiFi Device Analytics를 통해 이 디바이스에 연결된 엔드포인트 집합에서 모델 번호 및 OS 버전 등의 특성을 학습하고 ISE와 공유할 수 있습니다. 그러면 ISE는 엔드포인트 분류(프로파일링이라고도 함)를 위해 이 정보를 사용할 수 있습니다.

현재 WiFi Analytics는 다음 벤더에서 지원됩니다.

- 애플
- 인텔
- 삼성

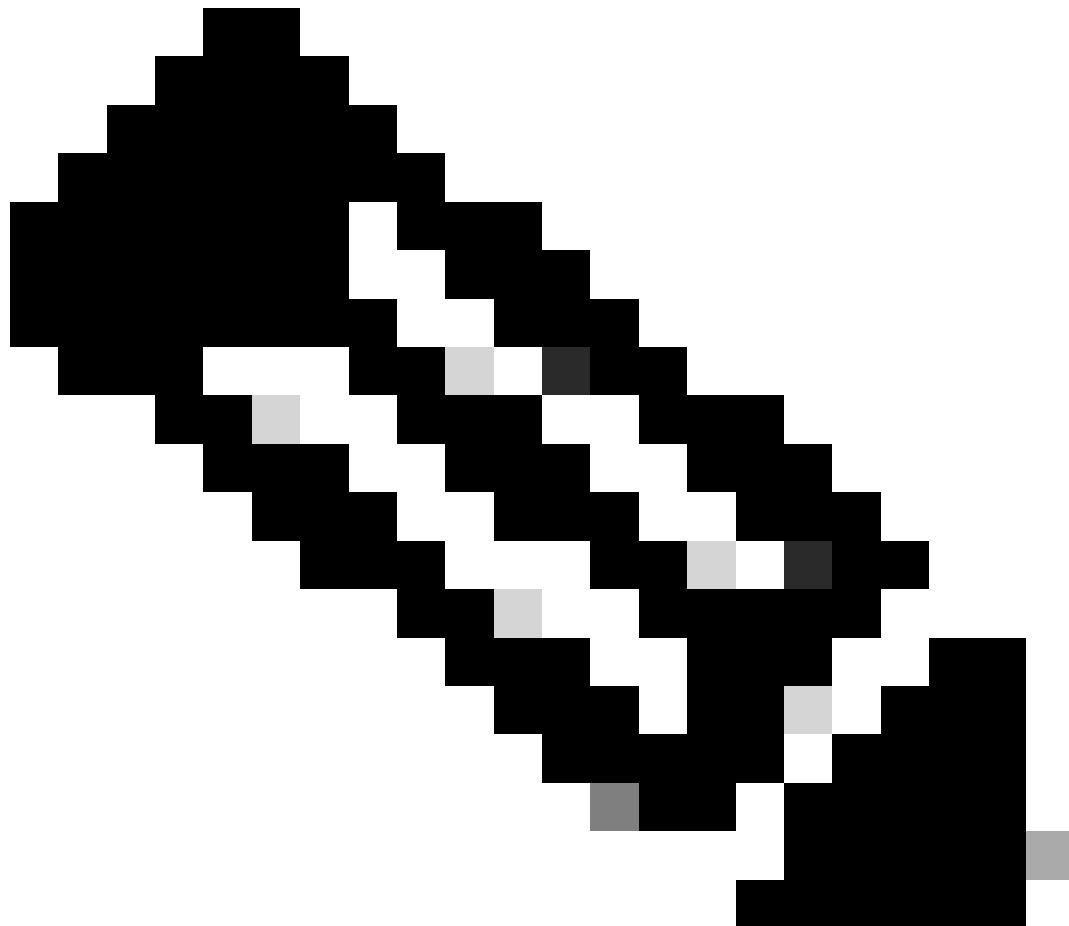
WLC는 RADIUS 계정 관리 패킷을 사용하여 ISE 서버와 특성 정보를 공유합니다.



RADIUS AAA 플로우의 RADIUS 계정 관리 패킷은 RADIUS 서버가 엔드포인트 인증 시도에 대한 응답으로 RADIUS 액세스 수락 패킷을 전송한 후에만 전송된다는 것을 기억해야 합니다. 즉, WLC는 RADIUS 서버(ISE)와 네트워크 액세스 디바이스(WLC) 간에 해당 엔드포인트에 대한 RADIUS 세션이 설정된 후에만 엔드포인트 특성 정보를 공유합니다.

이는 ISE에서 엔드포인트 분류 및 권한 부여에 사용할 수 있는 모든 특성입니다.

- DEVICE_INFO_FIRMWARE_VERSION
- 장치_정보_하드웨어_모델
- 장치_정보_제조업체_모델
- DEVICE_INFO_MODEL_NAME
- DEVICE_INFO_MODEL_NUM
- 장치_정보_OS_버전
- DEVICE_INFO_VENDOR_TYPE



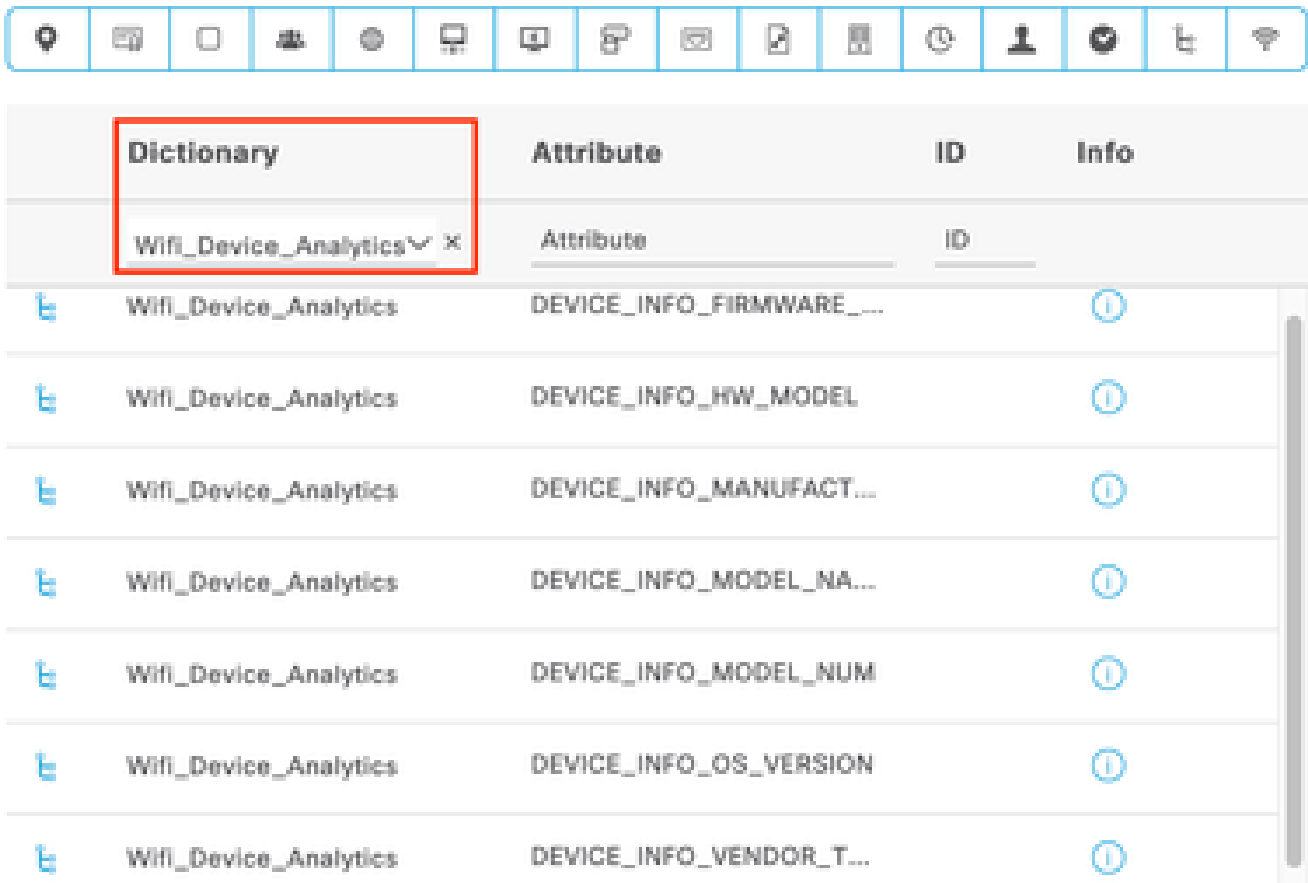
참고: WLC는 연결하는 엔드포인트 유형에 따라 더 많은 특성을 보낼 수 있지만 나열된 특

성만 ISE에서 권한 부여 정책을 생성하는 데 사용할 수 있습니다.

ISE는 어카운팅 패킷을 수신하면 그 내부에서 이 분석 데이터를 처리하고 사용하며, 이를 사용하여 엔드포인트 프로파일/ID 그룹을 재할당할 수 있습니다.

WiFi Endpoint Analytics 특성은 WiFi_Device_Analytics 사전 아래에 나열됩니다. 네트워크 관리자는 엔드포인트 권한 부여 정책 및 조건에 이러한 특성을 포함할 수 있습니다.

Select attribute for condition



Dictionary	Attribute	ID	Info
Wifi_Device_Analytics	Attribute	ID	
Wifi_Device_Analytics	DEVICE_INFO_FIRMWARE_...		ⓘ
Wifi_Device_Analytics	DEVICE_INFO_HW_MODEL		ⓘ
Wifi_Device_Analytics	DEVICE_INFO_MANUFACT...		ⓘ
Wifi_Device_Analytics	DEVICE_INFO_MODEL_NA...		ⓘ
Wifi_Device_Analytics	DEVICE_INFO_MODEL_NUM		ⓘ
Wifi_Device_Analytics	DEVICE_INFO_OS_VERSION		ⓘ
Wifi_Device_Analytics	DEVICE_INFO_VENDOR_T...		ⓘ

WiFi 장치 분석 사전

ISE가 엔드포인트에 대해 저장하는 현재 특성 값에 대한 변경 사항이 발생하면 ISE는 CoA(Change of Authorization)를 시작하며, 엔드포인트가 평가되어 업데이트된 특성을 확인할 수 있도록 합니다.

구성

WLC의 구성

1단계. 전역적으로 장치 분류 기능 활성화

Configuration(컨피그레이션) > Wireless(무선) > Wireless Global(무선 글로벌)로 이동하고 Device

Classification(디바이스 분류) 확인란을 선택합니다.

Configuration > Wireless > Wireless Global

Default Mobility Domain *	<input type="text" value="default"/>
RF Group Name*	<input type="text" value="default"/>
Maximum Login Sessions Per User*	<input type="text" value="0"/>
Management Via Wireless	<input type="checkbox"/>
Device Classification	<input checked="" type="checkbox"/>
AP LAG Mode	<input type="checkbox"/>
Dot15 Radio	<input type="checkbox"/>
Wireless Password Policy	<input type="text" value="None"/> ⓘ

디바이스 분류 컨피그레이션

2단계. TLV 캐싱 및 RADIUS 프로파일링 활성화

Configuration(컨피그레이션) > Tags and Profiles(태그 및 프로필) > Policy(정책)로 이동하고 RADIUS 클라이언트가 연결된 WLAN에서 사용하는 Policy Profile(정책 프로필)을 선택합니다.

Configuration > Tags & Profiles > Policy

Admin Status	Associated Policy Tags	Policy Profile Name	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ise-policy	
<input type="checkbox"/>	<input type="checkbox"/>	default-policy-profile	default policy profile

무선 정책 선택

Access Policies(액세스 정책)를 클릭하고 RADIUS Profiling(RADIUS 프로파일링), HTTP TLV

Caching(HTTP TLV 캐싱) 및 DHCP TLV Caching(DHCP TLV 캐싱) 옵션을 확인합니다. 이전 단계에서 수행한 작업으로 인해 이제 Global State of Device Classification(디바이스 분류의 전역 상태)이 Enabled(활성화됨) 상태로 표시됩니다.

Edit Policy Profile ✕

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL ⓘ

IPv6 ACL ⓘ

URL Filters ⓘ

Pre Auth ⓘ

Post Auth ⓘ

RADIUS 프로파일링 및 캐싱 컨피그레이션

WLC CLI에 로그인하고 dot11 TLV Accounting을 활성화합니다.

```
vimontes-wlc#configure terminal
vimontes-wlc(config)#wireless profile policy policy-profile-name
vimontes-wlc(config-wireless-policy)#dot11-tlv-accounting
```





참고: 이 명령을 사용하려면 먼저 무선 정책 프로필을 비활성화해야 합니다. 이 명령은 Cisco IOS XE Dublin 17.10.1 버전 이상에서만 사용할 수 있습니다.







ISE의 컨피그레이션


1단계. 구축의 PSN에서 프로파일링 서비스 활성화

Administration(관리) > **Deployment(구축)**로 이동하고 PSN의 이름을 클릭합니다.

Deployment Nodes

Selected 0 Total 1  

 Edit  Register  Syncup  Deregister  All 


<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ise1ab	Administration, Monitoring, Policy Service	STANDALONE	SESSION,PROFILER	


ISE PSN 노드 선택


아래로 스크롤하여 **Policy Service(정책 서비스)** 섹션으로 이동하고 **Enable Profiling Service(프로파일링 서비스 활성화) 확인란**을 선택합니다. **Save(저장)** 버튼을 클릭합니다.

Policy Service


Enable Session Services


Include Node in Node Group 


Enable Profiling Service 

Enable Threat Centric NAC Service 

> Enable SXP Service

Enable Device Admin Service 

Enable Passive Identity Service 

> pxGrid 

[Reset](#)

프로파일러 서비스 컨피그레이션

2단계. ISE PSN에서 RADIUS 프로파일링 프로브 활성화

페이지 상단으로 스크롤하여 Profiling Configuration(프로파일링 컨피그레이션) 탭을 클릭합니다. ISE에서 사용할 수 있는 모든 프로파일링 프로브가 표시됩니다. RADIUS 프로브를 **활성화**하고 **Save**를 클릭합니다.

Edit Node

General Settings

Profiling Configuration

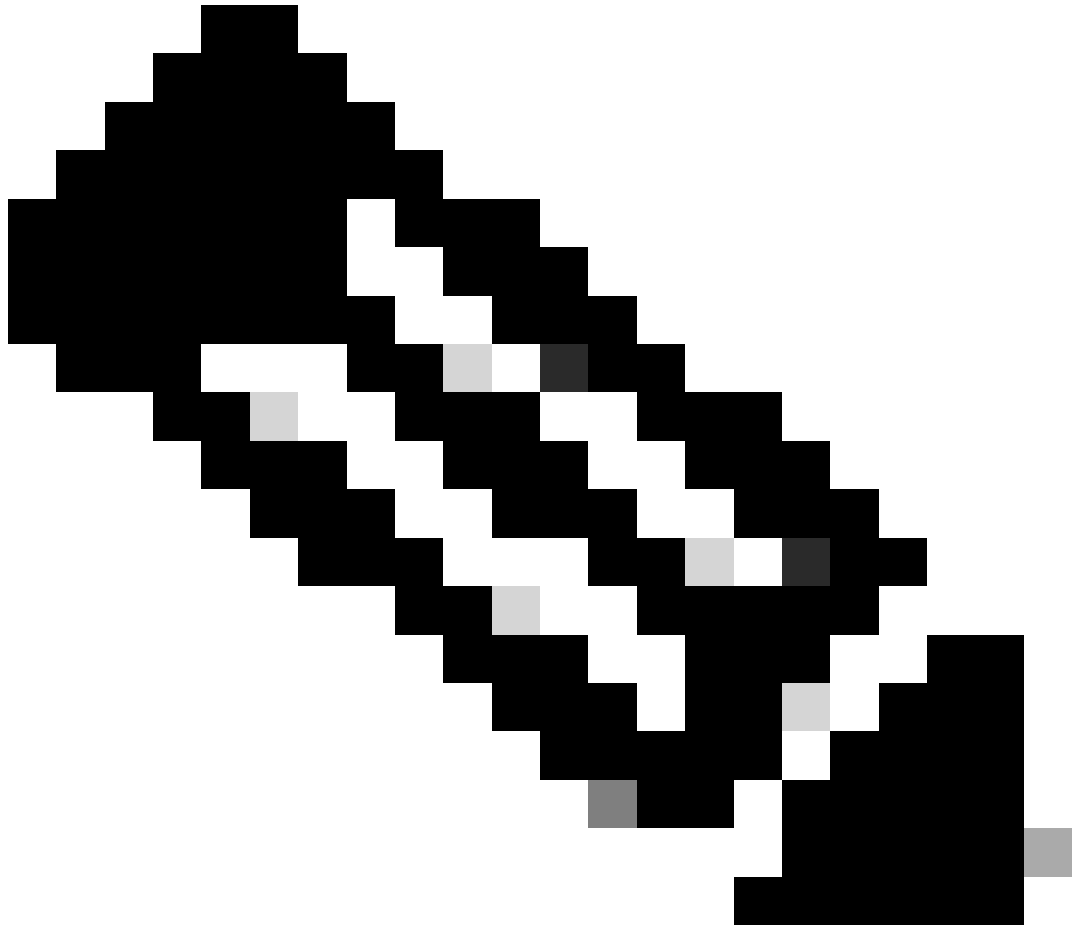
> NETFLOW

> DHCP

> DHCPSPAN

> HTTP

를 성공적으로 전송한 후 엔드포인트가 재인증됩니다. 이번에는 새 할당 된 엔드 포인트 프로필을 관찰 할 수 있으며 다른 인증 결과가 할당 되었음을 확인 합니다.



참고: CoA 패킷에는 항상 빈 ID 필드가 있지만 엔드포인트 ID는 첫 번째 인증 패킷과 동일합니다.

Change of Authorization 레코드의 **Details** 열에 있는 아이콘을 클릭합니다.

Sep 27, 2023 06:19:24.36...



0A:5A:F0:B3:B5:9C

CoA 패킷 세부 정보에 액세스

CoA 세부 정보가 새 브라우저 탭에 표시됩니다. 아래로 스크롤하여 **Other Attributes** 섹션으로 이동합니다.

CoA 소스 구성 요소는 프로 파 일러로 표시 됩니다. CoA Reason은 권한 부여 정책에서 사용 되는 엔드 포인트 ID 그룹/정책/논리 적 인 프로필에 변경 으로 표시 됩니다.

Other Attributes

ConfigVersionId	1493
Event-Timestamp	1695838764
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	89167978-be8f-4145-8801-45e2fffa1fe8
TotalAuthenLatency	3621649740
ClientLatency	3621649732
CoASourceComponent	Profiler
CoAReason	Change in endpoint identity group/policy/logical profile which are used in authorization policies
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
Device IP Address	172.16.5.169
CPMSessionID	A90510AC00000058D7DD0AA7
CiscoAVPair	subscriber:reauthenticate-type=last, subscriber:command=reauthenticate, audit-session-id=A90510AC00000058D7DD0AA7

CoA 트리거 구성 요소 및 이유

Context

Visibility(상황 가시성) > Endpoints(엔드포인트) > Authentication(인증) 탭으로 이동합니다. 이 탭에서 필터를 사용하여 테스트 끝 점을 찾습니다.

엔드포인트 특성에 액세스하려면 엔드포인트 MAC 주소를 클릭합니다.

<input type="checkbox"/>	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authen...	Authentication ...	Authorization P...
×	0A:5A:F0:B3:B5:9C	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentic...	Authentication Polic	Authorization Policy
<input type="checkbox"/>	0A:5A:F0:B3:B5:9C	...		bob	Victor-s-S22	Location...	Android	-	Default	Wifi Endpoint Analy...

컨텍스트 가시성의 엔드포인트

이 작업은 ISE가 이 엔드포인트에 대해 저장하고 있는 모든 정보를 표시합니다. 속성 섹션을 클릭한 다음 기타 속성을 선택합니다.

MAC ADDRESS: 0A:5A:F0:B3:B5:9C

Username: bob

Endpoint Profile: Android

Current IP Address: -

Location: Location → All Locations

MFC Endpoint Type: Phone

MFC Hardware: Samsung Electronics Co.,Ltd

Manufacturer: Samsung Electronics Co.,Ltd

MFC Hardware Model: Samsung Galaxy S22+

MFC Operating System: Android 13

Applications | **Attributes** | Authentication | Threats | Vulnerabilities

General Attributes | Custom Attributes | **Other Attributes**

컨텍스트 가시성에 대한 엔드포인트 기타 특성 선택

WiFi_Device_Analytics 사전 속성을 찾을 때까지 아래로 스크롤합니다. 이 섹션에서 이러한 특성을 찾는다 것은 ISE가 어카운팅 패킷을 통해 해당 특성을 성공적으로 받았으며 엔드포인트 분류에 사용할 수 있음을 의미합니다.

DEVICE_INFO_COUNTRY_CODE	Unknown
DEVICE_INFO_DEVICE_FORM	PHONE
DEVICE_INFO_FIRMWARE_VERSION	WH6
DEVICE_INFO_MODEL_NUM	Samsung Galaxy S22+
DEVICE_INFO_OS_VERSION	Android 13
DEVICE_INFO_SALES_CODE	MXO
DEVICE_INFO_VENDOR_TYPE	SAMSUNG

컨텍스트 가시성의 WiFi 분석 특성

참고로 다음은 Windows 10 및 iPhone 특성의 예입니다.

DEVICE_INFO_DEVICE_FORM	0
DEVICE_INFO_FIRMWARE_VERSION	22.180.02.01
DEVICE_INFO_HW_MODEL	AX201/AX1650
160MHZ	
DEVICE_INFO_MANUFACTURER_NAME	LENOVO
DEVICE_INFO_MODEL_NAME	20RAS0C000
DEVICE_INFO_MODEL_NUM	LENOVO
20RAS0C000	
DEVICE_INFO_OS_VERSION	WINDOWS 10
DEVICE_INFO_POWER_TYPE	AC POWERED
DEVICE_INFO_VENDOR_TYPE	3

Windows 10 엔드포인트 특성

DEVICE_INFO_DEVICE_FORM	0
DEVICE_INFO_MODEL_NUM	IPHONE
11 PRO	
DEVICE_INFO_OS_VERSION	IOS 16.4
DEVICE_INFO_VENDOR_TYPE	1

에이아이폰 엔드포인트 특성 예

문제 해결

1단계. 계정 관리 패킷이 ISE에 도달함

WLC CLI에서 정책 프로파일 컨피그레이션에서 DOT11 TLV 어카운팅, DHCP TLV 캐싱 및 HTTP TLV 캐싱이 활성화되어 있는지 확인합니다.

<#root>

```
vimontes-wlc#show running-config | section wireless profile policy policy-profile-name
wireless profile policy policy-profile-name
aaa-override
accounting-list AAA-LIST
```

dhcp-tlv-caching

dot11-tlv-accounting

http-tlv-caching

radius-profiling

no shutdown

엔드포인트에 연결하는 동안 WLC 또는 ISE에서 패킷 캡처를 수집합니다. Wireshark와 같은 잘 알려진 패킷 분석 도구를 사용하여 수집된 파일을 분석할 수 있습니다.

RADIUS 계정 관리 패킷 및 호출 스테이션 ID(엔드포인트 MAC 주소 테스트)로 필터링합니다. 예를 들어, 이 필터를 사용할 수 있습니다.

```
radius.code == 4 && radius.Calling_Station_Id == "xx-xx-xx-xx-xx-xx"
```

위치가 확인되면 Cisco-AVPair 필드를 확장하여 어카운팅 패킷에서 WiFi 분석 데이터를 찾습니다.

```

No. | Time | Source | Destination | Protocol | Length | Info
---|---|---|---|---|---|---
104 2023-09-27 12:19:23.584661 172.16.5.169 172.16.5.112 RADIUS 976 Accounting-Request id=39

> AVP: t=Vendor-Specific(26) l=28 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=39 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  Type: 26
  Length: 49
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=43 val=dot11-device-info=\000\000\000\023Samsung Galaxy S22+
> AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
  Type: 26
  Length: 33
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=27 val=dot11-device-info=\000\001\000\003WH6
> AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
  Type: 26
  Length: 33
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=27 val=dot11-device-info=\000\002\000\003MX0
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
  Type: 26
  Length: 31
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=25 val=dot11-device-info=\000\003\000\0011
> AVP: t=Vendor-Specific(26) l=40 vnd=ciscoSystems(9)
  Type: 26
  Length: 40
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=34 val=dot11-device-info=\000\004\000\0aAndroid 13
> AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)
  Type: 26
  Length: 37
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=31 val=dot11-device-info=\000\005\000\0aUnknown
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
  Type: 26
  Length: 31
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=25 val=dot11-device-info=\000\n\000\0012
> AVP: t=Framed-IP-Address(8) l=6 val=172.16.5.76

```

어카운팅 패킷 내의 엔드포인트 TLV 특성

2단계. ISE는 엔드포인트 특성을 사용하여 어카운팅 패킷을 구문 분석합니다

ISE에서 이러한 구성 요소는 DEBUG 레벨로 설정하여 WLC에서 보낸 RADIUS 어카운팅 패킷이 ISE에 도달하여 올바르게 처리되도록 할 수 있습니다.

그런 다음 ISE 지원 번들을 수집하여 로그 파일을 수집할 수 있습니다. 지원 번들을 수집하는 방법에 대한 자세한 내용은 [관련 정보 섹션](#)을 참조하십시오.

Component Name	Log Level	Description	Log file Name
× Component Name	DEBUG	× Description	Log file Name
nsf	DEB... ▾	NSF related messages	ise-psc.log
nsf-session	DEB... ▾	Session cache messages	ise-psc.log
profiler	DEB... ▾	profiler debug messages	profiler.log
runtime-AAA	DEB... ▾	AAA runtime messages (prrt)	prrt-server.log

문제 해결을 위해 디버깅할 구성 요소

참고: 구성 요소는 엔드포인트를 인증하는 PSN에서만 DEBUG 레벨로 활성화됩니다.

iseLocalStore.log에서 Accounting-Start 메시지는 어떤 구성 요소도 DEBUG 레벨로 활성화하지 않고 기록됩니다. 여기서 ISE는 WiFi Analytics 특성을 포함하는 수신 어카운팅 패킷을 확인해야 합니다.

<#root>

2023-09-27 18:19:23.600 +00:00 0000035538 3000

NOTICE Radius-Accounting: RADIUS Accounting start request,

ConfigVersionId=1493,
Device IP Address=172.16.5.169,


```
[1] User-Name - value: [bob]
[4] NAS-IP-Address - value: [172.16.5.169] [5] NAS-Port - value: [260613] [8] Framed-IP-Address - value: [172.16.5.169]
[26] cisco-av-pair - value: [dot11-device-info=<00><00><00><13>Samsung Galaxy S22+] [26] cisco-av-pair - value: [dot11-device-info=<00><00><00><13>Samsung Galaxy S22+]
[26] cisco-av-pair - value: [audit-session-id=A90510AC0000005BD7DDDA7] [26] cisco-av-pair - value: [audit-session-id=A90510AC0000005BD7DDDA7]
```

3단계. 엔드포인트 특성이 업데이트되고 엔드포인트가 분류됨

이 syslog 메시지는 프로파일러 구성 요소와 공유됩니다. Profiler.log는 구문 분석된 syslog 메시지를 수신하고 엔드포인트 특성을 추출합니다.

<#root>

2023-09-27 1

8:19:23,601 DEBUG [SyslogListenerThread]

[[]] cisco.profiler.probes.radius.SyslogMonitor -:::::-

Radius Packet Received 1266

2023-09-27

18:19:23,601 DEBUG [SyslogListenerThread]

[[]] cisco.profiler.probes.radius.SyslogDefragmenter -:::::- parseHeader inBuffer=<181>Sep 27 18:19:23

CISE_RADIUS_Accounting 000000297

3 0 2023-09-27 18:19:23.600 +00:00 0000035538

3000 NOTICE Radius-Accounting: RADIUS Accounting start request

, ConfigVersionId=1493, Device IP Address=172.16.5.169,

UserName=bob

, NetworkDeviceName=lab-wlc, User-Name=bob, NAS-IP-Address=172.16.5.169, NAS-Port=260613, Framed-IP-Address=172.16.5.169, Called-Station-ID=00-1e-f6-5c-16-ff,

Calling-Station-ID=0a-5a-f0-b3-b5-9c

, NAS-Identifier=vimontes-wlc, Acct-Status-Type=Start, Acct-Delay-Time=0, Acct-Session-Id=00000018, Acct-Event-Timestamp=1695838756, NAS-Port-Type=Wireless - IEEE 802.11, cisco-av-pair=dc-profile-name=Samsung, cisco-av-pair=dc-device-class-tag=Samsung Galaxy S22+, cisco-av-pair=dc-certainty-metric=40, cisco-av-pair=64:63:2d:6f:70:61:71:75:65:3d:01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00, cisco-av-pair=dc-protocol=TCP

18:19:23,601 DEBUG

[SyslogListenerThread][[]] cisco.profiler.probes.radius.SyslogMonitor -:::::-

Radius Packet Received 1267

2023-09-27

18:19:23,601 DEBUG

[SyslogListenerThread][[]] cisco.profiler.probes.radius.SyslogDefragmenter -:::::- parseHeader inBuffer=<181>Sep 27 18:19:23

CISE_RADIUS_Accounting 000000297 3 1

cisco-av-pair=dhcp-option=host-name=Victor-s-S22, cisco-av-pair=dhcp-option=dhcp-class-identifier=andro
cisco-av-pair=dot11-device-info=DEVICE_INFO_MODEL_NUM=Samsung Galaxy S22+, cisco-av-pair=dot11-device-in

cisco-av-pair=dot11-device-info=DEVICE_INFO_DEVICE_FORM=1, cisco-av-pair=dot11-device-info=DEVICE_INFO_C

cisco-av-pair=dot11-device-info=DEVICE_INFO_VENDOR_TYPE=2, cisco-av-pair=audit-session-id=A90510AC000000
, cisco-av-pair=vlan-id=2606, cisco-av-pair=method=dot1x, cisco-av-pair=cisco-wlan-ssid=VICSSID,
cisco-av-pair=wlan-profile-name=ISE-AAA, Airespace-Wlan-Id=1, AcsSessionID=iselab/484624451/304,

엔드포인트 특성 정보가 업데이트됩니다.

<#root>

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_FIRMWARE_VERSION=[WH6]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_SALES_CODE=[MXO]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_DEVICE_FORM=[1]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_OS_VERSION=[Android 13]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_COUNTRY_CODE=[Unknown]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_VENDOR_TYPE=[2]

<#root>

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7:::- Endpoint: EndPoint[id=,name=

MAC: 0A:5A:F0:B3:B5:9C

Attribute:AAA-Server value:iselab Attribute:Acct-Authentic value:Remote Attribute:Acct-Delay-Time valu

Attribute:DEVICE_INFO_COUNTRY_CODE value:Unknown Attribute:DEVICE_INFO_DEVICE_FORM value:PHONE Attribute

Attribute:Device IP Address value:172.16.5.169 Attribute:Device Type value:Device Type#All Device Type

특성 업데이트는 이벤트를 프로파일링 새 엔드 포인트를 시작 합니다. 프로파일링 정책이 다시 평가되고 새 프로파일이 할당됩니다.

<#root>

2023-09-27 18:19:24,098

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7::62cc7a10-5d62-

Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

2023-09-27 18:19:24,098

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7::62cc7a10-5d62-

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7::62cc7a10-5d62-

Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

com.cisco.profiler.infrastructure.profiling.ProfilerManager\$MatchingPolicyInternal@14ec7800

4단계. CoA 및 재인증

ISE는 WiFi Device Analytics 특성이 변경됨에 따라 엔드포인트 세션에 대한 CoA를 보내야 합니다.

<#root>

2023-09-27 18:19:24,103

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7::62cc7a10-5d62-

Endpoint 0A:5A:F0:B3:B5:9C IdentityGroup / Logical Profile Changed/ WiFi device analytics attribute chan

2023-09-27 18:19:24,103

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC000005BD7DDDA7::62cc7a10-5d62-

ConditionalCoAEvent with Endpoint Details : EndPoint[id=62caa550-5d62-11ee-bf1f-b6bb1580ab0d,name=] MAC:

Attribute:AAA-Server value:iselab Attribute:Airespace-Wlan-Id value:1 Attribute:AllowedProtocolMatched

Attribute:DEVICE_INFO_COUNTRY_CODE value:Unknown Attribute:DEVICE_INFO_DEVICE_FORM value:PHONE Attribute

Attribute:DTLSSupport value:Unknown Attribute:DestinationIPAddress value:172.16.5.112 Attribute:Destin

패킷 캡처는 ISE가 CoA를 WLC에 전송하도록 하는 데 도움이 됩니다. 또한 CoA 처리 후 새로운 Access-Request 패킷이 수신됨을 보여줍니다.

111	2023-09-27 12:19:24.357572	172.16.5.112	172.16.5.169	RADIUS	244 CoA-Request id=13
112	2023-09-27 12:19:24.361138	172.16.5.169	172.16.5.112	RADIUS	111 CoA-ACK id=13

```

> Frame 111: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
> Ethernet II, Src: Vmware_b3:f0:73 (00:50:56:b3:f0:73), Dst: Cisco_5c:16:ff (00:1e:f6:5c:16:ff)
> Internet Protocol Version 4, Src: 172.16.5.112, Dst: 172.16.5.169
> User Datagram Protocol, Src Port: 41440, Dst Port: 1700
< RADIUS Protocol
  Code: CoA-Request (43)
  Packet identifier: 0xd (13)
  Length: 202
  Authenticator: d622a25b73d3b2b475cf5d4ad2b00b5c
  [The response to this request is in frame 112]
  Attribute Value Pairs
  > AVP: t=NAS-IP-Address(4) l=6 val=172.16.5.169
  > AVP: t=Calling-Station-Id(31) l=19 val=0A:5A:F0:B3:B5:9C
    Type: 31
    Length: 19
    Calling-Station-Id: 0A:5A:F0:B3:B5:9C
  > AVP: t=Event-Timestamp(55) l=6 val=Sep 27, 2023 12:19:24.000000000 CST
  > AVP: t=Message-Authenticator(80) l=18 val=3edaf9ffdb25ceee5451e90a1cef21af
  > AVP: t=Vendor-Specific(26) l=43 vnd=ciscoSystems(9)
    Type: 26
    Length: 43
    Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=37 val=subscriber:reauthenticate-type=last
  > AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
    Type: 26
    Length: 41
    Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=35 val=subscriber:command=reauthenticate
  > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    Type: 26
    Length: 49
    Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=43 val=audit-session-id=A90510AC000005BD7DDDA7

```

엔드포인트 프로파일링 후 RADIUS CoA 패킷

111	2023-09-27 12:19:24.357572	172.16.5.112	172.16.5.169	RADIUS	244 CoA-Request id=13
112	2023-09-27 12:19:24.361138	172.16.5.169	172.16.5.112	RADIUS	111 CoA-ACK id=13
113	2023-09-27 12:19:24.373874	172.16.5.169	172.16.5.112	RADIUS	480 Access-Request id=55
114	2023-09-27 12:19:24.386280	172.16.5.112	172.16.5.169	RADIUS	167 Access-Challenge id=55
115	2023-09-27 12:19:24.397609	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=63
116	2023-09-27 12:19:24.400463	172.16.5.112	172.16.5.169	RADIUS	167 Access-Challenge id=63
117	2023-09-27 12:19:24.413943	172.16.5.169	172.16.5.112	RADIUS	720 Access-Request id=71
118	2023-09-27 12:19:24.456036	172.16.5.112	172.16.5.169	RADIUS	1179 Access-Challenge id=71
119	2023-09-27 12:19:24.477140	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=79
120	2023-09-27 12:19:24.481172	172.16.5.112	172.16.5.169	RADIUS	1175 Access-Challenge id=79
121	2023-09-27 12:19:24.496743	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=87
122	2023-09-27 12:19:24.499901	172.16.5.112	172.16.5.169	RADIUS	289 Access-Challenge id=87
123	2023-09-27 12:19:24.546538	172.16.5.169	172.16.5.112	RADIUS	715 Access-Request id=95
124	2023-09-27 12:19:24.553619	172.16.5.112	172.16.5.169	RADIUS	218 Access-Challenge id=95
125	2023-09-27 12:19:24.568069	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=103
126	2023-09-27 12:19:24.571945	172.16.5.112	172.16.5.169	RADIUS	201 Access-Challenge id=103
127	2023-09-27 12:19:24.584229	172.16.5.169	172.16.5.112	RADIUS	594 Access-Request id=111
128	2023-09-27 12:19:24.588165	172.16.5.112	172.16.5.169	RADIUS	232 Access-Challenge id=111
129	2023-09-27 12:19:24.599493	172.16.5.169	172.16.5.112	RADIUS	648 Access-Request id=119
130	2023-09-27 12:19:24.624360	172.16.5.112	172.16.5.169	RADIUS	247 Access-Challenge id=119
131	2023-09-27 12:19:24.638515	172.16.5.169	172.16.5.112	RADIUS	592 Access-Request id=127
132	2023-09-27 12:19:24.642039	172.16.5.112	172.16.5.169	RADIUS	200 Access-Challenge id=127
133	2023-09-27 12:19:24.654578	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=135
134	2023-09-27 12:19:24.677792	172.16.5.112	172.16.5.169	RADIUS	330 Access-Accept id=135

엔드포인트 프로파일링 후 RADIUS CoA 및 새 액세스 요청

관련 정보

- [Cisco Identity Services Engine 관리자 가이드, 릴리스 3.3](#)
- [Cisco Identity Services Engine 릴리스 정보, 릴리스 3.3](#)
- [Identity Services Engine에서 지원 번들 수집](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.