

ISE 프로파일링을 위한 디바이스 센서 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계. 표준 AAA 컨피그레이션](#)

[2단계. 장치 센서 구성](#)

[3단계. ISE에서 프로파일링 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[1단계. CDP/LLDP에서 수집한 정보 확인](#)

[2단계. 디바이스 센서 캐시 확인](#)

[3단계. Radius 어카운팅에 특성이 있는지 확인](#)

[4단계. ISE에서 프로파일러 디버깅 확인](#)

[5단계. 새 특성 및 장치 할당 프로파일링](#)

[관련 정보](#)

소개

이 문서에서는 ISE에서 프로파일링 목적으로 사용할 수 있도록 디바이스 센서를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Radius 프로토콜
- CDP(Cisco Discovery Protocol), LLDP(Link Layer Discovery Protocol) 및 DHCP(Dynamic Host Configuration Protocol)
- Cisco ISE(Identity Service Engine)
- Cisco Catalyst 스위치 2960

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

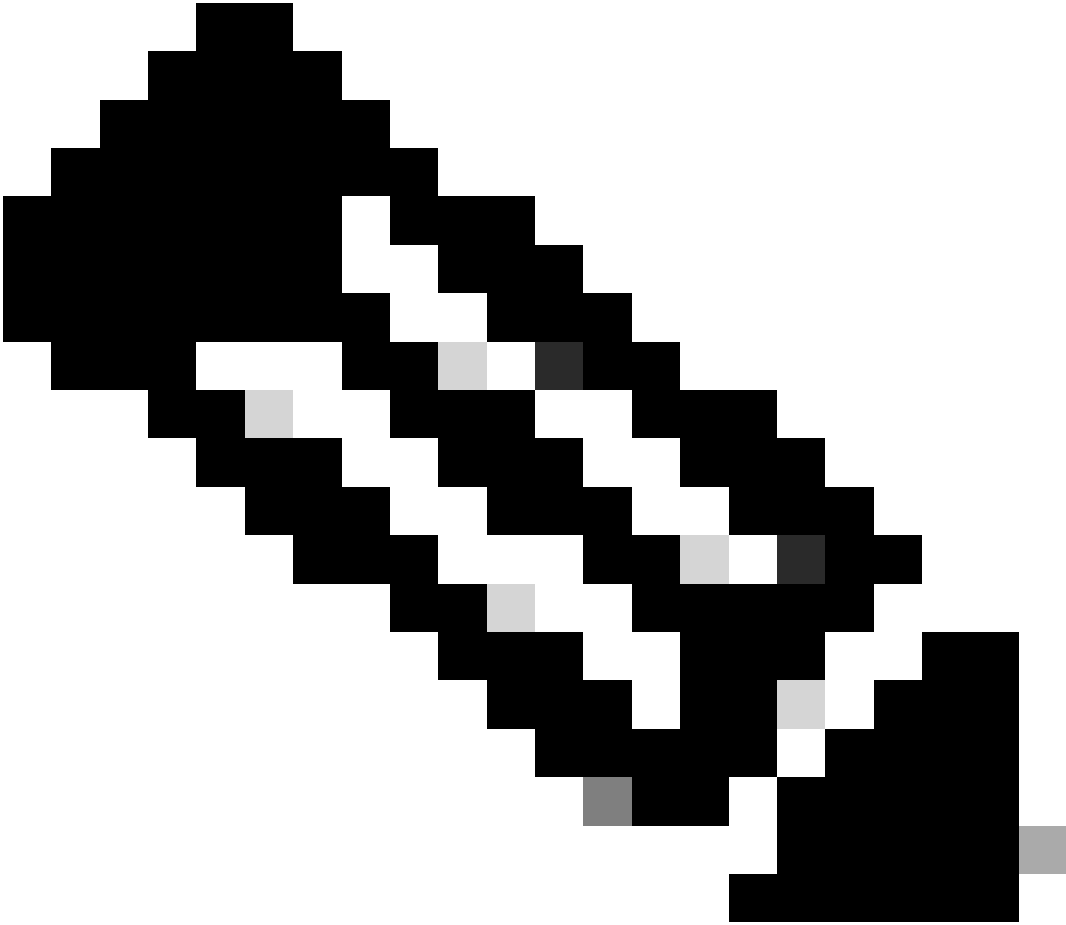
- Cisco ISE 버전 1.3 패치 3
- Cisco Catalyst Switch 2960s 버전 15.2(2a)E1
- Cisco IP Phone 8941 버전 SCCP 9-3-4-17

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

디바이스 센서는 액세스 디바이스의 기능입니다. 연결된 엔드포인트에 대한 정보를 수집할 수 있습니다. 대개 디바이스 센서가 수집하는 정보는 다음 프로토콜에서 가져올 수 있습니다.

- CDP
- LLDP
- DHCP



참고: 일부 플랫폼에서는 H323, SIP(Session Initiation Protocol), MDNS(Multicast Domain Resolution) 또는 HTTP 프로토콜을 사용할 수도 있습니다. 디바이스 센서 기능에 대한 컨피그레이션 가능성은 프로토콜마다 다를 수 있습니다. 예를 Cisco Catalyst 3850(소프트웨어 03.07.02.E)에서 찾을 수 있습니다.

정보가 수집되면 RADIUS 어카운팅에서 캡슐화하여 프로파일링 서버로 전송할 수 있습니다. 이 문서에서는 ISE가 프로파일링 서버로 사용됩니다.

구성

1단계. 표준 AAA 컨피그레이션

AAA(Authentication, Authorization, and Accounting)를 구성하려면 다음 단계를 참조하십시오.

1. 명령을 사용하여 AAA를 `aaa new-model` 활성화하고 스위치에서 802.1X를 전역적으로 활성화합니다.
2. Radius 서버를 구성하고 동적 권한 부여(Change of Authorization - CoA)를 활성화합니다.

3. CDP 및 LLDP 프로토콜을 활성화합니다.

4. switchport 인증 컨피그레이션 추가

```
!  
aaa new-model  
!  
aaa authentication dot1x default group radius  
aaa authorization network default group radius  
aaa accounting update newinfo  
aaa accounting dot1x default start-stop group radius  
!  
aaa server radius dynamic-author  
client 1.1.1.1 server-key xyz  
!  
dot1x system-auth-control  
!  
lldp run  
cdp run  
!  
interface GigabitEthernet1/0/13  
description IP_Phone_8941_connected  
switchport mode access  
switchport voice vlan 101  
authentication event fail action next-method  
authentication host-mode multi-domain  
authentication order dot1x mab  
authentication priority dot1x mab  
authentication port-control auto  
mab  
dot1x pae authenticator  
dot1x timeout tx-period 2  
spanning-tree portfast  
end  
!  
radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key xyz  
!
```

참고: 최신 소프트웨어 버전에서는 이 명령 `radius-server vsa send accounting`이 기본적으로 활성화됩니다. 어카운팅에서 전송된 속성을 볼 수 없는 경우 명령이 활성화되었는지 확인합니다.

2단계. 장치 센서 구성

1. 디바이스를 프로파일링하기 위해 CDP/LLDP에서 어떤 특성이 필요한지 결정합니다. Cisco IP Phone 8941의 경우 다음을 사용할 수 있습니다.

- LLDP SystemDescription 특성

- CDP CachePlatform 특성

The screenshot displays the Cisco Identity Services Engine (ISE) Profiler Policy configuration interface. The main configuration area is titled 'Profiler Policy' and is for the policy 'Cisco-IP-Phone-8941'. Key configuration details include:

- Name:** Cisco-IP-Phone-8941
- Description:** Policy for Cisco
- Policy Enabled:**
- * Minimum Certainty Factor:** 70 (Valid Range 1 to 65535)
- * Exception Action:** NONE
- * Network Scan (NMAP) Action:** NONE
- Create an Identity Group for the policy:** Yes, create matching Identity Group; No, use existing Identity Group hierarchy
- * Parent Policy:** Cisco-IP-Phone
- * Associated CoA Type:** Global Settings
- System Type:** Cisco Provided

The 'Rules' section shows two conditions:

- If Condition:** CiscoIPPhone8941Check1
- If Condition:** CiscoIPPhone8941Check2

A 'Conditions Details' popup is open for 'CiscoIPPhone8941Check2', providing the following information:

- Name:** CiscoIPPhone8941Check2
- Description:** Check for Cisco IP Phone 8941
- Expression:** LLDP:lldpSystemDescription CONTAINS Cisco IP Phone 8941

Cisco의 목적상 둘 다 Certainty Factory를 70으로 늘리고 Cisco-IP-Phone-8941로 프로파일링해야 하는 Minimum Certainty Factory는 70이므로 둘 중 하나만 얻으면 충분합니다.

- Profiling
- Cisco-IP-Phone-7940
 - Cisco-IP-Phone-7941
 - Cisco-IP-Phone-7942
 - Cisco-IP-Phone-7945
 - Cisco-IP-Phone-7945G
 - Cisco-IP-Phone-7960
 - Cisco-IP-Phone-7961
 - Cisco-IP-Phone-7962
 - Cisco-IP-Phone-7965
 - Cisco-IP-Phone-7970
 - Cisco-IP-Phone-7971
 - Cisco-IP-Phone-7975
 - Cisco-IP-Phone-7985
 - Cisco-IP-Phone-8831
 - Cisco-IP-Phone-8841
 - Cisco-IP-Phone-8851
 - Cisco-IP-Phone-8861
 - Cisco-IP-Phone-8941
 - Cisco-IP-Phone-8945

Profiler Policy List > Cisco-IP-Phone-8941

Profiler Policy

* Name: Cisco-IP-Phone-8941 Description: Policy for C

Policy Enabled

* Minimum Certainty Factor: 70 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: Yes, create matching Identity Group No, use existing Identity Group hierarchy

* Parent Policy: Cisco-IP-Phone

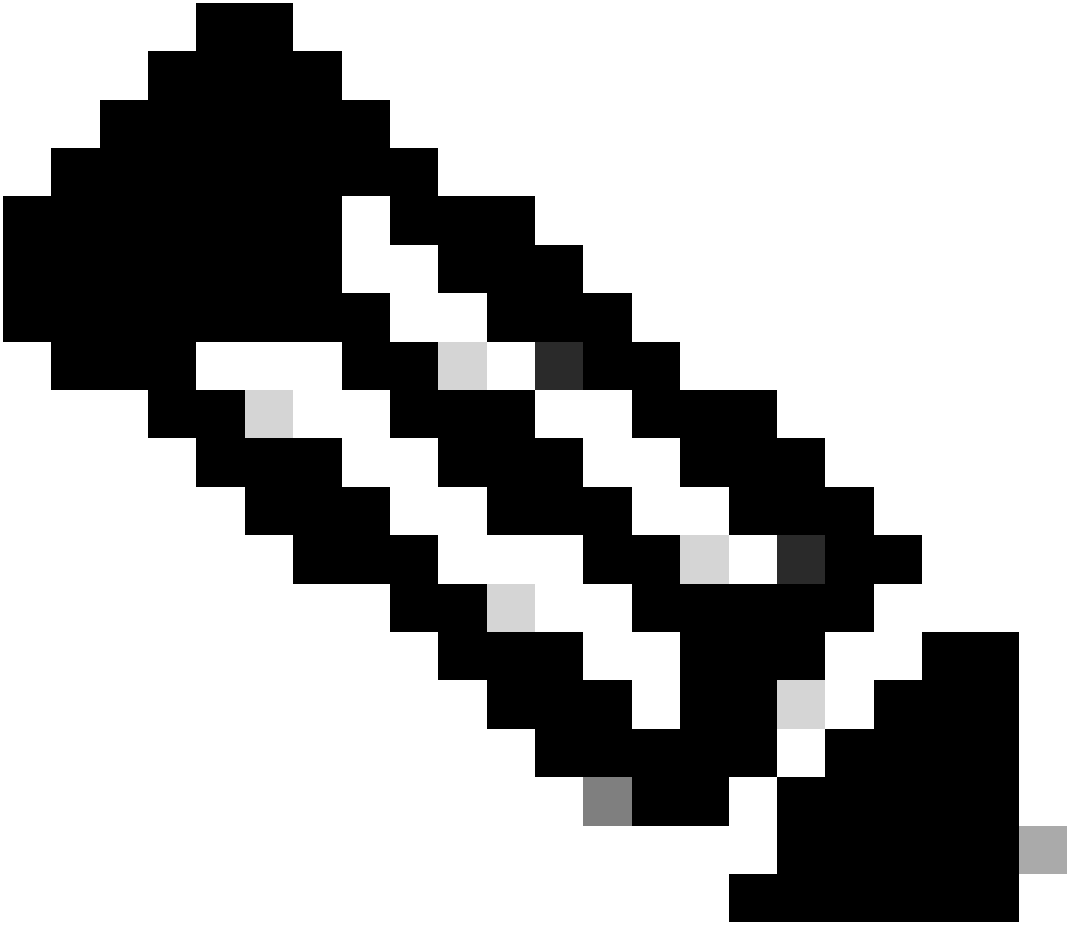
* Associated CoA Type: Global Settings

System Type: Cisco Provided

Rules

If Condition	CiscoIPPhone8941Check1	Then	Certainty Factor Increases	70
If Condition	CiscoIPPhone8941Check2	Then	Certainty Factor Increases	70

Save Reset



참고: 특정 Cisco IP Phone으로 프로파일링하려면 모든 상위 프로필에 대한 최소 조건을 충족해야 합니다. 이는 프로파일러가 Cisco-Device(Minimum Certainty Factor 10) 및 Cisco-IP-Phone(Minimum Certainty Factor 20)과 일치해야 함을 의미합니다. 프로파일러가 이 두 프로파일과 일치하더라도, 각 IP Phone 모델은 최소 Certainty Factor가 70이므로 특정 Cisco IP Phone으로 프로파일링해야 합니다. 디바이스는 가장 확실성 요소가 높은 프로파일에 할당됩니다.

2. 두 개의 필터 목록(CDP용 필터 목록과 LLDP용 필터 목록)을 구성합니다. 이러한 특성은 Radius 계정 관리 메시지에 포함해야 하는 특성을 나타냅니다. 이 단계는 선택 사항입니다.

3. CDP 및 LLDP에 대한 2개의 필터 사양을 생성합니다. filter-spec에서 어카운팅 메시지에 포함하거나 제외해야 하는 특성 목록을 표시할 수 있습니다. 이 예에는 다음 특성이 포함되어 있습니다.

- CDP

의 디바이스 이름

- system-description from LLDP(LLDP의 시스템 설명)

필요한 경우 Radius를 통해 ISE로 전송할 추가 특성을 구성할 수 있습니다. 이 단계도 선택 사항입니다.

4. 명령을 추가합니다device-sensor notify all-changes. 현재 세션에 대해 TLV가 추가, 수정 또는 제거될 때마다 업데이트가 트리거됩니다.

5. 디바이스 센서 기능을 통해 수집된 정보를 실제로 전송하려면 스위치에서 명령을 사용하여 이를 수행하도록 명시적으로 지시해야 합니다device-sensor accounting.

```
! device-sensor filter-list cdp list cdp-list tlv name device-name
```

```
tlv name platform-type ! device-sensor filter-list lldp list lldp-list tlv name system-description ! device-sensor filter-spec lldp include list lldp-list device-se
```

3단계. ISE에서 프로파일링 구성

1. 스위치를 네트워크 디바이스로 추가합니다Administration > Network Resources > Network Devices. 스위치의 radius 서버 키를 Authentication Settings(인증 설정)에서 공유 비밀로 사용합니다.

CISCO Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service

Network Devices | Network Device Groups | External RADIUS Servers | RADIUS Server Sequences | TrustSec AAA Servers | NAC Managers

Network Devices

Network Devices List > deskswitch

Network Devices

* Name: test_switch
Description: []

* IP Address: 1.1.1.1 / 32

Model Name: []
Software Version: []

* Network Device Group

Location: All Locations [Set To Default]
Device Type: All Device Types [Set To Default]

Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: [] [Show]

Enable KeyWrap: [i]

* Key Encryption Key: [] [Show]

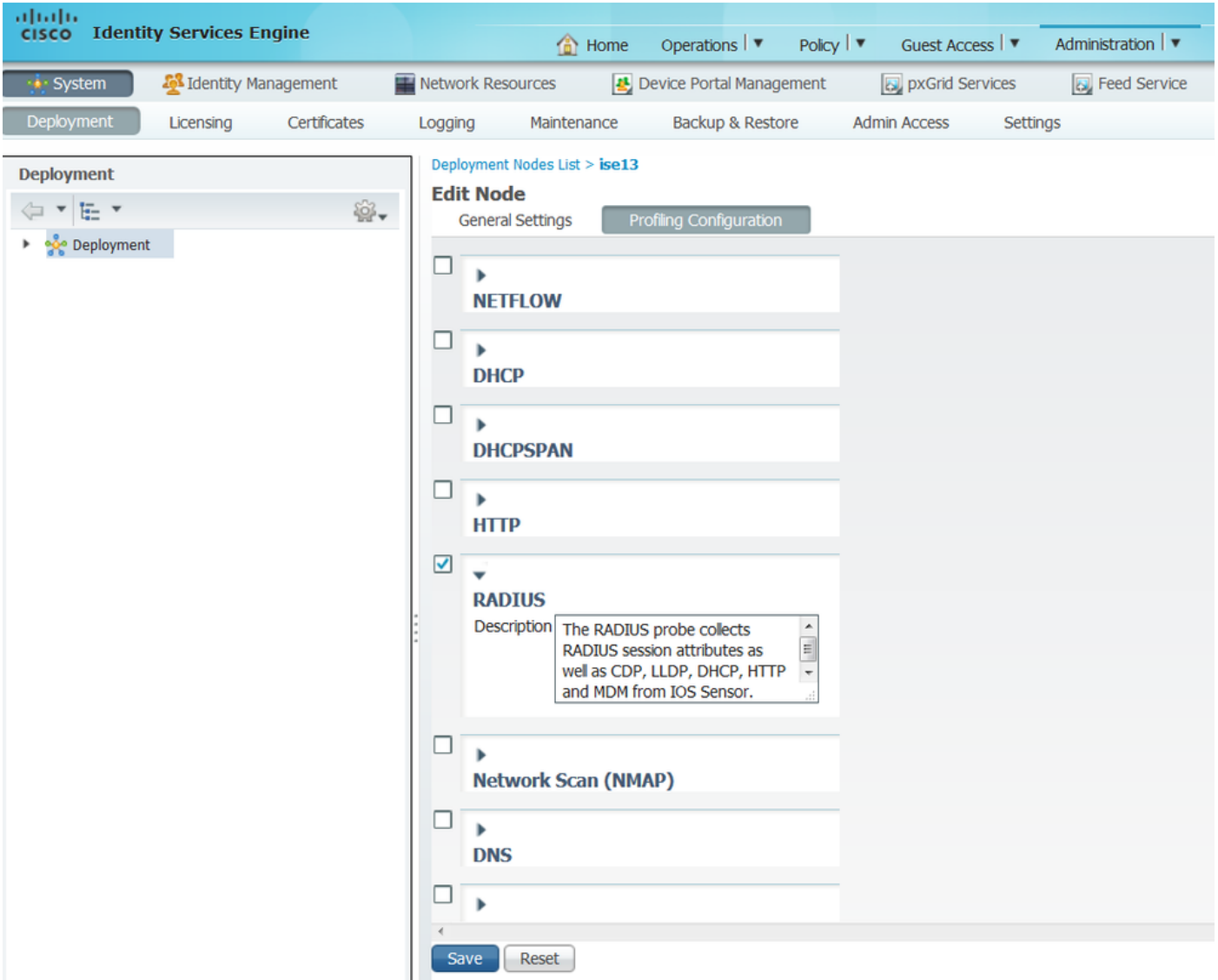
* Message Authenticator Code Key: [] [Show]

Key Input Format: ASCII HEXADECIMAL

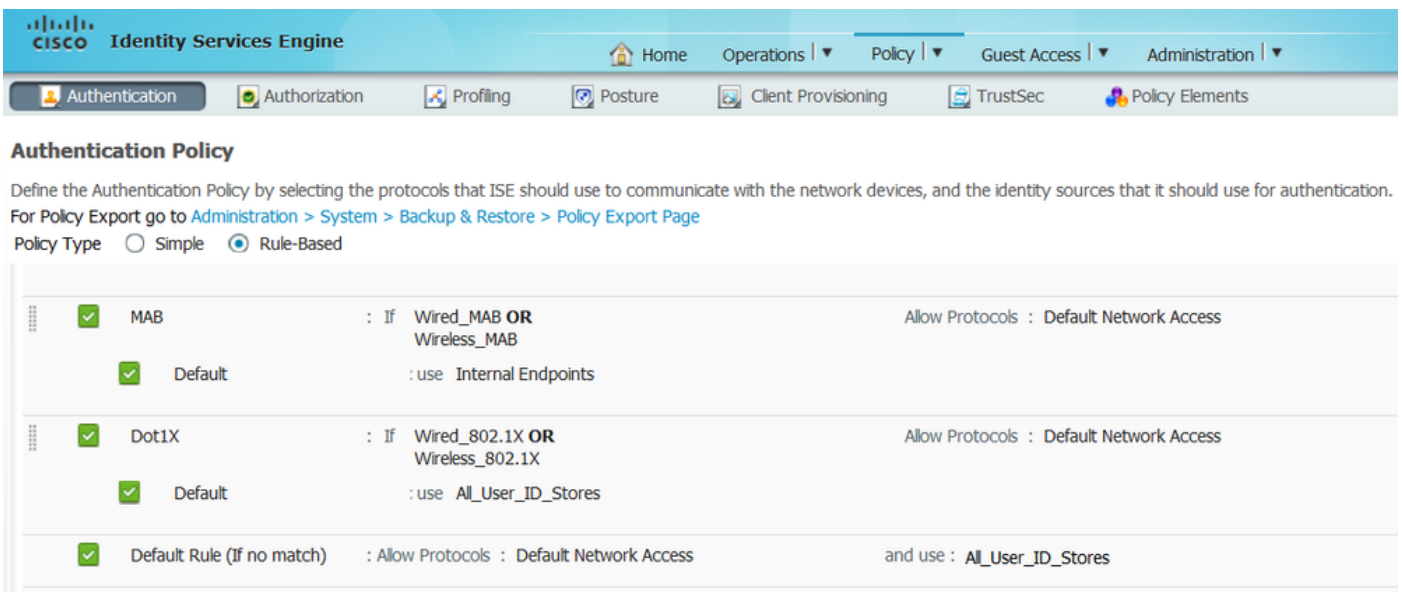
SNMP Settings
 Advanced TrustSec Settings

[Save] [Reset]

2. 프로파일링 노드에서 Radius 프로브를 활성화합니다 Administration > System > Deployment > ISE node > Profiling Configuration. 프로파일링에 모든 PSN 노드를 사용해야 하는 경우 다음 모든 노드에서 프로브를 활성화합니다.



3. ISE 인증 규칙을 구성합니다. 이 예에서는 ISE에서 사전 구성된 기본 인증 규칙이 사용됩니다.



4. ISE 권한 부여 규칙을 구성합니다. ISE에서 미리 구성된 'Profiled Cisco IP Phones' 규칙이 사용됩니다.

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.
 For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	Cisco-IP-Phone	then Cisco_IP_Phones

다음을 확인합니다.

프로파일링이 올바르게 작동하는지 확인하려면 ISE에서 Operations > Authentications 참조하십시오.

The screenshot shows the Cisco ISE Authentications page. At the top, there are summary statistics: Misconfigured Supplcants (0), Misconfigured Network Devices (0), RADIUS Drops (0), and Client Stopped Responding (0). Below this is a table of live sessions with columns for Time, Status, Identity, Endpoint ID, Endpoint Profile, Authentication Policy, Authorization Policy, Authorization Profiles, Identity Group, and Event.

Time	Status	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2015-11-25 18:49:51.737	ⓘ	0	20:BB:C0:DE:06; 20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941					Session State is Started
2015-11-25 18:49:42.433	✓	#ACSACL#-IP-PE							ACL Download Succeeded
2015-11-25 18:49:42.417	✓	20:BB:C0:DE:06; 20:BB:C0:DE:06:AE	20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941	Default >> MAB >> D...	Default >> Profiled Cis..	Cisco_IP_Phones	Cisco-IP-Phone	Authentication succeeded
2015-11-25 18:49:42.401	✓		20:BB:C0:DE:06:AE						Dynamic Authorization succeeded
2015-11-25 18:49:10.802	✓	20:BB:C0:DE:06; 20:BB:C0:DE:06:AE	20:BB:C0:DE:06:AE	Cisco-Device	Default >> MAB >> D...	Default >> Default	PermitAccess	Profiled	Authentication succeeded
2015-11-25 18:49:10.780	✓		20:BB:C0:DE:06:AE						Dynamic Authorization succeeded
2015-11-25 18:49:00.720	✓	20:BB:C0:DE:06; 20:BB:C0:DE:06:AE			Default >> MAB >> D...	Default >> Default	PermitAccess		Authentication succeeded

먼저 MAB(18:49:00)를 사용하여 디바이스를 인증했습니다. 10초 후(18:49:10) Cisco-Device로 다시 프로파일링되었으며, 첫 인증(18:49:42) 42초 후 Cisco-IP-Phone-8941 프로필을 받았습니다. 그 결과 ISE는 IP Phone(Cisco_IP_Phones)에 특정한 권한 부여 프로파일 및 모든 트래픽을 허용하는(ip any 허용) 다운로드 가능한 ACL을 반환합니다. 이 시나리오에서 알 수 없는 디바이스는 네트워크에 대한 기본 액세스 권한을 갖습니다. ISE 내부 엔드포인트 데이터베이스에 Mac 주소를 추가하거나 이전에 알려지지 않은 디바이스에 대해 매우 기본적인 네트워크 액세스를 허용하면 이 작업을 수행할 수 있습니다.



참고: 이 예에서 초기 프로파일링은 약 40초가 걸렸습니다. 다음 인증에서는 ISE가 프로파일을 이미 알고 있으며, ISE가 새/업데이트된 특성을 받지 않고 디바이스를 다시 프로파일링해야 하는 경우가 아니면 올바른 특성(음성 도메인 및 DACL에 가입할 수 있는 권한)이 즉시 적용됩니다.

The screenshot shows the Cisco Identity Services Engine (ISE) dashboard. At the top, there are navigation tabs: Home, Operations, Policy, Guest Access, and Administration. Below these are sub-tabs: Authentications, Reports, Endpoint Protection Service, and Troubleshoot. A summary row shows four metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), and Client Stopped Responses (0). Below this is a table of authentication events.

Time	Status	Details	R...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2015-11-25 18:55:39.772	0			20:BB:C0:DE:06: 20:BB:C0:DE:06:AE		Cisco-IP-Phone-8941					Session State is Started
2015-11-25 18:55:38.721	✓			#ACSACL#-IP-PE							DACL Download Succeeded
2015-11-25 18:55:38.707	✓			20:BB:C0:DE:06: 20:BB:C0:DE:06:AE		Cisco-IP-Phone-8941	Default >> MAB >> D...	Default >> Profiled Cs..	Cisco_IP_Phones	Cisco-IP-Phone	Authentication succeeded
2015-11-25 18:49:42.433	✓			#ACSACL#-IP-PE							DACL Download Succeeded
2015-11-25 18:49:42.417	✓			20:BB:C0:DE:06: 20:BB:C0:DE:06:AE		Cisco-IP-Phone-8941	Default >> MAB >> D...	Default >> Profiled Cs..	Cisco_IP_Phones	Cisco-IP-Phone	Authentication succeeded

에서 Administration > Identity Management > Identities > Endpoints > tested endpoint Radius 프로브가 수집한 속성의 종류와 해당 값은 다음과 같습니다.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for viewing endpoint attributes. The left sidebar shows a tree view with 'Users' and 'Endpoints' expanded. The main area displays a list of attributes and their values for a specific endpoint.

NAS-IP-Address	10.229.20.43
NAS-Port	60000
NAS-Port-Id	GigabitEthernet1/0/13
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	deskswitch
OUI	Cisco Systems, Inc
OriginalUserName	20bbc0de06ae
PolicyVersion	2
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthorizationProfiles	Cisco_IP_Phones
Service-Type	Call Check
StaticAssignment	false
StaticGroupAssignment	false
StepData	5= Radius.Service-Type, 6= Radius.NAS-Port-Type, 7=MAB, 10=Intern
Total Certainty Factor	210
UseCase	Host Lookup
User-Name	20-BB-C0-DE-06-AE
UserType	Host
cdpCachePlatform	Cisco IP Phone 8941
cdpUndefined28	00:02:00
ldpSystemDescription	Cisco IP Phone 8941, V3, SCCP 9-3-4-17

관찰할 수 있듯이, 이 시나리오에서 계산된 총 확실성 요소는 210입니다. 이는 엔드포인트가 Cisco-Device 프로파일(총 확실성 요인 30)과 Cisco-IP-Phone 프로파일(총 확실성 요인 40)과도 일치한다는 사실에서 비롯되었습니다. 프로파일러가 Cisco-IP-Phone-8941 프로파일의 두 조건을 모두 일치했으므로 이 프로파일의 확실성 요소는 140(프로파일링 정책에 따라 각 특성에 대해 70)입니다. 모두 합하면 30+40+70=210입니다.

문제 해결

1단계. CDP/LLDP에서 수집한 정보 확인

```
switch#sh cdp neighbors g1/0/13 detail ----- Device ID: SEP20BBC0DE06AE Entry address(es): Platform: Cisco IP Phone 8941 , Capabil
```

```
switch#
```

```
switch#sh lldp neighbors g1/0/13 detail
```

```
-----  
Chassis id: 0.0.0.0
```

```
Port id: 20BBC0DE06AE:P1
```

```
Port Description: SW Port
```

```
System Name: SEP20BBC0DE06AE.
```

```
System Description:
```

```
Cisco IP Phone 8941, V3, SCCP 9-3-4-17
```

```
Time remaining: 164 seconds
```

```
System Capabilities: B,T
```

```
Enabled Capabilities: B,T
```

```
Management Addresses - not advertised
```

```
Auto Negotiation - supported, enabled
```

```
Physical media capabilities:
```

```
1000baseT(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: 3
```

```
F/W revision: 0.0.1.0
```

```
S/W revision: SCCP 9-3-4-17
```

```
Serial number: PUC17140FBO
```

```
Manufacturer: Cisco Systems , Inc.
```

```
Model: CP-8941
```

```
Capabilities: NP, PD, IN
```

```
Device type: Endpoint Class III
```

```
Network Policy(Voice): VLAN 101, tagged, Layer-2 priority: 0, DSCP: 0
```

```
Network Policy(Voice Signal): VLAN 101, tagged, Layer-2 priority: 3, DSCP: 24
```

```
PD device, Power source: Unknown, Power Priority: Unknown, Wattage: 3.8
```

```
Location - not advertised
```

```
Total entries displayed: 1
```

수집된 데이터를 볼 수 없는 경우 다음을 확인합니다.

- 스위치에서 인증 세션의 상태를 확인합니다(성공해야 함).

piborowi#show authentication sessions int g1/0/13 details Interface: GigabitEthernet1/0/13 MAC Address: 20bb.c0de.06ae IPv6 Address: Unknown IPv4 A

- CDP 및 LLDP 프로토콜이 활성화되어 있는지 확인합니다. CDP/LLDP/등과 관련된 기본이 아닌 명령이 있는지, 그리고 이 러한 명령이 엔드포인트의 특성 검색에 어떤 영향을 미칠 수 있는지 확인합니다

```
switch#sh running-config all | in cdp run
cdp run
switch#sh running-config all | in lldp run
lldp run
```

- CDP/LLDP/등을 지원하는 엔드포인트의 컨피그레이션 가이드에서 확인하십시오.

2단계. 디바이스 센서 캐시 확인

switch#show device-sensor cache interface g1/0/13 Device: 20bb.c0de.06ae on port GigabitEthernet1/0/13 ----- Proto

이 필드에 데이터가 표시되지 않거나 정보가 완전하지 않은 경우 'device-sensor' 명령, 특히 filter-lists 및 filter-specs를 확인합니다.

3단계. Radius 어카운팅에 특성이 있는지 확인

스위치에서 명령을 사용하거나 debug radius 스위치와 ISE 간에 패킷 캡처를 수행하는지 확인할 수 있습니다.

Radius 디버그:

<#root>

Mar 30 05:34:58.716: RADIUS(00000000): Send Accounting-Request to 1.1.1.1:1813 id 1646/85, len 378 Mar 30 05:34:58.716: RADIUS: authenticator 1

cdp-tlv

= " Mar 30 05:34:58.716: RADIUS: Vendor, Cisco [26] 23 Mar 30 05:34:58.716: RADIUS: Cisco AVpair [1] 17

cdp-tlv


```

= " Mar 30 05:34:58.721: RADIUS: Vendor, Cisco [26] 59 Mar 30 05:34:58.721: RADIUS: Cisco AVpair [1] 53
lldp-tlv
= " Mar 30 05:34:58.721: RADIUS: User-Name [1] 19 "20-BB-C0-DE-06-AE" Mar 30 05:34:58.721: RADIUS: Vend

```

패킷 캡처:

Filter: radius.code==4

No.	Time	Source	Destination	Protocol	Length	Info
27	2015-11-25 21:51:52.233942	10.229.20.43	10.62.145.51	RADIUS	432	Accounting-Request(4) (id=86, l=390)
77	2015-11-25 21:52:02.860652	10.229.20.43	10.62.145.51	RADIUS	333	Accounting-Request(4) (id=87, l=291)

Frame 27: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits)

Ethernet II, Src: 58:f3:9c:6e:45:c3 (58:f3:9c:6e:45:c3), Dst: 00:50:56:9c:49:54 (00:50:56:9c:49:54)

Internet Protocol Version 4, Src: 10.229.20.43 (10.229.20.43), Dst: 10.62.145.51 (10.62.145.51)

User Datagram Protocol, Src Port: 1646 (1646), Dst Port: 1813 (1813)

Radius Protocol

- Code: Accounting-Request (4)
- Packet identifier: 0x56 (86)
- Length: 390
- Authenticator: 7008a6239a5f3ddbcee380d648c4782d
- [\[The response to this request is in frame 28\]](#)
- Attribute Value Pairs
 - AVP: l=40 t=Vendor-Specific(26) v=ciscoSystems(9)
 - VSA: l=34 t=Cisco-AVPair(1): cdp-tlv=0000000024Cisco IP Phone 8941
 - AVP: l=23 t=Vendor-Specific(26) v=ciscoSystems(9)
 - VSA: l=17 t=Cisco-AVPair(1): cdp-tlv=000034000003000002000
 - AVP: l=59 t=Vendor-Specific(26) v=ciscoSystems(9)
 - VSA: l=53 t=Cisco-AVPair(1): lldp-tlv=0000060000&Cisco IP Phone 8941, V3, SCCP 9-3-4-17
 - AVP: l=19 t=User-Name(1): 20-BB-C0-DE-06-AE
 - AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
 - AVP: l=19 t=Vendor-Specific(26) v=ciscoSystems(9)
 - AVP: l=18 t=Vendor-Specific(26) v=ciscoSystems(9)
 - AVP: l=19 t=Called-Station-Id(30): F0-29-29-49-67-0D
 - AVP: l=19 t=Calling-Station-Id(31): 20-BB-C0-DE-06-AE
 - AVP: l=6 t=NAS-IP-Address(4): 10.229.20.43
 - AVP: l=6 t=NAS-Port(5): 60000
 - AVP: l=23 t=NAS-Port-Id(87): GigabitEthernet1/0/13
 - AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
 - AVP: l=10 t=Acct-Session-Id(44): 00000018
 - AVP: l=6 t=Acct-Terminate-Cause(49): Unknown(0)
 - AVP: l=6 t=Acct-Status-Type(40): Stop(2)
 - AVP: l=6 t=Event-Timestamp(55): Mar 30, 2011 07:37:53.000000000 Central European Daylight Time
 - AVP: l=6 t=Acct-Session-Time(46): 175
 - AVP: l=6 t=Acct-Input-Octets(42): 544411
 - AVP: l=6 t=Acct-Output-Octets(43): 3214015
 - AVP: l=6 t=Acct-Input-Packets(47): 1706
 - AVP: l=6 t=Acct-Output-Packets(48): 35467
 - AVP: l=6 t=Acct-Delay-Time(41): 0

4단계. ISE에서 프로파일러 디버깅 확인

특성이 스위치에서 전송된 경우 ISE에서 수신되었는지 확인할 수 있습니다. 이를 확인하려면 올바른 PSN 노드(Administration > System > Logging > Debug Log Configuration > PSN > profiler > debug)에 대한 프로파일러 디버깅을 활성화하고 엔드포인트의 인증을 한 번 더 수행합니다.

다음 정보를 확인하십시오.

- Radius 프로브가 특성을 받았음을 나타내는 디버그:

```
<#root>
```

```

2015-11-25 19:29:53.641 DEBUG [RADIUSParser-1-thread-1][]
cisco.profiler.probes.radius.RadiusParser -:-
MSG_CODE=[3002], VALID=[true], PRRT_TIMESTAMP=[2015-11-25 19:29:53.637 +00:00],
ATTRS=[Device IP Address=10.229.20.43, RequestLatency=7,
NetworkDeviceName=deskswitch, User-Name=20-BB-C0-DE-06-AE,

```

NAS-IP-Address=10.229.20.43, NAS-Port=60000, Called-Station-ID=F0-29-29-49-67-0D,
Calling-Station-ID=20-BB-C0-DE-06-AE, Acct-Status-Type=Interim-Update,
Acct-Delay-Time=0, Acct-Input-Octets=362529, Acct-Output-Octets=2871426,
Acct-Session-Id=00000016, Acct-Input-Packets=1138, Acct-Output-Packets=32272,
Event-Timestamp=1301458555, NAS-Port-Type=Ethernet, NAS-Port-Id=GigabitEthernet1/0/13,

cisco-av-pair=cdp-tlv=cdpCachePlatform=Cisco IP Phone 8941

cisco-av-pair=cdp-tlv=cdpUndefined28=00:02:00,

cisco-av-pair=lldp-tlv=lldpSystemDescription=Cisco IP Phone 8941\, V3\, SCCP 9-3-4-17,

**cisco-av-pair=audit-session-id=0AE5182000002040099C216, cisco-av-pair=vlan-id=101,
cisco-av-pair=method=mab, AcsSessionID=ise13/235487054/2511, SelectedAccessService=Default Network Acce
Step=11004, Step=11017, Step=15049, Step=15008, Step=15004, Step=11005, NetworkDeviceGroups=Location#A1
NetworkDeviceGroups=Device Type#All Device Types, Service-Type=Call Check, CPMSessionID=0AE51820000020
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All Device Typ**

- 특성이 성공적으로 구문 분석되었음을 나타내는 디버그:

2015-11-25 19:29:53,642 DEBUG [RADIUSParser-1-thread-1][] cisco.profiler.probes.radius.RadiusParser -:::- Parsed IOS Sensor 1: cdpCachePlatform=[

- 전달자가 특성을 처리함을 나타내는 디버그:

<#root>

2015-11-25 19:29:53,643 DEBUG [forwarder-6][] cisco.profiler.infrastructure.probemgr.Forwarder -:20:BB:C0:DE:06:AE:ProfilerCollection:- Endpoint A

Attribute:cdpCachePlatform value:Cisco IP Phone 8941 Attribute:cdpUndefined28 value:00:02:00 Attribute:I

Attribute:SkipProfiling value:false



참고: 전달자는 Cisco ISE 데이터베이스에 엔드포인트를 특성 데이터와 함께 저장한 다음 네트워크에서 탐지된 새 엔드포인트를 분석기에 알립니다. 분석기는 엔드포인트를 엔드포인트 ID 그룹으로 분류하고 일치하는 프로필이 있는 엔드포인트를 데이터베이스에 저장합니다.

5단계. 새 특성 및 장치 할당 프로파일링

일반적으로 특정 디바이스의 기존 컬렉션에 새 특성이 추가된 후 이 디바이스/엔드포인트는 새 특성을 기반으로 다른 프로필을 할당해야 하는지 확인하기 위해 프로파일링 큐에 추가됩니다.

<#root>

2015-11-25 19:29:53,646 DEBUG [EndpointHandlerWorker-6-31-thread-1][

cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Classify hierarchy 20:BB:C0:DE:06:AE

2015-11-25 19:29:53,656 DEBUG [EndpointHandlerWorker-6-31-thread-1] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Policy Cisco-Device matched 20:BB:C0:DE:06:AE (certainty 30)

2015-11-25 19:29:53,659 DEBUG [EndpointHandlerWorker-6-31-thread-1] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Policy Cisco-IP-Phone matched 20:BB:C0:DE:06:AE (certainty 40)

2015-11-25 19:29:53,663 DEBUG [EndpointHandlerWorker-6-31-thread-1] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Policy Cisco-IP-Phone-8941 matched 20:BB:C0:DE:06:AE (certainty 140)

2015-11-25 19:29:53,663 DEBUG [EndpointHandlerWorker-6-31-thread-1] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

After analyzing policy hierarchy: Endpoint: 20:BB:C0:DE:06:AE EndpointPolicy: Cisco-IP-Phone-8941 for: 210

관련 정보

- <https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html>
- https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html
- [Cisco 기술 지원 및 다운로드](#)

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.