ISE 2.7 pxGrid CCV 3.1.0 통합 구성

목차

소개

이 문서에서는 pxGrid(Platform Exchange Grid v2)를 통해 Cisco CCV(Cyber Vision) 3.1.0과의 ISE(Identity Services Engine) 2.7 통합을 구성하고 문제를 해결하는 방법에 대해 설명합니다 .CCV는 pxGrid v2에 게시자로 등록되며 IOTASSET Dictionary용 엔드포인트 특성에 대한 정보를 ISE에 게시합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- ISE
- Cisco 사이버 비전

사용되는 구성 요소

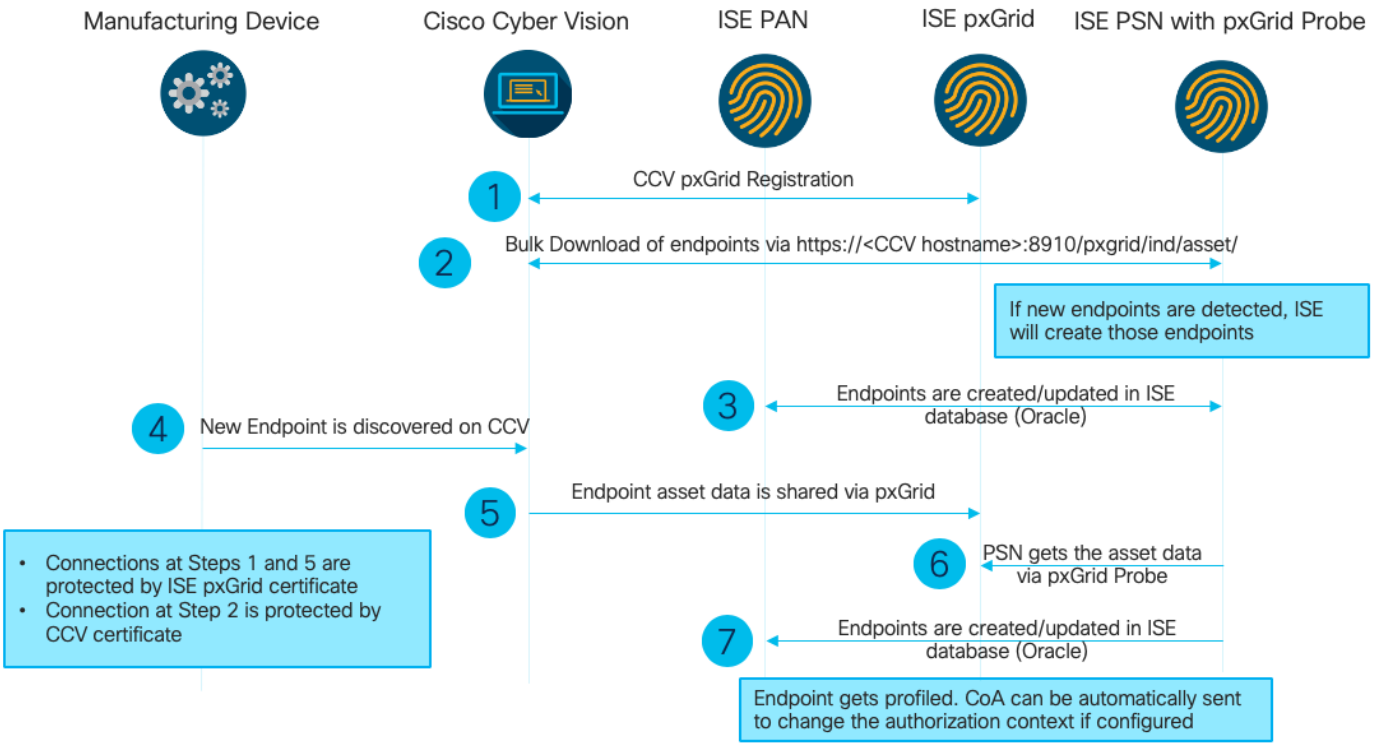
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 2.7 패치 1
- Cisco Cyber Vision 버전 3.1.0
- Industrial Ethernet Switch IE-4000-4TC4G-E with s/w 15.2(6)E

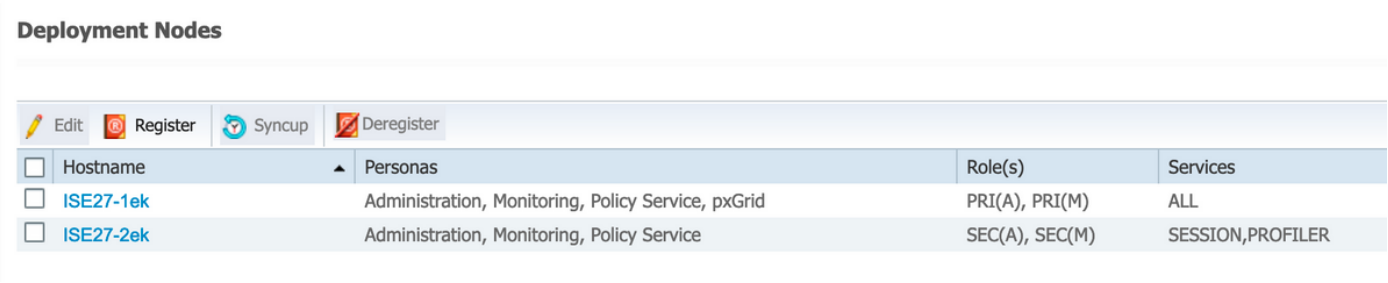
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

상위 레벨 플로우 다이어그램



이 ISE 구축은 설정에서 사용됩니다.



ISE 2.7-1ek는 PAN(Primary Admin Node) 노드와 pxGrid Node입니다.

ISE 2.7-2ek는 pxGrid 프로브가 활성화된 PSN(Policy Service Node)입니다.

앞서 설명한 다이어그램에 해당하는 단계는 다음과 같습니다.

1. CCV는 pxGrid 버전 2를 통해 ISE의 assetTopic에 등록합니다. CCV의 해당 로그:

참고:CCV에서 pxGrid 로그를 검토하려면 다음 명령 **journalctl -u pxgrid-agent를 실행합니다.**

```
root@center:~# journalctl -u pxgrid-agent -f
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent RPC server listening to:
'/tmp/pxgrid-agent.sock' [caller=main.go:102]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/AccountActivate body={}
[caller=control.go:127]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Account activated
[caller=pxgrid.go:76]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/ServiceRegister
body={"name":"com.cisco.endpoint.asset","properties":{"assetTopic":"/topic/com.cisco.endpoint.as
set
```

```
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Service registered, ID:
4b9af94b-9255-46df-b5ef-24bdbba99f3a
[caller=pxgrid.go:94]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/ServiceLookup
body={"name":"com.cisco.ise.pubsub"} [caller=control.go:127]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/AccessSecret
body={"peerNodeName":"com.cisco.ise.pubsub"} [caller=control.go:127]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Websocket connect
url=wss://ISE27-1ek.example.com:8910/pxgrid/ise/pubsub [caller=endpoint.go:102]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent STOMP CONNECT host=10.48.17.86
[caller=endpoint.go:111]
Jun 24 13:33:27 center pxgrid-agent-start.sh[1310]: pxgrid-agent API: getSyncStatus
[caller=sync_status.go:34]
Jun 24 13:33:28 center pxgrid-agent-start.sh[1310]: pxgrid-agent Cyber Vision is in sync with
ISE [caller=assets.go:67]
Jun 24 13:36:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/ServiceReregister
body={"id":"4b9af94b-9255-46df-b5ef-24bdbba99f3a"} [caller=control.go:127]
```

2. pxGrid 프로브가 활성화된 ISE PSN은 기존 pxGrid 에셋(profiler.log)을 대량 다운로드합니다.

```
2020-06-24 13:41:37,091 DEBUG [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Looking for new publishers ...
2020-06-24 13:41:37,104 DEBUG [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Existing services are:
[Service [name=com.cisco.endpoint.asset, nodeName=cv-jens,
properties={assetTopic=/topic/com.cisco.endpoint.asset,
restBaseUrl=https://Center:8910/pxgrid/ind/asset/,
wsPubsubService=com.cisco.ise.pubsub}]]
2020-06-24 13:41:37,104 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- New services are: []
2020-06-24 13:41:37,114 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- NODENAME:cv-jens
2020-06-24 13:41:37,114 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- REQUEST
BODY{"offset":"0","limit":"500"}
2020-06-24 13:41:37,158 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Response status={}200
2020-06-24 13:41:37,159 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Content: {OUT_OF_SYNC}
2020-06-24 13:41:37,159 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Status is :{OUT_OF_SYNC}
2020-06-24 13:41:37,159 DEBUG [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-
Static set after adding new services: [Service [name=com.cisco.endpoint.asset,
nodeName=cv-jens, properties={assetTopic=/topic/com.cisco.endpoint.asset,
restBaseUrl=https://Center:8910/pxgrid/ind/asset/, wsPubsubService=com.cisco.ise.pubsub}]]
2020-06-24 13:41:37,169 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- NODENAME:cv-jens
2020-06-24 13:41:37,169 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- REQUEST
BODY{"offset":"0","limit":"500"}
2020-06-24 13:41:37,600 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Response status={}200
2020-06-24 13:41:37,604 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Content:
{"assets":[{"assetId":"88666e21-6eba-5c1e-b6a9-930c6076119d","assetName":"Xerox
0:0:0","assetIpAddress":"",
"assetMacAddress":"00:00:00:00:00:00","assetVendor":"XEROX
```

3. 엔드포인트는 pxGrid 프로브가 활성화된 PSN에 추가되고 PSN은 PAN에 지속 이벤트를 보내 이

러한 엔드포인트(profiler.log)를 저장합니다. ISE에서 생성된 엔드포인트는 Context Visibility(상황 가시성) 아래의 엔드포인트 세부사항에서 볼 수 있습니다.

```
2020-06-24 13:41:37,677 DEBUG [ProfilerINDSubscriberBulkRequestPool-77-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- mac address is :28:63:36:1e:10:05ip
address is :192.168.105.150
2020-06-24 13:41:37,677 DEBUG [ProfilerINDSubscriberBulkRequestPool-77-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- sending endpoint to
forwarder{"assetId":
"01c8f9dd-8538-5eac-a924-d6382ce3df2d","assetName":"Siemens
192.168.105.150","assetIpAddress":"192.168.105.150",
"assetMacAddress":"28:63:36:1e:10:05","assetVendor":"Siemens
AG","assetProductId":"","assetSerialNumber":"",
"assetDeviceType":"","assetSwRevision":"","assetHwRevision":"","assetProtocol":"ARP,
S7Plus","assetCustomAttributes":[],
"assetConnectedLinks":[]}
2020-06-24 13:41:37,677 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][]
cisco.profiler.infrastructure.probemgr.Forwarder -::::- Forwarder Mac 28:63:36:1E:10:05
MessageCode null epSource pxGrid Probe
2020-06-24 13:41:37,677 DEBUG [ProfilerINDSubscriberBulkRequestPool-77-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Endpoint is
proccessedEndPoint[id=<null>,name=<null>]
MAC: 28:63:36:1E:10:05
Attribute:BYODRegistration value:Unknown
Attribute:DeviceRegistrationStatus value:NotRegistered
Attribute:EndPointPolicy value:Unknown
Attribute:EndPointPolicyID value:
Attribute:EndPointSource value:pxGrid Probe
Attribute:MACAddress value:28:63:36:1E:10:05
Attribute:MatchedPolicy value:Unknown
Attribute:MatchedPolicyID value:
Attribute:NmapSubnetScanID value:0
Attribute:OUI value:Siemens AG
Attribute:PolicyVersion value:0
Attribute:PortalUser value:
Attribute:PostureApplicable value:Yes
Attribute:StaticAssignment value:false
Attribute:StaticGroupAssignment value:false
Attribute:Total Certainty Factor value:0
Attribute:assetDeviceType value:
Attribute:assetHwRevision value:
Attribute:assetId value:01c8f9dd-8538-5eac-a924-d6382ce3df2d
Attribute:assetIpAddress value:192.168.105.150
Attribute:assetMacAddress value:28:63:36:1e:10:05
Attribute:assetName value:Siemens 192.168.105.150
Attribute:assetProductId value:
Attribute:assetProtocol value:ARP, S7Plus
Attribute:assetSerialNumber value:
Attribute:assetSwRevision value:
Attribute:assetVendor value:Siemens AG
Attribute:ip value:192.168.105.150
Attribute:SkipProfiling value:false
```

4. 엔드포인트를 그룹에 배치한 후 CCV는 포트 8910을 통해 CUSTOMER 메시지를 전송하여 엔드포인트를 사용자 지정 특성의 그룹 데이터로 업데이트합니다.CCV의 해당 로그:

```
root@center:~# journalctl -u pxgrid-agent -f
Jun 24 14:32:04 center pxgrid-agent-start.sh[1216]: pxgrid-agent STOMP SEND
destination=/topic/com.cisco.endpoint.asset
body={"opType":"UPDATE","asset":{"assetId":"ce01ade2-eb6f-53c8-a646-9661b10c976e",
"assetName":"Cisco
```

```
a0:3a:59","assetIpAddress":"","assetMacAddress":"00:f2:8b:a0:3a:59","assetVendor":"Cisco
Systems, Inc",
"assetProductId":"","assetSerialNumber":"","assetDeviceType":"","assetSwRevision":"","assetHwRev
ision":"","assetProtocol":"",
"assetCustomAttributes":[{"key":"assetGroup","value":"Group1"},{"key":"assetCCVGrp","value":"Gro
up1"}],
"assetConnectedLinks":[]}} [caller=endpoint.go:118]
```

5. pxGrid 노드는 STOMP 업데이트를 수신하고 이 메시지를 모든 가입자에게 전달합니다. 여기에는 pxGrid 프로브가 활성화된 PSN이 포함됩니다.**pxGrid 노드의 pxgrid-server.log**에 있습니다.

```
2020-06-24 14:40:13,765 TRACE [Thread-1631][] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -
::::::-
stomp=SEND:{content-length=453, destination=/topic/com.cisco.endpoint.asset}
2020-06-24 14:40:13,766 TRACE [Thread-1631][] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -
::::::-
session [2b,cv-jens,OPEN] is permitted (cached) to send to
topic=/topic/com.cisco.endpoint.asset:
2020-06-24 14:40:13,766 TRACE [Thread-1631][]
cpm.pxgridwebapp.ws.pubsub.SubscriptionThreadedDistributor -::::::-
Distributing stomp frame from=[2b,cv-jens,OPEN], topic=/topic/com.cisco.endpoint.asset,
true:true
2020-06-24 14:40:13,766 TRACE [Thread-1631][]
cpm.pxgridwebapp.ws.pubsub.SubscriptionThreadedDistributor -::::::-
Distributing stomp frame from=[2b,cv-jens,OPEN],
topic=/topic/com.cisco.endpoint.asset,to=[19,ise-admin-ise27-2ek,OPEN]
2020-06-24 14:40:13,766 TRACE [Thread-1631][]
cpm.pxgridwebapp.ws.pubsub.SubscriptionThreadedDistributor -::::::-
Distributing stomp frame from=[2b,cv-jens,OPEN], topic=/topic/wildcard,to=[2a,ise-fanout-ise27-
1ek,OPEN]
```

6. 자산 항목의 가입자가 되는 pxGrid 프로브가 활성화된 PSN은 pxGrid 노드로부터 메시지를 수신하고 엔드포인트(profiler.log)를 업데이트합니다. ISE의 업데이트된 엔드포인트는 Context Visibility(상황 가시성) 아래의 엔드포인트 세부사항에서 볼 수 있습니다.

```
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-
Parsing push notification response: {"opType":"UPDATE","asset":{"assetId":"ce01ade2-eb6f-53c8-
a646-9661b10c976e",
"assetName":"Cisco
a0:3a:59","assetIpAddress":"","assetMacAddress":"00:f2:8b:a0:3a:59","assetVendor":"Cisco
Systems, Inc",
"assetProductId":"","assetSerialNumber":"","assetDeviceType":"","assetSwRevision":"","assetHwRev
ision":"",
"assetProtocol":"","assetCustomAttributes":[{"key":"assetGroup","value":"Group1"},{"key":"assetC
CVGrp","value":"Group1"}],
"assetConnectedLinks":[]}}
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-
sending endpoint to forwarder{"assetId":"ce01ade2-eb6f-53c8-a646-
9661b10c976e","assetName":"Cisco a0:3a:59","assetIpAddress":"",
"assetMacAddress":"00:f2:8b:a0:3a:59","assetVendor":"Cisco Systems,
Inc","assetProductId":"","assetSerialNumber":"",
"assetDeviceType":"","assetSwRevision":"","assetHwRevision":"","assetProtocol":"",
"assetCustomAttributes":[{"key":"assetGroup","value":"Group1"},{"key":"assetCCVGrp","value":"Gro
up1"}],"assetConnectedLinks":[]}
2020-06-24 14:40:13,768 INFO [Grizzly(2)][] cisco.profiler.infrastructure.probemgr.Forwarder -
::::-
Forwarder Mac 00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,768 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.probemgr.ForwarderHelper -:
00:F2:8B:A0:3A:59:87026690-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:- sequencing Radius
```

```
message for mac = 00:F2:8B:A0:3A:59
2020-06-24 14:40:13,768 INFO [forwarder-9][] cisco.profiler.infrastructure.probemgr.Forwarder -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:-
Processing endpoint:00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,768 DEBUG [forwarder-9][] com.cisco.profiler.im.EndPoint -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:-
filtered custom attributes are:{assetGroup=Group1, assetCCVGrp=Group1}
2020-06-24 14:40:13,768 DEBUG [forwarder-9][] cisco.profiler.infrastructure.probemgr.Forwarder -
:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:- Radius
Filtering:00:F2:8B:A0:3A:59
2020-06-24 14:40:13,768 DEBUG [forwarder-9][] cisco.profiler.infrastructure.probemgr.Forwarder -
:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:- Endpoint
Attributes:EndPoint[id=<null>,name=<null>]
MAC: 00:F2:8B:A0:3A:59
Attribute:2309ae60-693d-11ea-9cbe-02251d8f7c49 value:Group1
Attribute:BYODRegistration value:Unknown
Attribute:DeviceRegistrationStatus value:NotRegistered
Attribute:EndPointProfilerServer value:ISE27-2ek.example.com
Attribute:EndPointSource value:pxGrid Probe
Attribute:MACAddress value:00:F2:8B:A0:3A:59
Attribute:NmapSubnetScanID value:0
Attribute:OUI value:Cisco Systems, Inc
Attribute:PolicyVersion value:0
Attribute:PortalUser value:
Attribute:PostureApplicable value:Yes
Attribute:assetDeviceType value:
Attribute:assetGroup value:Group1
Attribute:assetHwRevision value:
Attribute:assetId value:ce01ade2-eb6f-53c8-a646-9661b10c976e
Attribute:assetIpAddress value:
Attribute:assetMacAddress value:00:f2:8b:a0:3a:59
Attribute:assetName value:Cisco a0:3a:59
Attribute:assetProductId value:
Attribute:assetProtocol value:
Attribute:assetSerialNumber value:
Attribute:assetSwRevision value:
Attribute:assetVendor value:Cisco Systems, Inc
Attribute:SkipProfiling value:false
```

7. pxGrid 프로브가 활성화된 PSN은 새 정책이 일치함에 따라 엔드포인트를 다시 프로파일링합니다(profiler.log).

```
2020-06-24 14:40:13,773 INFO [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Classify Mac
00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,777 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Policy Cisco-Device matched
00:F2:8B:A0:3A:59 (certainty 10)
2020-06-24 14:40:13,777 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Policy ekorneyc_ASSET_Group1
matched 00:F2:8B:A0:3A:59 (certainty 20)
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- After analyzing policy
hierarchy: Endpoint:
00:F2:8B:A0:3A:59 EndpointPolicy:ekorneyc_ASSET_Group1 for:20 ExceptionRuleMatched:false
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
```

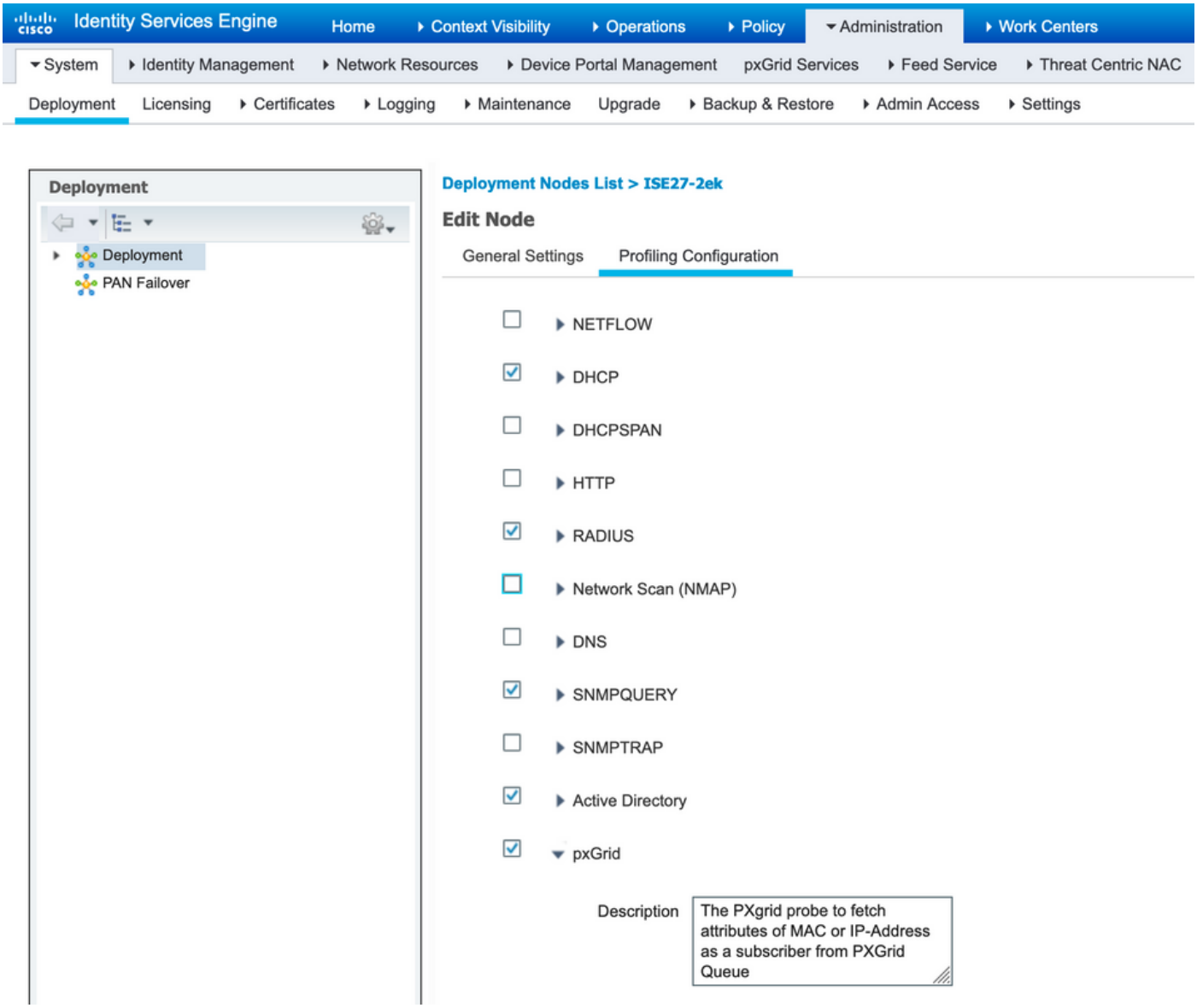
```
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
Matched Policy Changed.
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
IdentityGroup Changed.
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Setting identity group ID on
endpoint
00:F2:8B:A0:3A:59 - 91b0fd10-a181-11ea-a1a3-fe7d097d8c61
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Calling end point cache with
profiled end point
00:F2:8B:A0:3A:59, policy ekorneyc_ASSET_Group1, matched policy ekorneyc_ASSET_Group1
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Sending event to persist end
point
00:F2:8B:A0:3A:59, and ep message code = null
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
IdentityGroup / Logical Profile Changed. Issuing a Conditional CoA
```

구성

> **참고:**assetGroup 및 Context Visibility에 대한 가시성만 확보하려는 경우에도 1~4단계가 필요합니다.

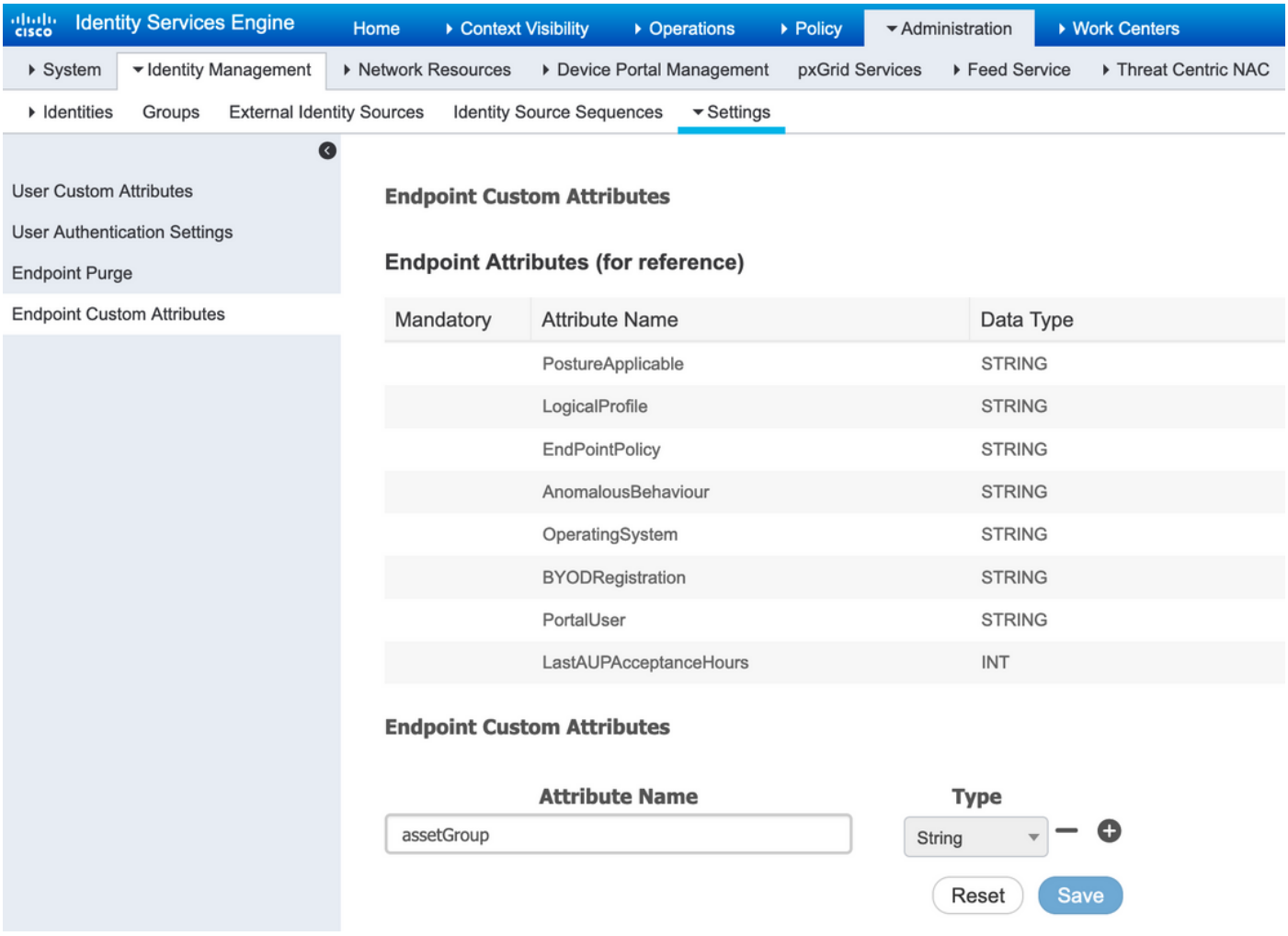
1. PSN 중 하나에서 pxGrid 프로브를 활성화합니다.

Administration(**관리) > System(시스템) > Deployment(구축)**로 이동하고 PSN Persona(PSN 페르소나)가 있는 ISE 노드를 선택합니다.Profiling **Configuration(프로파일링 컨피그레이션)** 탭으로 전환합니다.pxGrid 프로브가 활성화되었는지 확인합니다.



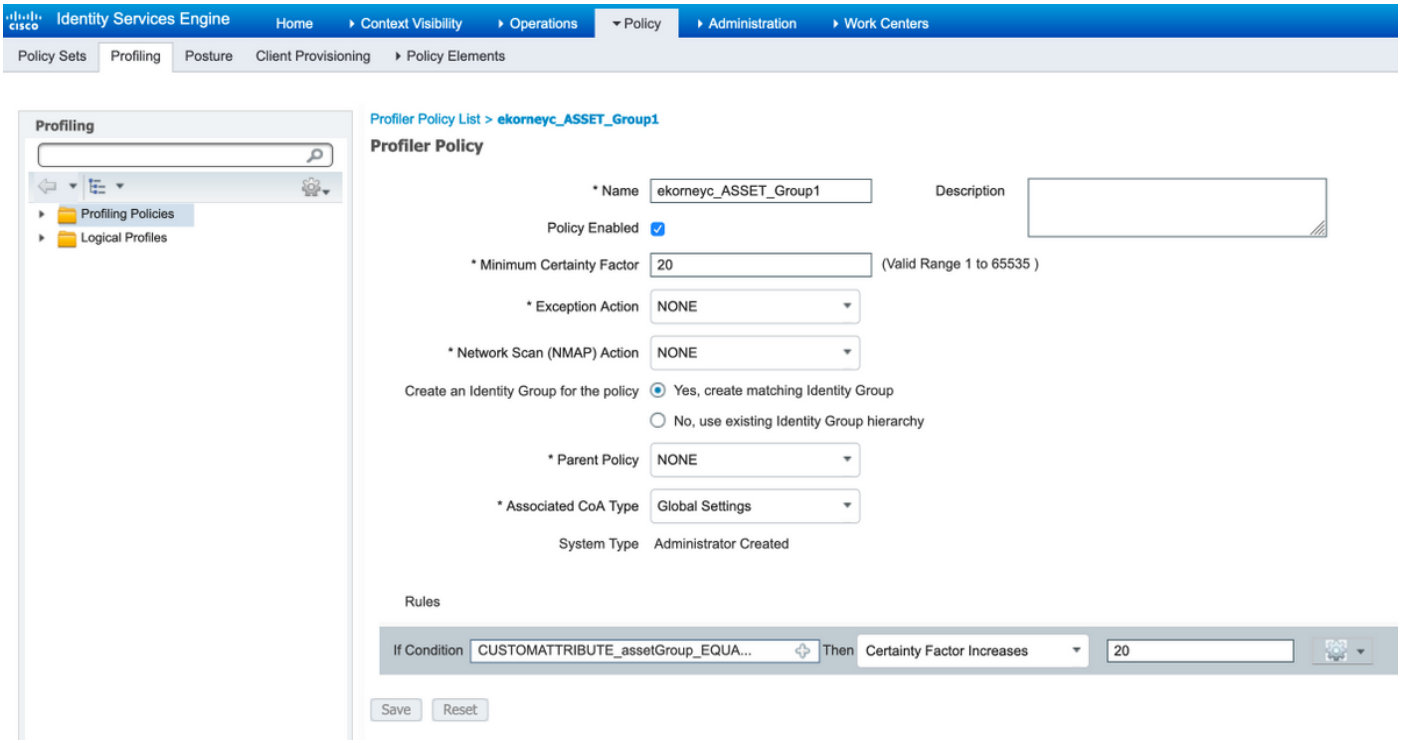
2. ISE에서 엔드포인트 사용자 지정 특성 구성

Administration(관리) **> Identity Management(ID 관리) > Settings(설정) > Endpoint Custom Attributes(엔드포인트 맞춤형 특성)로 이동합니다**.이 이미지에 따라 사용자 지정 특성(assetGroup)을 구성합니다.CCV 3.1.0은 Custom AssetGroup Attribute만 **지원합니다**.



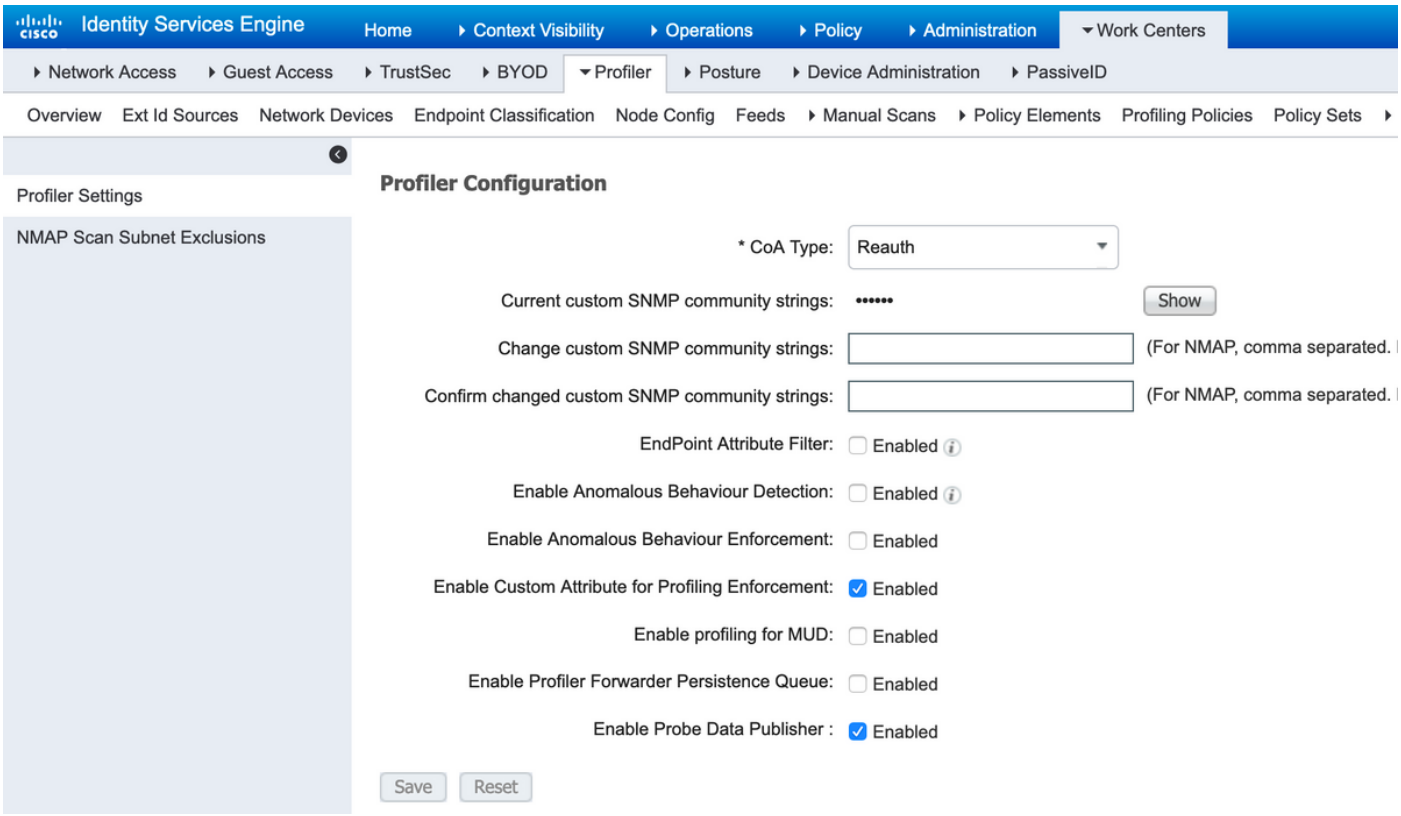
3. 사용자 지정 특성을 사용하여 프로파일러 정책 구성

Work Centers(**작업 센터) > Profiler(프로파일러) > Profiling Policies(프로파일링 정책)로 이동합니다**.Add(추가)를 **클릭합니다**.이 이미지와 유사한 프로파일러 정책을 구성합니다.이 정책에 사용된 조건 표현식은 CUSTOMATTRIBUTE:**assetGroup EQUALS Group1입니다.**



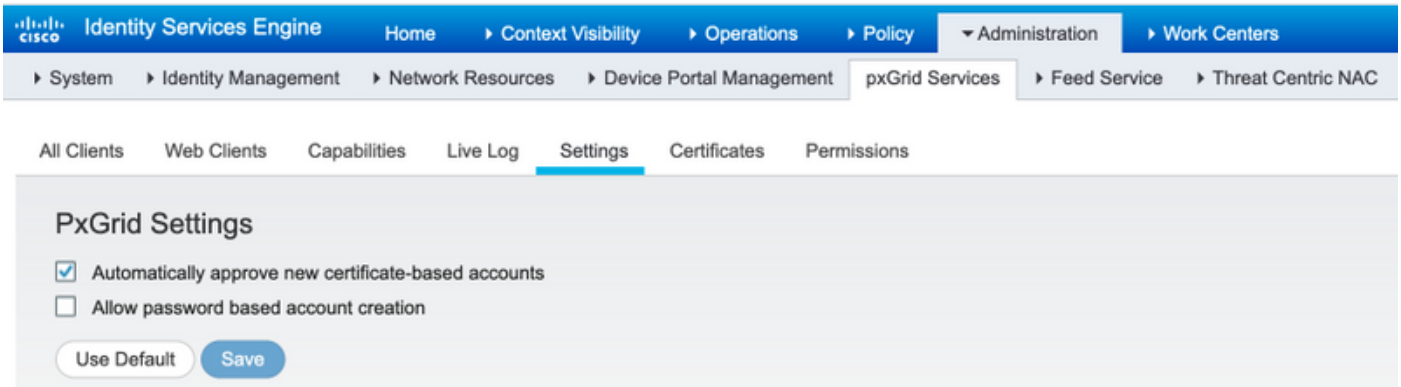
4. 프로파일링 시행을 위한 사용자 정의 속성 활성화

Work Centers(**작업 센터) > Profiler(프로파일러) > Profiling Policies(프로파일링 정책)로 이동합니다**.Add(추가)를 **클릭합니다**.이 이미지와 유사한 프로파일러 정책을 구성합니다.프로파일링 **시행을 위한 사용자 지정 특성 사용**이 활성화되었는지 확인합니다.



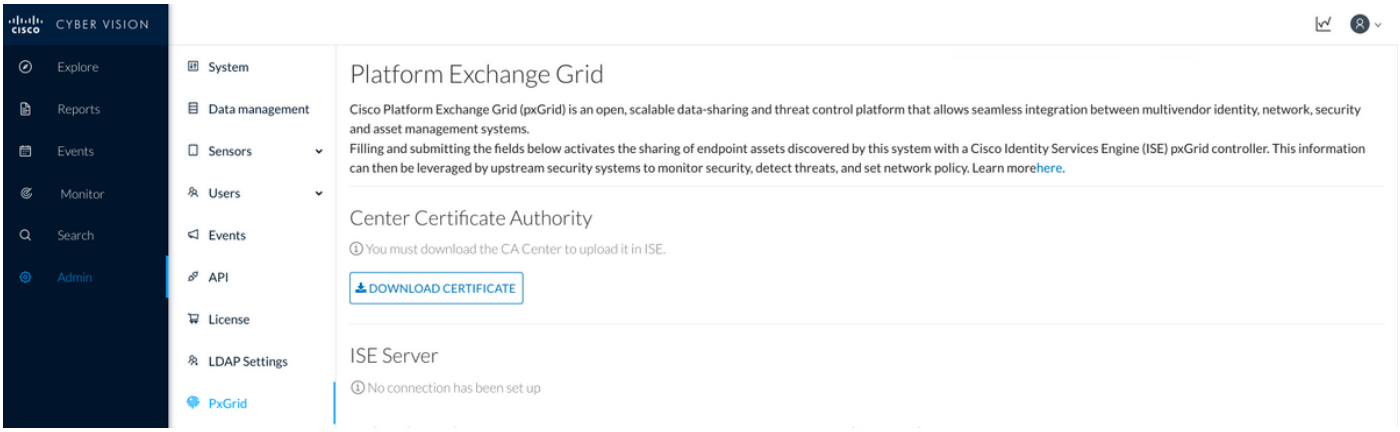
5. pxGrid 클라이언트에 대한 자동 승인 구성

Administration(관리) **> pxGrid Services(pxGrid 서비스) > Settings(설정)로 이동합니다** .Automatically approve **new certificate-based accounts(새 인증서 기반 계정 자동 승인)를** 선택하고 Save(저장)를 **클릭합니다**.이 단계를 수행하면 통합 후에는 CCV를 승인할 필요가 없습니다.



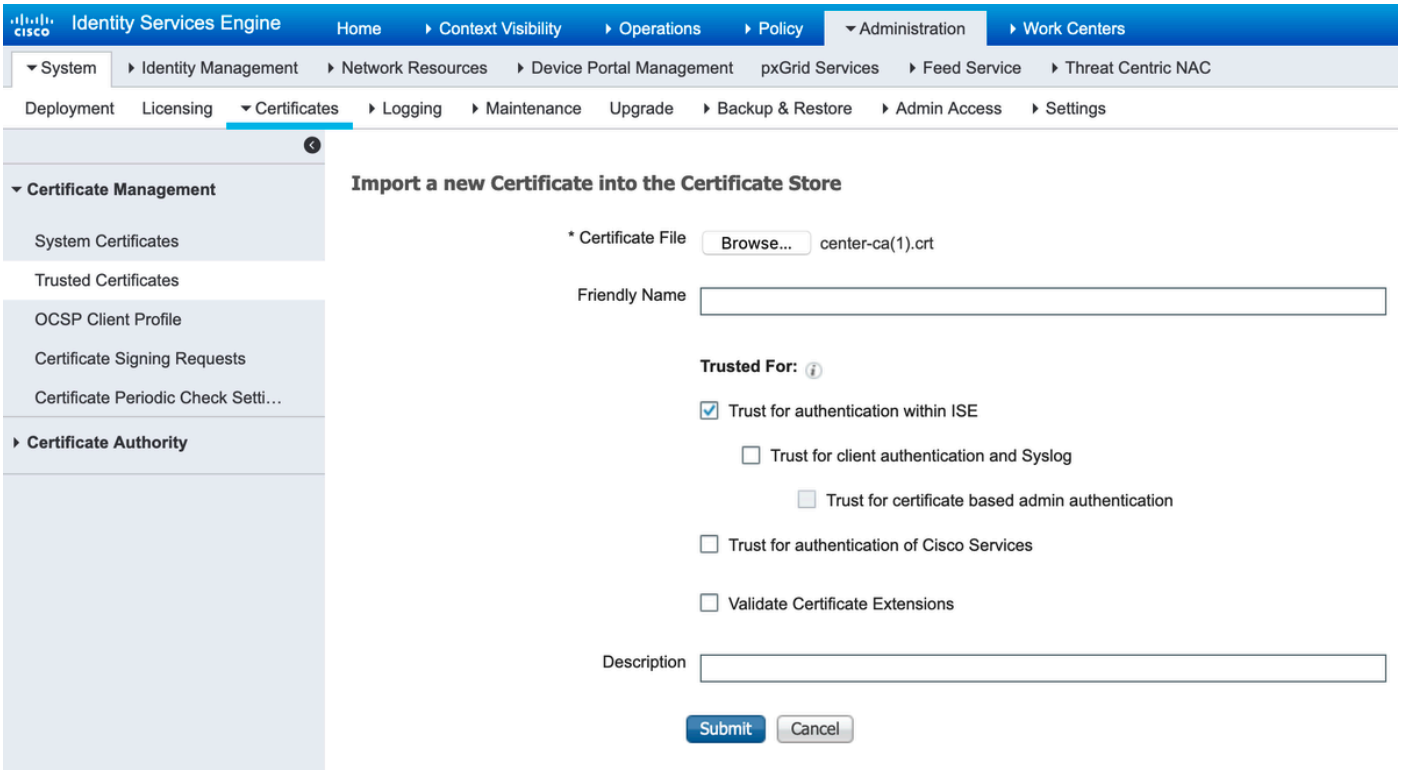
6. CCV 인증서 내보내기

Admin(관리) **> pxGrid로 이동합니다**.DOWNLOAD **CERTIFICATE를 클릭합니다**.이 인증서는 pxGrid 등록 중에 사용되므로 ISE에서 신뢰해야 합니다.



7. CCV ID 인증서를 ISE 신뢰할 수 있는 저장소에 업로드

Administration(관리) **> Certificates(인증서) > Certificate Management(인증서 관리) > Trusted Certificates(신뢰할 수 있는 인증서)로 이동합니다**.Import(가져오기)를 **클릭합니다**.Browse(찾아보기)를 **클릭하고** 5단계에서 CCV 인증서를 선택하고 Submit(제출)을 **클릭합니다**.



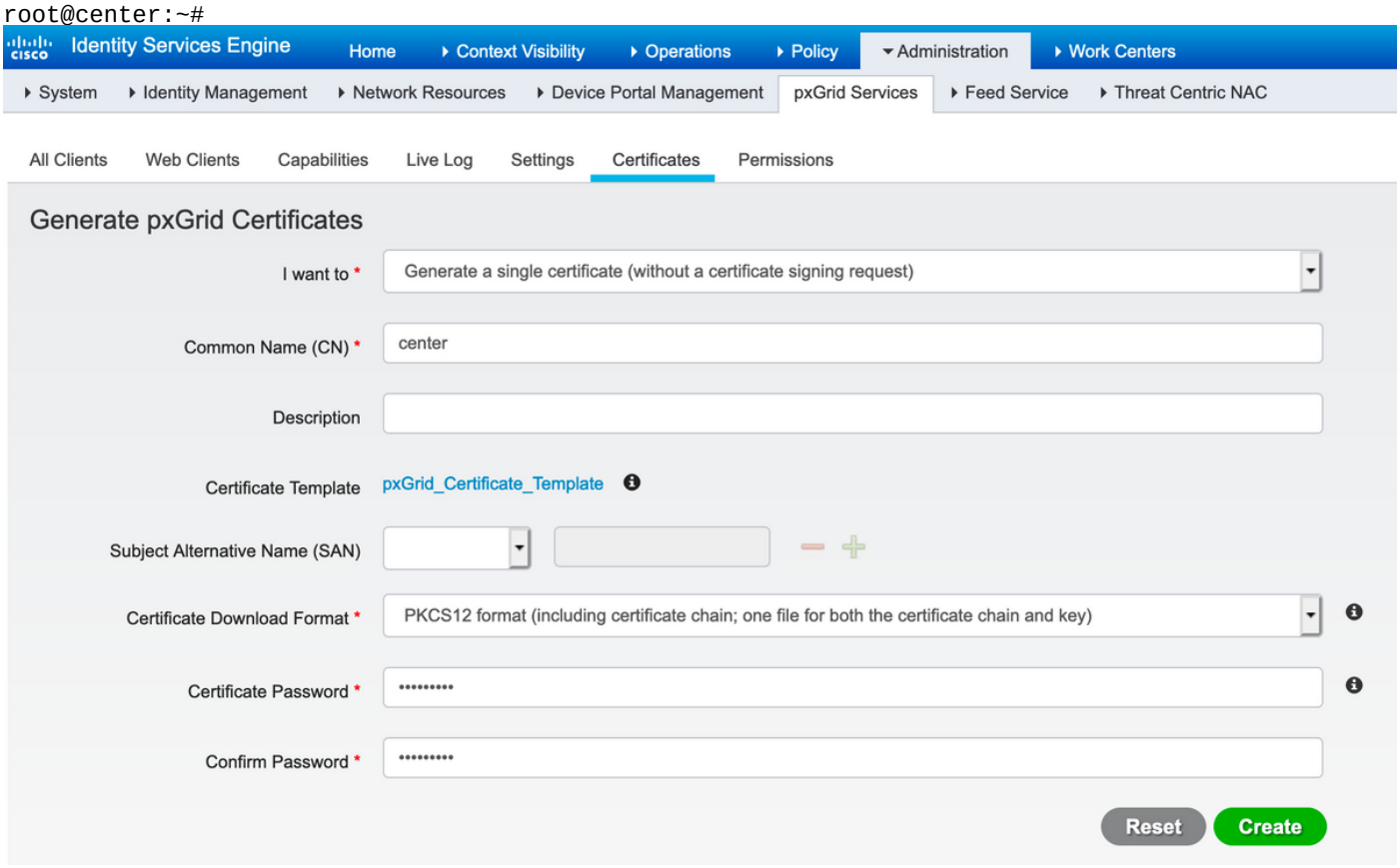
8. CCV용 인증서 생성

pxGrid 통합 및 업데이트 중에 CCV에는 클라이언트 인증서가 필요합니다 .PxGrid_**Certificate_Template**을 사용하여 ISE 내부 CA에서 **발행해야 합니다**.

Administration(관리) **> pxGrid Services(pxGrid 서비스) > Certificates(인증서)로 이동합니다**.이 이미지에 따라 필드를 채웁니다.ISE CA의 목표는 ID 인증서를 발급하기 때문에 CN(Common Name) 필드는 필수입니다.CCV의 호스트 이름을 입력해야 합니다. CN 필드 값은 중요합니다.CCV의 호스트 이름을 확인하려면 hostname 명령을 **실행합니다**.PKCS12를 **Certificate Download Format(인증서 다운로드 형식)으로 선택합니다.**

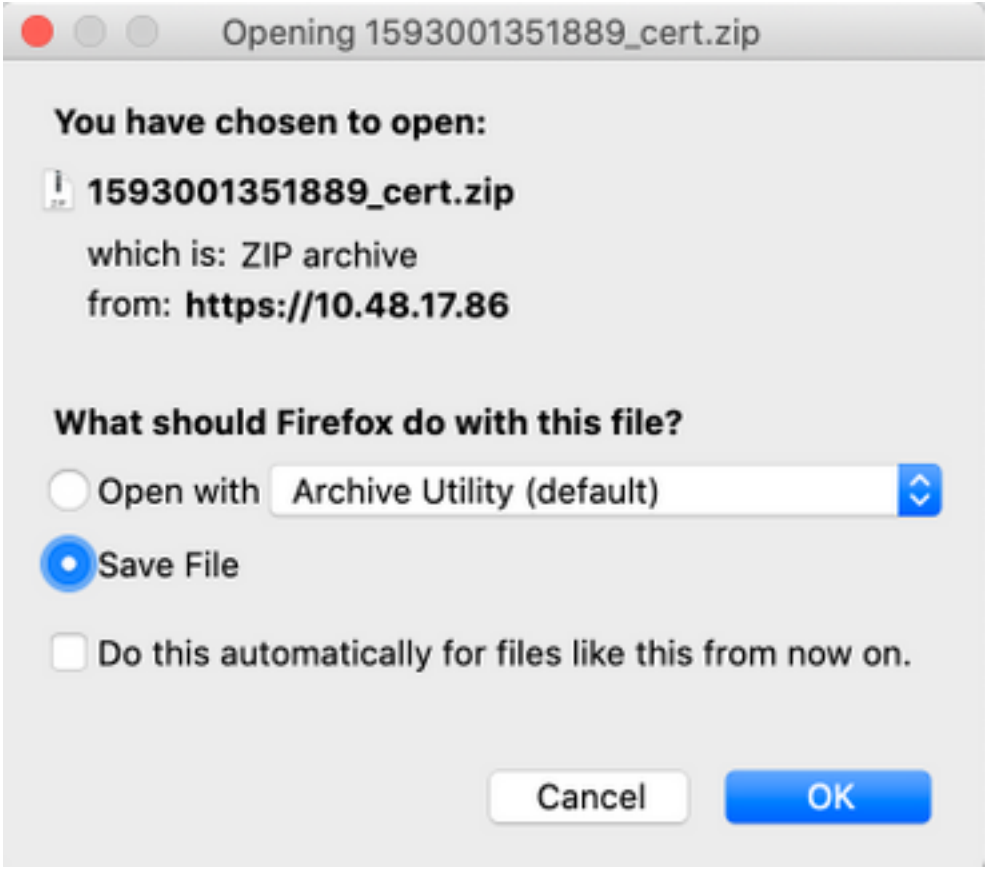
```
root@center:~# hostname
center
```

```
root@center:~#
```



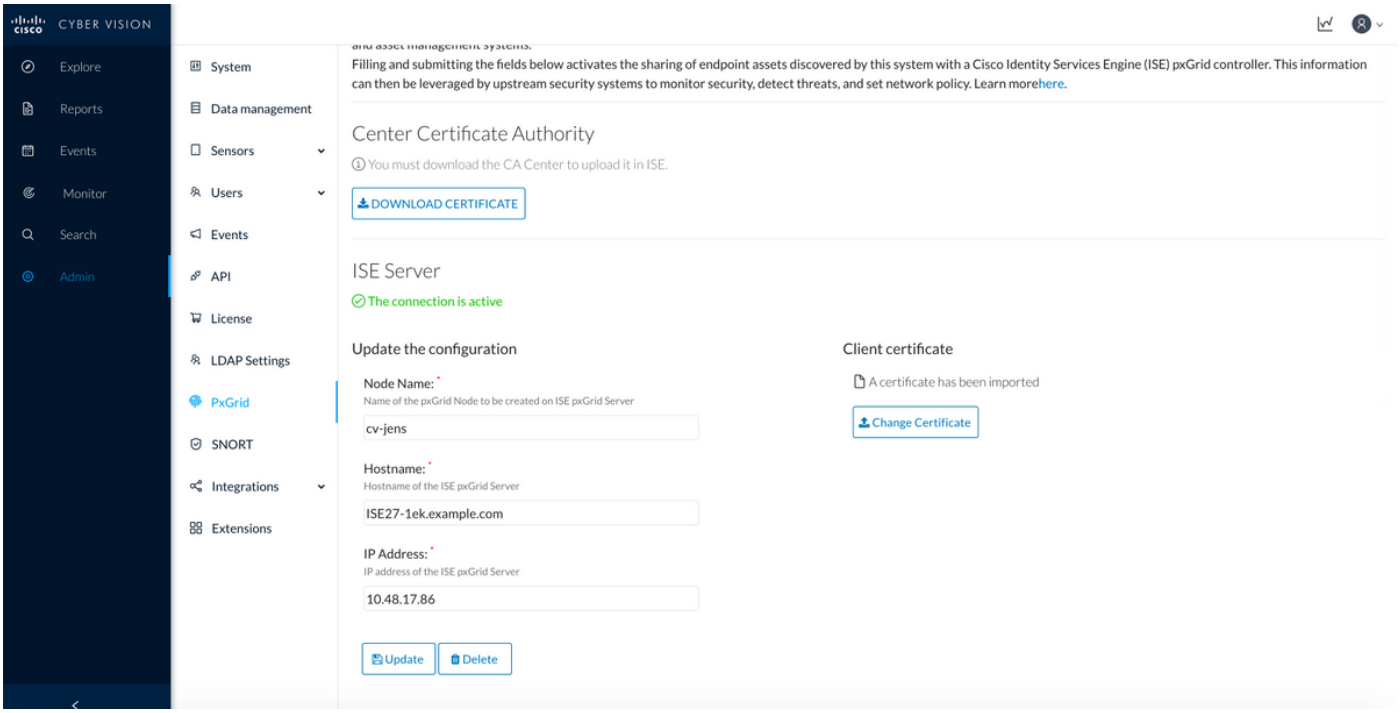
9. PKCS12 형식으로 인증서 체인 다운로드

CCV ID 인증서 ISE 내부 CA 체인과 함께 PKCS12 형식으로 인증서를 설치할 경우 pxGrid 통신이 ISE에서 시작될 때(예: pxGrid keepalive 메시지) CCV가 ISE를 신뢰하도록 CCV에 설치됩니다.



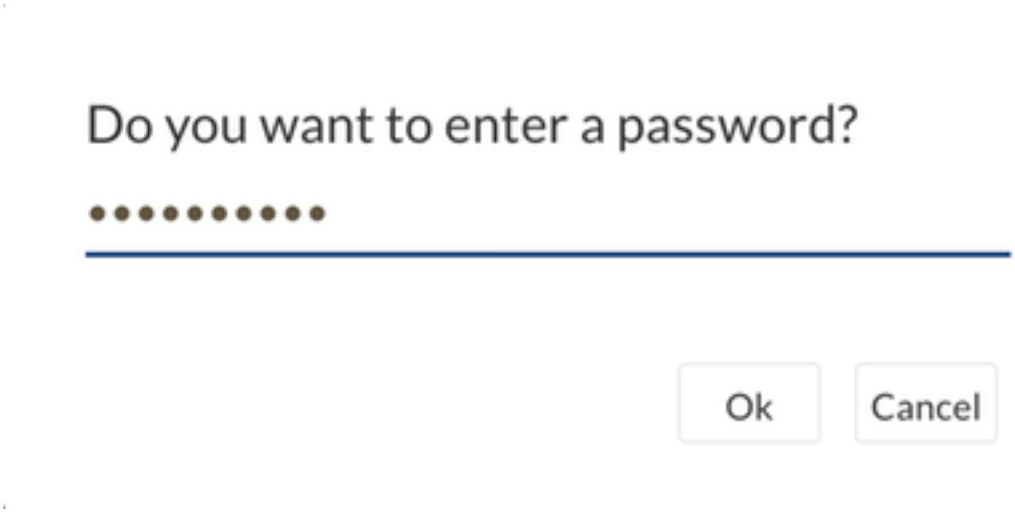
10. CCV에서 ISE 통합 세부 정보 구성

Admin(관리) **> pxGrid로 이동합니다**.노드 이름을 구성합니다. 이 이름은 ISE에 Administration(관리) > pxGrid **Services(pxGrid 서비스) > Web Clients(웹 클라이언트)**에서 클라이언트 이름으로 **표시됩니다.**ISE **pxGrid** 노드의 호스트 이름 및 IP 주소를 구성합니다.CCV에서 ISE FQDN을 확인할 수 있는지 확인합니다.



11. CCV에 인증서 체인 업로드 및 통합 시작

Admin(관리) **> pxGrid로 이동합니다**.Change **Certificate**(인증서 **변경)를 클릭합니다**.8-9단계에서 ISE CA에서 발급한 인증서를 선택합니다. 8단계에서 비밀번호를 입력하고 **확인**을 클릭합니다.



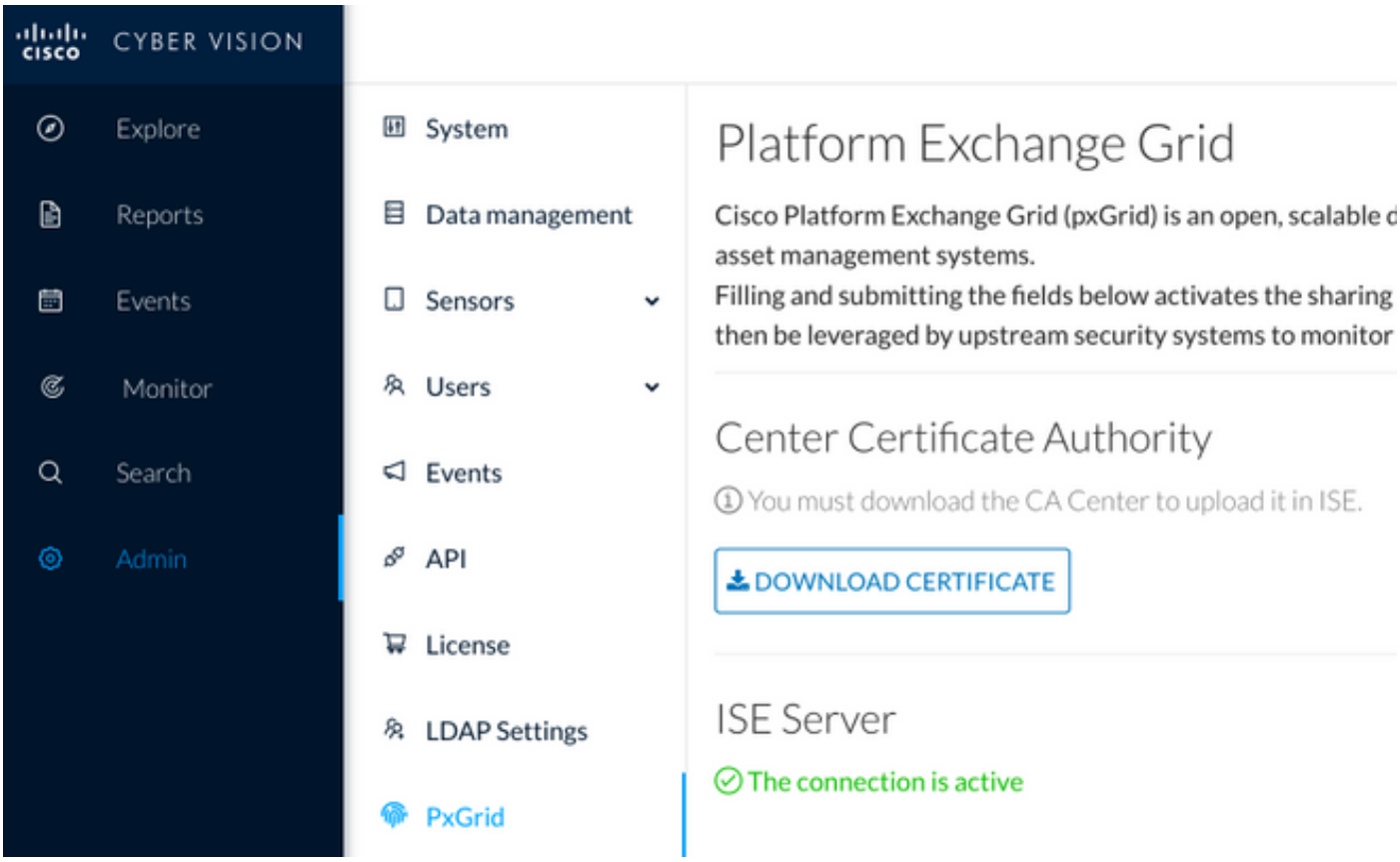
실제 CCV - ISE 통합을 트리거하는 **Update(업데이트**)를 클릭합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

CCV 통합 확인

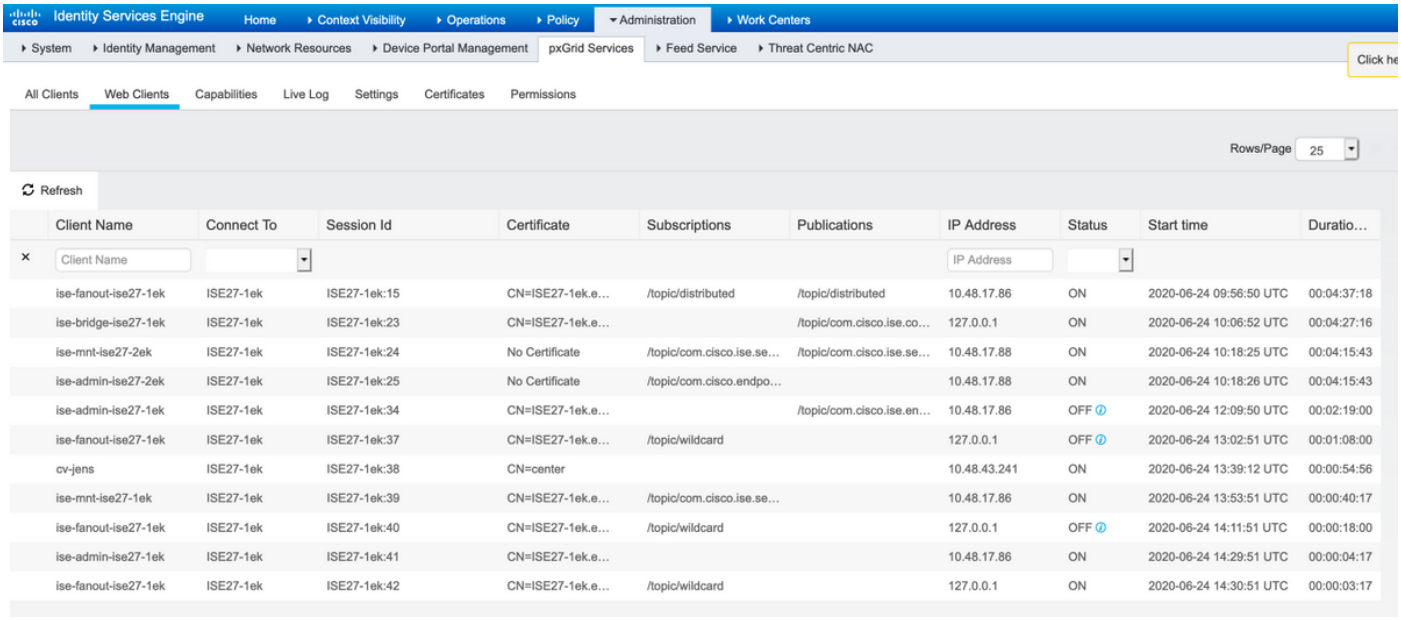
통합이 완료되면 Admin(관리) **> pxGrid**로 이동하여 성공적인 통합을 확인할 수 있습니다.ISE 서버에서 **The connection is active(연결이 활성** 상태임) 메시지가 표시되어야 합니다.



ISE 통합 확인

Administration(관리) **> pxGrid Services(pxGrid 서비스) > Web Clients(웹 클라이언트)로 이동합니다**.CCV 클라이언트(cv-jens)의 상태가 **ON인지 확인합니다.**

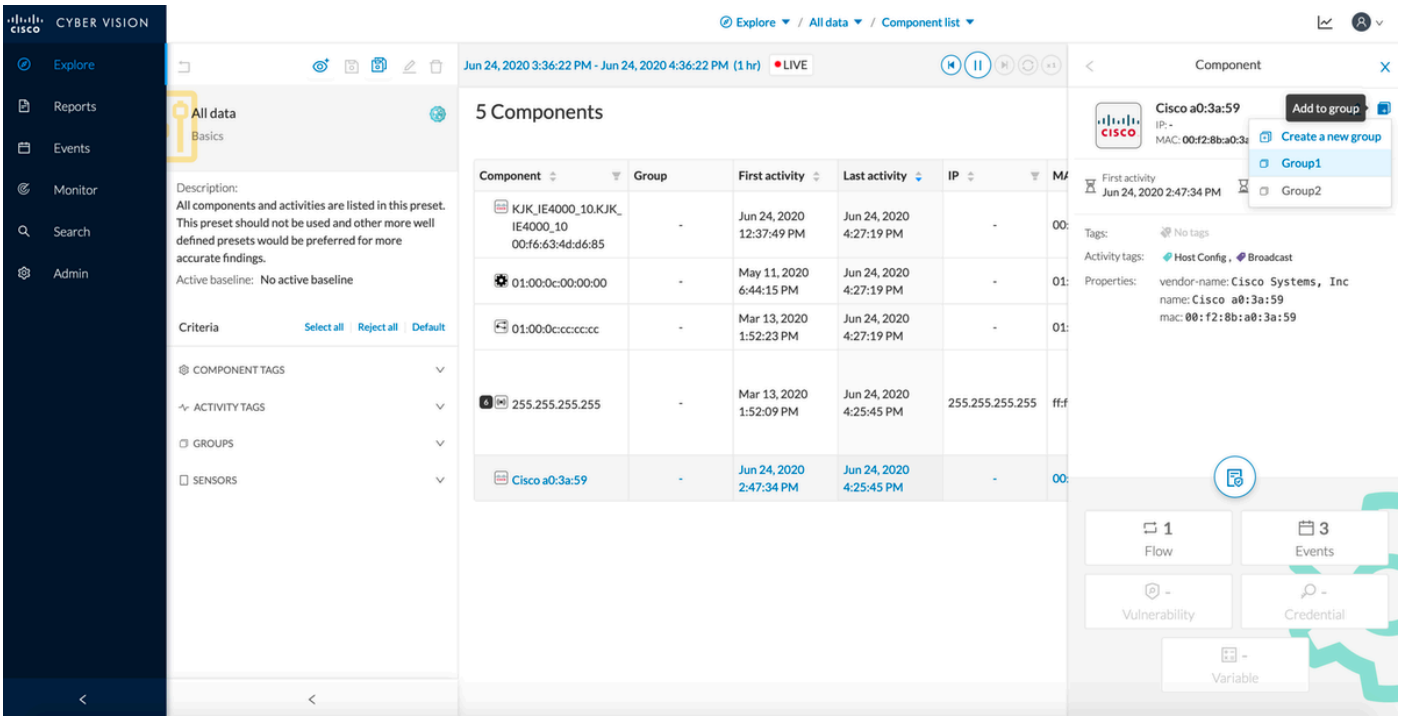
> **참고:**pxGrid v1 상태만 표시되므로 CCV pxGrid 클라이언트의 상태가 **All Clients** 메뉴에서 **Offline**(오프라인)으로 표시되어야 합니다.



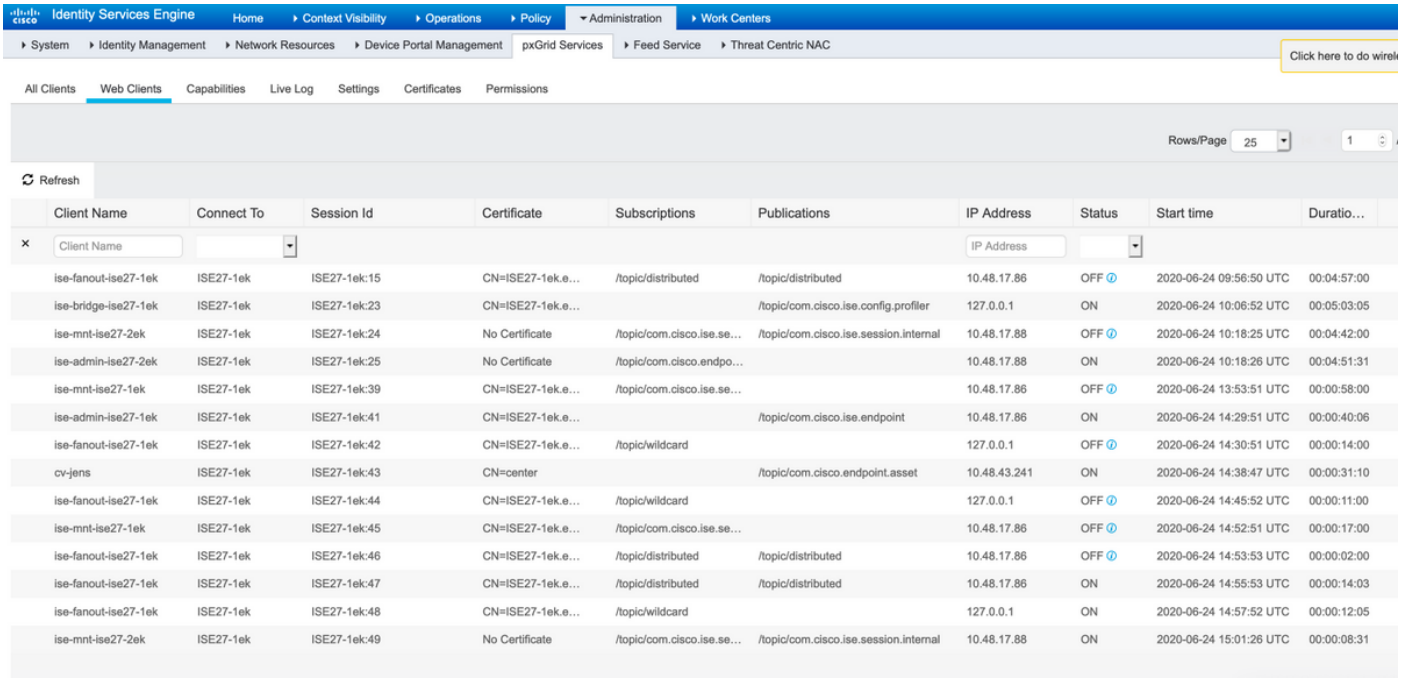
참고:CSCvt78208로 인해 CCV에 /topic/com.cisco.ise.endpoint.**asset이** 있는 것은 즉시 표시되지 않으며, 이는 첫 번째 게시 시에만 표시됩니다.

CCV 그룹 변경 확인

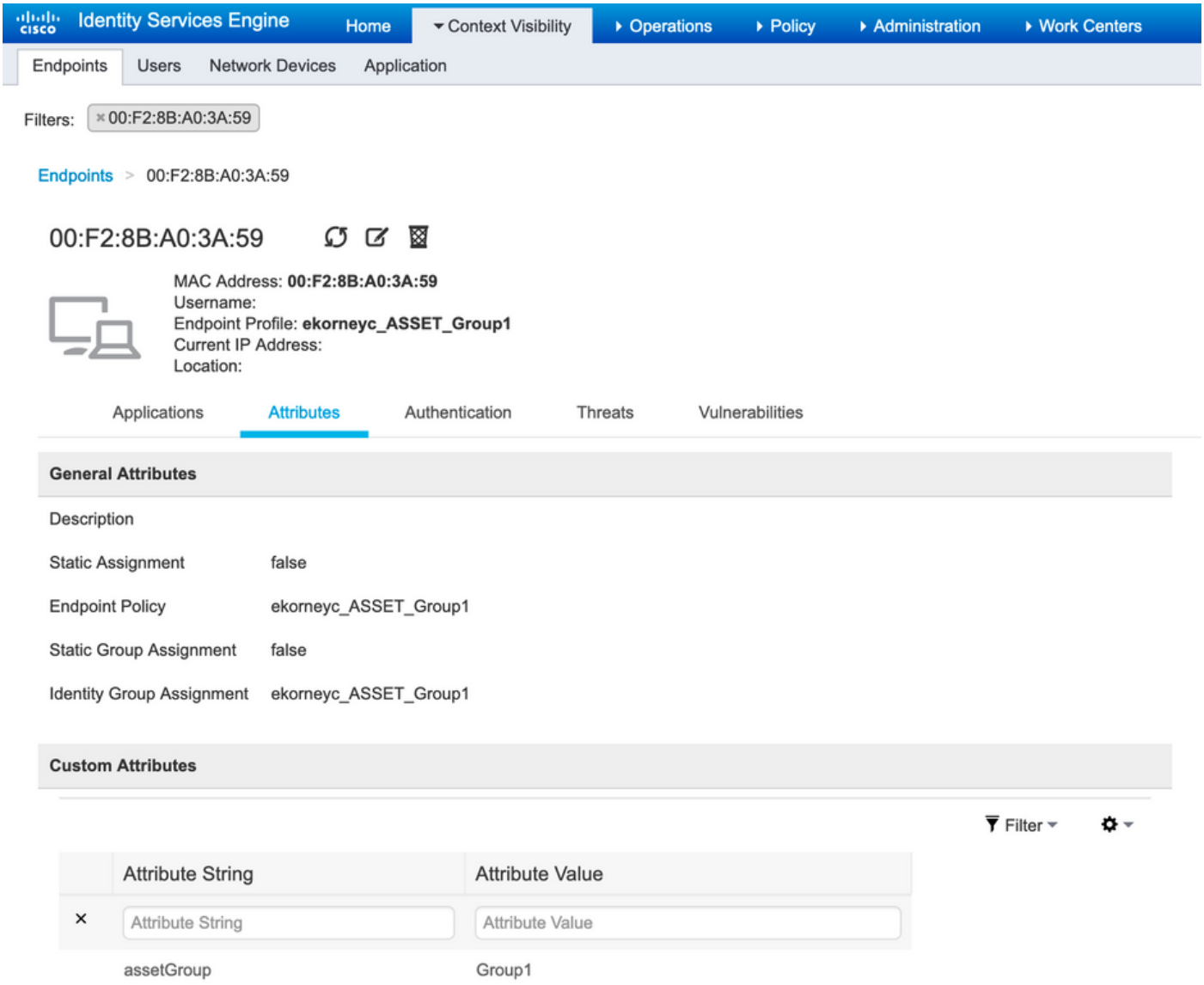
탐색 > **모든 데이터 > 구성 요소 목록으로 이동합니다**.구성 요소 중 하나를 클릭하고 **그룹에** 추가합니다.



/topic/com.cisco.**ise.endpoint.asset**이 CCV에 대한 게시물로 표시되는지 확인합니다.



CCV를 통해 할당된 Group1이 ISE에 반영되고 Context Visibility(상황 가시성) **> Endpoints(엔드포인트)**로 이동하여 프로파일링 정책이 적용되었는지 **확인합니다**.이전 단계에서 업데이트된 엔드포인트를 선택합니다.속성 탭으로 전환합니다.사용자 지정 특성 섹션은 새로 구성된 그룹을 반영해야 합니다.



다른 Attributes 섹션에는 CCV에서 수신한 기타 모든 자산 속성이 나열됩니다.

Other Attributes	
BYODRegistration	Unknown
DeviceRegistrationStatus	NotRegistered
ElapsedDays	0
EndPointPolicy	ekorneyc_ASSET_Group1
EndPointProfilerServer	ISE27-2ek.example.com
EndPointSource	pxGrid Probe
EndPointVersion	14
IdentityGroup	ekorneyc_ASSET_Group1
InactiveDays	0
MACAddress	00:F2:8B:A0:3A:59
MatchedPolicy	ekorneyc_ASSET_Group1
OUI	Cisco Systems, Inc
PolicyVersion	9
PostureApplicable	Yes
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	20
assetId	ce01ade2-eb6f-53c8-a646-9661b10c976e
assetMacAddress	00:f2:8b:a0:3a:59
assetName	Cisco a0:3a:59
assetVendor	Cisco Systems, Inc

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

ISE에서 디버깅 사용

ISE에서 디버그를 활성화하려면 Administration(관리) **> System(시스템) > Logging(로깅) > Debug Log Configuration(디버그 로그 컨피그레이션)으로 이동합니다**.로그 레벨을 다음으로 설정:

페르소나	구성 요소 이름	로그 레벨	확인할 파일
PAN(선택 사항)	프로 파 일러	디버그	profiler.log
pxGrid 프로브가 활성화된 PSN	프로 파 일러	디버그	profiler.log
px그리드	pxgrid	추적	pxgrid-server.log

CCV에서 디버깅 사용

CCV에서 디버그를 활성화하려면

- **touch** /data/etc/sbs/pxgrid-agent.conf 명령을 사용하여 **/data/etc/sbs/pxgrid-agent.conf** 파일 만들기
- vi **편집기**를 사용하여 **vi /data/etc/sbs/pxgrid-agent.conf** 명령으로 pxgrid**-agent.conf** 파일에 이 내용을 붙여넣습니다.

```
# /data/etc/sbs/pxgrid-agent.conf
base:
loglevel: debug
```

- systemctl restart pxgrid**-agent** 명령을 실행하여 pxgrid-agent**를 다시 시작합니다.**
- journalctl **-u pxgrid-agent** 명령으로 로그 보기

대량 다운로드 실패

CCV는 통합 중에 ISE에 대량 다운로드 URL을 게시합니다.pxGrid 프로브가 활성화된 ISE PSN은 이 URL을 사용하여 대량 다운로드를 수행합니다.다음을 확인합니다.

- URL의 호스트 이름은 ISE 관점에서 올바르게 확인 가능
- 포트 8910의 PSN에서 CCV로의 통신이 허용됩니다.

pxGrid 프로브가 활성화된 PSN의 profiler.log:

```
INFO [ProfilerINDSubscriberPoller-58-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- New services are:
[Service [name=com.cisco.endpoint.asset, nodeName=cv-jens4,
properties={assetTopic=/topic/com.cisco.endpoint.asset,
restBaseUrl=https://Center:8910/pxgrid/ind/asset/, wsPubsubService=com.cisco.ise.pubsub}]]
```

CSCvt75422로 인해 대량 다운로드가 실패할 수 있습니다. 확인하려면 ISE의 **profiler.log**에서 이 오류를 확인해야 합니다.결함은 CCV 3.1.0에 있습니다.

```
2020-04-09 10:47:22,832 ERROR [ProfilerINDSubscriberBulkRequestPool-212-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber
-::::- ProfilerError while sending bulkrequest to cv-jens4:This is not a JSON Object.
java.lang.IllegalStateException: This is not a JSON Object.
at com.google.gson.JsonElement.getAsJsonObject(JsonElement.java:83)
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber.parseJsonBulkResponse(INDSubscriber.jav
a:161)
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber$BulkRequestWorkerThread.run(INDSubscrib
er.java:532)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
at java.lang.Thread.run(Thread.java:748)
```

모든 엔드포인트가 ISE에서 생성되는 것은 아님

CCV의 일부 엔드포인트에는 너무 많은 속성이 연결되어 있으므로 ISE 데이터베이스에서 처리할 수 없습니다.ISE의 profiler**.log**에서 이러한 오류가 표시되면 확인이 가능합니다.

```
2020-05-29 00:01:25,228 ERROR [admin-http-pool1][] com.cisco.profiler.api.EDFEndPointHandler -
::::-
Failed to create endpoint 00:06:F6:2A:C4:2B ORA-12899:
value too large for column "CEPM"."EDF_EP_MASTER"."EDF_ENDPOINTIP" (actual:660, maximum: 100)
```

```
2020-05-29 00:01:25,229 ERROR [admin-http-pool1][] com.cisco.profiler.api.EDFEndPointHandler -
::::-
Unable to create the endpoint.:ORA-12899:
value too large for column "CEPM"."EDF_EP_MASTER"."EDF_ENDPOINTIP" (actual: 660, maximum: 100)
com.cisco.epm.edf2.exceptions.EDF2SQLException: ORA-12899:
value too large for column "CEPM"."EDF_EP_MASTER"."EDF_ENDPOINTIP" (actual: 660, maximum: 100)
```

ISE에서 AssetGroup을 사용할 수 없음

AssetGroup을 ISE에서 사용할 수 없는 경우, 대부분 프로파일링 정책이 사용자 지정 특성을 사용하여 구성되지 않은 것일 수 있습니다(문서의 구성 부분에서 2-4단계 참조). 컨텍스트 가시성의 경우에도 2-4단계에서 그룹 특성, 프로파일링 정책 및 기타 설정을 표시하는 것에만 필요합니다.

엔드포인트 그룹 업데이트가 ISE에 반영되지 않음

CSCvu80175로 인해 통합 직후 CCV가 재부팅될 때까지 CCV는 ISE에 엔드포인트 업데이트를 게시하지 않습니다.통합이 완료되면 CCV를 재부팅할 수 있습니다.

CCV에서 그룹을 제거하는 것은 ISE에서 제거되지 않음

이 문제는 CCV CSCvu47880의 알려진 결함으로 인해 발생합니다. CCV에서 그룹을 제거하는 동안 pxGrid 업데이트가 예상 형식과 다르게 전송되어 그룹이 제거되지 않습니다.

웹 클라이언트에서 CCV 삭제

이 문제는 ISE CSCvu47880에서 알려진 결함 때문에 클라이언트가 OFF 상태로 전환되고 웹 클라이언트에서 완전히 제거됩니다.이 문제는 ISE의 2.6 패치 7 및 2.7 패치 2에서 해결되었습니다.

ISE의 pxgrid-**server.log**에서 다음 오류가 표시되면 확인할 수 있습니다.

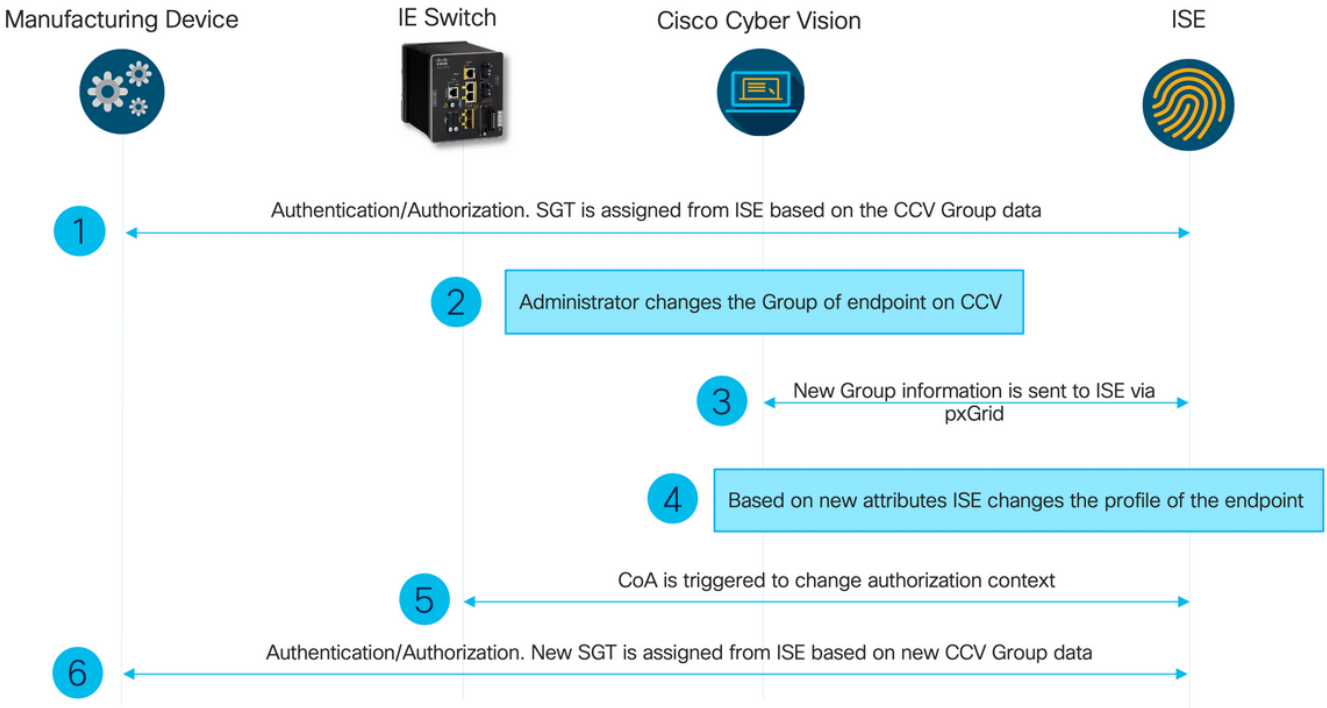
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionID=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726, closeTime=2020-06-26 09:42:28.772,
reason=VIOLATED_POLICY:Did not receive a pong: too slow ...,
subscriptions=[], publications=[/topic/com.cisco.endpoint.asset]]
```

CCV TrustSec 활용 사례와 ISE 통합

이 컨피그레이션에서는 TrustSec이 구축되었을 때 ISE와 CCV의 통합이 보안 엔드 투 엔드 이점을 제공하는 방법을 보여줍니다.통합이 완료되면 통합을 사용할 수 있는 방법의 예시입니다.

> **참고:**TrustSec 스위치 컨피그레이션 설명은 이 문서의 범위를 벗어납니다. 그러나 부록에서 확인할 수 있습니다.

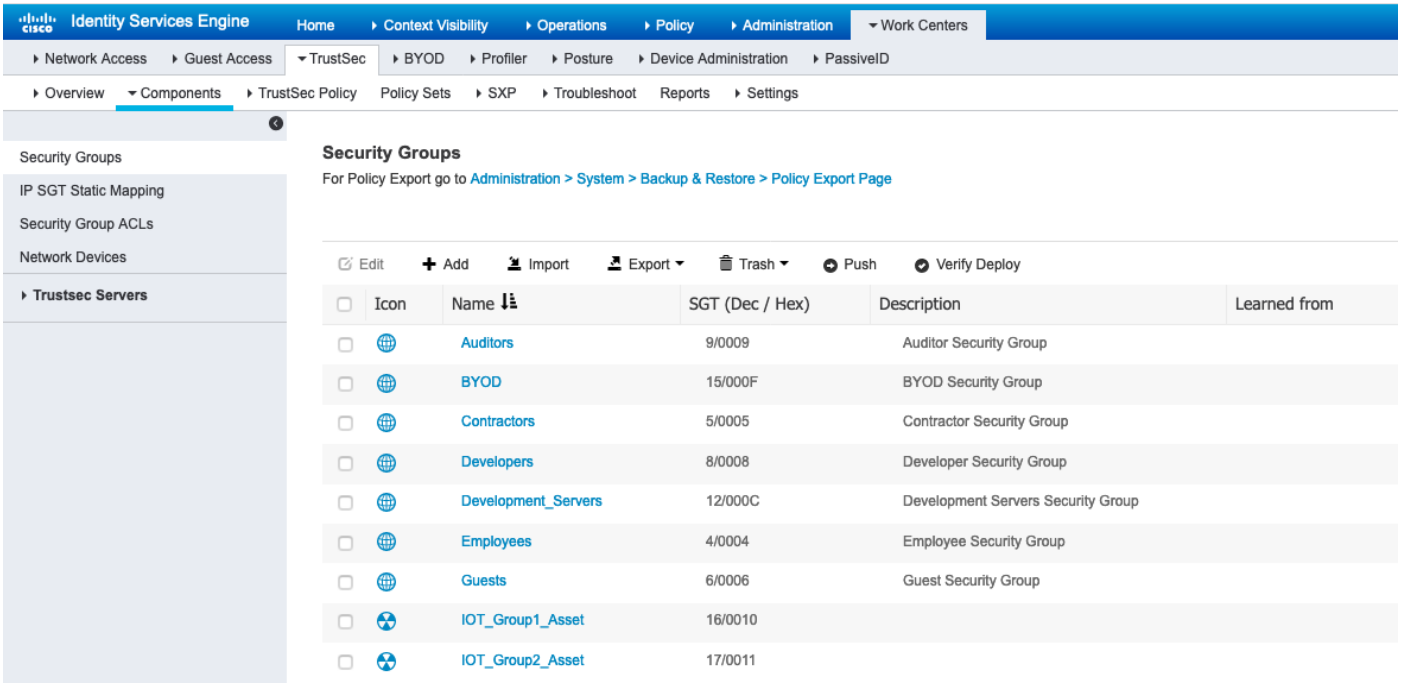
토폴로지 및 흐름



구성

1. ISE에서 확장 가능한 그룹 태그 구성

앞서 언급한 활용 사례를 달성하기 위해 TrustSec 태그의 IOT_Group1_Asset 및 IOT_Group2_Asset은 Group1 CCV 자산을 각각 Group2와 구분하도록 수동으로 구성됩니다.Work Centers(작업 **센터) > TrustSec > Components(구성 요소) > Security Groups(보안 그룹)로 이동합니다**.Add(추가)를 **클릭합니다.**이미지에 표시된 대로 SGT의 이름을 지정합니다.

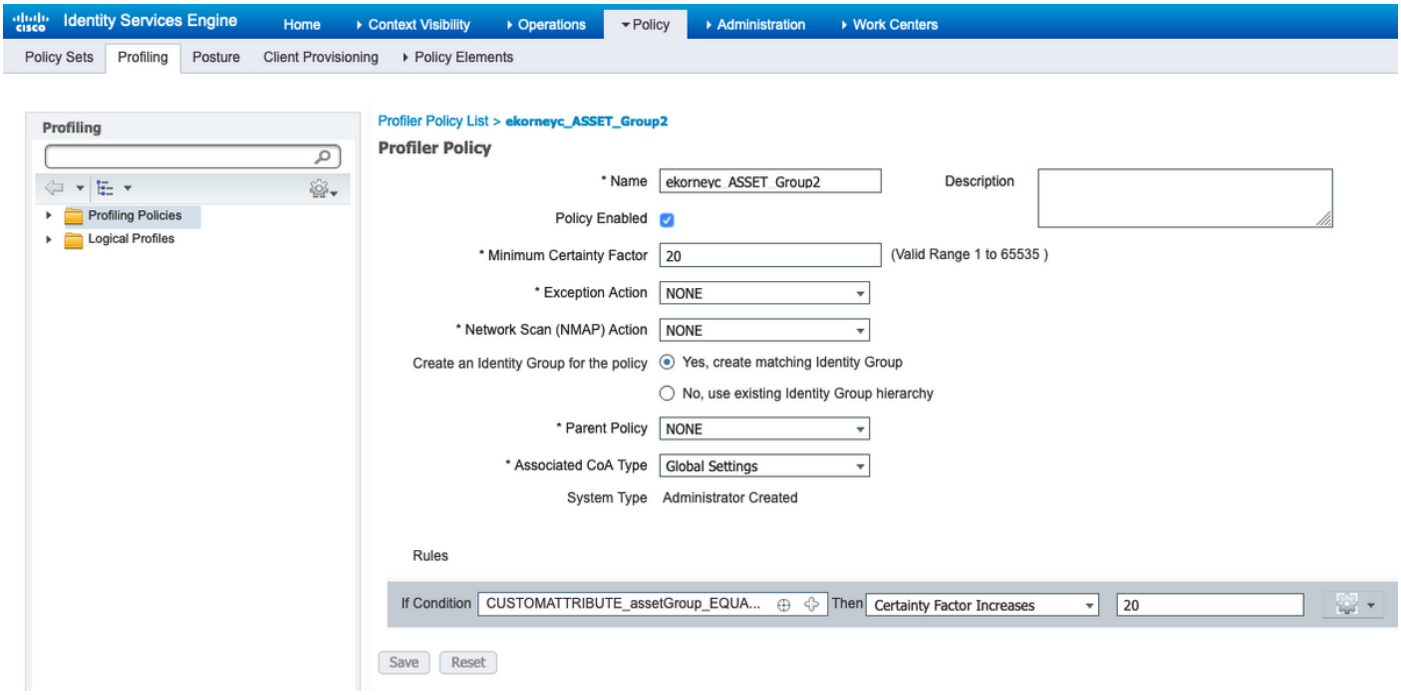


2. 그룹 2에 대한 사용자 지정 특성으로 프로파일러 정책 구성

참고:그룹 1에 대한 프로파일링 컨피그레이션은 문서의 첫 번째 부분의 3단계에서 수행되었

습니다.

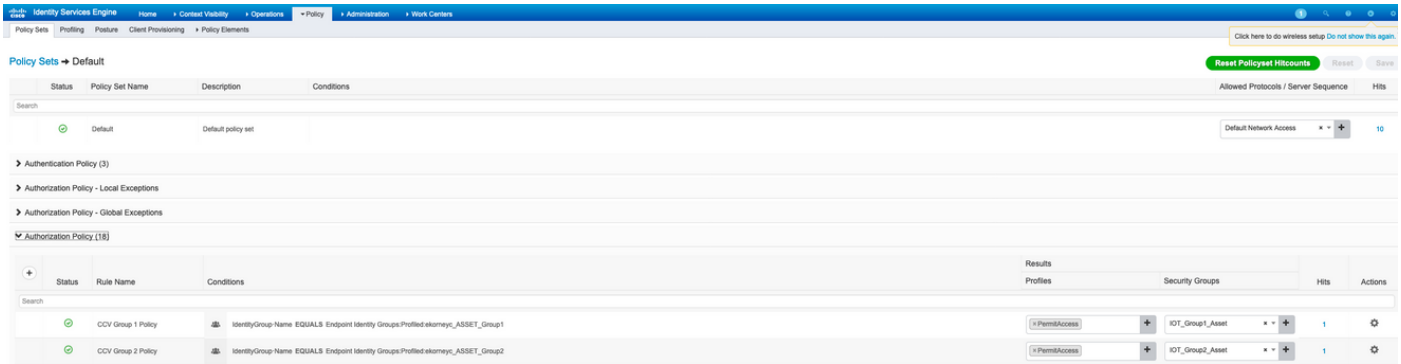
Work Centers(**작업 센터) > Profiler(프로파일러) > Profiling Policies(프로파일링 정책)로 이동합니다.**Add(추가)를 **클릭합니다.**이 이미지와 유사한 프로파일러 정책을 구성합니다.이 정책에 사용된 조건 표현식은 CUSTOMATTRIBUTE:**assetGroup EQUALS Group2입니다.**



3. ISE의 엔드포인트 ID 그룹을 기반으로 SGT를 할당하도록 권한 부여 정책을 구성합니다.

Policy(정책) **> Policy Sets(정책 세트)로 이동합니다.**Policy **Set를** 선택하고 이 이미지에 따라 권한 부여 정책을 구성합니다.따라서 1단계에서 SGT가 구성됩니다.

규칙 이름	조건	프로파일	보안 그룹
CCV 그룹 1 정책	IdentityGroup·Name EQUALS 엔드포인트 ID 그룹 :Profiled:ekorneyc_ASSET_Group1	액세스 허용	IOT_Group1_자산
CCV 그룹 2 정책	IdentityGroup·Name EQUALS 엔드포인트 ID 그룹 :Profiled:ekorneyc_ASSET_Group2	액세스 허용	IOT_Group2_자산



다음을 확인합니다.

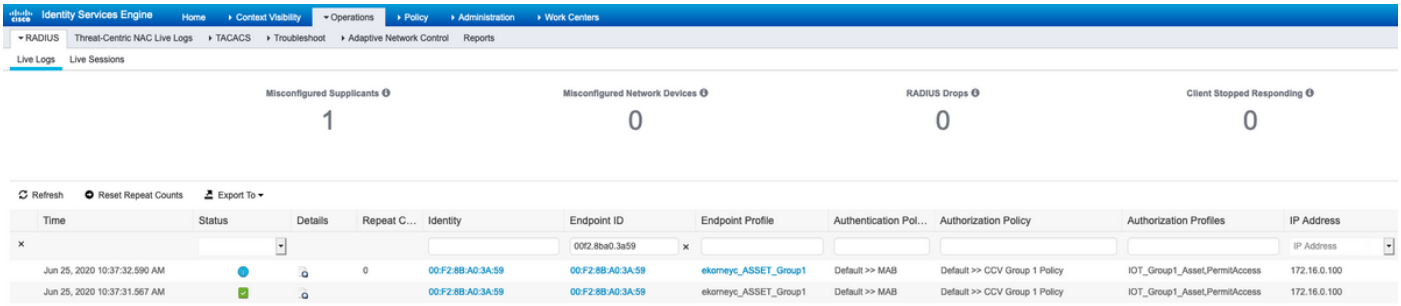
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

1. 엔드포인트는 CCV 그룹 1에 따라 인증됩니다.

스위치에서 환경 데이터에 SGT의 **16-54:IOT_Group1_Asset** 및 **17-54:IOT_Group2_Asset**이 모두 포함되어 있음을 확인할 수 있습니다.

```
KJK_IE4000_10#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
SGT tag = 0-00:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
*Server: 10.48.17.86, port 1812, A-ID 11A2F46141F0DC8F082EFBC4C49D217E
Status = ALIVE
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0-54:Unknown
2-54:TrustSec_Devices
3-54:Network_Services
4-54:Employees
5-54:Contractors
6-54:Guests
7-54:Production_Users
8-54:Developers
9-54:Auditors
10-54:Point_of_Sale_Systems
11-54:Production_Servers
12-54:Development_Servers
13-54:Test_Servers
14-54:PCI_Servers
15-54:BYOD
   16-54:IOT_Group1_Asset
   17-54:IOT_Group2_Asset
255-54:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 16:39:44 UTC Wed Jun 13 2035
Env-data expires in 0:23:59:53 (dd:hr:mm:sec)
Env-data refreshes in 0:23:59:53 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
KJK_IE4000_10#
```

엔드포인트가 인증되고 그 결과, **CCV 그룹 1 정책**이 일치하고 SGT IOT_Group1_Asset이 할당됩니다.



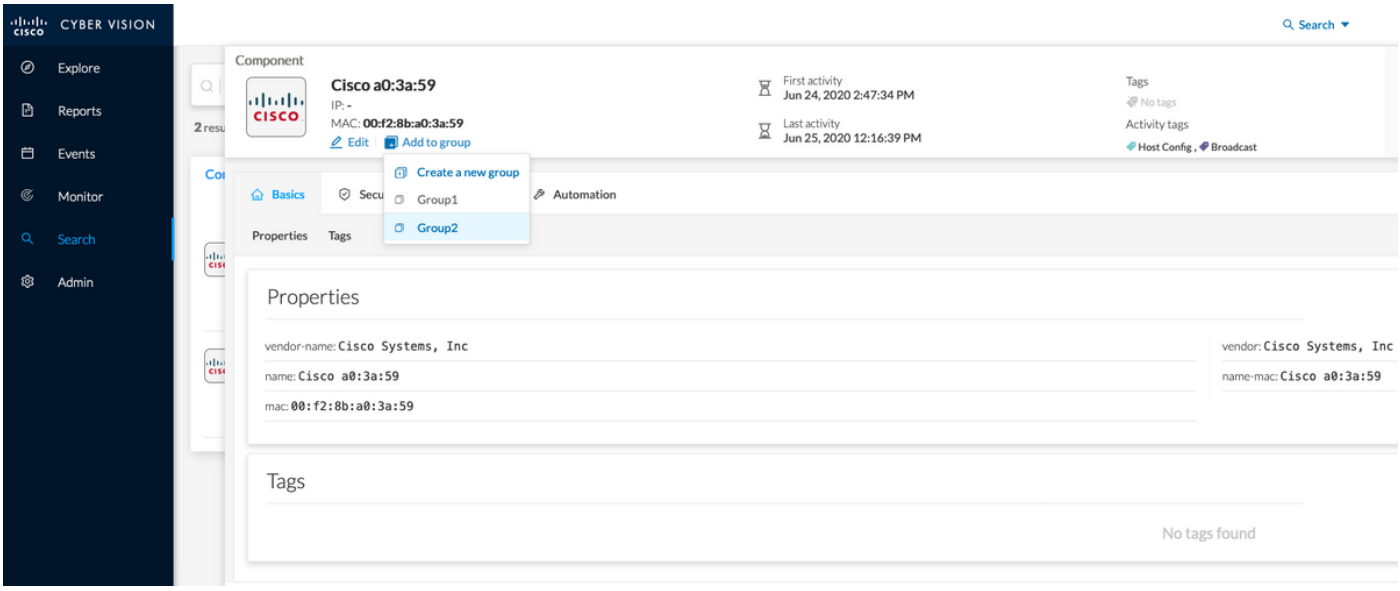
스위치 **show authentication sessions interface fa1/7 detail**은 Access-Accept 데이터가 성공적으로 적용되었음을 확인합니다.

```
KJK_IE4000_10#show authentication sessions interface fa1/7 detail
Interface: FastEthernet1/7
MAC Address: 00f2.8ba0.3a59
IPv6 Address: Unknown
IPv4 Address: 172.16.0.100
User-Name: 00-F2-8B-A0-3A-59
Status: Authorized
Domain: DATA
Oper host mode: single-host
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 128s
Common Session ID: 0A302BFD0000001B02BE1E9C
Acct Session ID: 0x00000010
Handle: 0x58000003
Current Policy: POLICY_Fa1/7

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure

Server Policies:
  SGT Value: 16

Method status list:
Method State

mab Authc Success

KJK_IE4000_10#
```

2. 관리자가 그룹을 변경합니다.

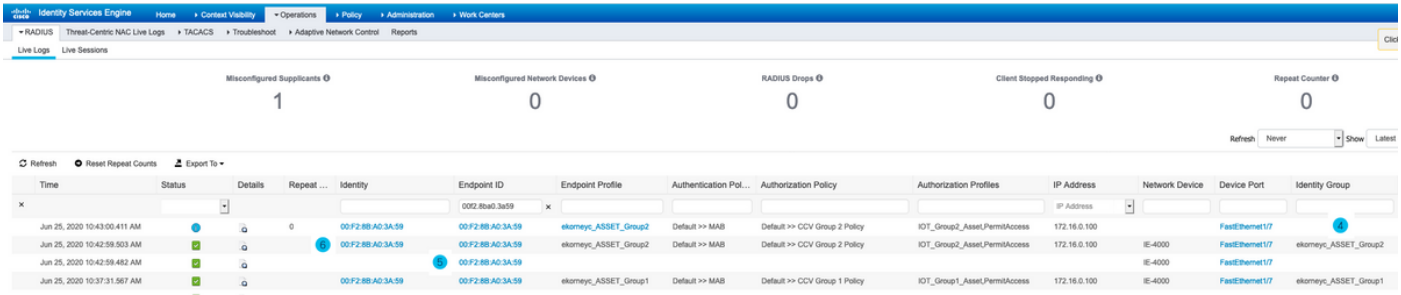
Search로 **이동합니다**.엔드포인트의 MAC 주소를 붙여넣고 이를 클릭한 다음 그룹 2에 추가합니다.

> **참고:**CCV에서는 한 번에 그룹을 1에서 2로 변경할 수 없습니다.따라서 먼저 그룹에서 엔드포인트를 제거하고 다음으로 그룹 2를 할당해야 합니다.



3-6. 엔드포인트 그룹 변경이 CCV에 미치는 영향

4., 5. 및 6. 단계는 이 이미지에 반영됩니다.프로파일링 덕분에 엔드포인트는 ID 그룹을 4단계에서 확인한 ecorneyc_ASSET_Group2로 변경했습니다. 이로 인해 ISE는 스위치에 CoA를 보내고(5단계) 엔드포인트 재인증(6단계)을 하게 되었습니다.



스위치 **show authentication sessions interface fa1/7 detail**은 새 SGT가 할당되었음을 확인합니다.

```
KJK_IE4000_10#show authentication sessions interface fa1/7 detail
Interface: FastEthernet1/7
MAC Address: 00f2.8ba0.3a59
IPv6 Address: Unknown
IPv4 Address: 172.16.0.100
User-Name: 00-F2-8B-A0-3A-59
Status: Authorized
Domain: DATA
Oper host mode: single-host
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 664s
Common Session ID: 0A302BFD0000001B02BE1E9C
Acct Session ID: 0x00000010
Handle: 0x58000003
Current Policy: POLICY_Fa1/7

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure
```

```
Server Policies:
  SGT Value: 17

Method status list:
Method State

mab Authc Success

KJK_IE4000_10#
```

부록

스위치 TrustSec 관련 컨피그레이션

> **참고:**cts 자격 증명은 running-config의 일부가 아니며, privilege exec 모드에서 cts credentials id **<id> password <password>** 명령을 사용하여 구성해야 합니다.

```
aaa new-model
!
aaa group server radius ISE
server name ISE-1
!
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa authorization network ISE group ISE
aaa accounting dot1x default start-stop group ISE
!
dot1x system-auth-control
!
aaa server radius dynamic-author
client 10.48.17.86
server-key cisco
!
aaa session-id common
!
cts authorization list ISE
cts role-based enforcement
!
interface FastEthernet1/7
description --- ekorneyc TEST machine ---
switchport access vlan 10
switchport mode access
authentication port-control auto
mab
!
radius server ISE-1
address ipv4 10.48.17.86 auth-port 1645 acct-port 1646
pac key cisco
!
end

KJK_IE4000_10#
```