

# ISE 2.7 PXgrid CCV 3.1.0 لم اكات ني وكت

## تا يوت حمل

[ةمدق مل](#)

[ةيساس ال ا تابلط مل](#)

[تابلط مل](#)

[ةمدختس مل ا تانوك مل](#)

[ني وكت](#)

[يوتس مل ا يلاع قفدت ل ل يطي طخت مسر](#)

[تان ني وكت](#)

[1. PSN تافل م دح ا يلع PxGrid Probe ني كمت](#)

[2. ISE يلع ةياهن ل ا ةطقن ل ةصصخ مل ا تامس ل ا ني وكت](#)

[3. ةصصخ م تامس مادختس اب في رع ت ل ا تافل م ئش نم جن ني وكت](#)

[4. تان ا ي ل ا في نصت ذافن ال ةصصخ مل ا تامس ل ا ني كمت](#)

[5. PXgrid ا ل م عمل ةيئ ا ق ل ل ا ةق ف اوم ل ا ني وكت](#)

[6. CCV ةداهش ري دصت](#)

[7. هب قو ووم ل ا ISE رجتم ي ل ا CCV ةيوه ةداهش لي محت](#)

[8. CCV ل ةداهش عاشن ا](#)

[9. PKCS12 قيس ن ت ب تاداهش ل ا ةلس لس لي زنت](#)

[10. CCV يلع ISE لم ا كت لي صافات ني وكت](#)

[11. قاطال ا لم ا كت و CCV يلع تاداهش ل ا ةلس لس لي محت](#)

[ةحص ل ا نم ققحت ل ا](#)

[CCV لم ا كت نم ققحت ل ا](#)

[ISE لم ا كت نم ققحت ل ا](#)

[CCV ةعومجم ري غت نم ققحت ل ا](#)

[اهال ص او ا طخال ا فاش كت سا](#)

[ISE يلع ا طخال ا حي حصت ني كمت](#)

[CCV يلع ا طخال ا حي حصت ني كمت](#)

[عمجم ل ا لي زنت ل ا لش ف](#)

[ISE يلع ةياهن ل ا طاقن ل ك عاشن ا متي ال](#)

[ISE يلع ةرفو تم ري غ AssetGroup](#)

[ISE يلع ةياهن ل ا طاقن ةعومجم ت ا ثي دحت س ك عن ت ال](#)

[ISE نم اهت ل ا زاب CCV نم ةعومجم ةلازا موقت ال](#)

[بيول ا ل م عمل نم CCV طقس ي](#)

[CCV TrustSec مادختس ا ةلا ح عم ISE جم د](#)

[قفدت ل ا و ا ي ج و ل و و ط ل ا](#)

[ني وكت](#)

[1. ISE يلع ري و ط ل ل ةل ب ا ق ل ا ةعومجم ل ا تام ال ع ني وكت](#)

[2. ةعومجم ل ل ةصصخ م تامس ب في رع ت ل ا تافل م ئش نم جن ني وكت](#)

[3. ةيوه تاعومجم يلع ةمئ ا ق ل ا SGT تاس ا ي س صي صخت ل ضي و ف ت ل ا تاس ا ي س ني وكت](#)

[ISE يلع ةي ف ر ط ل ا ةطقن ل ا](#)

[ةحص ل ا نم ققحت ل ا](#)

[1. CCV ةعومجم ي ل ا ا دان ت سا ةياهن ل ا طاقن ةق داص م](#)

[ةومجملا ريغت ب لوؤسمل موق ي .2](#)  
[CCV لىل عةياهنلا طاقن ةومجم ريغت ريثأت . 3-6](#)  
[قحلملا](#)  
[Switch TrustSec ب طبترملا نيوكتل](#)

## ةمدقملا

cisco عم لم اكت 2.7 (ISE) كرحم ةيوهلا ءاطخأ فاشكتساو لكشي نأ فيك ةقيثو اذه فص ي  
Cyber Vision (CCV) 3.1.0 Exchange Grid v2 (pxGrid). CCV عم لجسم pxGrid v2  
IOTASSET Dictionary ل ISE لىل ةياهنلا ةطقن تامس نع تامولعم رشن يورشانك

## ةيساسال تابلطتملا

### تابلطتملا

ةيلاتل عيضاوملاب ةيساسا ةفرعم كي دل نوكت نأب Cisco ي صوت

- (ISE) ةيوهلا فشك تامدخ كرحم
- Cisco Cyber ةيؤر

### ةمدختسملا تانوكملا

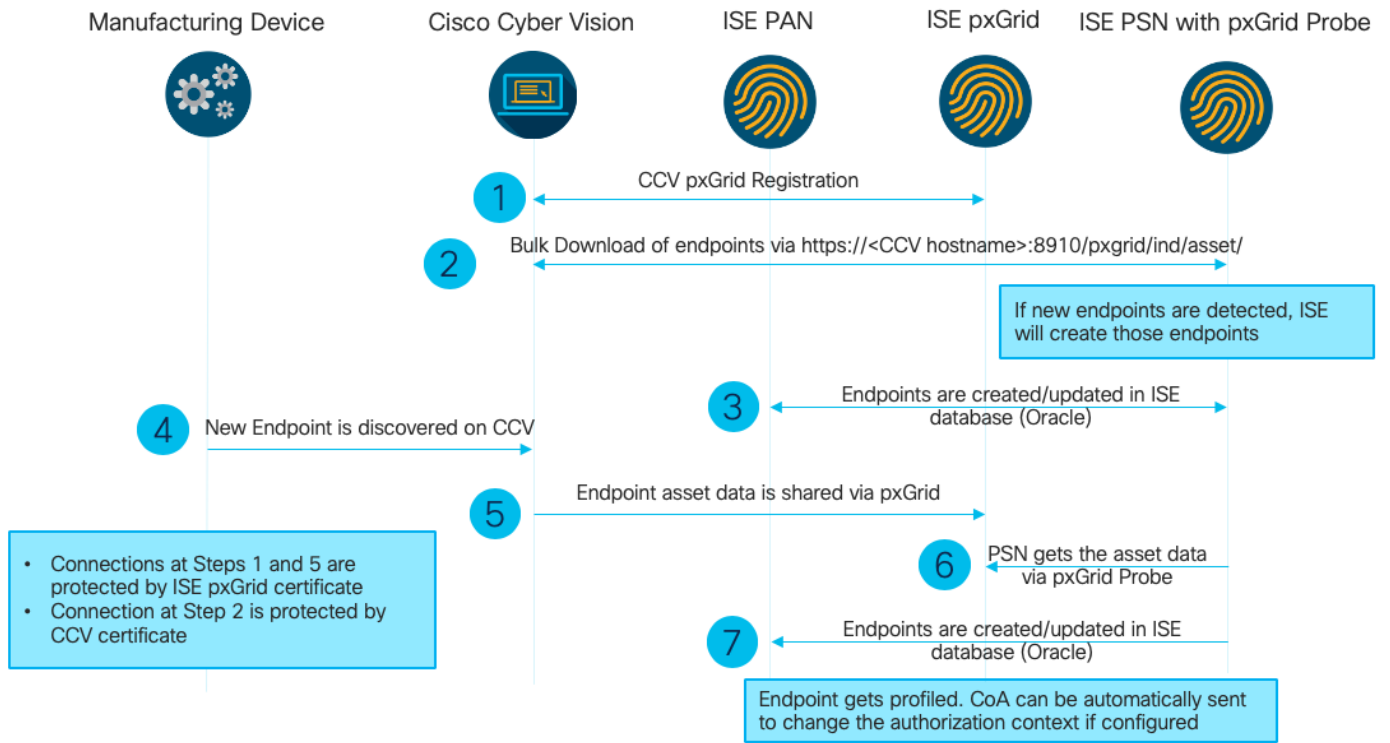
ةيلاتل ةيدامل تانوكملا وجماربل تارادصل لىل دننتملا اذه في ةدراول تامولعملا دننست

- Cisco 1 نم 2.7 رادصلال ISE
- Cisco Cyber Vision، رادصلال 3.1.0
- Industrial IE-4000-4TC4G-E نم 15.2(6)E عم ت نرثي ل وحم

ةصاخ ةيلمعم ةئي ب في ةدوجوملا ةزهجال نم دننتملا اذه في ةدراول تامولعملا ءاشنإ مت  
ت ناك اذإ. (يضا رتفا) حوسمم نيوكتب دننتملا اذه في ةمدختسملا ةزهجال عيجم تادب  
رمأ يال لم تحملا ريثأتل لك م هف نم دكأت ف، ليغشتلا دي ق ك تكبش

## نيوكتل

### يوتسملا يلاع قفدتلل يطي طخت مسر



دادع إال يف اذه ISE رشن مادختسا متي.

#### Deployment Nodes

Hostname	Personas	Role(s)	Services
ISE27-1ek	Administration, Monitoring, Policy Service, pxGrid	PRI(A), PRI(M)	ALL
ISE27-2ek	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION, PROFILER

ISE 2.7-1ek و pxGrid ةدقعو (PAN) ةيساسألا ةرادإلا ةدقعو وه.

ISE 2.7-2ek و PxGrid Probe نيكمت عم (PSN) ةسايسلا ةمدخ ةدقعو وه.

اقباس روكذمال طاطخمال عم قباطت يتلا تاوطخال يلي امي.

نم ةلباقمال تالجسلا 2. رادصإلا PxGrid ربع ISE يف AssetTopic إلى CCV لجست متي 1. CCV:

**مظحالم** journalCTL -u pxgrid-agent رمال رادصإاب مق، CCV إلى pxGrid تالجس ةعجارم لجأ نم: **مظحالم agent.**

```
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. دوجوم ل pxGrid لوصاً نم ةري ب ك تاي م ك ليزن ت ب PxGrid Probe ني ك م ت عم ISE PSN م وقي ي (profiler.log):

```

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. إلى ارم تسم ائدح PSN لاسر او PxGrid Probe نكمت عم PSN إلى اةاهنلا طاقن ةفاضل متت 3. إلى اءواشنل مت يتل اةاهنلا طاقن ضرع نكمي (profiler.log). هذ ةاهنلا طاقن ظفحل PAN قاي سلال ةيؤر ةيناكمل نمض ةاهنلا ةطقن لياصافات في ISE.

```
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  
processedEndPoint[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. شيدحتل 8910 ذفنملا ربع STOMP ةلاسر CCV لسري، ةومجم في ةاهنلا ةطقن عضو دعب 4. نم ةلباقملا تالجلسلا. ةصصخم تامس في ةومجملا تانايب مادختساب ةاهنلا ةطقن:

```
root@center:~# journalctl -u pxgrid-agent -f  
Jun 24 14:32:04 center pxgrid-agent-start.sh[1216]: pxgrid-agent STOMP SEND
```



```
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. ةديج ةسايسك ةياهنلا ةطقن فيرعت فلم pxGrid ني كمت عم PSN دي عت (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-ala3-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
```

## تاني وكتال

ةلداع ةيؤر لىل لوصح لاي ف ب غرت تنك اذا ىتح 4 لىل 1 نم تاو طخل ذاخا مزلي :ةظالم  
قاي س ل ةيؤر لاي ف و AssetGroup ل

### 1. اتافل م دحا لىل PxGrid Probe نيكمت

ةمالع لىل ليدبتال PSN Persona مادختساب ISE ةدقع دح ،رشن > ماظن > ةراد لىل لقتنا  
pxGrid قيقحت نيكمت نم دكات . فيرعتال فل م نيوكت بيوبت



**Deployment**

Deployment

PAN Failover

Deployment Nodes List > ISE27-2ek

**Edit Node**

General Settings Profiling Configuration

- ▶ NETFLOW
- ▶ DHCP
- ▶ DHCPSPAN
- ▶ HTTP
- ▶ RADIUS
- ▶ Network Scan (NMAP)
- ▶ DNS
- ▶ SNMPQUERY
- ▶ SNMPTRAP
- ▶ Active Directory
- ▼ pxGrid

Description: The PXgrid probe to fetch attributes of MAC or IP-Address as a subscriber from PXGrid Queue

2. ISE ىل عىاهنلا ةطقنل ةصصخمل تامسلا نىوكت

تامس نىوكت. ةصصخمل ةاهنلا ةطقن تامس > تاداعل > ةيوهلا ةرادل > ةرادل ىل لقتنا ةصصخمل AssetGroup ةمس 3.1.0 CCV مءى. ةروصل هذهل اقفو (assetGroup) ةصصخمل طقف.

- User Custom Attributes
- User Authentication Settings
- Endpoint Purge
- Endpoint Custom Attributes

### Endpoint Custom Attributes

#### Endpoint Attributes (for reference)

Mandatory	Attribute Name	Data Type
	PostureApplicable	STRING
	LogicalProfile	STRING
	EndPointPolicy	STRING
	AnomalousBehaviour	STRING
	OperatingSystem	STRING
	BYODRegistration	STRING
	PortalUser	STRING
	LastAUPAcceptanceHours	INT

#### Endpoint Custom Attributes

Attribute Name:

Type:  - +

### 3. ةصصخم تامس مادختساب فيرعتلا تافلنم جنه نيوكت

يلع رقنا . فيرعتلا تافلنم ءاشن | جنه > فيرعتلا تافلنم ءاشنم > لمعلا زكارم | ل لقتنا  
 طرشل ريبعت . ةروصلل هذلل لثاملل فيرعتلا تافلنم ءاشنم جنه نيوكت . ةفاضل  
 CUSTOMATTRIBUTE:AssetGroup EQUALS Group1 وه جنه ل اذه في مدختسمل

**Profiling**

- Profiling Policies
- Logical Profiles

Profiler Policy List > ekornecy\_ASSET\_Group1

**Profiler Policy**

\* Name:  Description:

Policy Enabled:

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

\* Exception Action:

\* Network Scan (NMAP) Action:

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

\* Parent Policy:

\* Associated CoA Type:

System Type: Administrator Created

Rules

If Condition:  Then:

#### 4. تانايا ب ل ف ي ن ص ت ذ ا ف ن ا ل ة ص ص خ م ل ا ت ا م س ل ل ن ي ك م ت

ي ل ع ر ق ن ا . ف ي ر ع ت ل ا ت ا ف ل م ء ا ش ن ا ج ه ن > ف ي ر ع ت ل ا ت ا ف ل م ئ ش ن م > ل م ع ل ا ز ك ا ر م ي ل ل ل ق ت ن ا ة م س ل ل ن ي ك م ت ن م د ك ا ت . ة ر و ص ل ا ه ذ ل ل ث ا م م ل ا ف ي ر ع ت ل ا ت ا ف ل م ئ ش ن م ج ه ن ن ي و ك ت . ة ف ا ض ا ل ف ي ر ع ت ل ا ف ل م ق ي ب ط ت ل ة ص ص خ م ل ا

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies Policy Sets

Profiler Settings

Profiler Configuration

NMAP Scan Subnet Exclusions

\* CoA Type: Reauth

Current custom SNMP community strings: \*\*\*\*\* Show

Change custom SNMP community strings: (For NMAP, comma separated.)

Confirm changed custom SNMP community strings: (For NMAP, comma separated.)

EndPoint Attribute Filter:  Enabled

Enable Anomalous Behaviour Detection:  Enabled

Enable Anomalous Behaviour Enforcement:  Enabled

Enable Custom Attribute for Profiling Enforcement:  Enabled

Enable profiling for MUD:  Enabled

Enable Profiler Forwarder Persistence Queue:  Enabled

Enable Probe Data Publisher:  Enabled

Save Reset

#### 5. ء ا ل م ع ل ة ي ة ا ق ل ل ت ل ا ق و ا و م ل ن ي و ك ت

ة د ن ت س م ل ا ت ا ب ا س ح ل ا ي ل ع ة ي ة ا ق ل ل ت ل ا ق و ا و م ل ا د ح . ت ا د ا د ع | > p x G r i d ت ا م د خ > ة ر ا د ا ي ل ل ل ق ت ن ا C C V ي ل ع ة ق و ا و م ل ا ي ل ل ا ج ا ت ح ت ا ل ك ن ا ة و ط خ ل ا ه ذ ه ن م ص ت . ط ف ح ق و ف ر ق ن ا و ة د ي د ج ة د ا ه ش ي ل ل ل م ا ك ت ل ا ء ا ر ج ا د ر ج م ب

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions

PxGrid Settings

Automatically approve new certificate-based accounts

Allow password based account creation

Use Default Save

#### 6. ة د ا ه ش ر ي د ص ت C C V

ء ا ن ث ا ة د ا ه ش ل ا ه ذ ه م ا د خ ت س ا م ت ي . ة د ا ه ش ل ا ل ي ز ن ت ي ل ع ر ق ن ا . p x G r i d > A d m i n ي ل ل ل ق ت ن ا ا ه ب I S E ق ت ي ن ا ب ج ي ك ل ل ذ ل ، P x G r i d ل ي ج س ت

## 7. هب قوٹوم ل ISE رجتم یل CCV ةیوه ةداهش لېمحت .

یلع رقنا . دارپتس ی قوف رقنا . اهب قوٹوم تاداهش > تاداهش قراد > تاداهش > قراد یل لقتنا لاسرا یل لقتنا . 5 ةوطخل نم CCV ةداهش ددحو ضارعتس یل

## 8. ل ةداهش عاشن یل CCV

ISE ةطساوب اهرادص یل بحی . لېمعل ةداهش یل CCV جاتحی ، تاتی دحتل او PxGrid لماتك ءانثأ Internal CA، PxGrid\_Certificate\_Template مادختسا ب .

عئاشل ل مسال ل قح . ةروصل ل هذهل اقبط لوقحل ل علم . تاداهش > pxGrid تامدخ > قراد یل لقتنا لقتنا CCV، نم مس یل فیضم ل تلخد ت فوس تنأ . ةیوه ةداهش رادص یل وه ISE CA فده نأل یل مازل ل (CN) ددحو . رمأ hostname ل، CCV نم hostname ل تصحف in order to تردصأ . مهم ةمیق ل لجم CN ةداهش ل لیزنت قیسنت ب PKCS12 .

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions

### Generate pxGrid Certificates

I want to \*

Common Name (CN) \*

Description

Certificate Template [pxGrid\\_Certificate\\_Template](#) ⓘ

Subject Alternative Name (SAN)   - +

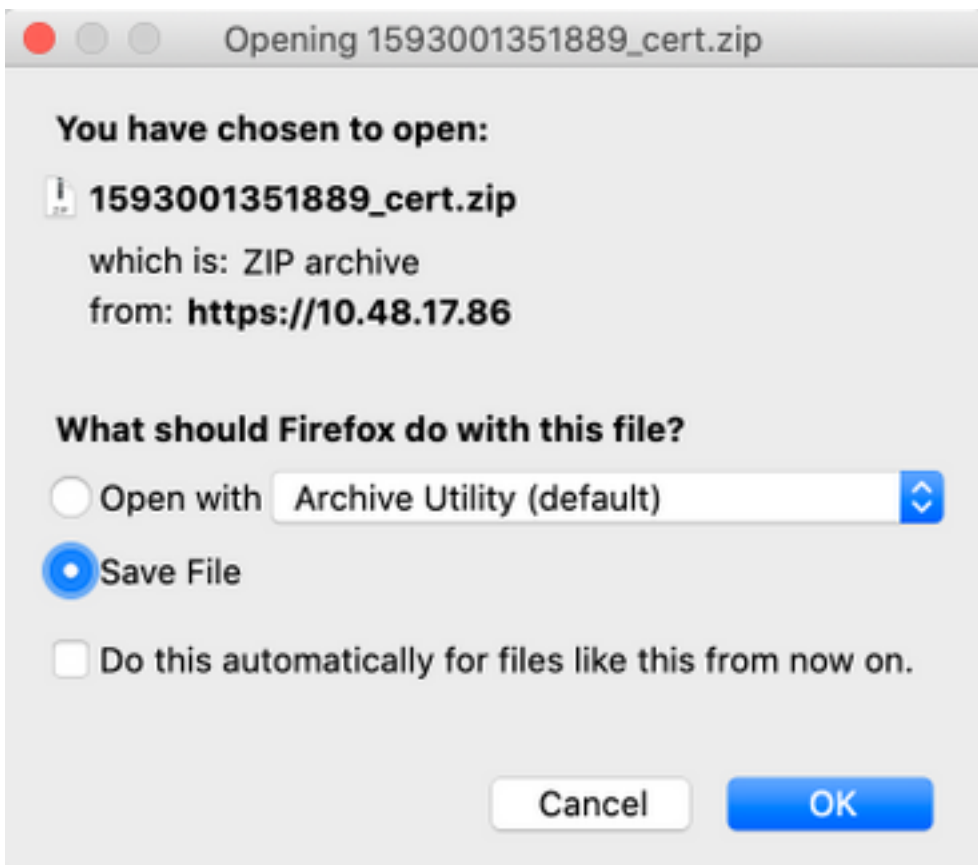
Certificate Download Format \*  ⓘ

Certificate Password \*  ⓘ

Confirm Password \*

## 9. PKCS12 قيسنتب تاداهشلا ةلسلس ليزنت

ةيلخادلا ISE ةلسلس لىل ةفاضل اب، PKCS12 قيسنتب تاداهشلا تيبتب موقت ام دنع نم pxGrid لاصتا ادبي ام دنع ISE قثي CCV نأ نامضل CCV لىل ةتبتبم CCV ةيوهلا ةداهشل pxGrid ب ةصاخلا keepalive لئاسر، لاثملا لىبس لىل ISE،





يرت نأ بجي. Admin > PxGrid إلى لاقاتنالا لالخ نم هحاجن ديكأت كنكمي، لمكالتا مامتإ درجمب ISE. مداخل تحت قطشن ةالسر لاصتالا نأ

## ISE لمكالت نم ققحتالا

ديق (CV-JENS) CCV ليمع ةلا ح نأ نم دكأت. بيولال عالمع > pxGrid تامدخ > ةرادا إلى لاقاتنالا ليغشتالا

عيمج ةمئاق يف لصتم ريغ CCV PXgrid ليمع ةلا ح يري نأ عقوتملال نم: ةظالم طوقف pxGrid v1 ةلا ح رهظت اهنإ شيح، عالعملالا

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duratio...
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:15	CN=ISE27-1ek.e...	/topic/distributed	/topic/distributed	10.48.17.86	ON	2020-06-24 09:56:50 UTC	00:04:37:18
ise-bridge-ise27-1ek	ISE27-1ek	ISE27-1ek:23	CN=ISE27-1ek.e...		/topic/com.cisco.ise.co...	127.0.0.1	ON	2020-06-24 10:06:52 UTC	00:04:27:16
ise-mnt-ise27-2ek	ISE27-1ek	ISE27-1ek:24	No Certificate	/topic/com.cisco.ise.se...	/topic/com.cisco.ise.se...	10.48.17.88	ON	2020-06-24 10:18:25 UTC	00:04:15:43
ise-admin-ise27-2ek	ISE27-1ek	ISE27-1ek:25	No Certificate	/topic/com.cisco.endpo...		10.48.17.88	ON	2020-06-24 10:18:26 UTC	00:04:15:43
ise-admin-ise27-1ek	ISE27-1ek	ISE27-1ek:34	CN=ISE27-1ek.e...		/topic/com.cisco.ise.en...	10.48.17.86	OFF	2020-06-24 12:09:50 UTC	00:02:19:00
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:37	CN=ISE27-1ek.e...	/topic/wildcard		127.0.0.1	OFF	2020-06-24 13:02:51 UTC	00:01:08:00
cv-jens	ISE27-1ek	ISE27-1ek:38	CN=center			10.48.43.241	ON	2020-06-24 13:39:12 UTC	00:00:54:56
ise-mnt-ise27-1ek	ISE27-1ek	ISE27-1ek:39	CN=ISE27-1ek.e...	/topic/com.cisco.ise.se...		10.48.17.86	ON	2020-06-24 13:53:51 UTC	00:00:40:17
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:40	CN=ISE27-1ek.e...	/topic/wildcard		127.0.0.1	OFF	2020-06-24 14:11:51 UTC	00:00:18:00
ise-admin-ise27-1ek	ISE27-1ek	ISE27-1ek:41	CN=ISE27-1ek.e...			10.48.17.86	ON	2020-06-24 14:29:51 UTC	00:00:04:17
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:42	CN=ISE27-1ek.e...	/topic/wildcard		127.0.0.1	ON	2020-06-24 14:30:51 UTC	00:00:03:17

هـ روفال الـ لـ CCV رت نـ CSCvt78208 نـ الـ ارظن :ةظـالـم  
 /topic/com.cisco.ise.endpoint.asset. لولـ ارشنـالـ دنـ طقـفـ هـضـرعـ مـتـيسـ .

## CCV ةومجم ريغت نم ققحتلا

مقو تانوكمل دحأ قوف رقنا . تانوكمل ةمئاق > تانايبلا لك > فاشكتسا لىل لقتنا  
 ةومجم لىل ةفاضاب .

Component	Group	First activity	Last activity	IP	MAC
KJK_IE4000_10.KJK_IE4000_10 00:f6:63:4d:d6:85	-	Jun 24, 2020 12:37:49 PM	Jun 24, 2020 4:27:19 PM	-	00:f6:63:4d:d6:85
01:00:0c:00:00:00	-	May 11, 2020 6:44:15 PM	Jun 24, 2020 4:27:19 PM	-	01:00:0c:00:00:00
01:00:0c:cccccc	-	Mar 13, 2020 1:52:23 PM	Jun 24, 2020 4:27:19 PM	-	01:00:0c:cccccc
255.255.255.255	-	Mar 13, 2020 1:52:09 PM	Jun 24, 2020 4:25:45 PM	255.255.255.255	fff
Cisco a0:3a:59	-	Jun 24, 2020 2:47:34 PM	Jun 24, 2020 4:25:45 PM	-	00:f6:63:4d:d6:85

CCV لباقم تاروشنمك نآل /topic/com.cisco.ise.endpoint.asset جاردا نم ققحت




Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duration
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:15	CN=ISE27-1ek.e...	/topic/distributed	/topic/distributed	10.48.17.86	OFF	2020-06-24 09:56:50 UTC	00:04:57:00
ise-bridge-ise27-1ek	ISE27-1ek	ISE27-1ek:23	CN=ISE27-1ek.e...	/topic/com.cisco.ise.config.profiler	/topic/com.cisco.ise.config.profiler	127.0.0.1	ON	2020-06-24 10:06:52 UTC	00:05:03:05
ise-mnt-ise27-2ek	ISE27-1ek	ISE27-1ek:24	No Certificate	/topic/com.cisco.ise.session.internal	/topic/com.cisco.ise.session.internal	10.48.17.88	OFF	2020-06-24 10:18:25 UTC	00:04:42:00
ise-admin-ise27-2ek	ISE27-1ek	ISE27-1ek:25	No Certificate	/topic/com.cisco.ise.endpoint.asset	/topic/com.cisco.ise.endpoint.asset	10.48.17.88	ON	2020-06-24 10:18:26 UTC	00:04:51:31
ise-mnt-ise27-1ek	ISE27-1ek	ISE27-1ek:39	CN=ISE27-1ek.e...	/topic/com.cisco.ise.session.internal	/topic/com.cisco.ise.session.internal	10.48.17.86	OFF	2020-06-24 13:53:51 UTC	00:00:58:00
ise-admin-ise27-1ek	ISE27-1ek	ISE27-1ek:41	CN=ISE27-1ek.e...	/topic/com.cisco.ise.endpoint.asset	/topic/com.cisco.ise.endpoint.asset	10.48.17.86	ON	2020-06-24 14:29:51 UTC	00:00:40:06
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:42	CN=ISE27-1ek.e...	/topic/wildcard	/topic/wildcard	127.0.0.1	OFF	2020-06-24 14:30:51 UTC	00:00:14:00
cv-jens	ISE27-1ek	ISE27-1ek:43	CN=center	/topic/com.cisco.ise.endpoint.asset	/topic/com.cisco.ise.endpoint.asset	10.48.43.241	ON	2020-06-24 14:38:47 UTC	00:00:31:10
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:44	CN=ISE27-1ek.e...	/topic/wildcard	/topic/wildcard	127.0.0.1	OFF	2020-06-24 14:45:52 UTC	00:00:11:00
ise-mnt-ise27-1ek	ISE27-1ek	ISE27-1ek:45	CN=ISE27-1ek.e...	/topic/com.cisco.ise.session.internal	/topic/com.cisco.ise.session.internal	10.48.17.86	OFF	2020-06-24 14:52:51 UTC	00:00:17:00
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:46	CN=ISE27-1ek.e...	/topic/distributed	/topic/distributed	10.48.17.86	OFF	2020-06-24 14:53:53 UTC	00:00:02:00
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:47	CN=ISE27-1ek.e...	/topic/distributed	/topic/distributed	10.48.17.86	ON	2020-06-24 14:55:53 UTC	00:00:14:03
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:48	CN=ISE27-1ek.e...	/topic/wildcard	/topic/wildcard	127.0.0.1	ON	2020-06-24 14:57:52 UTC	00:00:12:05
ise-mnt-ise27-2ek	ISE27-1ek	ISE27-1ek:49	No Certificate	/topic/com.cisco.ise.session.internal	/topic/com.cisco.ise.session.internal	10.48.17.88	ON	2020-06-24 15:01:26 UTC	00:00:08:31

قيبطت أدب دقو، ISE لىل سكتنت CCV ربع اهنىيغت مت يتل 1 ةومجم لىل نأ نم دكأت  
 دح . ةياهنلا طاقن > قاييسلا ةيؤر لىل لاقنتناب (ISE) فيرعتلا تافل م عاشن ةسايس  
 بيوبتلا ةمالع لىل ليدبتلاب مق . ةقباسلا ةوطخلال في اهثيدحت مت يتل ةياهنلا ةطقن  
 اثيدح اهنوك مت يتل ةومجم لىل ةصصم لىل تامس لىل مسق سكتني نأ بجي . تامس



Filters: \*00:F2:8B:A0:3A:59

Endpoints > 00:F2:8B:A0:3A:59

00:F2:8B:A0:3A:59   



MAC Address: 00:F2:8B:A0:3A:59  
Username:  
Endpoint Profile: ekorneyc\_ASSET\_Group1  
Current IP Address:  
Location:

Applications **Attributes** Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment false  
Endpoint Policy ekorneyc\_ASSET\_Group1  
Static Group Assignment false  
Identity Group Assignment ekorneyc\_ASSET\_Group1

Custom Attributes

Filter 

	Attribute String	Attribute Value
x	<input type="text" value="Attribute String"/>	<input type="text" value="Attribute Value"/>
	assetGroup	Group1

CCV. نم ةاقلتم لا ىرخألا لوصألا تامس لك ىرخألا تامس لا مسق درسي

## 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

## اه حال صا و ااطخ ال فاشك سا

اه حال صا و نيوك ال ااطخ ا فاشك سا ال اهم ادخ سا كن كم ي تام ول عم مس ق ل اذ رفوي

## ISE ال ع ااطخ ال ح حصت ني كم ت

نيوك ت > لوخد ال ليجست > ماظن ال > قراد ال ال ل لقتنا، ISE ال ع ااطخ ال ح حصت ني كم ت ل  
ي: لي ام ال ل ل ج سا ل تا يوت سم ني ي عت ب م ق. ااطخ ال ح حصت ل ج س

انوس رب	نوك م ال م سا	ليجست ال يوت سم	ال بول ط م ال فل م ال نم
PAN (ي را ي تخا)	ل ل ح م	ااطخ ال ح حصت	ت اف لم ئ ش نم log. في رع ت ال
PSN ني كم ت عم PxGrid Probe	ل ل ح م	ااطخ ال ح حصت	ت اف لم ئ ش نم log. في رع ت ال
PxGrid	pxgrid	رثا	pxgrid-server.log

## CCV ال ع ااطخ ال ح حصت ني كم ت

in order to CCV: **طبضي تنك**

- **touch /data/etc/sbs/pxgrid-agent.conf** رماً مادختساب **/data/etc/sbs/pxgrid-agent.conf** فلم عاشنإ
- **vi** رماً مادختساب **vi** ررحملا مادختساب **pxgrid-agent.conf** فلم ي ف يوتحمل اذه قصل **/data/etc/sbs/pxgrid-agent.conf**

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

- **system restart pxgrid-agent** رماً لئغشت لال خ نم **pxgrid** لماع لئغشت ةداعإ مق
- **journalctl -u pxgrid-agent** رماً مادختساب تالجال ضرع

## عجمملا لئزنتلا لشف

عم **ISE PSN** موقوي. لمكالتلا ءانثأ **ISE** لئ عجمملا لئزنتلا ل **URL** ناو نع رشن **CCV** موقوي  
ي: لئ ام نامض. اذه **URL** ناو نع مادختساب عجمملا لئزنتلا لئ فنتب **PxGrid** نئكمت

- **ISE** روظنم نم حئحص لكشب **URL** ناو نع ي ف يضمملا مسال ح نكمي
- **CCV** لئ **8910** ءانئم لئ **PSN** نم لاصلتإ حمسي

**profiler.log** on **PSN** عجمملا لئ **pxGrid** نئكمت ع

```
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}]]
```

**profiler.log** ي ف أطخال اذه ىرت نأ بجي [CSCvt75422](#). ببسب عجمملا لئزنتلا لشف ي نأ نكمي  
لئ **CCV 3.1.0** ي ف بعيل حالصال مت. لكذ دئكألت **ISE** لئ

```
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.java:161)
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber$BulkRequestWorkerThread.run(INDSubscriber.java:532)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
at java.lang.Thread.run(Thread.java:748)
```

## ISE لئ ةياهنلا طاقن لك عاشنإ متي ال

نكمتت نل لكذل، ةقفرم ادج ةريثك تامس لئ **CCV** لئ ةياهنلا طاقن ضع ب يوتحت دق  
**profiler.log** on **ISE**. ي ف أطخال اذه روهظ نم دكألت نكمي. اهتجالام نم **ISE** تانايب ةدعاق

```
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)
```

## AssetGroup ىل ع ةرفوتم ريغ ISE

تافلماش نإ جهن نيوكت م تي ال نأ لم تحم ال نم ف، ISE ىل ع ةرفوتم AssetGroup نكت مل اذإ نم "تانيوكتلا" عزج ي ف 2-4 تاوطلخ ال ا عجررا) ةصصخم تامس مادختساب فيرعتلا جهن نوكت، ةومجم ال تامس ضرعل طقف، قاي س ال ةيؤر ةي ناكم ال ةبسنلاب ى تح. (دنتس مل ةيمازلإ 2-4 تاوطلخ ال نم ىرخلال تادادع ال او فيرعتلا تافلماش نإ

## ISE ىل ع ةيها ن ال طاقن ةومجم تاتي دحت س ك عنت ال

ديهمت ال دي عي CCV ى تح ISE ال ةيها ن ال ةطقن تاتي دحت رشن ي ال CCV. [CSCvu80175](#) ببسب لي دب لك لم ا كت ال م تي ن ا م reboot CCV عي طتسي تنأ. لم ا كت ال دع ب ةرشابم

## ISE نم اهتلازاب CCV نم ةومجم ةلازا موقت ال

ءانثأ لسري تاتي دحت ال pxGrid [CSCvu47880](#) ال CCV ىل ع فورعم بي ع ال ببسب رادصا اذ تيار ل ازا ال ةومجم ال ك لذل، ع قوتم ال نع فلتخم قيسنت هل CCV نم ةومجم ةلازا

## بيولا ءالمع نم CCV طقس ي

ءالمع ال لقتني شيح [CSCvu47880](#) ISE ىل ع فورعم ال بي ع ال ببسب ةلكشم ال هذه ىل رظني 2.7 و 7 جي حصت 2.6 ي ةلكشم ال ل ح م ت. بيولا ءالمع نم ةلمك ةلازا اه ع بتي "جراخ" ةلا ح ىل ISE نم 2 جي حصت

pxgrid-server.log on ISE: اذ تني ا ي ري ن ا وه تدك ا عي طتسي تنأ

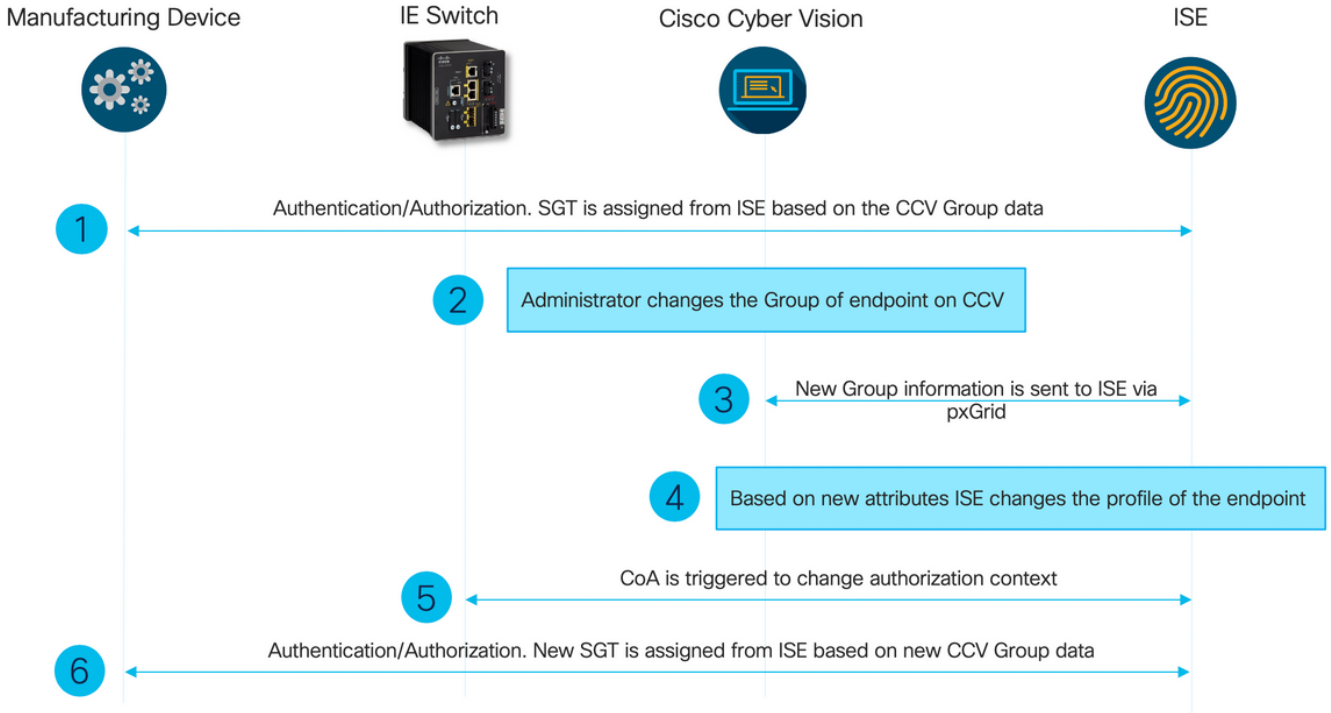
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionId=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726, 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 مادختسا ةلا ح عم ISE جم د

امدنع ةيها ن ال ةيها ن نم نام ال CCV عم ISE جم دي في نأ نكمي فيك نيوكتلا اذ ح ضوي، لم ا كت ال مادختسا ةي فيك ىل ع ةلثم ال نم دحاو ل ا ثم درجم اذ ه. ع ضوم ي ف TrustSec نوكتي، لم ا كت ال م اي ق ال درجم ب

روثع ال نكمي، ك لذل عم و، ةلاقم ال هذه قاطن جراخ TrustSec ل و ح م نيوكت ح رش ع ق ي: ةظالم ق. ح ل م ال ي ف هي ل ع

## ق ف دتلا و ا ي ج و ل و ب و ط ل ا



## نيوكتا

### 1. ISE يلع ريوطتلل ةلباقلا ةعومجملا تامالع نيوكت

ةمالع IOT\_Group1\_Asset نيوكت متي ،اقباس ةروكذمل مادختسالال ةلاح قيقت لجا نم 1 ةعومجملاب ةصاخلا CCV لوصأ نيبي زييمتلل ايودي IOT\_Group2\_Asset و TrustSec نامألا تاعومجم > تانوكملا > TrustSec > لمعل زكارم يلا لقتنا .يلاوتلا يلع 2 ةعومجملا ةروصلال ي ف حصوصم وه امك بيقرلا ةيمستب مق .ةفاضل قوف رقنا

Identity Services Engine      Home      Context Visibility      Operations      Policy      Administration      Work Centers

Network Access      Guest Access      TrustSec      BYOD      Profiler      Posture      Device Administration      PassiveID

Overview      Components      TrustSec Policy      Policy Sets      SXP      Troubleshoot      Reports      Settings

Security Groups

IP SGT Static Mapping

Security Group ACLs

Network Devices

Trustsec Servers

**Security Groups**

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit      Add      Import      Export      Trash      Push      Verify Deploy

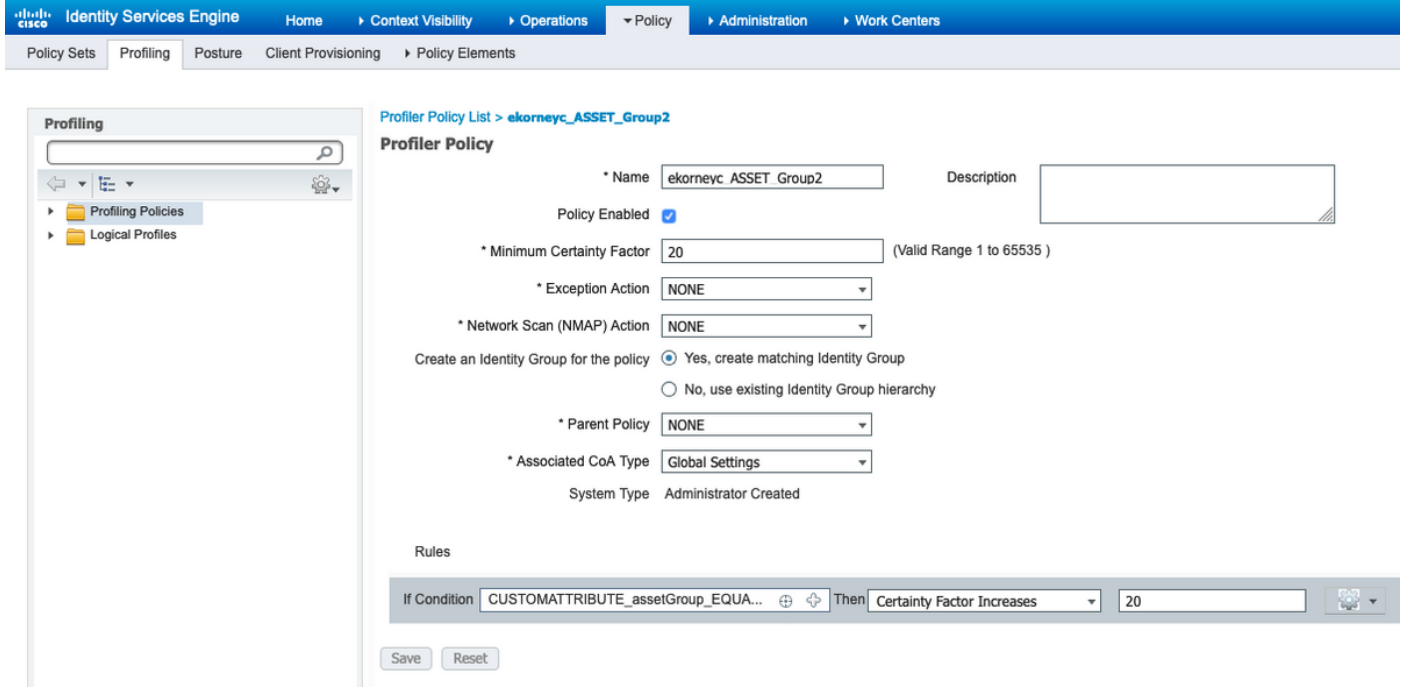
<input type="checkbox"/>	Icon	Name ↓	SGT (Dec / Hex)	Description	Learned from
<input type="checkbox"/>		Auditors	9/0009	Auditor Security Group	
<input type="checkbox"/>		BYOD	15/000F	BYOD Security Group	
<input type="checkbox"/>		Contractors	5/0005	Contractor Security Group	
<input type="checkbox"/>		Developers	8/0008	Developer Security Group	
<input type="checkbox"/>		Development_Servers	12/000C	Development Servers Security Group	
<input type="checkbox"/>		Employees	4/0004	Employee Security Group	
<input type="checkbox"/>		Guests	6/0006	Guest Security Group	
<input type="checkbox"/>		IOT_Group1_Asset	16/0010		
<input type="checkbox"/>		IOT_Group2_Asset	17/0011		

### 2. ةعومجملل ةصصخم تامسب فيرعتلا تافلئشنم جهن نيوكت

عزلال ي ف 3 ةوطخلال ي ف 1 ةعومجملل فيرعتلا تافلئشنم ءاشن نيوكت ءارج مت :ةظحالم

دنتسم لآ نم لولآ

لآ رقنآ . فآرعتلآ تآفلم ءآشن | آهن > فآرعتلآ تآفلم ئشنم > لمعلآ زكارم لآ لقتنآ  
طرشلآ رآبعت . ةروصلآ هذهل لآ ثامم لآ فآرعتلآ تآفلم ئشنم آهن نآوكت . ةفاصلآ  
CUSTOMATTRIBUTE:AssetGroup EQUALS Group2. وه آهن لآ اذآ فآ مدآتسم لآ



3. ةآوه تآعومآم لآ ةمئآق لآ SGT تآسآف س صآ صآ صآ ضآ فآو فآلآ تآسآف س نآوكت .

لآ فآو فآلآ آهن نآوكت ب م قوآ آهن لآ ةعومآم دآآ . تآسآف س لآ تآعومآم > ةسآف س لآ لآ لقتنآ  
فآ هنآوكت مآ فآلآ بآق رلآ نآفآعت مآفآ ، لآ لآ ةآآفآ نآ هنآ ظآلآ . ةروصلآ هذهل آق فو  
1. ةوطآلآ

نام آلآ تآعومآم	فآرعتلآ تآفلم	طورش	ةدعآق لآ مسآ
IOT_GROUP1_ASSE	PermitAccess	IdentityGroup-Name ةآوه تآعومآم فآسآف ةطقن ةآفآهن لآ:Profiled:ekorneyc _ASSET_GROUP1	مقر CCV ةعومآم ةسآف س 1
IOt_GROUP2_ASSE	PermitAccess	IdentityGroup-Name ةآوه تآعومآم فآسآف ةطقن ةآفآهن لآ:Profiled:ekorneyc _ASSET_GROUP2	ةعومآم لآ ةسآف س ةآفآهن لآ CCV

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits		
🟢	Default	Default policy set		Default Network Access	10		
▶ Authentication Policy (3)							
▶ Authorization Policy - Local Exceptions							
▶ Authorization Policy - Global Exceptions							
▼ Authorization Policy (18)							
+	Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
🟢	CCV Group 1 Policy	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled.stormyc_ASSET_Group1		Permissions	IOT_Group1_Asset	1	🔗
🟢	CCV Group 2 Policy	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled.stormyc_ASSET_Group2		Permissions	IOT_Group2_Asset	1	🔗

## ةحصل ل نم ققحت ل

ححص لكشب نيوكتل لمع ديكأتل مسقلا اذه مدختسا.

### 1. ةومجم ل ادا نسا ةياهن ل طاقن ةقداصم

و 17-54:IOT\_Group2\_Asset و 16-54:IOT\_Group1\_Asset نم لك نمضتت ةئيب ل تانايب نأ ىرت نأ كنكمي، ل وحم ل لىل ع 54:IOT\_Group2\_Asset.

```
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#

نبيعت متيف 1، ةومجم CCV ةسايس قباطت ،كلذل ةجيتنكو قداصت ةياهنلا طاقن  
ب IOT\_Group1\_Asset.

The screenshot shows the Cisco ISE dashboard with the following statistics:

- Misconfigured Supplicants: 1
- Misconfigured Network Devices: 0
- RADIUS Drops: 0
- Client Stopped Responding: 0

Below the statistics is a table of authentication sessions:

Time	Status	Details	Repeat C...	Identity	Endpoint ID	Endpoint Profile	Authentication Pol...	Authorization Policy	Authorization Profiles	IP Address
Jun 25, 2020 10:37:32.590 AM	Authorized		0	00F2.8B.A0.3A.59	00F2.8B.A0.3A.59	ekomeyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermiAccess	172.16.0.100
Jun 25, 2020 10:37:31.567 AM	Authorized			00F2.8B.A0.3A.59	00F2.8B.A0.3A.59	ekomeyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermiAccess	172.16.0.100

مت لوصول لوبق تانايب نأ show authentication session interface fa1/7 detail لوجمل دكؤي  
حاجنبا اهقيا ببطت.

```
KJK_IE4000_10#show authentication sessions interface fal/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_Fal/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
```

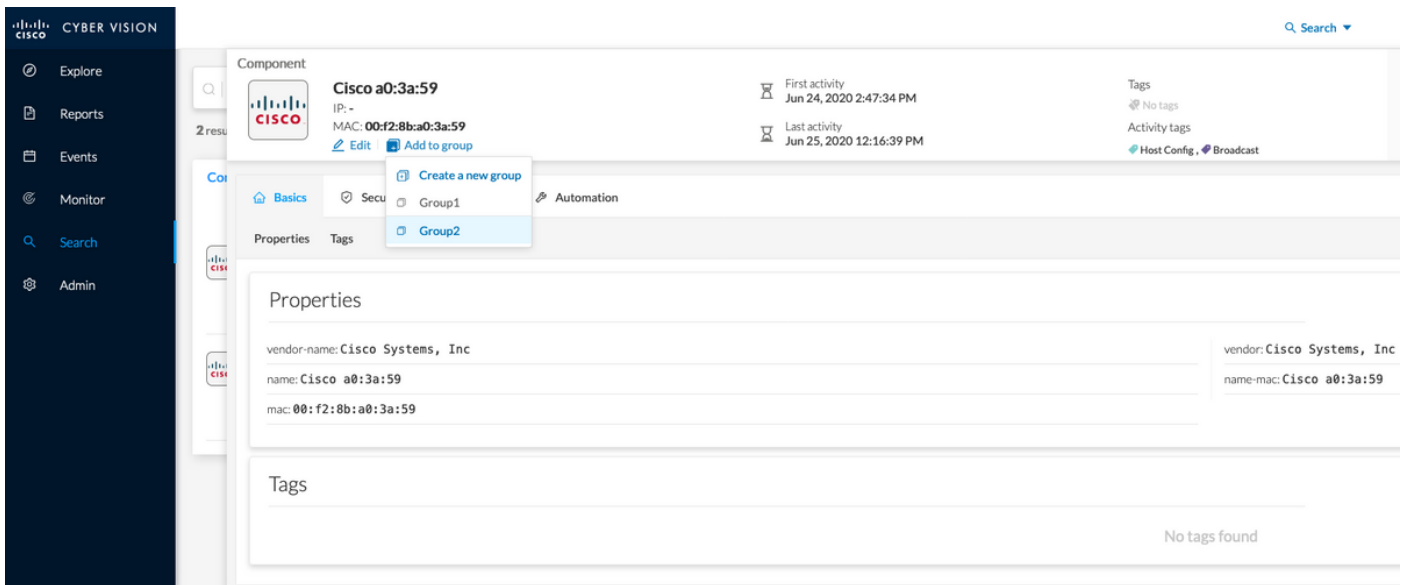
KJK\_IE4000\_10#

## ةومجم لريغت ب لوؤسمل موق ي 2.

ةومجم لىل هفصأو هيلع رقنا ،ةياهنلا ةطقنل Mac ناوع قصلل .ثحبلا لىل لقتنا

،يللاتلابو .دحاو لاقنتا ي 2 لىل 1 نم ةومجم لريغت كنكمي ال ،CCV ي :ةظحال  
،ةيلاتل 2 ةومجم لنيعتو الو ةومجم ل نم ةياهنلا ةطقن ةلازا بجي .





### 3-6 ىل ع ة ياهنلا طاقن ة عومجم ري يغت ري ثأت . CCV

تم اق ، في رعتلا تافلم ءاشن ة يلمع لض فب . ةروصلال هذه في 6 و 5 و 4 تاوطلال سكعنت ة وطلال في رهطت يتلا ekorneC\_ASSET\_GROUP2 ىل ة يوهلا ة عومجم ري يغت تب ة ياهنلا ةطقن ة ياهنلا ةطقن ة قداصم ة داع ء اريخا و (5 ة وطلال) ل وحملال ىل ء CoA ل اس راب ISE م ايق ىل ء ا م ام ، 4 (6 ة وطلال).

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Profile	Authentication Pol.	Authorization Policy	Authorization Profiles	IP Address	Network Device	Device Port	Identity Group
Jun 25, 2020 10:43:00.411 AM	Success		0	00F2:8B:AO:3A:59	00F2:8B:AO:3A:59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_AssetPermiAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59.503 AM	Success		0	00F2:8B:AO:3A:59	00F2:8B:AO:3A:59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_AssetPermiAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59.482 AM	Success		0	00F2:8B:AO:3A:59	00F2:8B:AO:3A:59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermiAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group1
Jun 25, 2020 10:37:31.567 AM	Success		0	00F2:8B:AO:3A:59	00F2:8B:AO:3A:59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermiAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group1

دي دجلال بيقرلا ني عت مت هن ا show authentication session interface fa1/7 detail ل وحملال دك و ي.

```
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#

## قحل مل

### Switch TrustSec ب طبترم ل ن ي و ك ت ل

م اد خ ت س اب اه ن ي و ك ت ب ج ي و running-config نم اعزج CTS دامتعا تاناي ب لكش ت ال :ةظ ح الم  
زاي ت م ال ل EXEC ع ض و ي ف CTS دامتعا تاناي ب فر ع م ل password <id> رم ال

```
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#

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة يرش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ل أ مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا