

# Configuratie ISE 2.7 pxGrid CCV 3.1.0-integratie

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Stroomdiagram op hoog niveau](#)

[Configuraties](#)

- [1. Schakel pxGrid-tests op een van de PSN's in](#)
- [2. Configureer endpoint aangepaste kenmerken op ISE](#)
- [3. Profielbeleid instellen met behulp van aangepaste kenmerken](#)
- [4. Aangepaste kenmerken voor het opstellen van profielen inschakelen](#)
- [5. Configuratie van automatische goedkeuring voor PxGrid-clients](#)
- [6. CCV-certificaat exporteren](#)
- [7. CCV-identiteitsbewijs uploaden naar ISE Trusted Store](#)
- [8. genereert certificaat voor CCV](#)
- [9. Downloadcertificaatketen in PKCS12-formaat](#)
- [10. ISE-integratiedetails op CCV configureren](#)
- [11. Upload certificaatketen op CSV en start integratie.](#)

[Verifiëren](#)

[CCV-integratieverificatie](#)

[ISE-integratieverificatie](#)

[Controleer CCV-groepswijziging](#)

[Problemen oplossen](#)

[Debugs op ISE inschakelen](#)

[Debugs op CCV inschakelen](#)

[Bulkdownloads](#)

[Niet alle endpoints worden op ISE gemaakt](#)

[Asset Group is niet beschikbaar op ISE](#)

[De updates van de Endpoint Group worden niet op ISE weerspiegeld](#)

[Een groep verwijderen uit CCV is niet uit ISE verwijderen](#)

[CCV zakt af van webclients](#)

[ISE-integratie met CCV TrustSec Use Case](#)

[Topologie en de stroom](#)

[Configureren](#)

- [1. Instellen van schaalbare groepstypen op ISE](#)
- [2. Profielbeleid instellen met aangepaste kenmerken voor groep 2](#)
- [3. Het machtigingsbeleid configureren om SGT's toe te wijzen op basis van Endpoint Identity Group op ISE](#)

[Verifiëren](#)

- [1. Endpoints voor verificatie op basis van CCV-groep 1](#)

[2. beheerder wijzigt de groep](#)

[3-6. Effect van verandering van endpointgroepen op CCV](#)

[Bijlage](#)

[Configuratie van switchvertrouwenSEC-gerelateerde](#)

## Inleiding

Dit document beschrijft hoe u Identity Services Engine (ISE) 2.7 kunt configureren en problemen oplossen met de integratie van Cisco Cyber Vision (CCV) 3.1.0 via Platform Exchange Grid v2 (pxGrid). CCV wordt geregistreerd met pxGrid v2 als uitgever en publiceert informatie over endpointkenmerken naar ISE voor IOTASSET-woordenboek.

## Voorwaarden

### Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- ISE
- Cisco Cyber Vision

### Gebruikte componenten

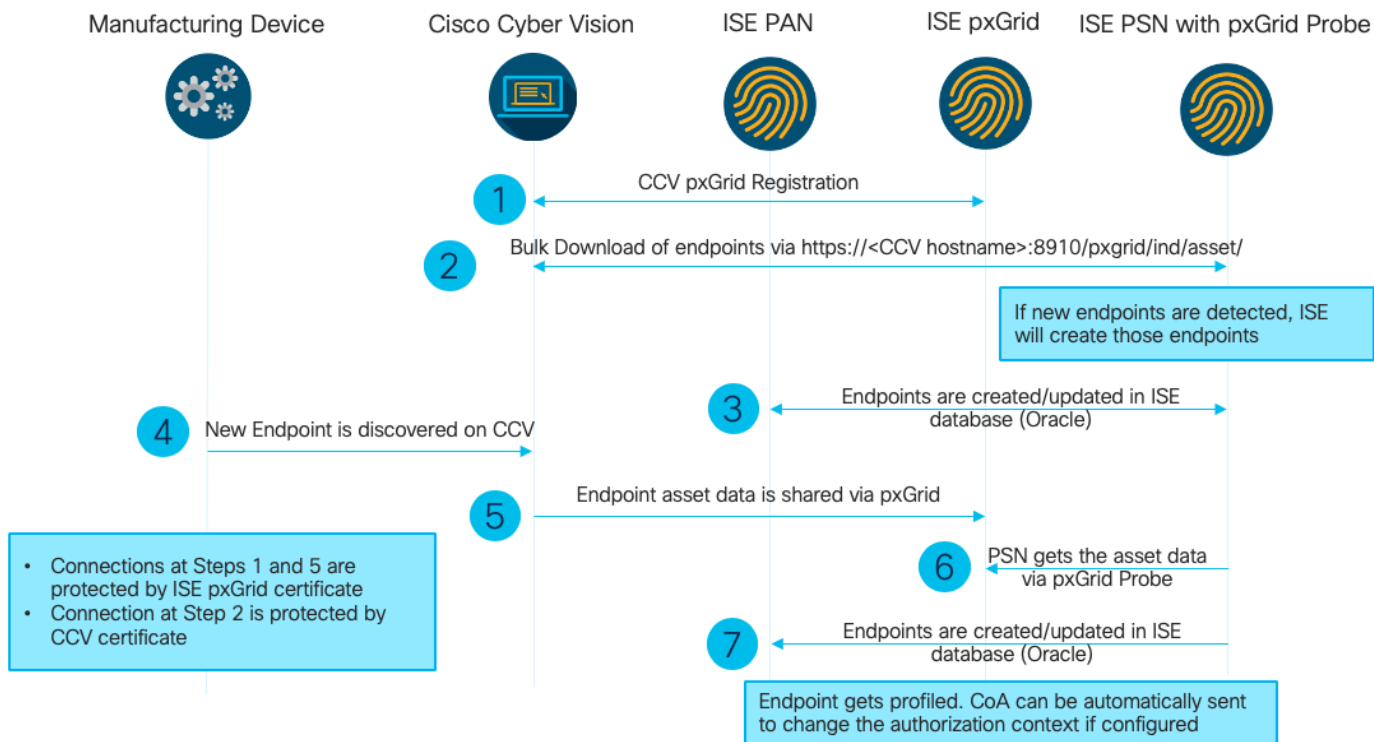
De informatie in dit document is gebaseerd op de volgende software- en hardwareversies:

- Cisco ISE versie 2.7 Patch 1
- Cisco Cyber Vision versie 3.1.0
- Industriële Ethernet-switch IE-4000-4TC4G-E met S/w 15.2(6)E

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Configureren

### Stroomdiagram op hoog niveau



Deze ISE-implementatie wordt in de instellingen gebruikt.

#### 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 is Primair Admin Node (PAN) en PxGrid-knooppunt.

ISE 2.7-2ek is Policy Service Node (PSN) met PxGrid-sonde ingeschakeld.

Dit zijn de stappen die overeenkomen met het eerder genoemde diagram.

1. CCV registreert activaTopic op ISE via PxGrid versie 2. Overeenkomstige stammen van CCV:

Opmerking: Om de pxGrid-logbestanden op CCV te bekijken, geeft u de volgende opdracht **journalist-u pxgrid-agent uit**.

```

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. ISE PSN met de PxGrid-sonde is ingeschakeld en kan bestaande pxGrid-activa (profiler.log) in één grote hoeveelheid downloaden:

```
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. Endpoints worden aan de PSN toegevoegd met behulp van pxGrid-sonde en PSN verzend persing naar de PAN om deze endpoints (**profiler.log**) op te slaan. Endpoints die op ISE zijn gemaakt, kunnen in endpointdetails worden bekeken onder Context Visibility.

```
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. Nadat u een eindpunt in een groep plaatst, stuurt CCV STOMP-bericht via poort 8910 om het eindpunt met de Gegevens van de Groep in Aangepaste Attributen bij te werken. Overeenkomende stammen van CCV:

```
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-knooppunt ontvangt STOMP-update en stuurt dit bericht naar alle abonnees, inclusief PSN's met de PxGrid-sonde ingeschakeld. **Pxgrid-server.log** op pxGrid-knooppunt.

```
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. PSN met pxGrid-sonde die is ingeschakeld als abonnee op activabereik ontvangt het bericht van pxGrid-knooppunt en werkt het eindpunt (**profiler.log**) bij. Updateerde eindpunten op ISE kunnen in eindpuntdetails onder Context Visibility and worden bekeken.

```
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSsubscriber -::::-
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.INDSsubscriber -::::-
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. PSN met de pxGrid-sonde het eindpunt opnieuw vormgeven als een nieuw beleid wordt aangepast (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
```

## Configuraties

Opmerking: De stappen 1 - 4 zijn vereist zelfs als u slechts het zicht van assetGroup en in Context Visibility and wilt hebben.

### 1. Schakel pxGrid-tests op een van de PSN's in

Navigeer naar **Beheer > Systeem > Plaatsing**, selecteer ISE knooppunt met PSN Persona. Naar het tabblad **Configuration** overschakelen. Zorg ervoor dat de **pxGrid**-sonde is ingeschakeld.



**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. Configureer endpoint aangepaste kenmerken op ISE

Navigeer naar **Administratie > Identity Management > Instellingen > Endpoint Custom Attributes**. Configureer aangepaste kenmerken (assetGroup) aan de hand van deze afbeelding. CCV 3.1.0 ondersteunt alleen Aangepaste **assetGroup**-kenmerk.

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

Identities Groups External Identity Sources Identity Source Sequences Settings

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. Profielbeleid instellen met behulp van aangepaste kenmerken

Navigeren in op **Workcenters > Profiler > Profileren > Profileren beleid**. Klik op **Toevoegen**. Configureer beleid dat vergelijkbaar is met deze afbeelding. De in dit beleid gebruikte uitdrukking van de conditionering is **CUSTOMATTRIBUTE:assetGroup EQUALS Group1**.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Profiling

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. Aangepaste kenmerken voor het opstellen van profielen inschakelen

Navigeren in op **Workcenters > Profiler > Profileren > Profileren beleid**. Klik op **Toevoegen**. Configureer beleid dat vergelijkbaar is met deze afbeelding. Zorg ervoor dat **Aangepaste eigenschap voor het maken van profielen** is ingeschakeld.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Profiler > Posture > Device Administration > PassiveID. The main content area is titled "Profiler Configuration". On the left, there is a sidebar with "Profiler Settings" and "NMAP Scan Subnet Exclusions". The main configuration area includes the following settings:

- \* CoA Type: Reauth (dropdown menu)
- Current custom SNMP community strings: \*\*\*\*\* (with a "Show" button)
- Change custom SNMP community strings: (text input field) (For NMAP, comma separated.)
- Confirm changed custom SNMP community strings: (text input field) (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

At the bottom of the configuration area, there are "Save" and "Reset" buttons.

## 5. Configuratie van automatische goedkeuring voor PxGrid-clients

Navigeer naar **Administratie > pxGrid Services > Instellingen**. Selecteer **Automatisch nieuwe op het certificaat gebaseerde rekeningen goedkeuren** en klik op **Opslaan**. Deze stap waarborgt dat u geen CCV hoeft goed te keuren zodra de integratie is voltooid.

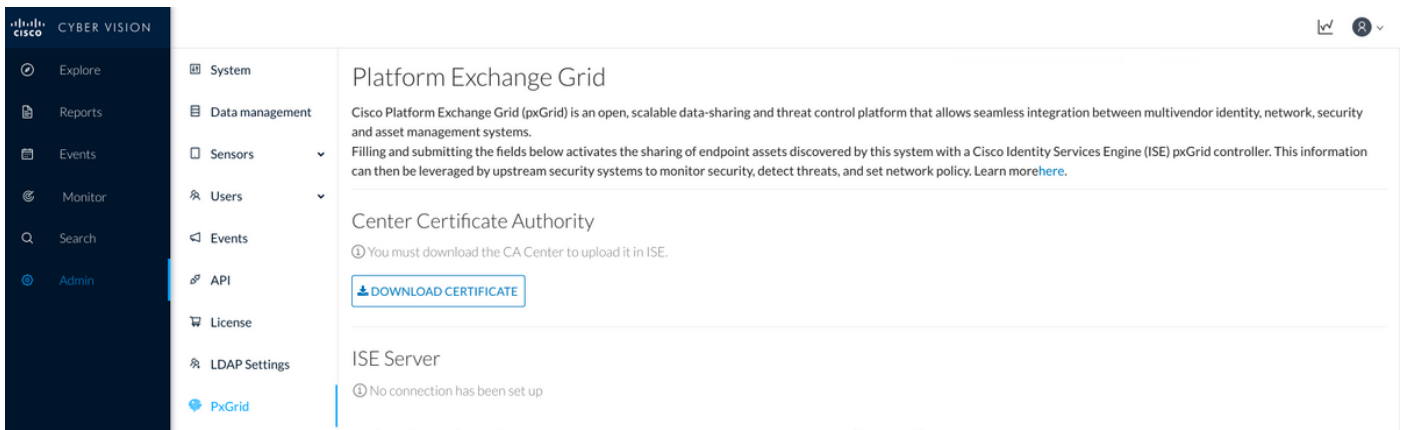
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > pxGrid Services > Feed Service > Threat Centric NAC. The main content area is titled "PxGrid Settings". The settings are:

- Automatically approve new certificate-based accounts
- Allow password based account creation

At the bottom of the settings area, there are "Use Default" and "Save" buttons.

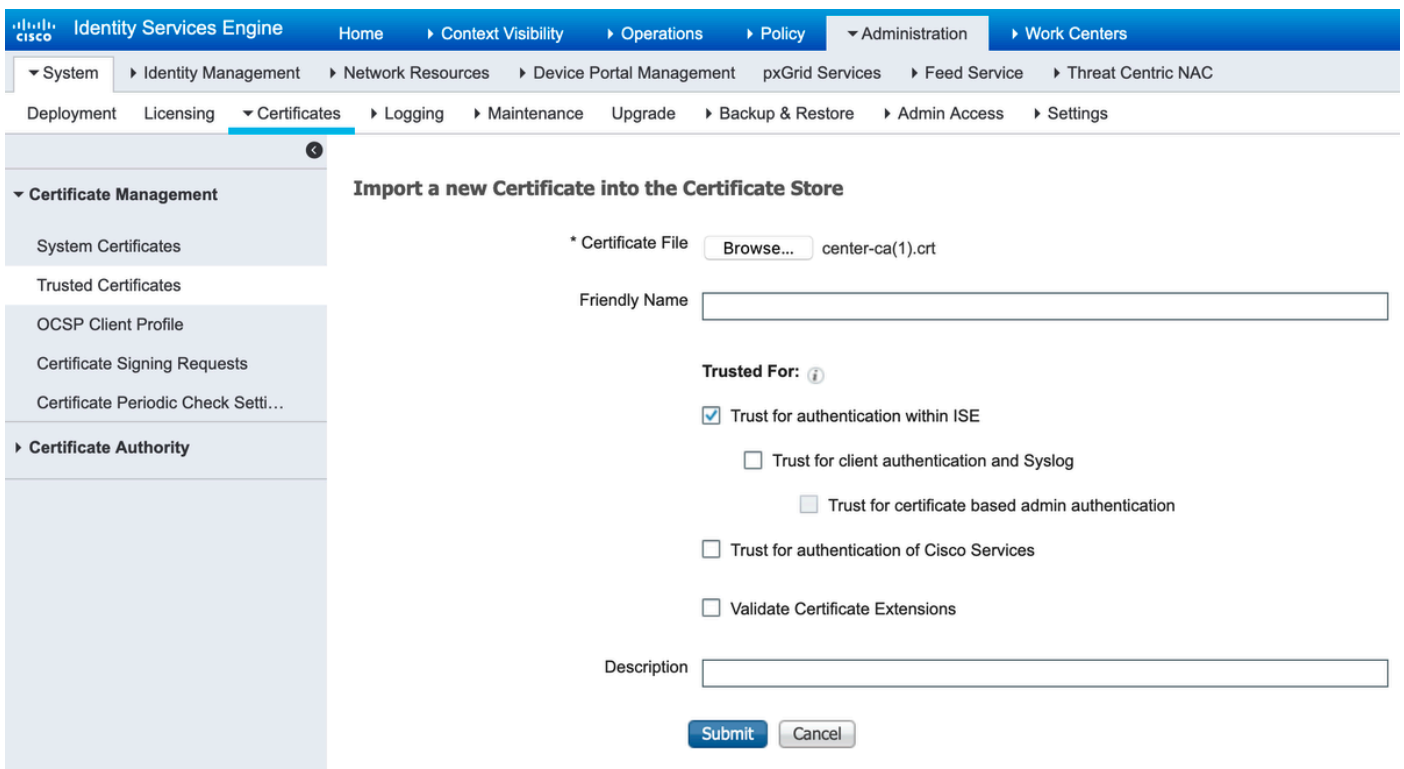
## 6. CCV-certificaat exporteren

Navigeer naar **Admin > pxGrid**. Klik op **DOWNLOADCERTIFICAAT**. Dit certificaat wordt gebruikt tijdens pxGrid-registratie, zodat ISE het moet vertrouwen.



## 7. CCV-identiteitsbewijs uploaden naar ISE Trusted Store

Navigeer naar **Administratie > Certificaten > certificaatbeheer > Trusted Certificaten**. Klik op **Importeren**. Klik op **Bladeren** en selecteer het CCV-certificaat in stap 5. Klik op **Inzenden**.



## 8. genereert certificaat voor CCV

Tijdens pxGrid-integratie en -updates heeft CCV het client-certificaat nodig. Het moet worden uitgegeven door ISE interne CA, gebruikmakend van **PxGrid\_certificaatmodel**.

Navigeer naar **Administratie > pxGrid Services > Certificaten**. Populeren velden volgens deze afbeelding. Veld van de gezamenlijke naam (CN) is verplicht, aangezien het doel van ISE CA is een identiteitsbewijs af te geven. U dient de hostname van CCV in te voeren. De GN-veldwaarde is van cruciaal belang. Om de hostname van CCV te controleren geeft u de opdracht **hostname** uit. Selecteer PKCS12 als **certificaatdownloads**.

```
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)   - +

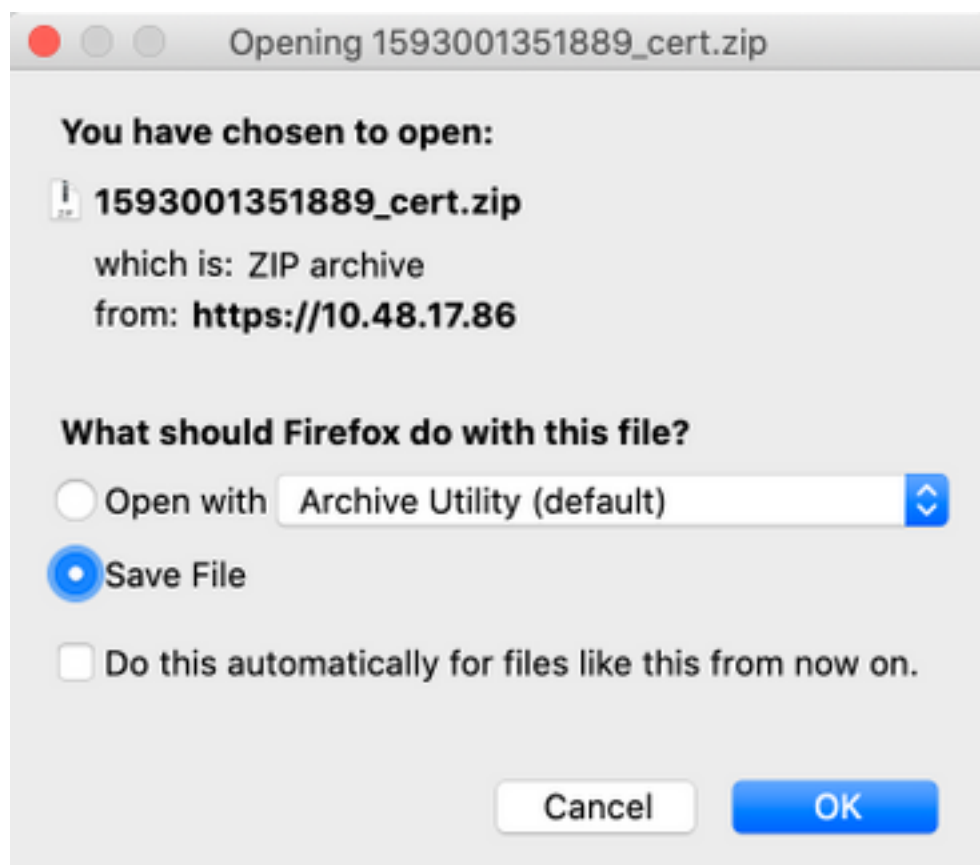
Certificate Download Format \*  ⓘ

Certificate Password \*  ⓘ

Confirm Password \*

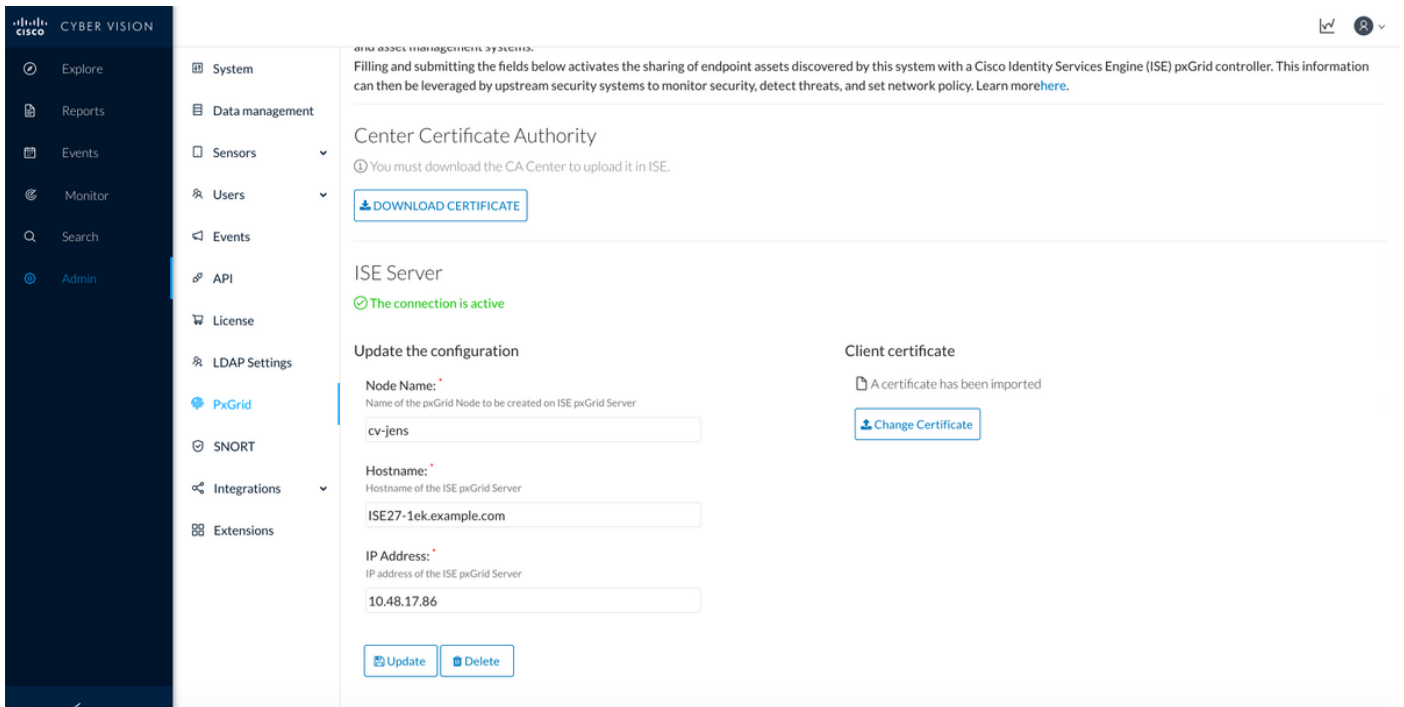
## 9. Downloadcertificaatketen in PKCS12-formaat

Wanneer u het certificaat in het PKCS12-formaat installeert, samen met het CCV-identiteitsbewijs ISE Interne CA-keten, is op CCV geïnstalleerd om ervoor te zorgen dat CCV ISE vertrouwt wanneer de PxGrid-communicatie vanaf ISE wordt gestart, bijvoorbeeld, PxGrid-overlevingsberichten.



## 10. ISE-integratiedetails op CCV configureren

Navigeer naar **Admin > pxGrid**. Configureer de naam van het knooppunt, deze naam wordt op ISE weergegeven als een clientnaam bij **Beheer > pxGrid Services > Web Clients**. Configureer de naam en het IP-adres van ISE pxGrid-knooppunt. Zorg ervoor dat CCV ISE FQDN kan oplossen.



The screenshot shows the Cisco Cyber Vision Admin interface. The left sidebar contains navigation options: Explore, Reports, Events, Monitor, Search, and Admin. The main content area is titled 'Center Certificate Authority' and includes a 'DOWNLOAD CERTIFICATE' button. Below this is the 'ISE Server' configuration section, which shows a green status indicator 'The connection is active'. The configuration fields are: Node Name (cv-jens), Hostname (ISE27-1ek.example.com), and IP Address (10.48.17.86). There are 'Update' and 'Delete' buttons at the bottom. To the right, the 'Client certificate' section shows a message 'A certificate has been imported' and a 'Change Certificate' button.

## 11. Upload certificaatketen op CSV en start integratie.

Navigeer naar **Admin > pxGrid**. Klik op **Wijzigingscertificaat**. Selecteer het certificaat dat door ISE CA is afgegeven uit stappen 8-9. Voer het wachtwoord in uit stap 8. en klik op **OK**.

Do you want to enter a password?

.....

Ok Cancel

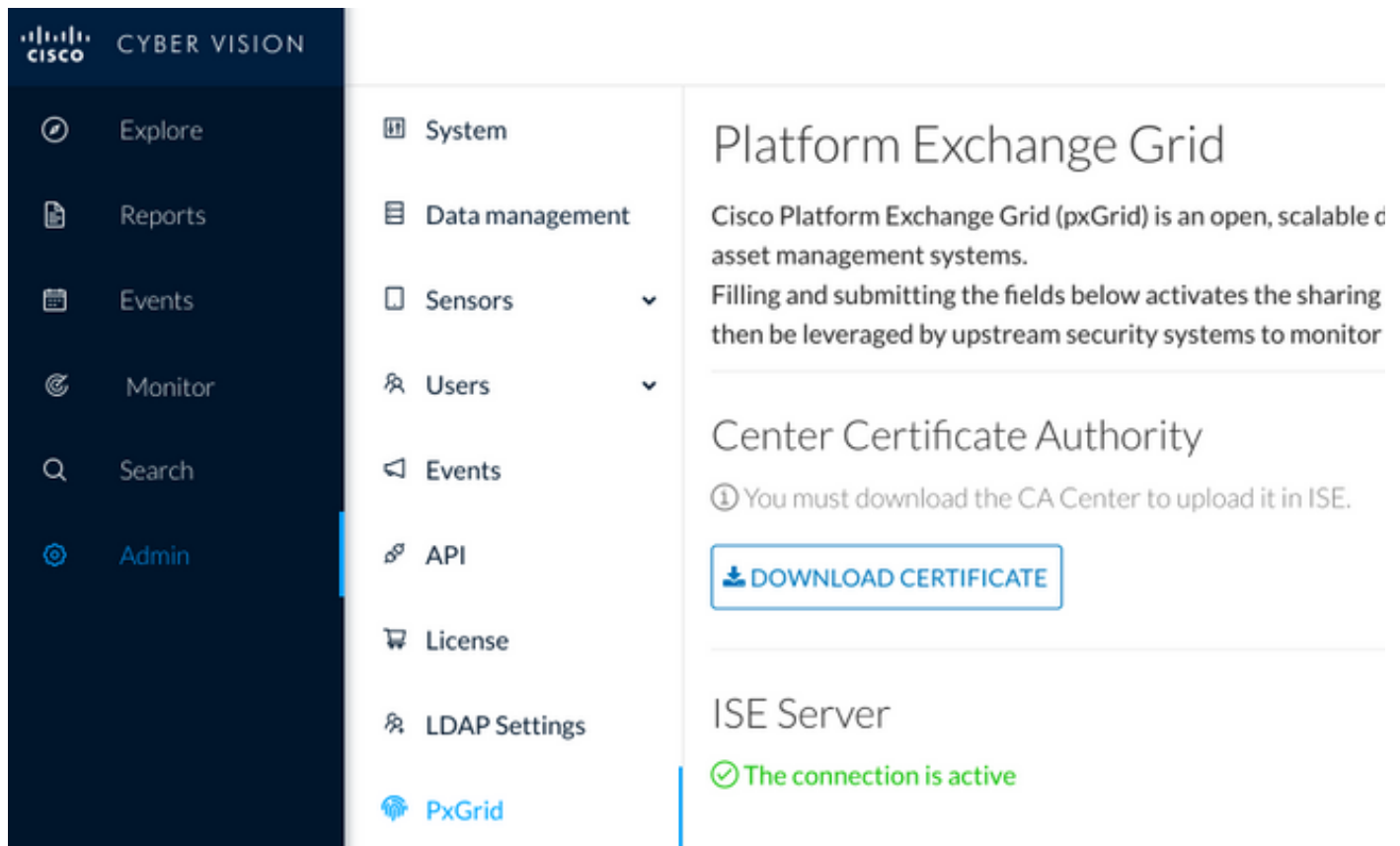
Klik op **Update**, die de eigenlijke CCV - ISE integratie in gang zet.

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

## CCV-integratieverificatie

Zodra de integratie voltooid is, kunt u bevestigen dat het geslaagd is door in **Admin > pxGrid** te navigeren. U dient te zien **dat de verbinding een actief bericht is** onder de ISE Server.



The screenshot displays the Cisco Cyber Vision Admin interface. The left sidebar shows the navigation menu with 'Admin' selected. The main content area is titled 'Platform Exchange Grid' and includes the following sections:

- Platform Exchange Grid**: A description stating that Cisco Platform Exchange Grid (pxGrid) is an open, scalable asset management system. It notes that filling and submitting the fields below activates sharing, which can be leveraged by upstream security systems.
- Center Certificate Authority**: A section with a warning icon and the text 'You must download the CA Center to upload it in ISE.' Below this is a blue button labeled 'DOWNLOAD CERTIFICATE'.
- ISE Server**: A section with a green checkmark icon and the text 'The connection is active'.

## ISE-integratieverificatie

Navigeer naar **Beheer > PxGrid Services > Web Clients**. Bevestig dat de status van CCV-client (cv-jens) is **ingeschakeld**.

Opmerking: Verwacht wordt dat de status van de CCV pxGrid-client als **offline** wordt weergegeven in het menu **Alle clients**, omdat de status alleen de PxGrid v1-status toont.



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...	/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

Opmerking: Vanwege [CSCvt78208](#) zal u niet onmiddellijk zien dat CCV /topic/com.cisco.ise.endpoints.asset heeft, zal het alleen bij eerste publicatie worden getoond.

## Controleer CCV-groepswijziging

Navigeren in **Verken > Alle gegevens > Lijst van componenten**. Klik op een van de componenten en **Voeg** het toe aan de groep.

The screenshot displays the Cisco Cyber Vision interface. On the left, a sidebar contains navigation options: Explore, Reports, Events, Monitor, Search, and Admin. The main area shows a list of 5 components. The component 'Cisco a0:3a:59' is selected, and a context menu is open over it, offering options: 'Add to group', 'Create a new group', 'Group1', and 'Group2'. The component list table is as follows:

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:cccc:cccc	-	Mar 13, 2020 1:52:23 PM	Jun 24, 2020 4:27:19 PM	-	01:00:0c:cccc:cccc
255.255.255.255	-	Mar 13, 2020 1:52:09 PM	Jun 24, 2020 4:25:45 PM	255.255.255.255	ff:ff:ff:ff:ff:ff
Cisco a0:3a:59	-	Jun 24, 2020 2:47:34 PM	Jun 24, 2020 4:25:45 PM	-	00:f6:63:4d:d6:85

Controleer of /topic/com.cisco.ise.endpoints.asset nu is opgenomen in de lijst van publicaties tegen CCV.



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

Click here to do wirel

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions

Rows/Page 25 1




Refresh

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	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	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.se...	/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.endpo...		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.se...		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	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		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.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		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.se...		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		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.se...	/topic/com.cisco.ise.session.internal	10.48.17.88	ON	2020-06-24 15:01:26 UTC	00:00:08:31

Bevestig dat Group1 die via CCV is toegewezen, wordt gereflecteerd op ISE en het profileringsbeleid werd van kracht door te navigeren naar **Context Visibility > Endpoints**. Selecteer het eindpunt dat in de vorige stap is bijgewerkt. Naar het tabblad Eigenschappen overschakelen. De sectie van de aangepaste eigenschappen zou de nieuw gevormde groep moeten weerspiegelen.

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

De sectie "Overige Eigenschappen" somt alle andere eigenschappen van activa op die van CCV worden ontvangen.

## 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

## Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

### Debugs op ISE inschakelen

Om insecten op ISE te kunnen selecteren, navigeer dan naar **Beheer > Systeem > Vastlegging > Logconfiguratie > Debug Log Configuration**. Logniveaus instellen op deze:

Persona	Naam van component	Logniveau	Bestand om te controleren
PAN (optioneel)	voortrekker	DEBUG	profiler.log
PSN met PxGrid-onde ingeschakeld	voortrekker	DEBUG	profiler.log
PxGrid	sproeier	TRACE	pxgrid-server.log

### Debugs op CCV inschakelen

Zo kunnen uiteinden op CCV worden ingeschakeld:

- Maak een bestand `/data/etc/sbs/pxgrid-agent.conf` met de opdracht `/data/etc/sbs/pxgrid-agent.conf`
- Plakt deze inhoud in `pxgrid-agent.conf`-bestand met behulp van de `vi`-editor met de opdracht `vi /data/etc/sbs/pxgrid-agent.conf`

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

- Start **Pxgrid-agent** opnieuw door de opdracht **Pxgrid-agent voor systeemherstarten uit te voeren**
- Bekijk logbestanden met de opdracht **journalist -u pxgrid-agent**

## Bulkdownloads

CCV publiceert Bulk Download URL aan ISE tijdens de integratie. ISE PSN met pxGrid-sonde is ingeschakeld voor Bulk Download met het gebruik van deze URL. Zorg ervoor dat:

- De hostname in de URL is correct oplosbaar vanuit het ISE-perspectief
- Mededeling van PSN in poort 8910 aan CCV is toegestaan

`profiler.log` op PSN met pxGrid-sonde ingeschakeld:

```
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}]]
```

Het bulkdownload kan mislukken door [CSCvt75422](#). u dient deze fout in `profiler.log` op ISE te zien om het te bevestigen. Het defect is vastgesteld in CCV 3.1.0.

```
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)
```

## Niet alle endpoints worden op ISE gemaakt

Sommige eindpunten op CCV kunnen te veel eigenschappen in bijlage hebben, zodat de ISE-database deze niet kan verwerken. Het kan worden bevestigd als u deze fouten ziet in `profiler.log` op ISE.

```
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)
```

## Asset Group is niet beschikbaar op ISE

Als AssetGroup niet beschikbaar is op ISE, wordt het beleid voor profielen hoogstwaarschijnlijk niet geconfigureerd met behulp van Aangepaste Attributen (raadpleeg stap 2-4.0 in het gedeelte Configuraties van het document). Zelfs voor Context Visibility and, enkel om groeieigenschappen weer te geven, zijn Profileringsbeleid en andere instellingen uit stap 2-4 verplicht.

## De updates van de Endpoint Group worden niet op ISE weerspiegeld

Ten gevolge van [CSCvu80175](#) publiceert CCV geen endpointupdates voor ISE totdat CCV direct na de integratie herstart. U kunt de CCV opnieuw opstarten als de integratie als een bewerking is uitgevoerd.

## Een groep verwijderen uit CCV is niet uit ISE verwijderen

Dit probleem wordt gezien als gevolg van het bekende defect op CCV [CSCvu47880](#). De PxGrid-update die tijdens het verwijderen van de groep van CCV met een ander dan verwacht formaat wordt verstuurd, wordt derhalve niet verwijderd.

## CCV zakt af van webclients

Dit probleem wordt gezien ten gevolge van het bekende defect op ISE [CSCvu47880](#), waar klanten zich naar OFF-staat begeven, gevolgd door volledige verwijdering van Web Clients. Het probleem is opgelost in 2,6 pleister 7 en 2,7 pleister 2 van ISE.

U kunt het bevestigen als u deze fouten in `pxgrid-server.log` ziet op ISE:

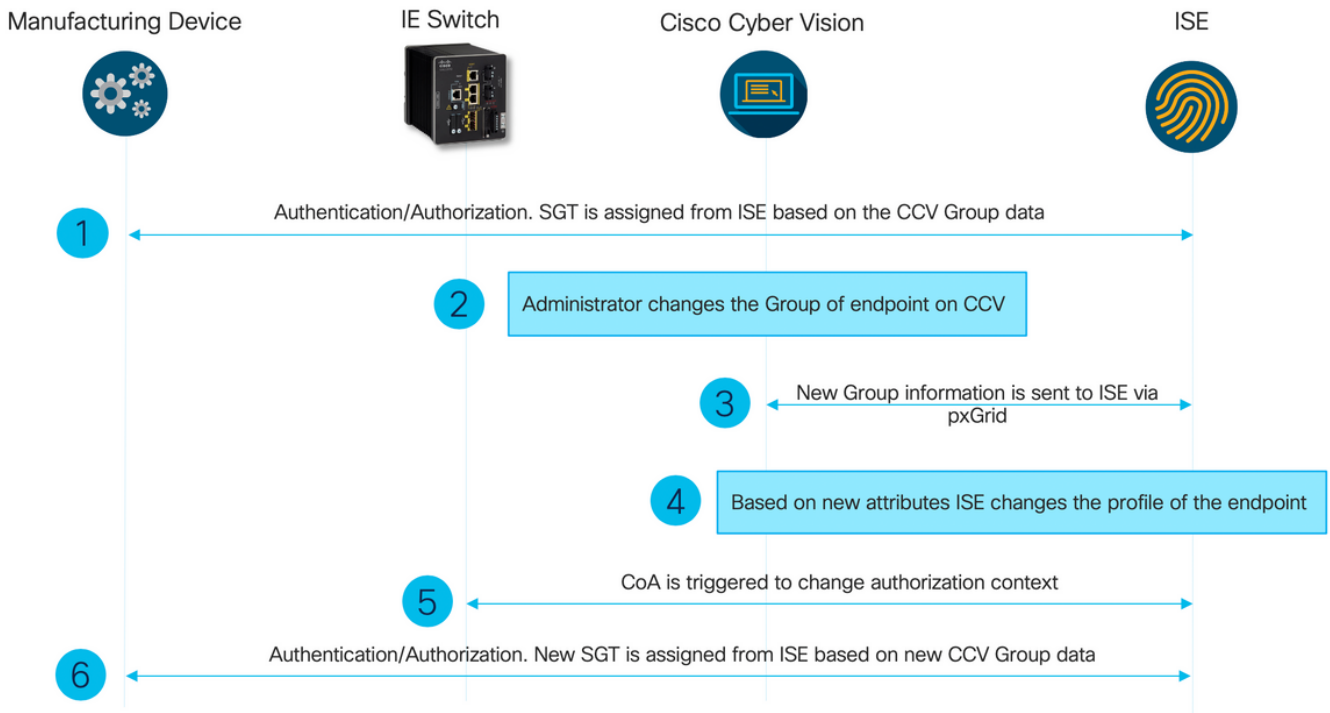
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionId=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726,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

## ISE-integratie met CCV TrustSec Use Case

Deze configuratie laat zien hoe ISE-integratie met CCV security end-to-end kan profiteren wanneer TrustSec in werking is. Dit is slechts één van de voorbeelden van hoe integratie kan worden gebruikt, zodra de integratie is voltooid.

Opmerking: VertrouwenSec schakelaar configuratie uitleg valt buiten het toepassingsgebied van dit artikel, maar kan worden gevonden in Bijlage.

# Topologie en de stroom



## Configureren

### 1. Instellen van schaalbare groepstypen op ISE

Om het eerder genoemde gebruiksgeschied te bereiken, wordt de IOT\_Group1\_Asset en IOT\_Group2\_Asset van de TrustSec Tag handmatig geconfigureerd om CCV activa van Group2 te differentiëren van Group2. Navigeer naar **werkcentra > TrustSec > Componenten > Security Groepen**. Klik op **Toevoegen**. Naam SGT's zoals weergegeven in de afbeelding.

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

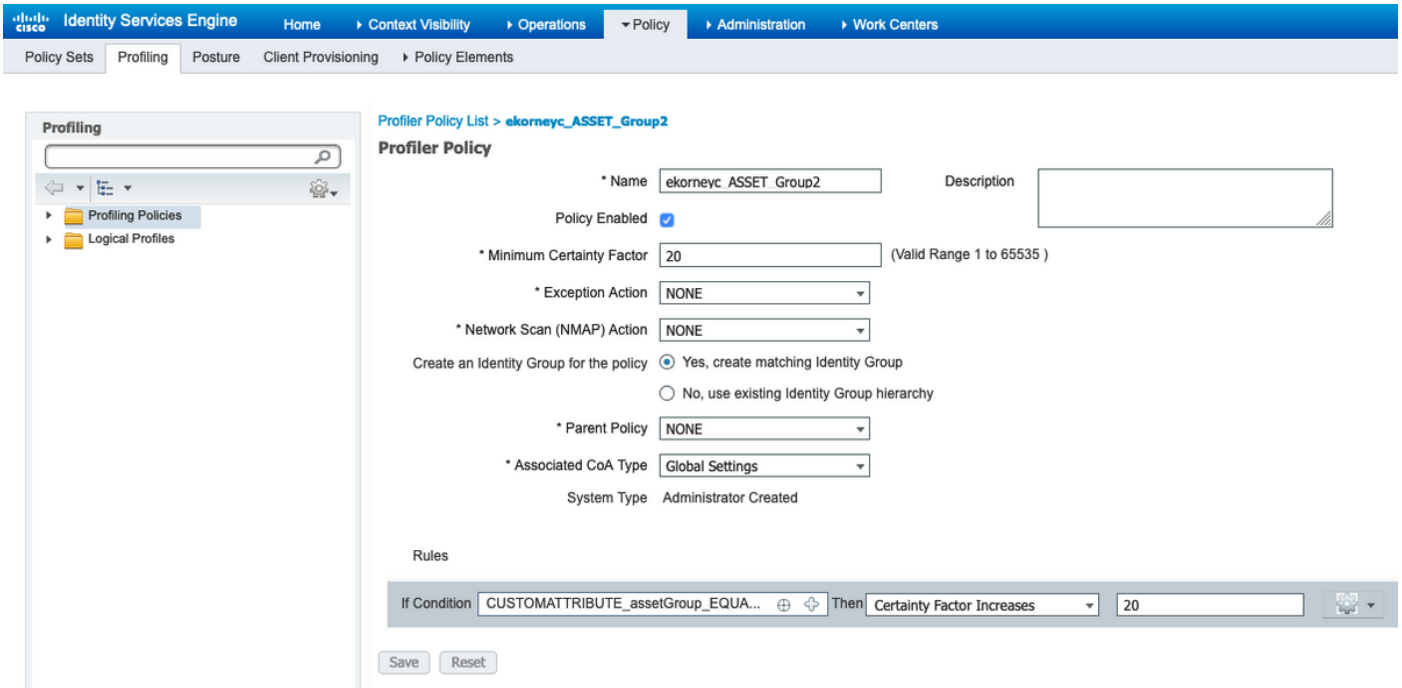
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

<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. Profielbeleid instellen met aangepaste kenmerken voor groep 2

Opmerking: Configuratie voor groep 1 beschreven in Stap 3. in het eerste deel van het document.

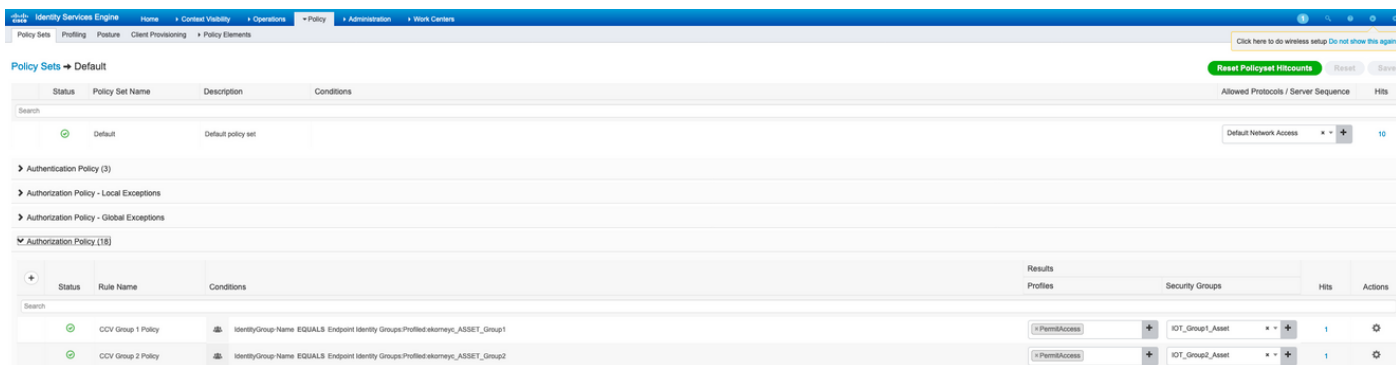
Navigeren in op **Workcenters > Profiler > Profileren > Profileren beleid**. Klik op **Toevoegen**. Configureer beleid dat vergelijkbaar is met deze afbeelding. De in dit beleid gebruikte uitdrukking van de conditionering is **CUSTOMATTRIBUTE:assetGroup EQUALS Group2**.



### 3. Het machtigingsbeleid configureren om SGT's toe te wijzen op basis van Endpoint Identity Group op ISE

Navigeren in op **beleid > Beleidsformaten**. Selecteer **Beleidsinstelling** en stel **autorisatiebeleid** in zoals in deze afbeelding. Merk op dat SGT als resultaat hiervan is ingesteld in Stap 1. wordt toegewezen.

Naam van regel	Voorwaarden	profielen	Beveiligingsgroepen
Beleid CCV Group 1	IdentityGroup· Naam EQUALS Endpoint Identity Group:Gedeeld:ekorneyc_ ASSET_Group1	Toegang	IOT_Group1_Asset
Beleid CCV Group 2	IdentityGroup· Naam EQUALS Endpoint Identity Group:Gedeeld:ekorneyc_ ASSET_Group2	Toegang	IOT_Group2_Asset



## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

### 1. Endpoints voor verificatie op basis van CCV-groep 1

Op de switch kun je zien dat de omgevingsgegevens zowel de **16-54:IOT\_Group1\_Asset** als de **17-54:IOT\_Group2\_Asset** omvatten.

```
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#

Endpoints authenticeren en als resultaat hiervan wordt **CCV Group 1 Policy** aangepast, SGT **IOT\_Group1\_Asset** toegewezen.

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 active 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_AssetPermitAccess	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_AssetPermitAccess	172.16.0.100

Switch **show Authenticatiesessies interface fa1/7 details** bevestigt dat de **Access-Accept** gegevens succesvol werden toegepast.

```
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
```

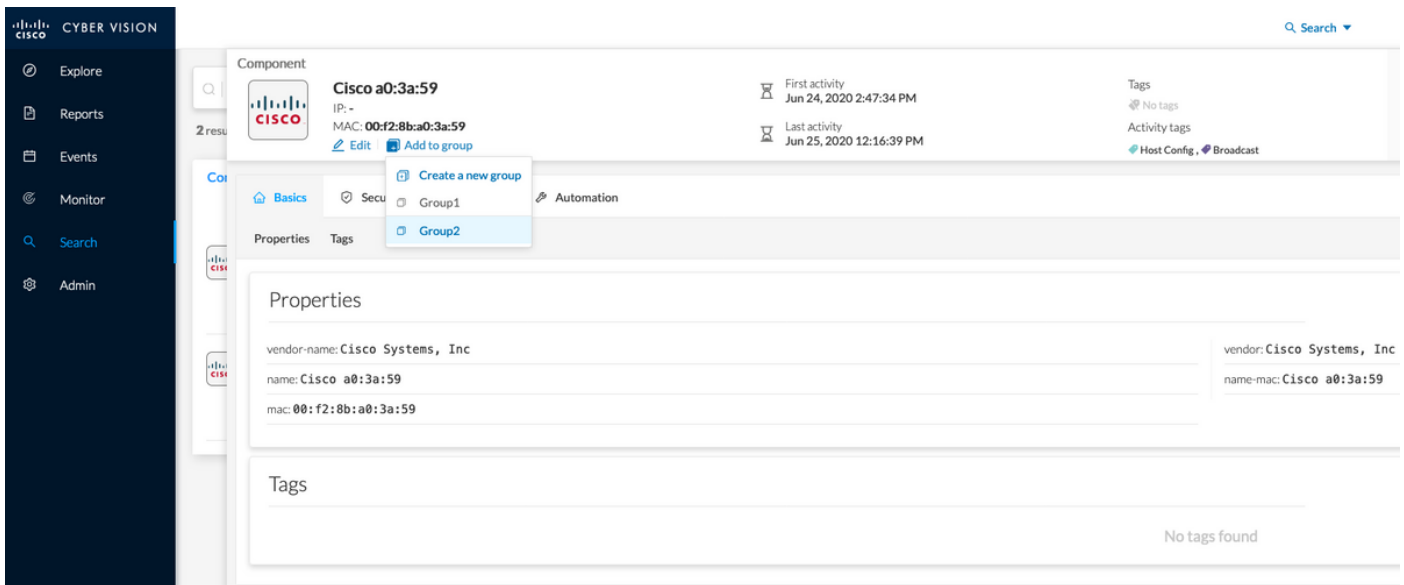
```
mab Authc Success
```

KJK\_IE4000\_10#

## 2. beheerder wijzigt de groep

Navigeer naar **Zoeken**. Plakt het Mac-adres van het Endpoint, klikt u op dit adres en **voegt** het toe aan Group 2.

Opmerking: Op CCV kunt u de groep niet van 1 tot 2 in één keer wijzigen. Daarom moet u eerst het Endpoint van de groep verwijderen en vervolgens groep 2 toewijzen.



### 3-6. Effect van verandering van endpointgroepen op CCV

De stappen 4, 5 en 6 worden in deze afbeelding weerspiegeld. Dankzij het profileren, veranderde het eindpunt Identity Group to ekorneyc\_ASSET\_Group2, gezien in Stap 4., wat ISE ertoe bracht CoA naar de switch te sturen (Stap 5) en uiteindelijk de authenticatie van het eindpunt (Stap 6).

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	00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_AssetPermitAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59:503 AM	Success			00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_AssetPermitAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59:482 AM	Success			00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermitAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group1
Jun 25, 2020 10:37:31:567 AM	Success			00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermitAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group1

Switch show authenticatiesessies interface fa1/7 detail bevestigt dat het nieuwe SGT is toegewezen.

```
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#

## Bijlage

### Configuratie van switchvertrouwenSEC-gerelateerde

Opmerking: Cts aanmeldingsgegevens maken geen deel uit van in werking stellen-configuratie en moeten worden geconfigureerd met het gebruik van **cts aanmeldingsgegevens in <id> wachtwoord <password> opdracht in bevoorrechte uitvoermodus.**

```
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#