Konfigurieren der ISE 2.7 pxGrid CCV 3.1.0-Integration

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Integration der Identity Services Engine (ISE) 2.7 in Cisco Cyber Vision (CCV) 3.1.0 über Platform Exchange Grid v2 (pxGrid) konfiguriert und Fehler behoben werden. CCV ist bei pxGrid v2 als Publisher registriert und veröffentlicht Informationen zu Endpunktattributen für die ISE für das IOTASSET Dictionary.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- ISE
- Cisco Cyber-Vision

Verwendete Komponenten

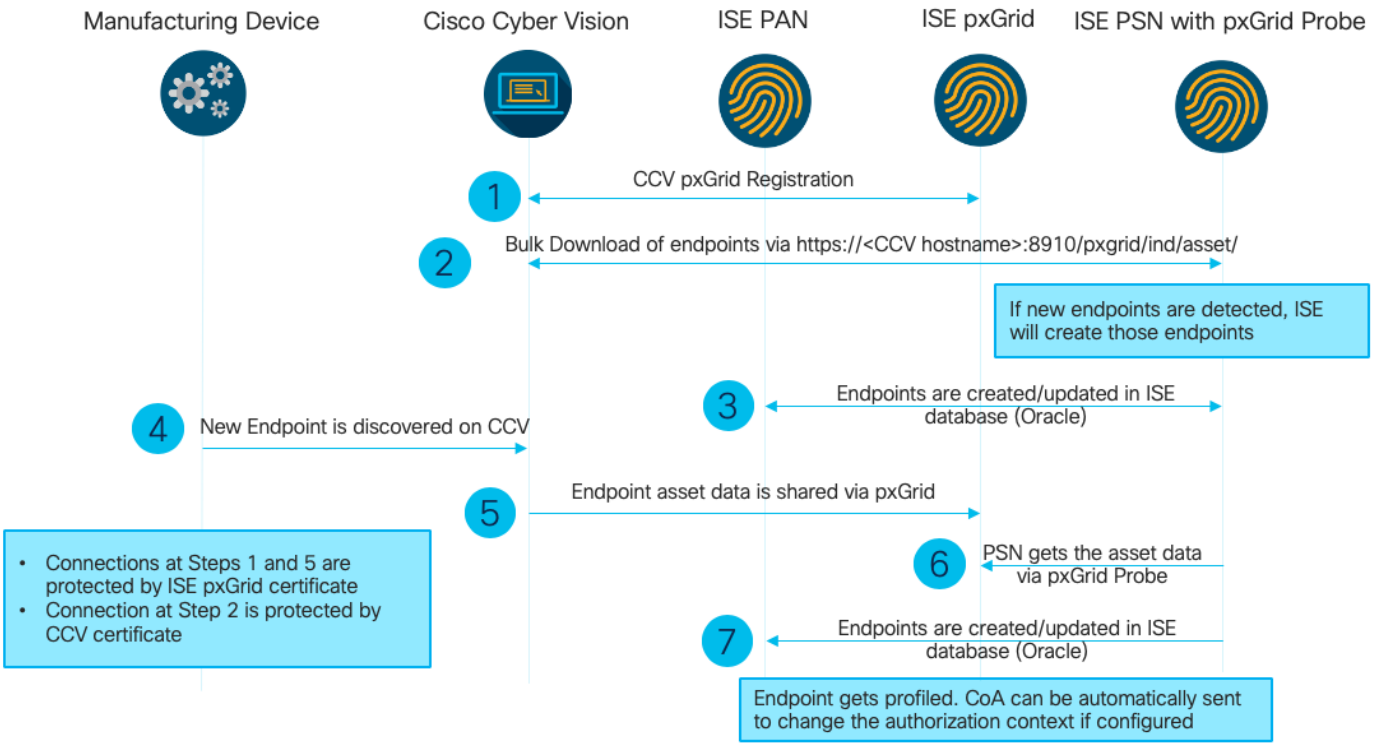
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ISE Version 2.7 Patch 1
- Cisco Cyber Vision Version 3.1.0
- Industrial Ethernet Switch IE-4000-4TC4G-E mit s/w 15.2(6)E

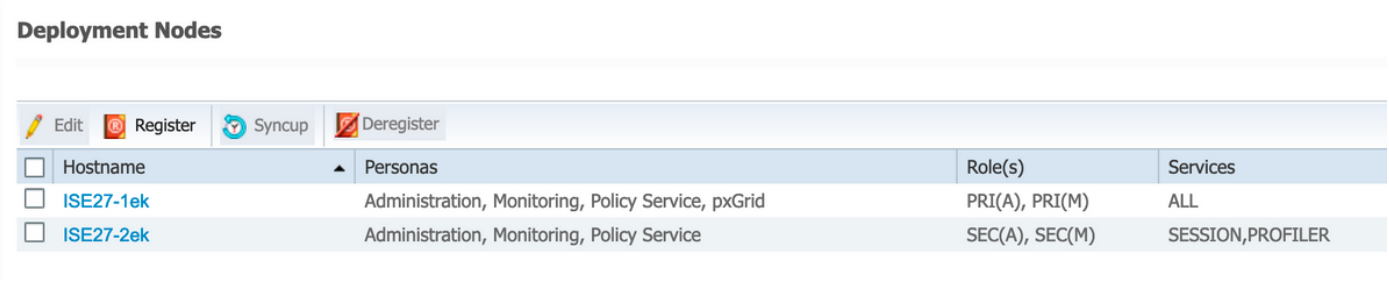
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Übergeordnetes Flussdiagramm



Diese ISE-Bereitstellung wird in der Konfiguration verwendet.



ISE 2.7-1ek ist der primäre Admin Node (PAN)-Knoten und der pxGrid-Knoten.

ISE 2.7-2ek ist Policy Service Node (PSN) mit aktivierter pxGrid-Abfrage.

Hier sind die Schritte, die dem oben erwähnten Diagramm entsprechen.

1. CCV registriert sich über pxGrid Version 2 bei assetTopic auf der ISE. Entsprechende Protokolle von CCV:

> **Hinweis**: Um die pxGrid-Protokolle in CCV zu überprüfen, führen Sie den folgenden Befehl **journalctl -u pxgrid-agent aus.**

```
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 mit aktivierter pxGrid-Sonde lädt eine große Anzahl vorhandener pxGrid-Ressourcen (profiler.log) herunter:

```
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. Endpunkte werden dem PSN mit aktivierter pxGrid-Abfrage hinzugefügt, und PSN sendet Persist-Ereignis an das PAN, um diese Endpunkte zu speichern (profiler.log). Auf der ISE erstellte Endpunkte können unter "Context Visibility" in den Endgerätdetails angezeigt werden.

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

4. Nachdem Sie einen Endpunkt in eine Gruppe eingefügt haben, sendet CCV über Port 8910 eine STOMP-Nachricht, um den Endpunkt mit der Gruppe Daten in benutzerdefinierten Attributen zu aktualisieren. Entsprechende Protokolle von 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. Der PxGrid-Knoten empfängt das STOMP-Update und leitet diese Nachricht an alle Abonnenten weiter. Er enthält PSNs mit aktivierter pxGrid-Abfrage. pxgrid-server.log auf pxGrid Node.

```
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 mit aktivierter pxGrid-Abfrage, da ein Abonnent zum Thema Ressourcen ist, empfängt die Nachricht vom pxGrid-Knoten und aktualisiert den Endpunkt (profiler.log). Aktualisierte Endgeräte auf der ISE können unter "Context Visibility" in den Endpunktdetails angezeigt werden.

```
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-
Parsing push notification response: {"opType":"UPDATE","asset":{"assetId":"ce01ade2-eb6f-53c8-
a646-9661b10c976e",
"assetName":"Cisco
a0:3a:59","assetIpAddress":"","assetMacAddress":"00:f2:8b:a0:3a:59","assetVendor":"Cisco
Systems, Inc",
"assetProductId":"","assetSerialNumber":"","assetDeviceType":"","assetSwRevision":"","assetHwRev
ision":"",
"assetProtocol":"","assetCustomAttributes":[{"key":"assetGroup","value":"Group1"},{"key":"assetC
CVGrp","value":"Group1"}],
"assetConnectedLinks":[]}}
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-
sending endpoint to forwarder{"assetId":"ce01ade2-eb6f-53c8-a646-
9661b10c976e","assetName":"Cisco a0:3a:59","assetIpAddress":"",
"assetMacAddress":"00:f2:8b:a0:3a:59","assetVendor":"Cisco Systems,
Inc","assetProductId":"","assetSerialNumber":"",
"assetDeviceType":"","assetSwRevision":"","assetHwRevision":"","assetProtocol":"",
"assetCustomAttributes":[{"key":"assetGroup","value":"Group1"},{"key":"assetCCVGrp","value":"Gro
```

```
up1"}],"assetConnectedLinks":[]}
2020-06-24 14:40:13,768 INFO [Grizzly(2)][] cisco.profiler.infrastructure.probemgr.Forwarder -
::::-
Forwarder Mac 00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,768 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.probemgr.ForwarderHelper -:
00:F2:8B:A0:3A:59:87026690-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:- sequencing Radius
message for mac = 00:F2:8B:A0:3A:59
2020-06-24 14:40:13,768 INFO [forwarder-9][] cisco.profiler.infrastructure.probemgr.Forwarder -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:-
Processing endpoint:00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,768 DEBUG [forwarder-9][] com.cisco.profiler.im.EndPoint -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:-
filtered custom attributes are:{assetGroup=Group1, assetCCVGrp=Group1}
2020-06-24 14:40:13,768 DEBUG [forwarder-9][] cisco.profiler.infrastructure.probemgr.Forwarder -
:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:- Radius
Filtering:00:F2:8B:A0:3A:59
2020-06-24 14:40:13,768 DEBUG [forwarder-9][] cisco.profiler.infrastructure.probemgr.Forwarder -
:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:- Endpoint
Attributes:EndPoint[id=<null>,name=<null>]
MAC: 00:F2:8B:A0:3A:59
Attribute:2309ae60-693d-11ea-9cbe-02251d8f7c49 value:Group1
Attribute:BYODRegistration value:Unknown
Attribute:DeviceRegistrationStatus value:NotRegistered
Attribute:EndPointProfilerServer value:ISE27-2ek.example.com
Attribute:EndPointSource value:pxGrid Probe
Attribute:MACAddress value:00:F2:8B:A0:3A:59
Attribute:NmapSubnetScanID value:0
Attribute:OUI value:Cisco Systems, Inc
Attribute:PolicyVersion value:0
Attribute:PortalUser value:
Attribute:PostureApplicable value:Yes
Attribute:assetDeviceType value:
Attribute:assetGroup value:Group1
Attribute:assetHwRevision value:
Attribute:assetId value:ce01ade2-eb6f-53c8-a646-9661b10c976e
Attribute:assetIpAddress value:
Attribute:assetMacAddress value:00:f2:8b:a0:3a:59
Attribute:assetName value:Cisco a0:3a:59
Attribute:assetProductId value:
Attribute:assetProtocol value:
Attribute:assetSerialNumber value:
Attribute:assetSwRevision value:
Attribute:assetVendor value:Cisco Systems, Inc
Attribute:SkipProfiling value:false
```

7. PSN mit pxGrid-Datensammlung ermöglichte die erneute Profilerstellung des Endpunkts, wenn eine neue Richtlinie zugeordnet wird (profiler.log).

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

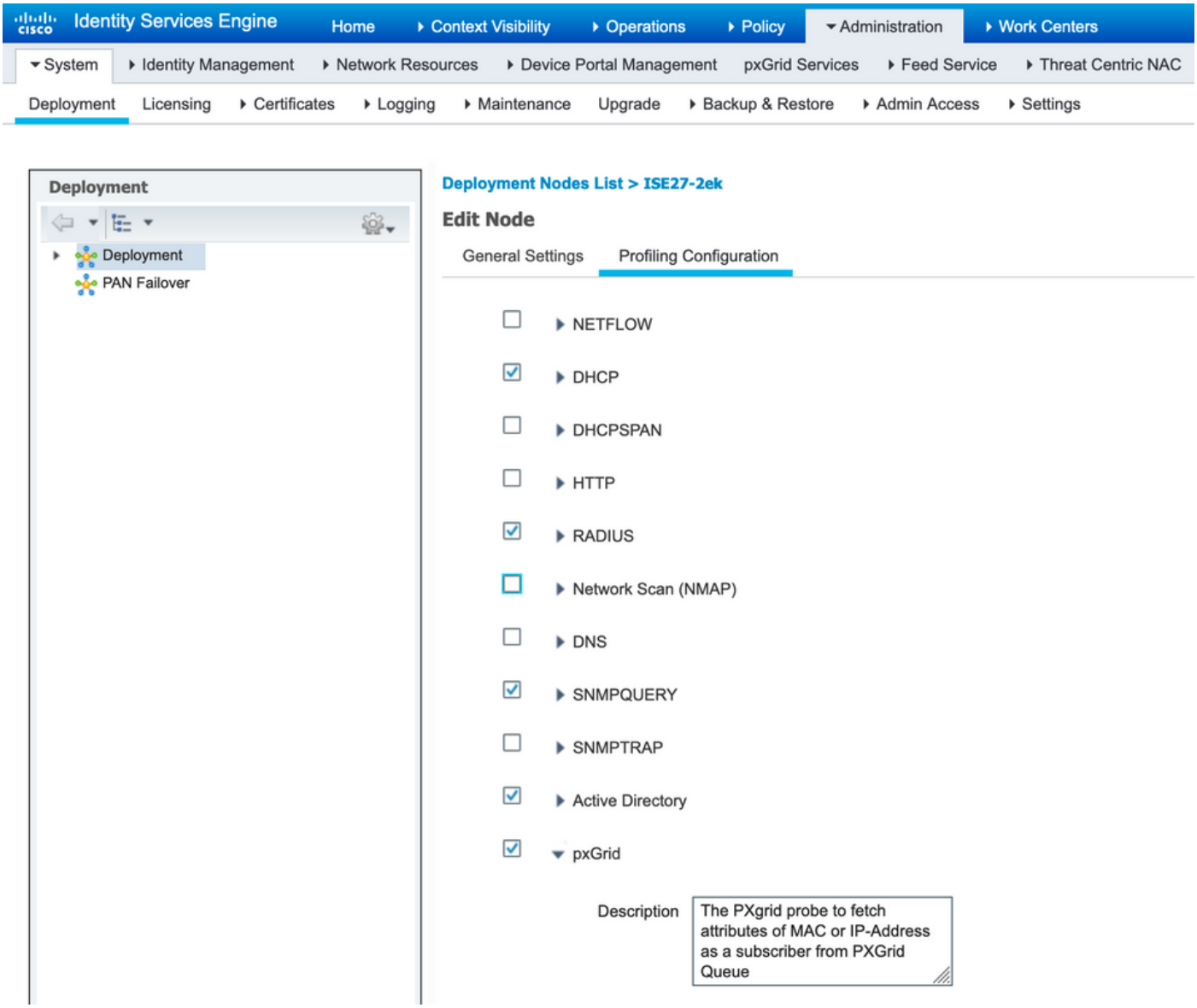
```
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- After analyzing policy
hierarchy: Endpoint:
00:F2:8B:A0:3A:59 EndpointPolicy:ekorneyc_ASSET_Group1 for:20 ExceptionRuleMatched:false
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
Matched Policy Changed.
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
IdentityGroup Changed.
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Setting identity group ID on
endpoint
00:F2:8B:A0:3A:59 - 91b0fd10-a181-11ea-a1a3-fe7d097d8c61
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Calling end point cache with
profiled end point
00:F2:8B:A0:3A:59, policy ekorneyc_ASSET_Group1, matched policy ekorneyc_ASSET_Group1
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Sending event to persist end
point
00:F2:8B:A0:3A:59, and ep message code = null
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
IdentityGroup / Logical Profile Changed. Issuing a Conditional CoA
```

Konfigurationen

> **Hinweis**: Die Schritte 1 bis 4 sind auch dann erforderlich, wenn Sie nur eine Übersicht über AssetGroup und Context Visibility wünschen.

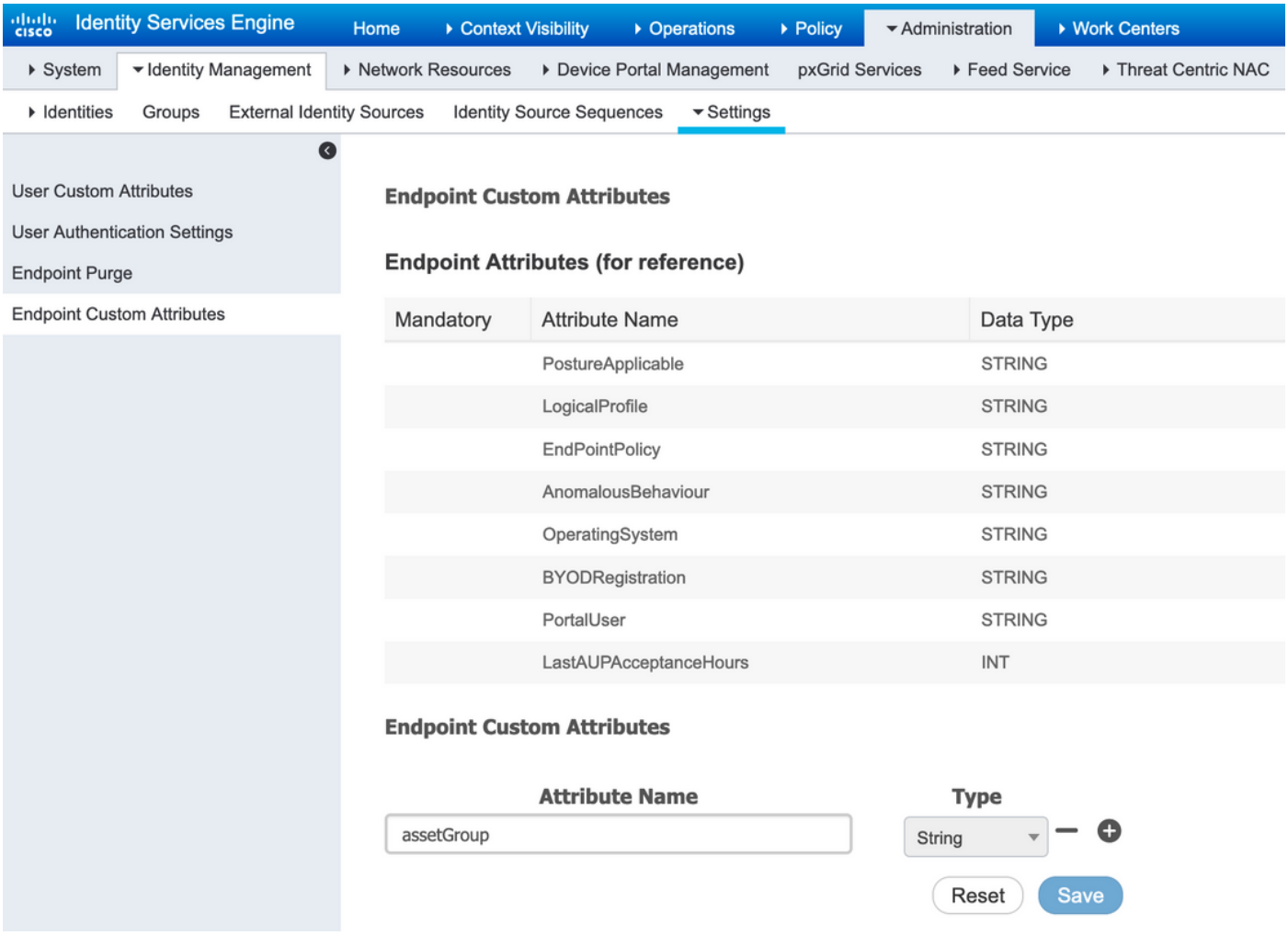
1. Aktivieren Sie die pxGrid-Anfrage auf einem der PSNs.

Navigieren Sie zu **Administration > System > Deployment**, und wählen Sie ISE-Knoten mit PSN Persona aus. Wechseln Sie zur Registerkarte **"Konfiguration der Profilerstellung"**. Stellen Sie sicher, dass die **pxGrid-**Sonde aktiviert ist.



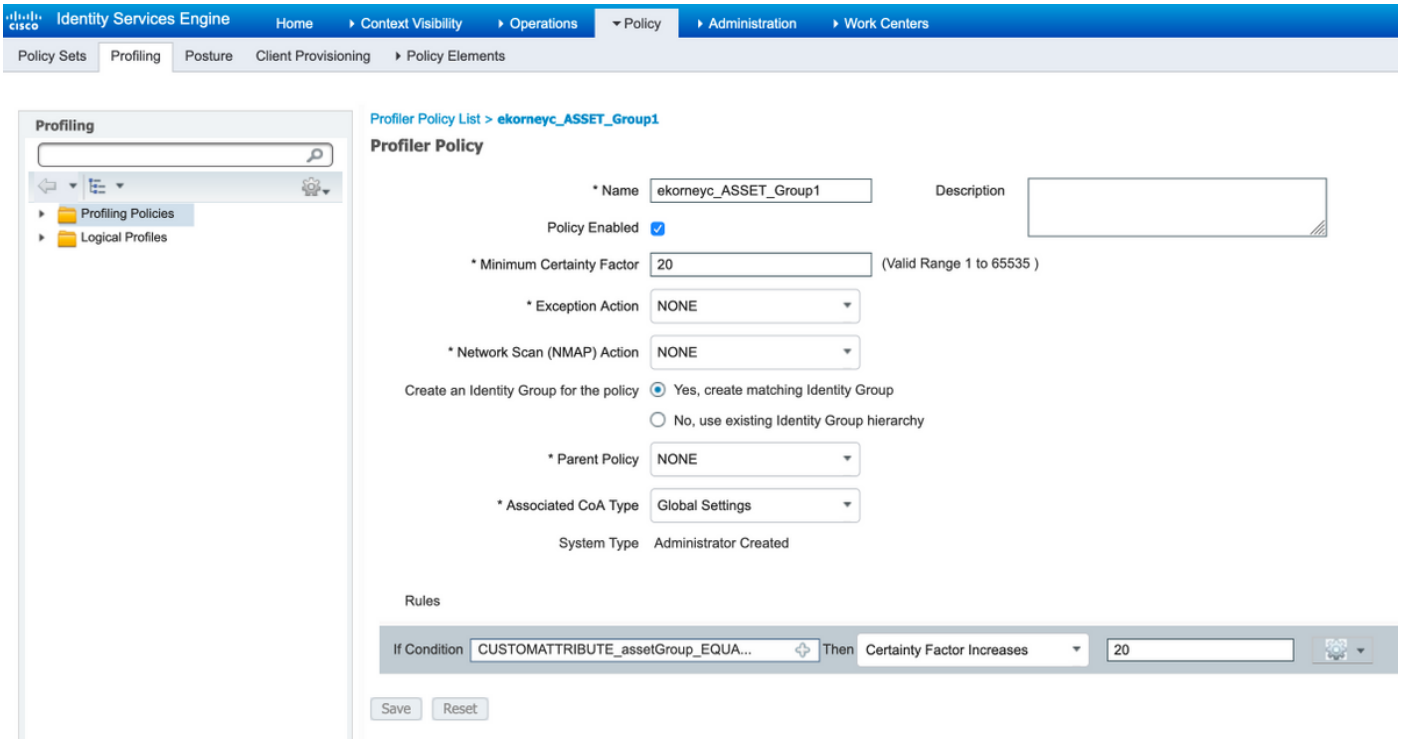
2. Konfigurieren benutzerdefinierter Endgeräteattribute auf der ISE

Navigieren Sie zu **Administration > Identity Management > Settings > Endpoint Custom Attributes**. Konfigurieren Sie benutzerdefinierte Attribute (assetGroup) entsprechend diesem Bild. CCV 3.1.0 unterstützt nur Custom **AssetGroup** Attribute.



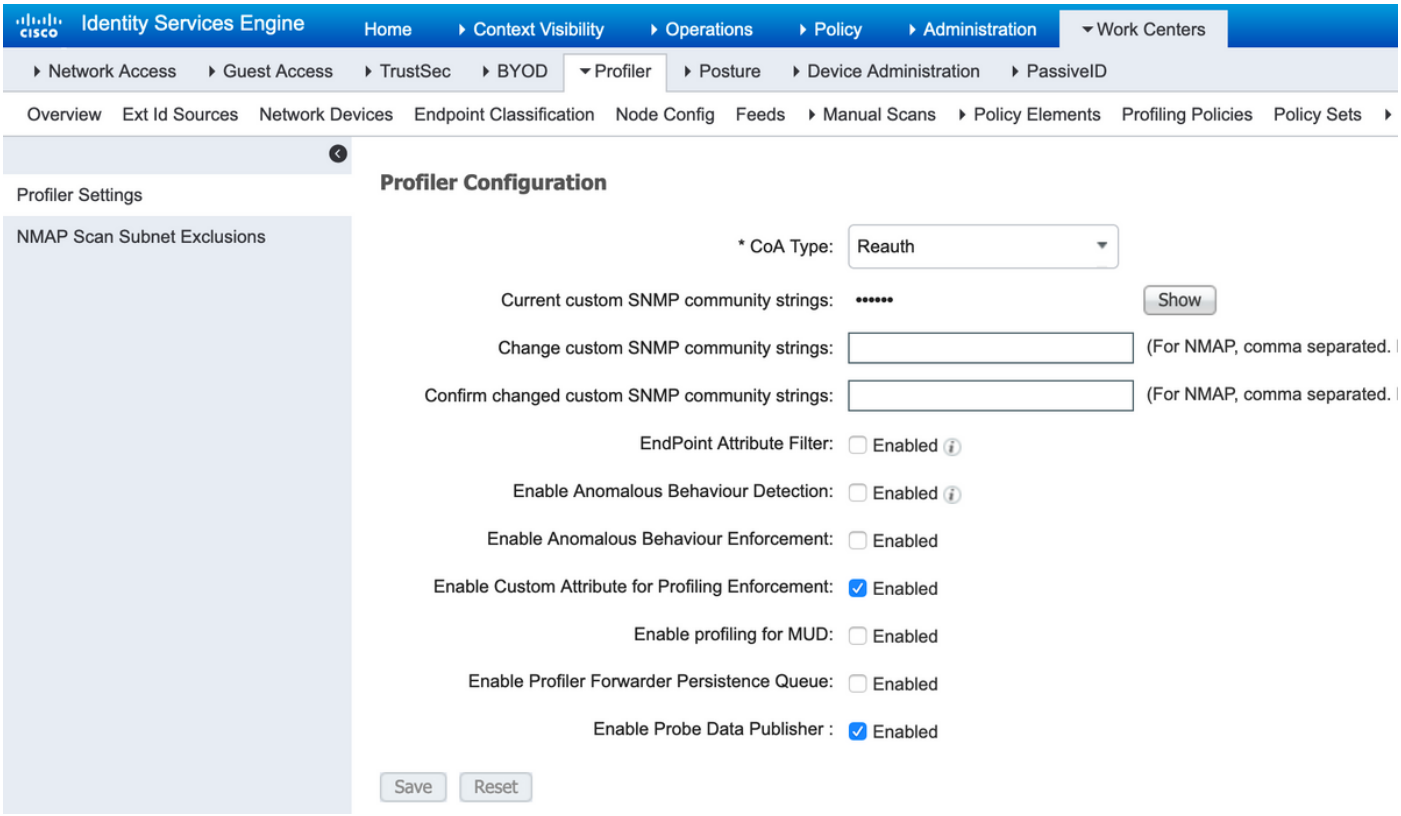
3. Konfigurieren der Profilerichtlinie mithilfe von benutzerdefinierten Attributen

Navigieren Sie zu **Work Center > Profiler > Profiling Policies (Profilerstellungsrichtlinien)**. Klicken Sie auf **Hinzufügen**. Konfigurieren Sie eine Profilerichtlinie, die diesem Bild ähnelt. Der in dieser Richtlinie verwendete Bedingungsausdruck lautet **CUSTOMATTRIBUTE:AssetGroup EQUALS Group1.**



4. Aktivieren benutzerdefinierter Attribute für die Profilerzwingung

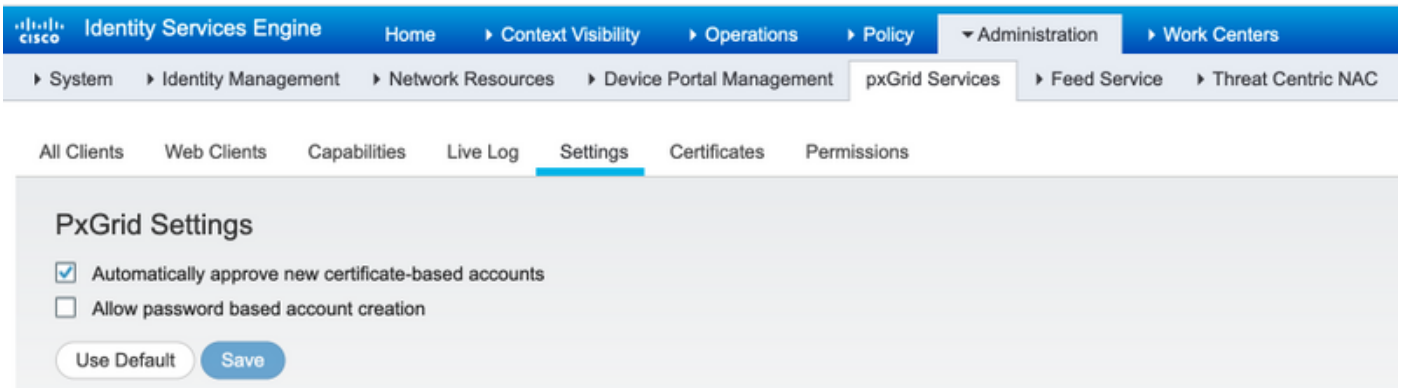
Navigieren Sie zu **Work Center > Profiler > Profiling Policies (Profilerstellungsrichtlinien)**. Klicken Sie auf **Hinzufügen**. Konfigurieren Sie eine Profilerichtlinie, die diesem Bild ähnelt. Stellen Sie sicher, dass **die Option Benutzerdefiniertes Attribut für die Profildurchsetzung aktivieren** aktiviert ist.



5. Automatische Genehmigung für pxGrid-Clients konfigurieren

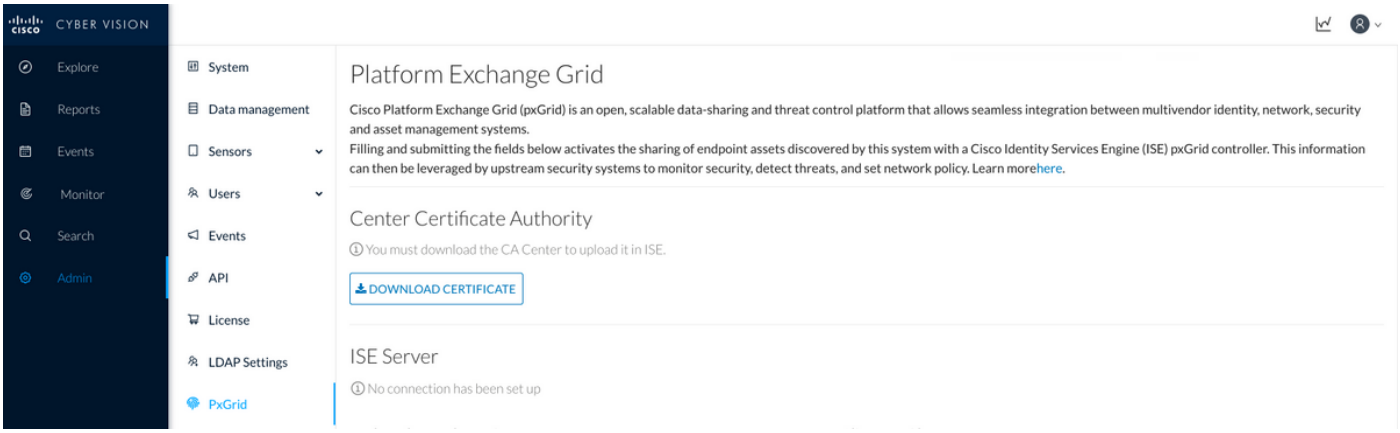
Navigieren Sie zu **Administration > pxGrid Services > Settings**. Wählen Sie **Neue zertifikatbasierte**

Konten automatisch genehmigen aus, und klicken Sie auf **Speichern**. Mit diesem Schritt wird sichergestellt, dass CCV nach der Integration nicht genehmigt werden muss.



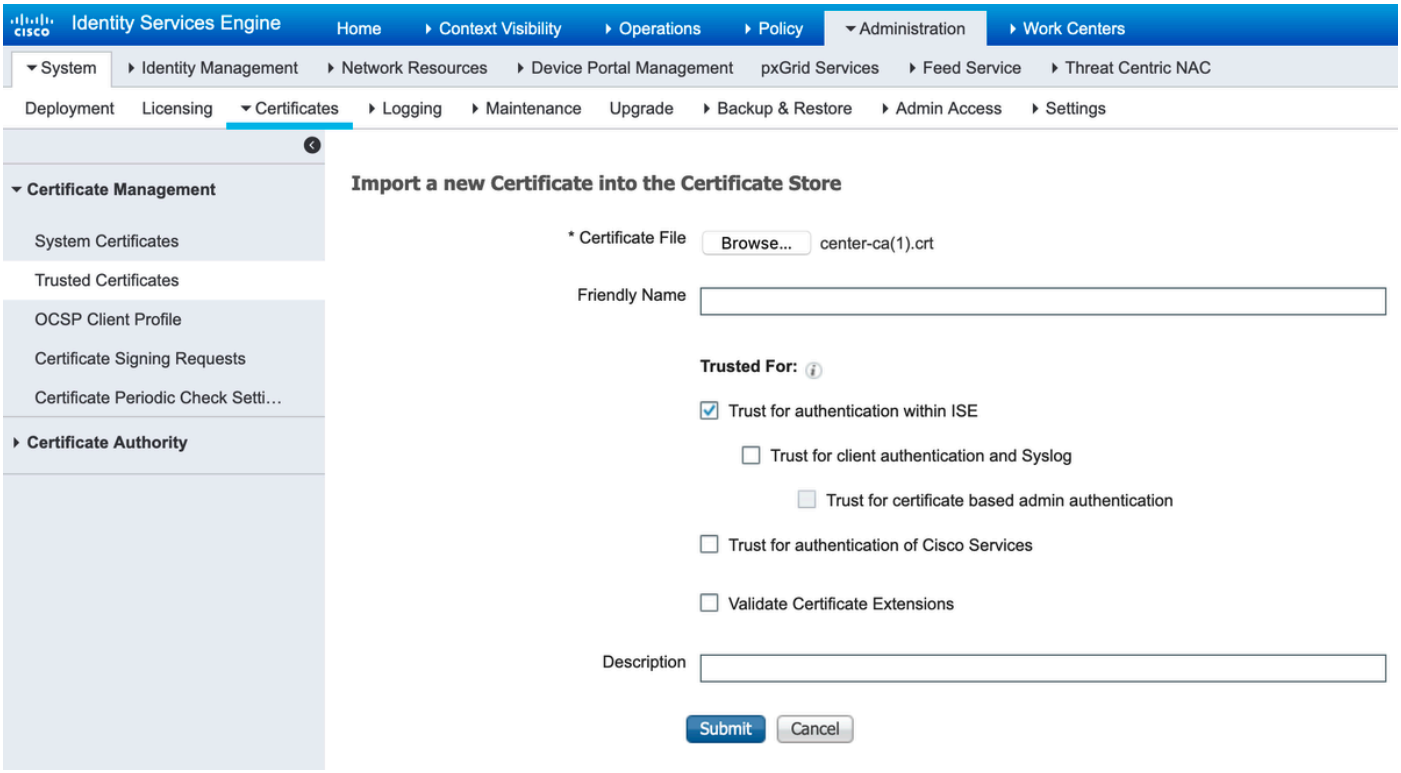
6. CCV-Zertifikat exportieren

Navigieren Sie zu **Admin > pxGrid**. Klicken Sie auf **ZERTIFIKAT HERUNTERLADEN**. Dieses Zertifikat wird während der pxGrid-Registrierung verwendet, daher sollte die ISE diesem Zertifikat vertrauen.



7. Laden Sie das CCV-Identitätszertifikat in den ISE Trusted Store hoch.

Navigieren Sie zu **Administration > Certificates > Certificate Management > Trusted Certificates**. Klicken Sie auf **Importieren**. Klicken Sie auf **Durchsuchen**, und wählen Sie CCV-Zertifikat aus Schritt 5 aus. Klicken Sie auf **Senden**.

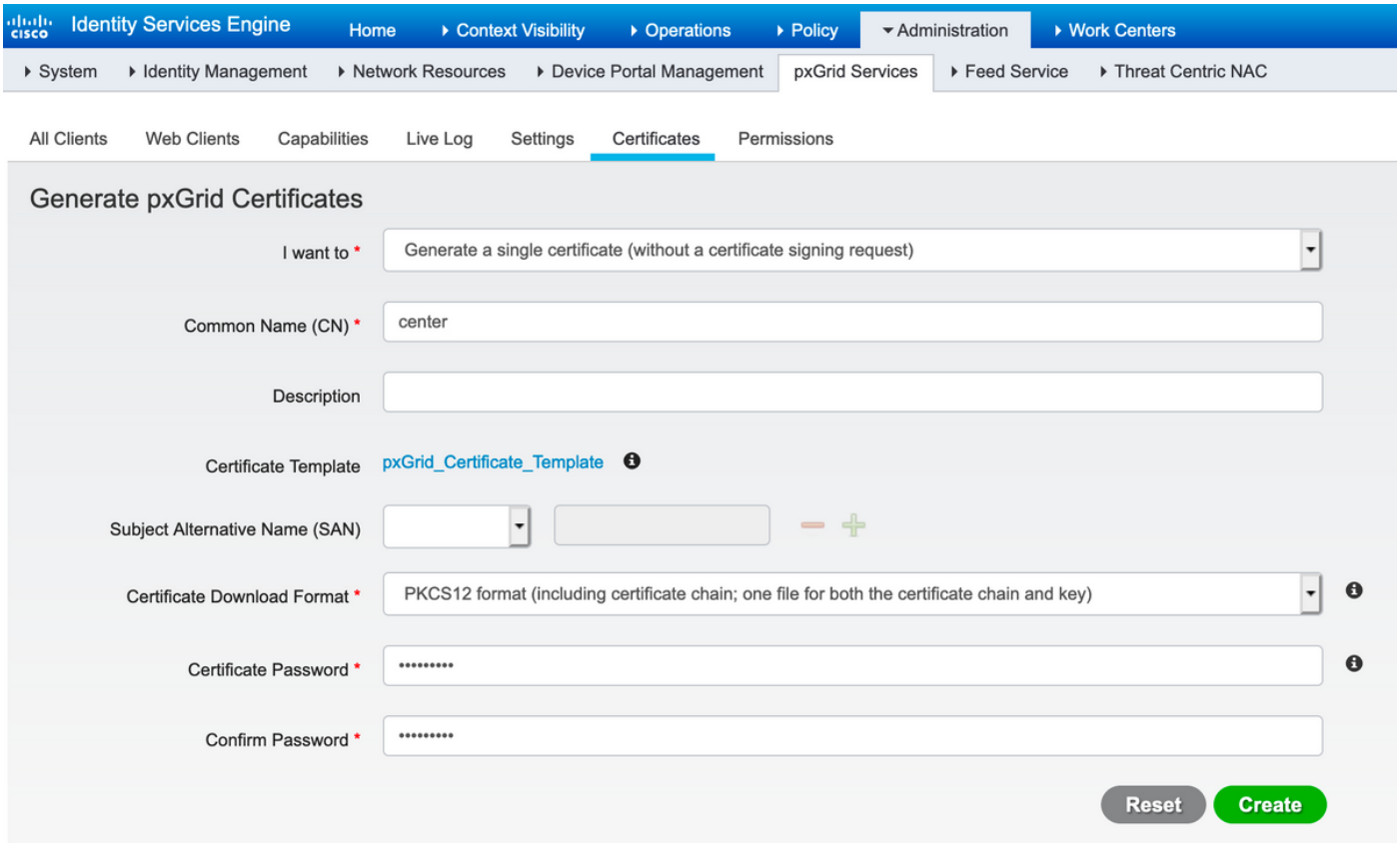


8. Zertifikat für CCV erstellen

Während der pxGrid-Integration und -Aktualisierungen benötigt CCV das Client-Zertifikat. Sie sollte von der internen ISE-CA unter Verwendung von **PxGrid_Certificate_Template** ausgestellt werden.

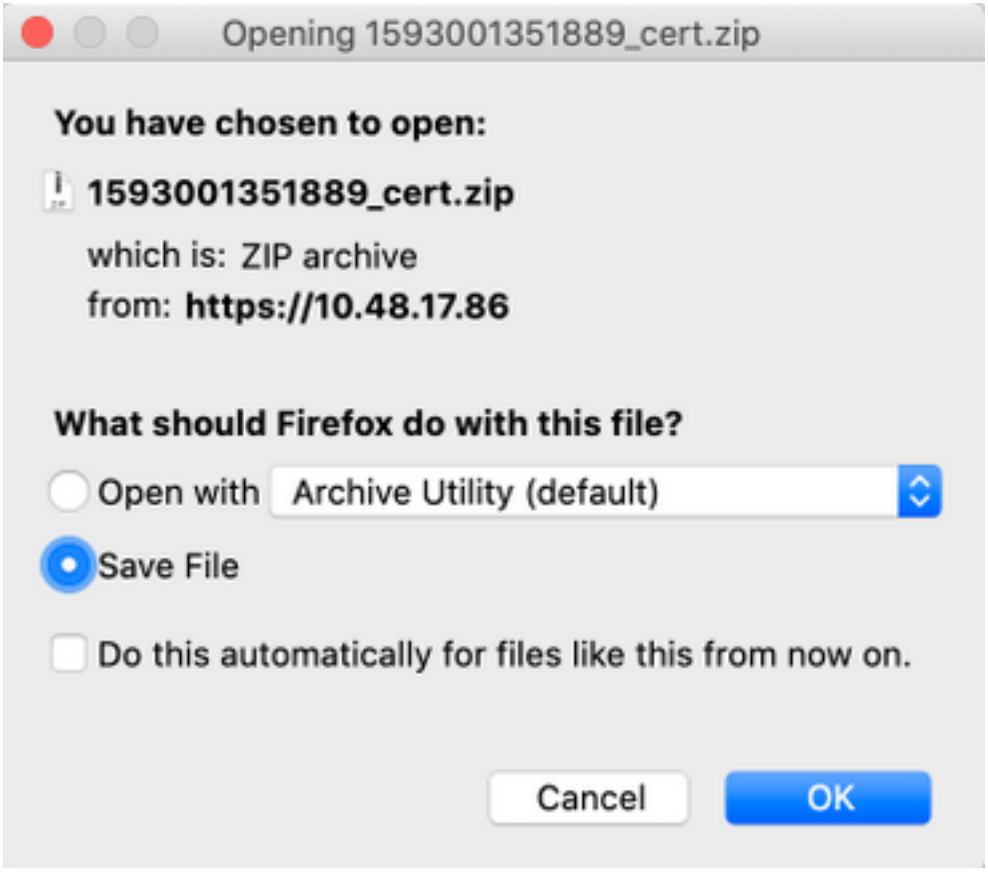
Navigieren Sie zu **Administration > pxGrid Services > Certificates**. Füllen Sie die Felder entsprechend diesem Bild aus. Das Feld "Common Name" (CN) ist obligatorisch, da das Ziel der ISE-Zertifizierungsstelle die Ausstellung eines Identitätszertifikats ist. Geben Sie den Hostnamen von CCV ein. Der Wert im CN-Feld ist kritisch. Um den Hostnamen von CCV zu überprüfen, geben Sie den Befehl **hostname ein**. Wählen Sie PKCS12 als **Certificate Download Format aus.**

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



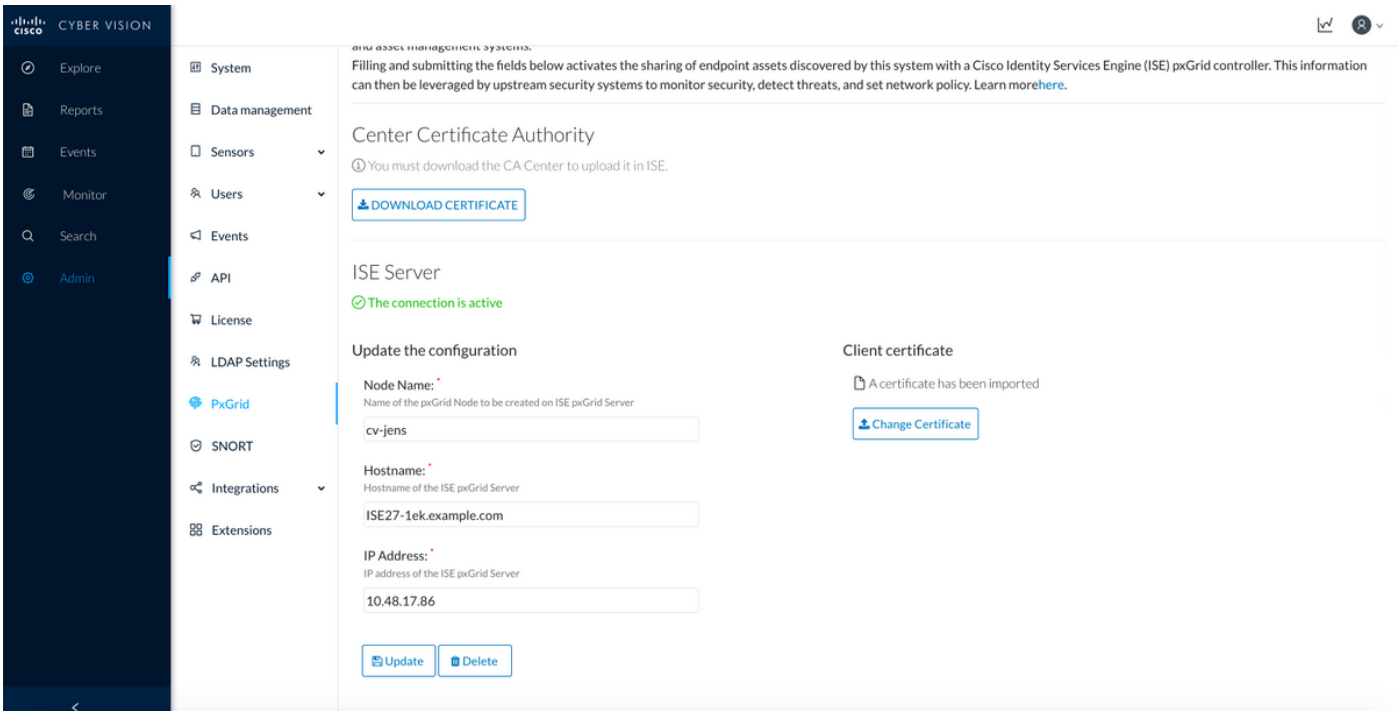
9. Zertifikatskette im PKCS12-Format herunterladen

Wenn Sie das Zertifikat im PKCS12-Format installieren, wird zusammen mit dem CCV-Identitätszertifikat die ISE Internal CA Chain in CCV installiert, um sicherzustellen, dass CCV der ISE vertraut, wenn die pxGrid-Kommunikation von der ISE initiiert wird, z. B. pxGrid-Keepalive-Nachrichten.



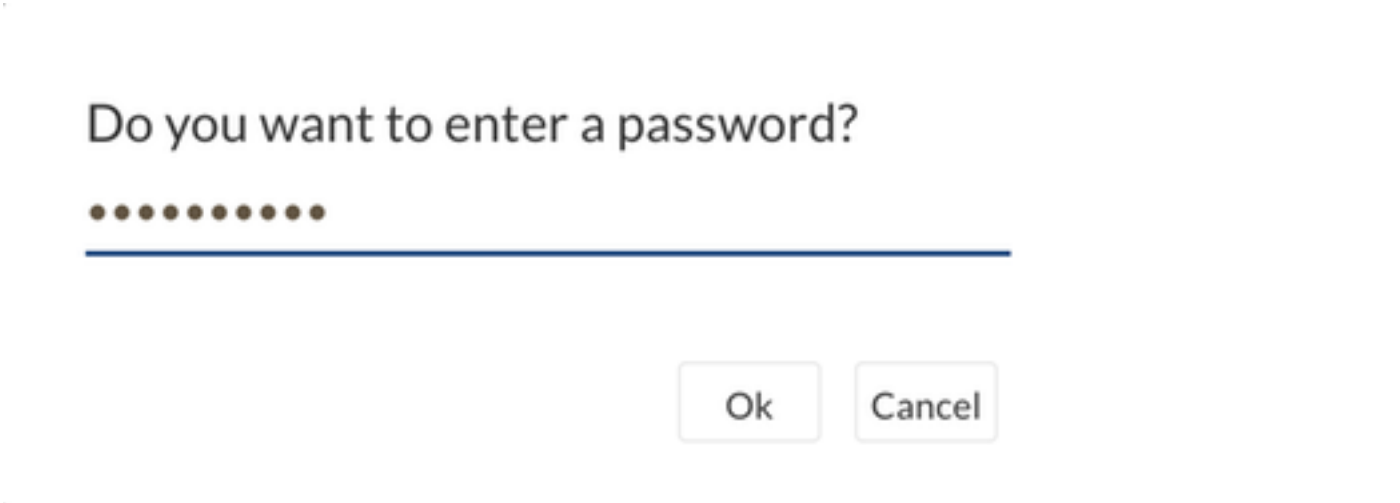
10. Konfigurieren der ISE-Integrationsdetails in CCV

Navigieren Sie zu **Admin > pxGrid**. Knotennamen konfigurieren: Dieser Name wird in der ISE als Client-Name unter **Administration > pxGrid Services > Web Clients** angezeigt**.** Konfigurieren Sie **Hostname** und **IP-Adresse** des ISE pxGrid Node. Stellen Sie sicher, dass CCV ISE FQDN auflösen kann.



11. Hochladen der Zertifikatskette in CCV und Einführen der Integration

Navigieren Sie zu **Admin > pxGrid**. Klicken Sie auf **Zertifikat ändern**. Wählen Sie ein von der ISE-CA ausgestelltes Zertifikat aus den Schritten 8 bis 9. Geben Sie das Kennwort aus Schritt 8 ein. und klicken Sie auf **OK.**



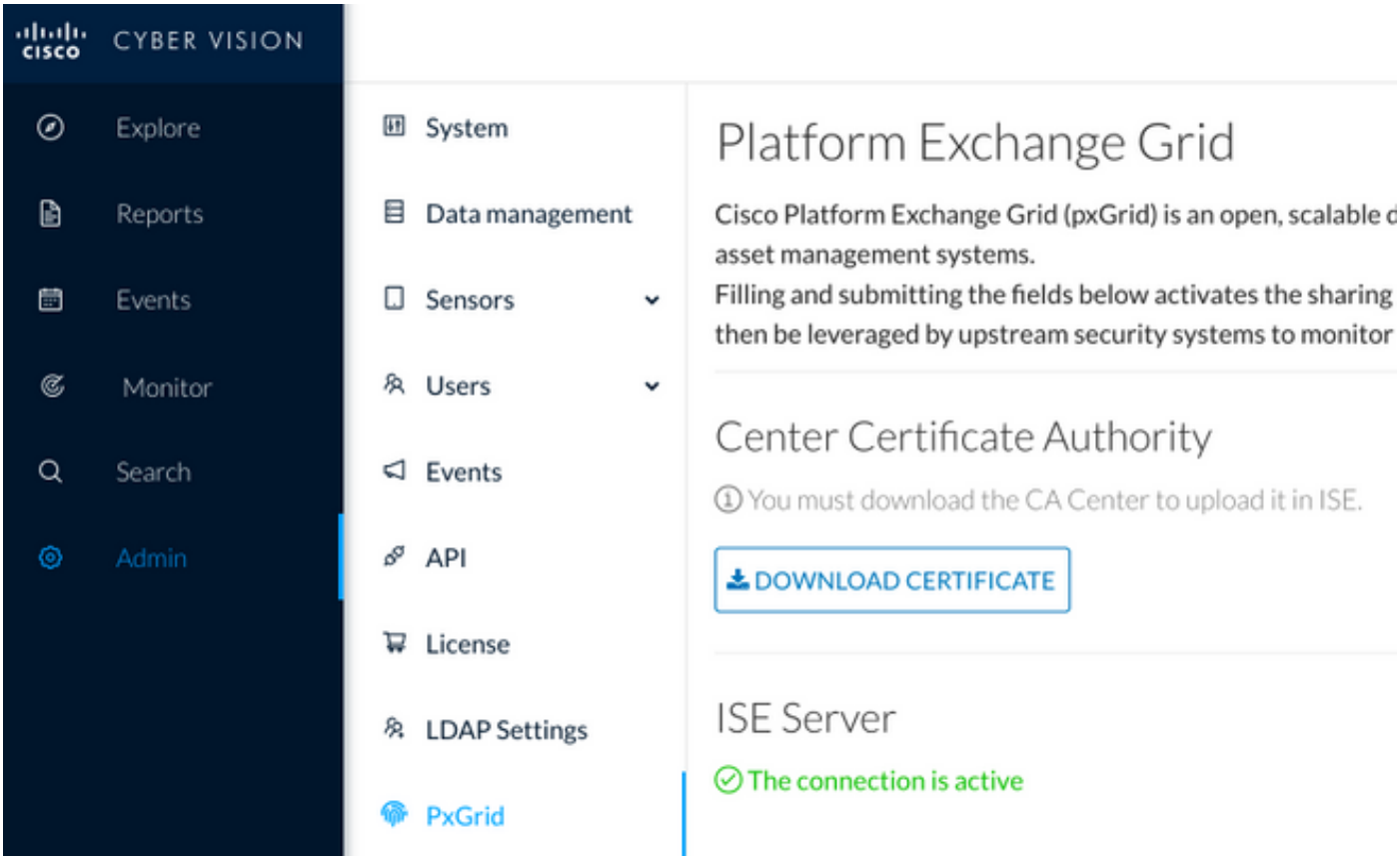
Klicken Sie auf **Aktualisieren**, um die eigentliche CCV-ISE-Integration zu starten.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfung der CCV-Integration

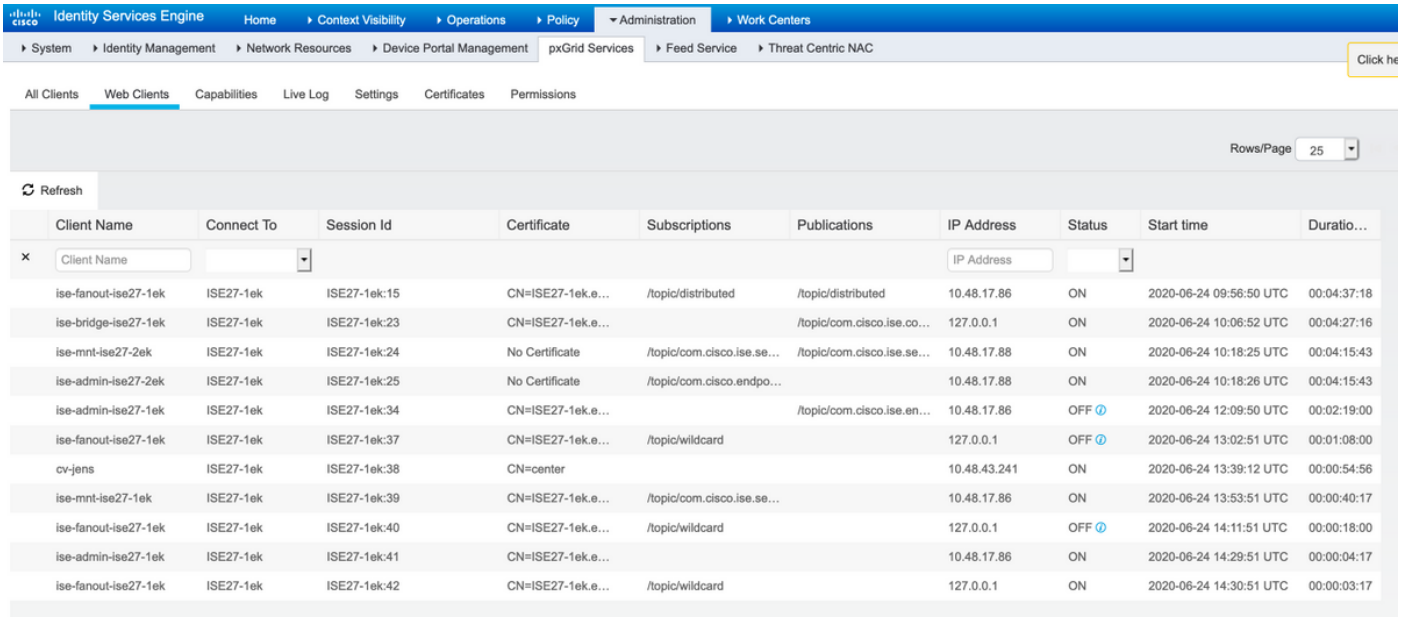
Wenn die Integration abgeschlossen ist, können Sie bestätigen, dass die Integration erfolgreich war, indem Sie zu **Admin > pxGrid** navigieren. Unter ISE-Server sollte **die Meldung Die Verbindung ist aktiv** angezeigt werden.



Überprüfung der ISE-Integration

Navigieren Sie zu **Administration > pxGrid Services > Web Clients**. Bestätigen Sie, dass der Status des CCV-Clients (cv-jens) **ON** ist.

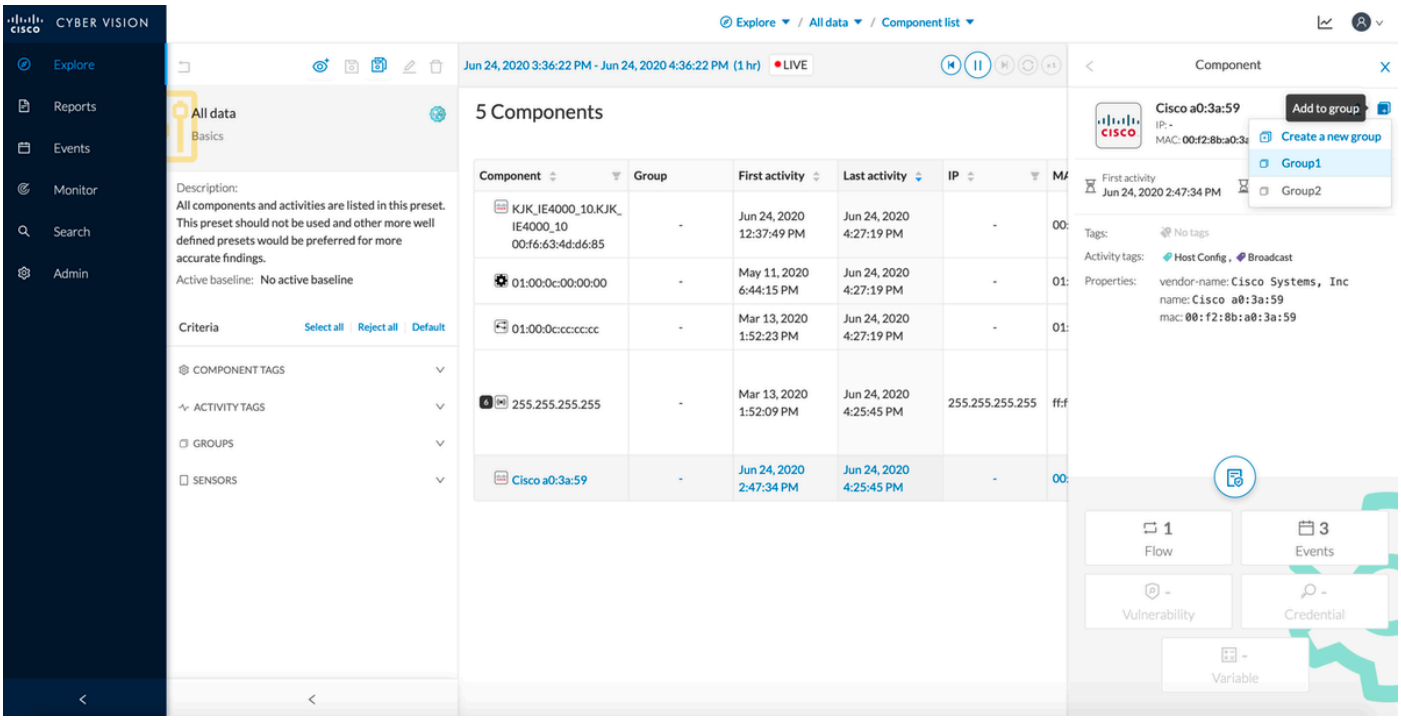
> **Hinweis**: Es wird erwartet, dass der Status des CCV pxGrid-Clients **Offline** im Menü **All Clients** angezeigt wird, da nur der pxGrid v1-Status angezeigt wird.



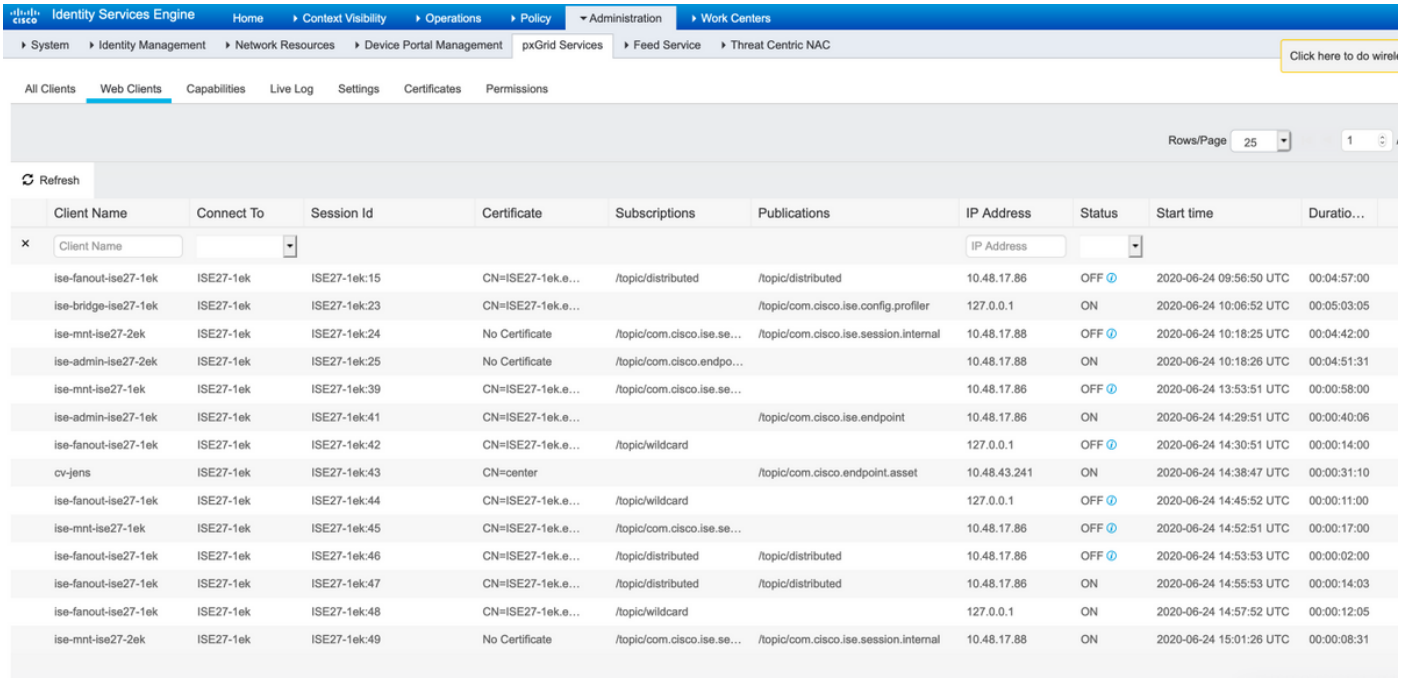
Hinweis: Aufgrund von CSCvt78208 wird CCV nicht sofort mit **/topic/com.cisco.ise.endpoint.asset angezeigt**, sondern nur bei der ersten Veröffentlichung.

CCV-Gruppenänderung überprüfen

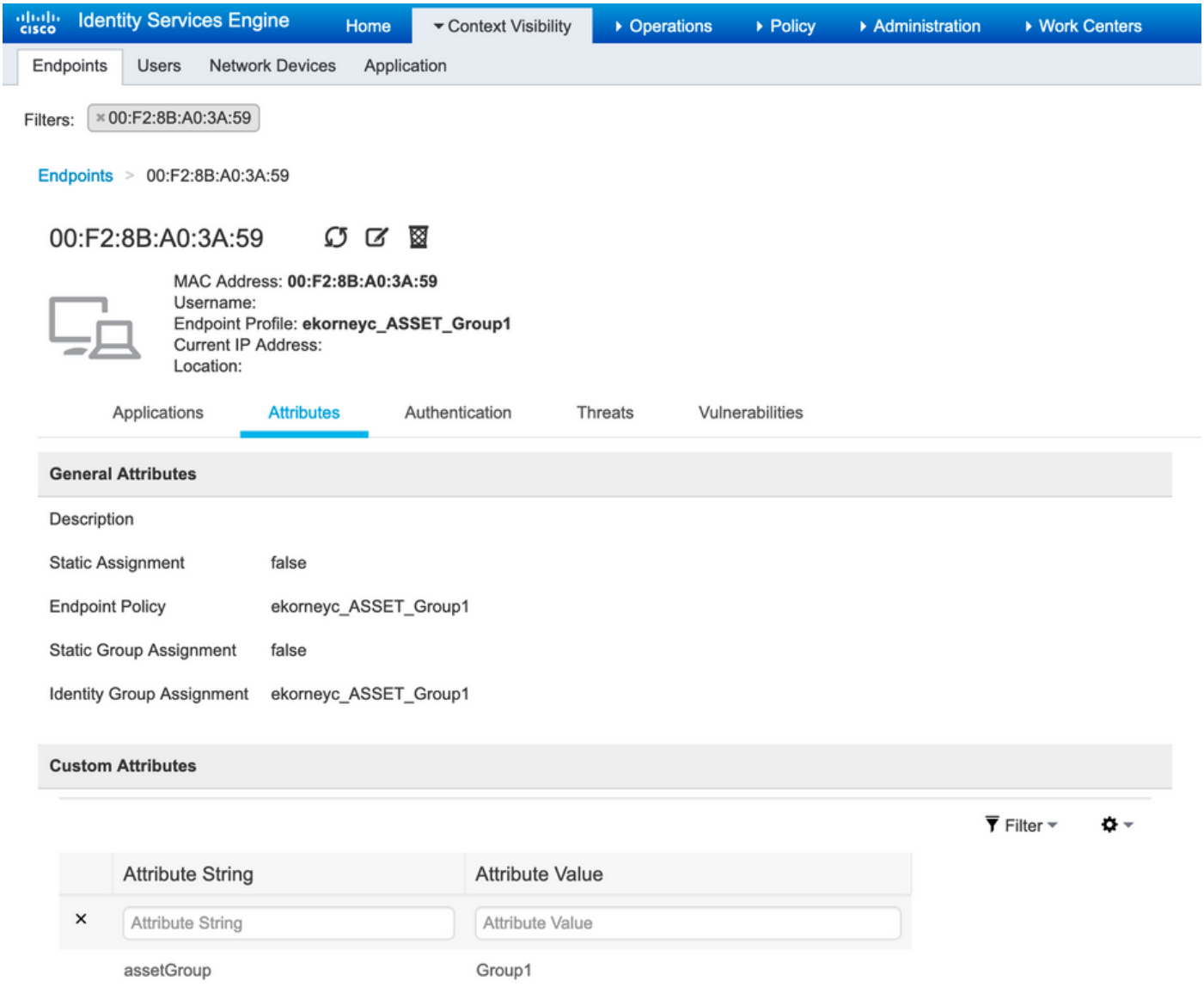
Navigieren Sie zu **Explorer > Alle Daten > Liste Komponente**. Klicken Sie auf eine der Komponenten, und **fügen Sie** sie der Gruppe hinzu.



Vergewissern Sie sich, dass **/topic/com.cisco.ise.endpoint.asset** jetzt als Veröffentlichungen gegen CCV aufgeführt ist.



Vergewissern Sie sich, dass die über CCV zugewiesene Gruppe1 auf der ISE wiedergegeben wird und die Profilerstellungsrichtlinie wirksam wurde, indem Sie zu **Context Visibility > Endpoints** navigieren. Wählen Sie den im vorherigen Schritt aktualisierten Endpunkt aus. Wechseln Sie zur Registerkarte Attribute. Der Abschnitt für benutzerdefinierte Attribute sollte der neu konfigurierten Gruppe entsprechen.



Im anderen Abschnitt "Attribute" werden alle anderen Ressourcenattribute aufgelistet, die von CCV empfangen wurden.

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

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Debugger auf der ISE aktivieren

Um das Debuggen auf der ISE zu aktivieren, navigieren Sie zu **Administration > System > Logging > Debug Log Configuration**. Legen Sie folgende Protokollstufen fest:

Persona	Komponentenname	Protokollstufe	Zu prüfende Datei
PAN (optional)	Profiler	DEBUG	Profiler.log
PSN mit aktivierter pxGrid-Sonde	Profiler	DEBUG	Profiler.log
PxGrid	Pxraster	NACHVERFOLGUNG	pxgrid-server.log

Debuggen in CCV aktivieren

So aktivieren Sie das Debuggen in CCV:

- Erstellen Sie eine Datei **/data/etc/sbs/pxgrid-agent.conf** mit dem Befehl **/data/etc/sbs/pxgrid-agent.conf**.
- Fügen Sie diesen Inhalt in die Datei **pxgrid-agent.conf ein**, indem Sie den **vi**-Editor mit dem Befehl **vi /data/etc/sbs/pxgrid-agent.conf** verwenden.

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

- Starten Sie pxgrid-agent neu, indem Sie den Befehl **systemctl restart pxgrid-agent** ausführen.
- Anzeigen von Protokollen mit dem Befehl **journalctl -u pxgrid-agent**

Massendownload-Fehler

CCV veröffentlicht während der Integration die Bulk Download-URL zur ISE. ISE PSN mit aktivierter pxGrid-Abfrage führt Bulk Download mithilfe dieser URL durch. Stellen Sie sicher, dass

- Der Hostname in der URL ist aus ISE-Perspektive korrekt auflösbar.
- Die Kommunikation von PSN auf Port 8910 zu CCV ist zulässig.

profiler.log auf PSN mit aktivierter pxGrid-Sonde:

```
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}]]
```

Der Bulk-Download kann aufgrund von CSCvt75422 fehlschlagen, sollte dieser Fehler in **profiler.log** auf ISE angezeigt werden, um ihn zu bestätigen. Der Fehler ist in CCV 3.1.0 behoben.

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

Nicht alle Endgeräte werden auf der ISE erstellt.

Einige Endpunkte in CCV können zu viele Attribute angehängt haben, sodass die ISE-Datenbank diese nicht verarbeiten kann. Sie können bestätigen, dass diese Fehler in **profiler.log** auf der ISE angezeigt werden.

```
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 ist für ISE nicht verfügbar

Wenn AssetGroup auf der ISE nicht verfügbar ist, wird die Profiling-Richtlinie höchstwahrscheinlich nicht mit benutzerdefinierten Attributen konfiguriert (siehe Schritte 2-4). im Abschnitt "Konfigurationen" des Dokuments). Sogar für die Sichtbarkeit des Kontexts sind nur Gruppenattribute, Profilerstellungsrichtlinien und andere Einstellungen aus den Schritten 2-4 erforderlich.

Endpunktgruppen-Updates werden auf der ISE nicht reflektiert.

Aufgrund von CSCvu80175 veröffentlicht CCV keine Endpunktaktualisierungen für die ISE, bis CCV unmittelbar nach der Integration neu startet. Sie können CCV neu starten, sobald die Integration als Problemumgehung erfolgt ist.

Gruppe aus CCV entfernen heißt nicht aus ISE entfernen

Dieses Problem ist auf den bekannten Fehler in CCV CSCvu47880 zurückzuführen.Das pxGrid-Update, das beim Entfernen der Gruppe aus CCV mit einem anderen als dem erwarteten Format gesendet wurde, sodass die Gruppe nicht entfernt wird.

CCV wird von Web-Clients gelöscht

Dieses Problem ist auf den bekannten Fehler in ISE CSCvu47880 zurückzuführen, bei dem Clients in den OFF-Status wechseln, gefolgt von der vollständigen Entfernung von Web-Clients. Das Problem wurde in 2.6 Patch 7 und 2.7 Patch 2 der ISE behoben.

Sie können dies bestätigen, wenn Sie diese Fehler in **pxgrid-server.log** auf der ISE sehen:

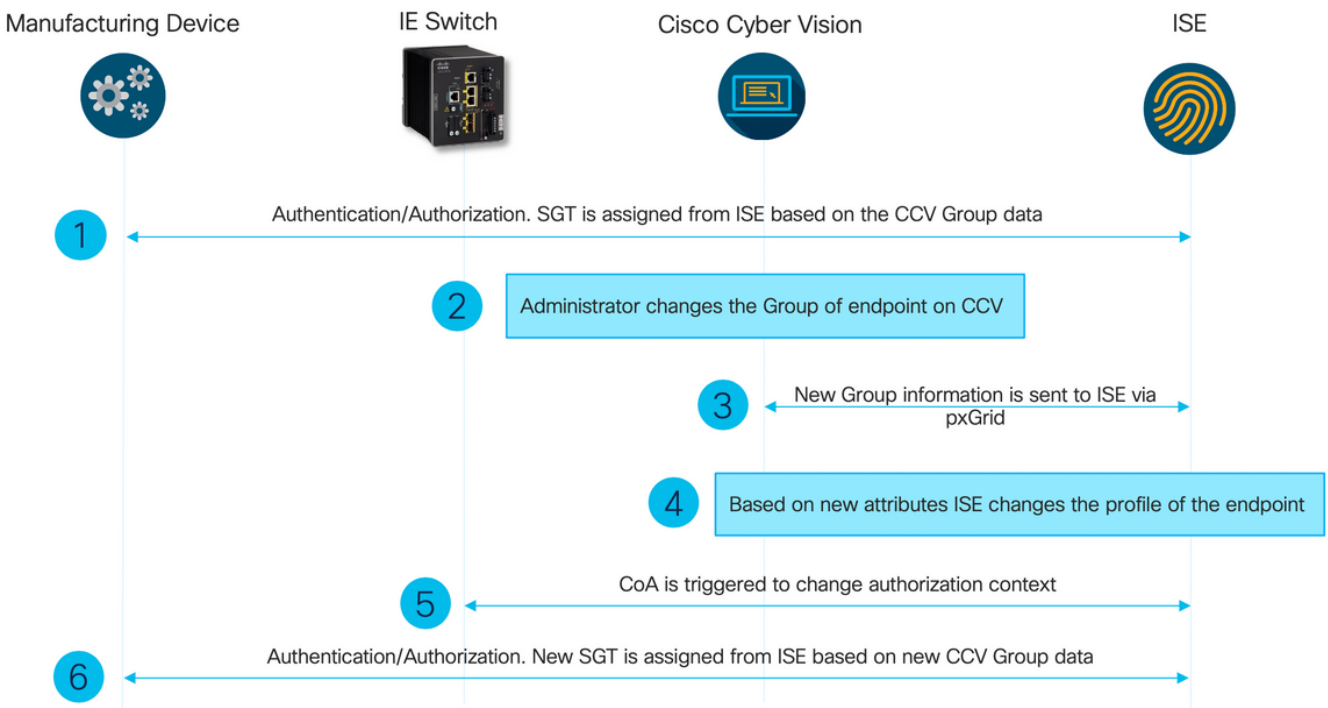
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionID=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726,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

Anwendungsbeispiel für ISE-Integration in CCV TrustSec

Diese Konfiguration zeigt, wie die ISE-Integration mit CCV von End-to-End-Sicherheit bei TrustSec profitieren kann. Dies ist nur eines der Beispiele dafür, wie die Integration nach Abschluss der Integration genutzt werden kann.

> **Hinweis**: Die Erläuterung der Konfiguration von TrustSec-Switches ist nicht in diesem Artikel enthalten. Sie finden sie jedoch im Anhang.

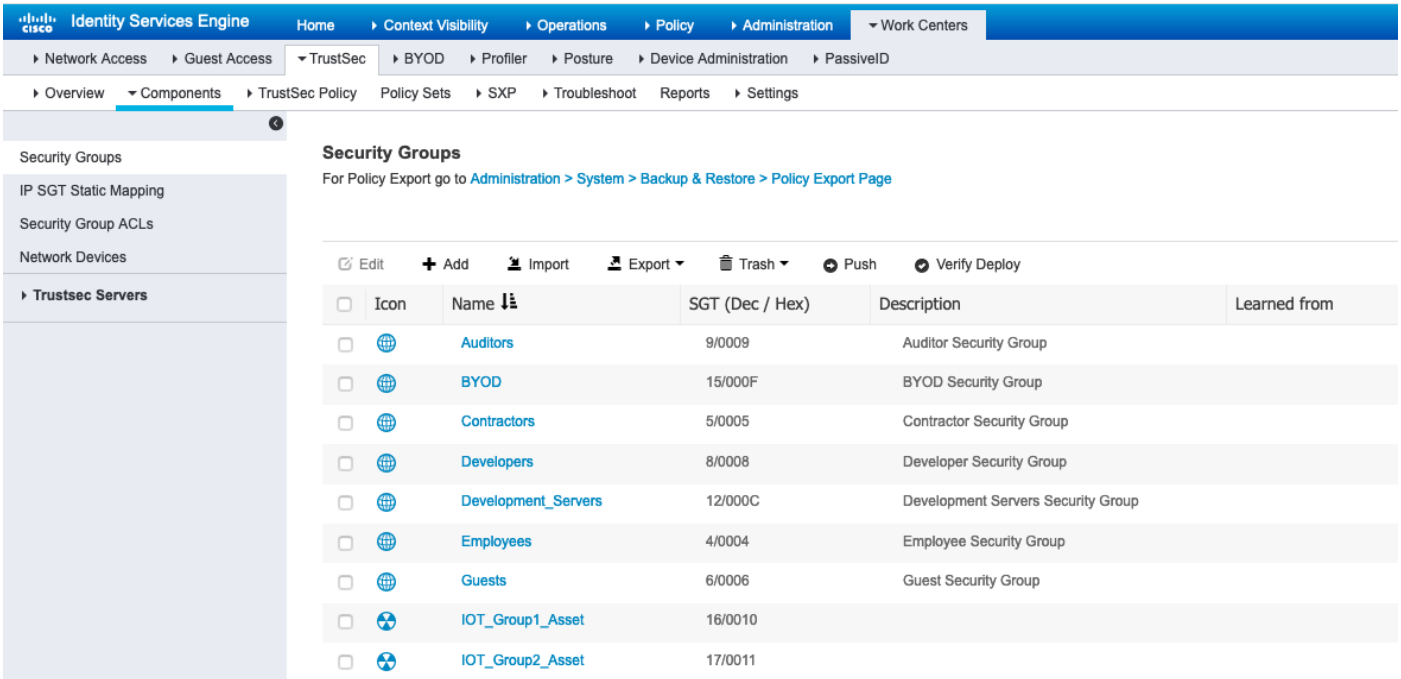
Topologie und Fluss



Konfigurieren

1. Skalierbare Gruppen-Tags auf der ISE konfigurieren

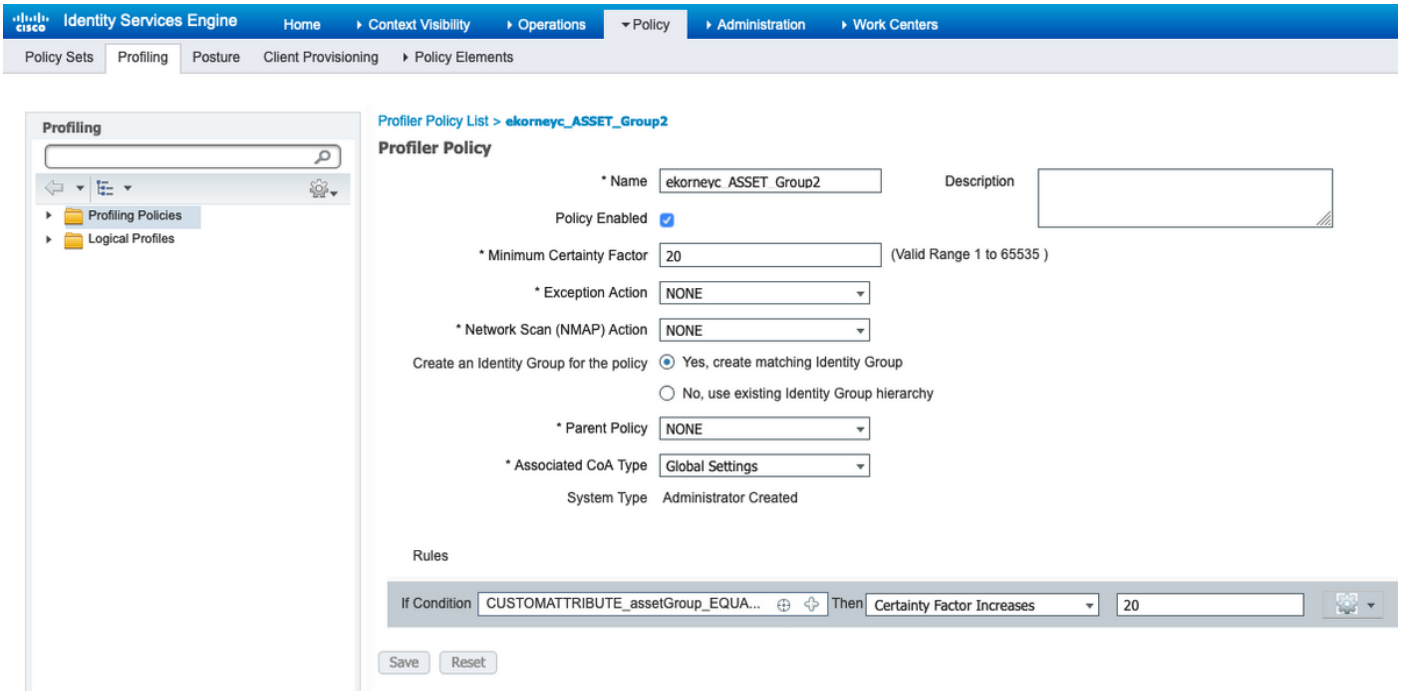
Um den oben genannten Anwendungsfall zu erreichen, werden die IOT_Group1_Asset und die IOT_Group2_Asset des TrustSec-Tags manuell konfiguriert, um CCV-Ressourcen der Gruppe1 von der Gruppe2 zu unterscheiden. Navigieren Sie zu **Work Centers > TrustSec > Components > Security Groups**. Klicken Sie auf **Hinzufügen.** Benennen Sie SGTs wie im Bild gezeigt.



2. Konfigurieren der Profilerichtlinie mit benutzerdefinierten Attributen für Gruppe 2

Hinweis: Die Profilkonfiguration für Gruppe 1 wurde in Schritt 3 durchgeführt. im ersten Teil des Dokuments.

Navigieren Sie zu **Work Center > Profiler > Profiling Policies (Profilerstellungsrichtlinien)**. Klicken Sie auf **Hinzufügen**. Konfigurieren Sie eine Profilerichtlinie, die diesem Bild ähnelt. Der in dieser Richtlinie verwendete Bedingungsausdruck lautet **CUSTOMATTRIBUTE:AssetGroup EQUALS Group2.**



3. Konfigurieren von Autorisierungsrichtlinien zum Zuweisen von SGTs basierend auf Endpunkt-Identitätsgruppen in der ISE

Navigieren Sie zu **Richtlinien > Richtliniensätze**. Wählen Sie **Policy Set** (Richtliniensatz) aus, und konfigurieren Sie **Autorisierungsrichtlinien** entsprechend diesem Bild. Beachten Sie, dass SGTs daher in Schritt 1 konfiguriert werden. zugewiesen werden.

Regelname	Bedingungen	Profile	Sicherheitsgruppen
CCV Group 1-Richtlinie	IdentityGroup · Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ASSET_Group1	Zugriff zulassen	IOT_Gruppe1_Resso
CCV Group 2-Richtlinie	IdentityGroup · Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ASSET_Group2	Zugriff zulassen	IOT_Gruppe2_Resso

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

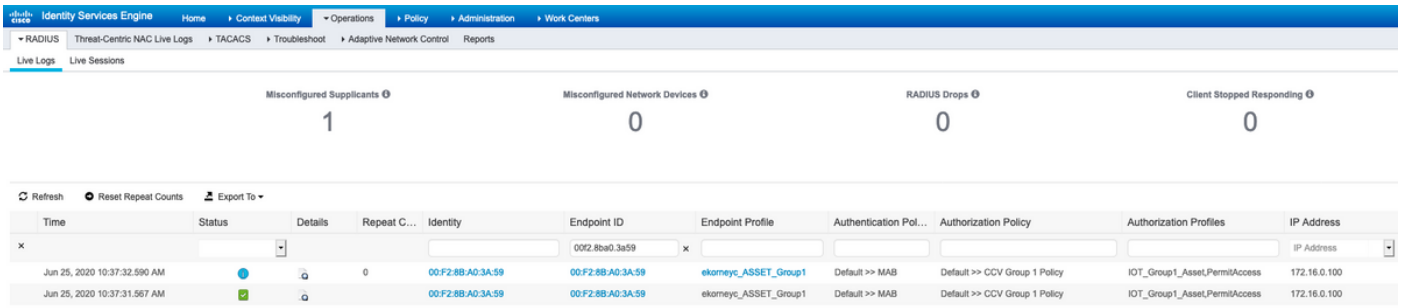
1. Endgeräte-Authentifizierung basierend auf CCV Group 1

Auf dem Switch sehen Sie, dass die Umgebungsdaten beide SGTs **16-54:IOT_Group1_Asset** und **17-54:IOT_Group2_Asset** enthalten.

```
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#
```

Endpunkte authentifizieren sich, und als Ergebnis wird die **CCV Group 1-Richtlinie** zugeordnet, SGT **IOT_Group1_Asset** zugewiesen.



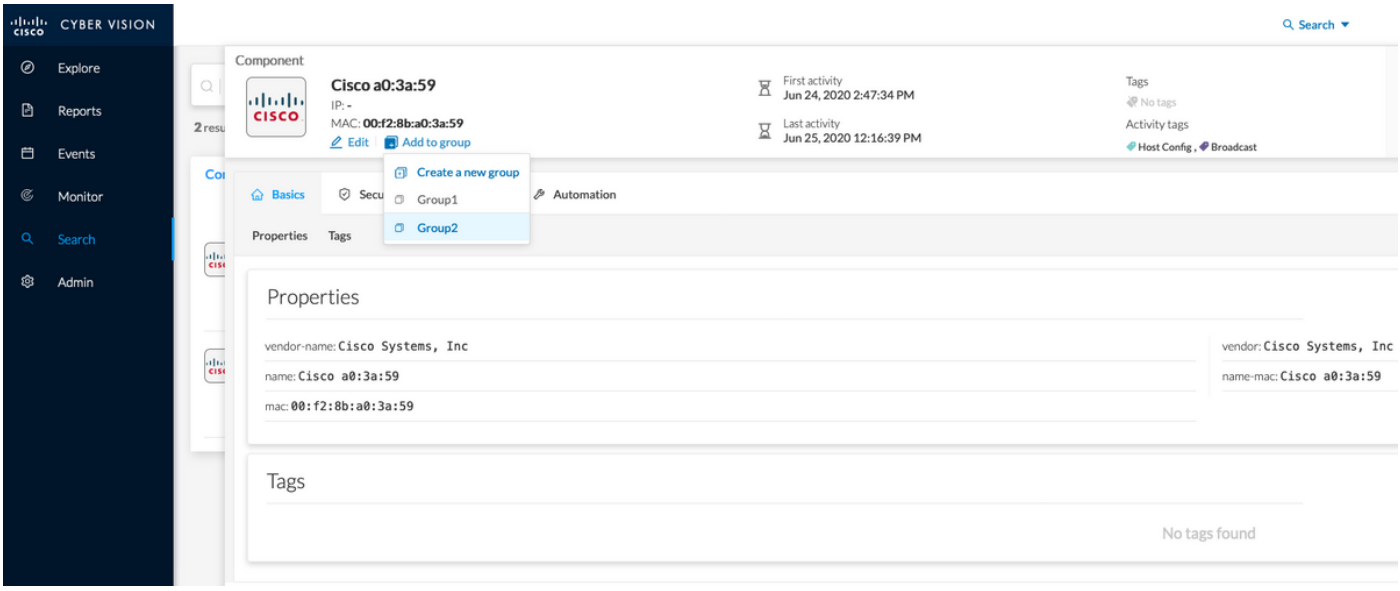
Switch **show authentication sessions interface fa1/7 detail** bestätigt, dass die Access-Accept-Daten erfolgreich angewendet wurden.

```
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. Administrator ändert Gruppe

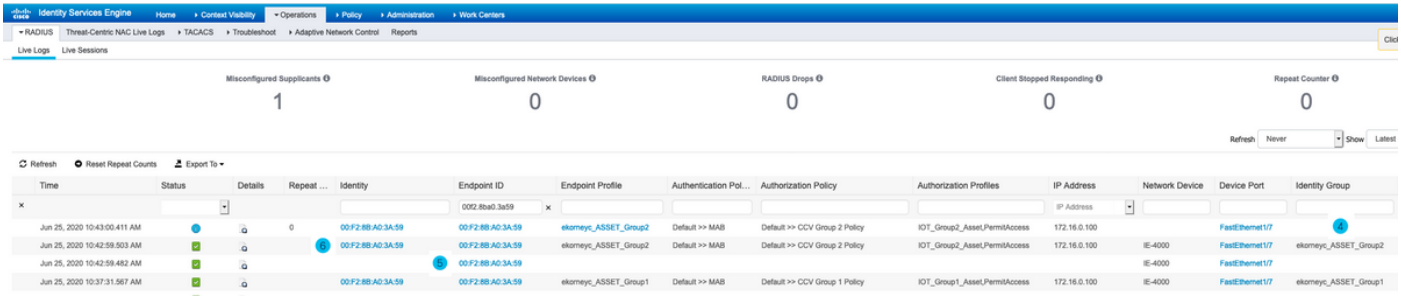
Navigieren Sie zu **Suchen**. Fügen Sie die MAC-Adresse des Endpunkts ein, klicken Sie darauf, und **fügen Sie** sie der Gruppe 2 hinzu.

> **Hinweis**: Bei CCV können Sie die Gruppe nicht von 1 auf 2 in einem Schritt ändern. Daher sollten Sie zuerst den Endpunkt aus der Gruppe entfernen und anschließend Gruppe 2 zuweisen.



3-6. Auswirkungen von Endpunktgruppenänderungen auf CCV

Schritte 4, 5. und 6. werden in diesem Bild angezeigt. Dank der Profilerstellung änderte der Endpunkt die Identitätsgruppe in ekorneyc_ASSET_Group2 (siehe Schritt 4), wodurch die ISE CoA an den Switch (Schritt 5) und schließlich die Endpunkt-Neuauthentifizierung (Schritt 6) schickte.



Der Switch **zeigt eine Authentifizierungssitzung mit fa1/7 an und** bestätigt, dass das neue SGT zugewiesen wurde.

```
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#
```

Anhang

Switch TrustSec-bezogene Konfiguration

> **Hinweis**: CTS-Anmeldeinformationen sind nicht Teil von running-config und sollten mit dem Befehl **cts login id <id> password <password>** im privilegierten exec-Modus konfiguriert werden.

```
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#
```