

# Configurazione dell'integrazione di ISE 2.7 pxGrid CCV 3.1.0

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Diagramma di flusso ad alto livello](#)

[Configurazioni](#)

[1. Abilitare il probe pxGrid su uno dei PSN](#)

[2. Configurazione degli attributi personalizzati dell'endpoint su ISE](#)

[3. Configurare i criteri del profiler utilizzando gli attributi personalizzati](#)

[4. Abilita attributi personalizzati per applicazione profilo](#)

[5. Configurare l'approvazione automatica per i client pxGrid](#)

[6. Esportazione di un certificato CCV](#)

[7. Carica il certificato di identità CCV nell'archivio sicuro ISE](#)

[8. Genera certificato per CCV](#)

[9. Scaricare la catena di certificati in formato PKCS12](#)

[10. Configurazione dei dettagli di integrazione ISE su CCV](#)

[11. Caricamento della catena di certificati in CCV e avvio dell'integrazione](#)

[Verifica](#)

[Verifica integrazione CCV](#)

[Verifica dell'integrazione di ISE](#)

[Verifica modifica gruppo CCV](#)

[Risoluzione dei problemi](#)

[Abilita debug su ISE](#)

[Abilita debug su CCV](#)

[Download in blocco non riuscito](#)

[Non tutti gli endpoint vengono creati ad ISE](#)

[AssetGroup non è disponibile ad ISE](#)

[Gli aggiornamenti del gruppo di endpoint non vengono riflessi su ISE](#)

[La rimozione del gruppo dal CCV non comporta la sua rimozione dall'ISE](#)

[Il CCV non viene utilizzato dai client Web](#)

[Integrazione di ISE con CCV TrustSec Use Case](#)

[Topologia e flusso](#)

[Configurazione](#)

[1. Configurazione dei tag di gruppo scalabili su ISE](#)

[2. Configurare i criteri del profiler con attributi personalizzati per il gruppo 2](#)

[3. Configurare i criteri di autorizzazione per assegnare i moduli SGT in base ai gruppi di identità degli endpoint su ISE](#)

[Verifica](#)

[1. Gli endpoint vengono autenticati in base al gruppo CCV 1](#)

[2. L'amministratore modifica il gruppo](#)

[3-6. Effetto della modifica del gruppo di endpoint sul CCV](#)

[Appendice](#)

[Configurazione correlata a Switch TrustSec](#)

## Introduzione

In questo documento viene descritto come configurare e risolvere i problemi di integrazione di Identity Services Engine (ISE) 2.7 con Cisco Cyber Vision (CCV) 3.1.0 su Platform Exchange Grid v2 (pxGrid). CCV è registrato con pxGrid v2 come publisher e pubblica informazioni sugli attributi degli endpoint su ISE per il dizionario IOTASSET.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- ISE
- Cisco Cyber Vision

### Componenti usati

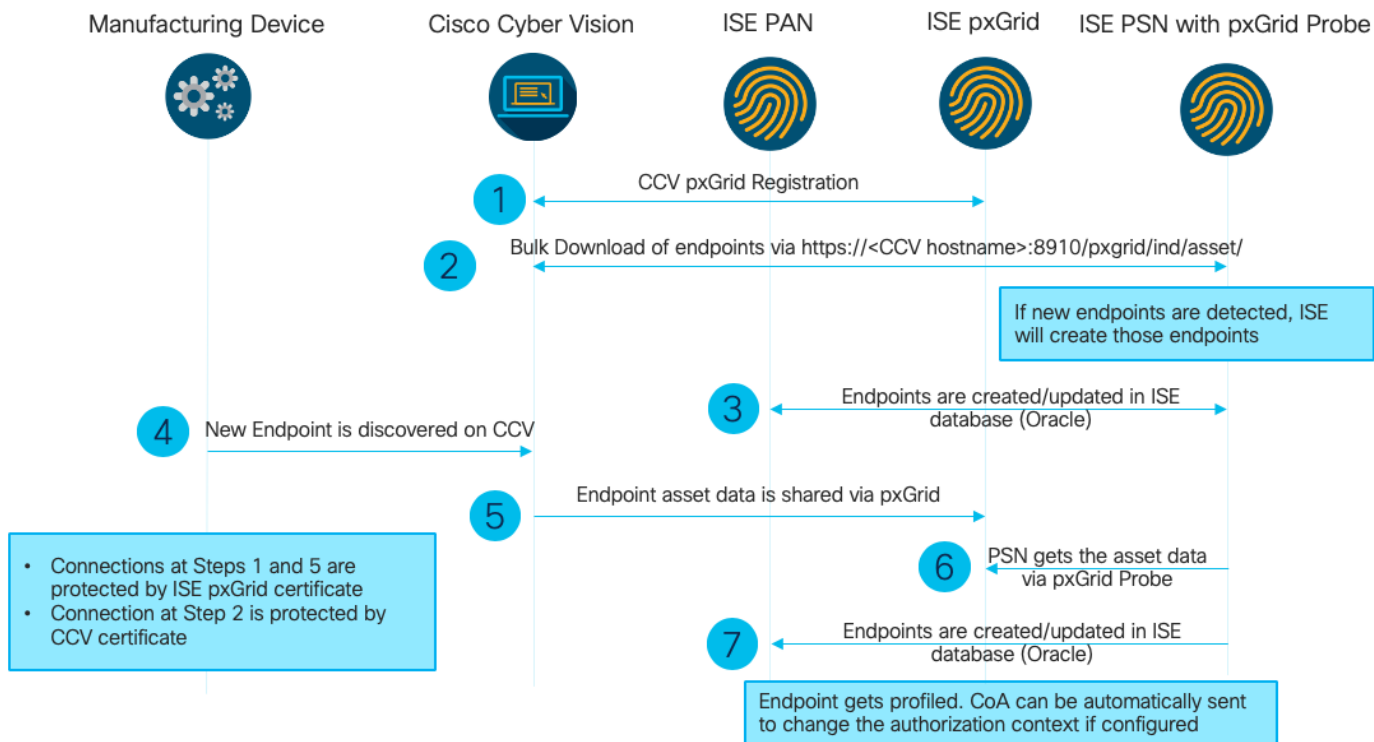
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

### Diagramma di flusso ad alto livello



Questa implementazione ISE viene utilizzata nella configurazione.

#### 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 è un nodo PAN (Primary Admin Node) e pxGrid Node.

ISE 2.7-2ek è un Policy Service Node (PSN) con probe pxGrid abilitato.

Di seguito sono riportati i passaggi che corrispondono al diagramma indicato in precedenza.

1. CCV si registra ad assetTopic su ISE tramite pxGrid versione 2. Log corrispondenti da CCV:

**Nota:** Per esaminare i registri pxGrid su CCV, usare il comando `journalctl -u pxgrid-agent`.

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

```

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

```

## 2. ISE PSN con probe pxGrid abilitato esegue un download in blocco delle risorse pxGrid esistenti (profiler.log):

```

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

```

3. Gli endpoint vengono aggiunti al PSN con il probe pxGrid abilitato e il PSN invia un evento persistente al PAN per salvare gli endpoint (**profiler.log**). Gli endpoint creati con ISE possono essere visualizzati nei dettagli nella sezione Visibilità del contesto.

```
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. Dopo aver inserito un endpoint in un gruppo, CCV invia un messaggio STOMP tramite la porta 8910 per aggiornare l'endpoint con i dati del gruppo negli attributi personalizzati. Log corrispondenti da 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. Il nodo PxGrid riceve l'aggiornamento STOMP e inoltra questo messaggio a tutti i sottoscrittori. Include i PSN con probe pxGrid abilitato. **pxgrid-server.log** su 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. Il PSN con il probe pxGrid abilitato come sottoscrittore nell'argomento asset riceve il messaggio dal nodo pxGrid e aggiorna l'endpoint (**profiler.log**). Gli endpoint aggiornati con ISE possono essere visualizzati nei dettagli in Context Visibility.

```
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. Il PSN con il probe pxGrid abilitato esegue nuovamente il profiling dell'endpoint quando viene trovata una corrispondenza per un nuovo criterio (**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
```

## Configurazioni

**Nota:** I passi da 1 a 4 sono obbligatori anche se si desidera avere una semplice visibilità di assetGroup e in Context Visibility.

### 1. Abilitare il probe pxGrid su uno dei PSN

Selezionare **Amministrazione > Sistema > Distribuzione**, quindi selezionare il nodo ISE con PSN Persona. Passare alla scheda **Configurazione profilo**. Verificare che la sonda **pxGrid** sia abilitata.



**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. Configurazione degli attributi personalizzati dell'endpoint su ISE

Passare a **Amministrazione > Gestione identità > Impostazioni > Attributi personalizzati endpoint**. Configurare gli attributi personalizzati (assetGroup) in base a questa immagine. CCV 3.1.0 supporta solo l'attributo personalizzato **assetGroup**.

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. Configurare i criteri del profiler utilizzando gli attributi personalizzati

Passare a **Centri di lavoro > Profiler > Criteri di profilatura**. Fare clic su **Add**. Configurare i criteri del profiler in modo simile a questa immagine. L'espressione della condizione utilizzata in questo criterio è **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. Abilita attributi personalizzati per applicazione profilo

Passare a **Centri di lavoro > Profiler > Criteri di profilatura**. Fare clic su **Add**. Configurare i criteri del profiler in modo simile a questa immagine. Assicurarsi che l'opzione **Abilita attributo personalizzato per l'applicazione della profilatura** sia abilitata.

The screenshot shows the 'Profiler Configuration' page in the Cisco Identity Services Engine. The navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The breadcrumb trail is 'Network Access > Guest Access > TrustSec > BYOD > Profiler'. The main content area is titled 'Profiler Configuration' and contains the following settings:

- \* CoA Type: Reauth (dropdown menu)
- Current custom SNMP community strings: \*\*\*\*\* (with a 'Show' button)
- Change custom SNMP community strings: [text input] (For NMAP, comma separated.)
- Confirm changed custom SNMP community strings: [text input] (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 are 'Save' and 'Reset' buttons.

#### 5. Configurare l'approvazione automatica per i client pxGrid

Selezionare **Amministrazione > pxGrid Services > Impostazioni**. Selezionare **Approva automaticamente nuovi account basati su certificato** e fare clic su **Salva**. Questa procedura garantisce che non sarà necessario approvare il CCV una volta completata l'integrazione.

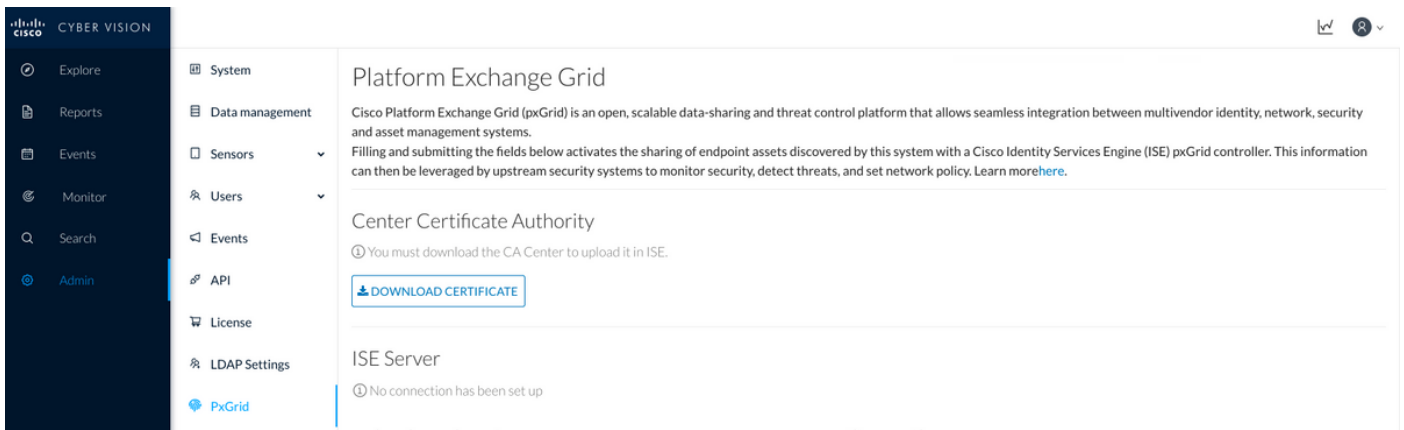
The screenshot shows the 'PxGrid Settings' page in the Cisco Identity Services Engine. The navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The breadcrumb trail is 'System > Identity Management > Network Resources > Device Portal Management > pxGrid Services'. The main content area is titled 'PxGrid Settings' and contains the following settings:

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

At the bottom of the settings area are 'Use Default' and 'Save' buttons.

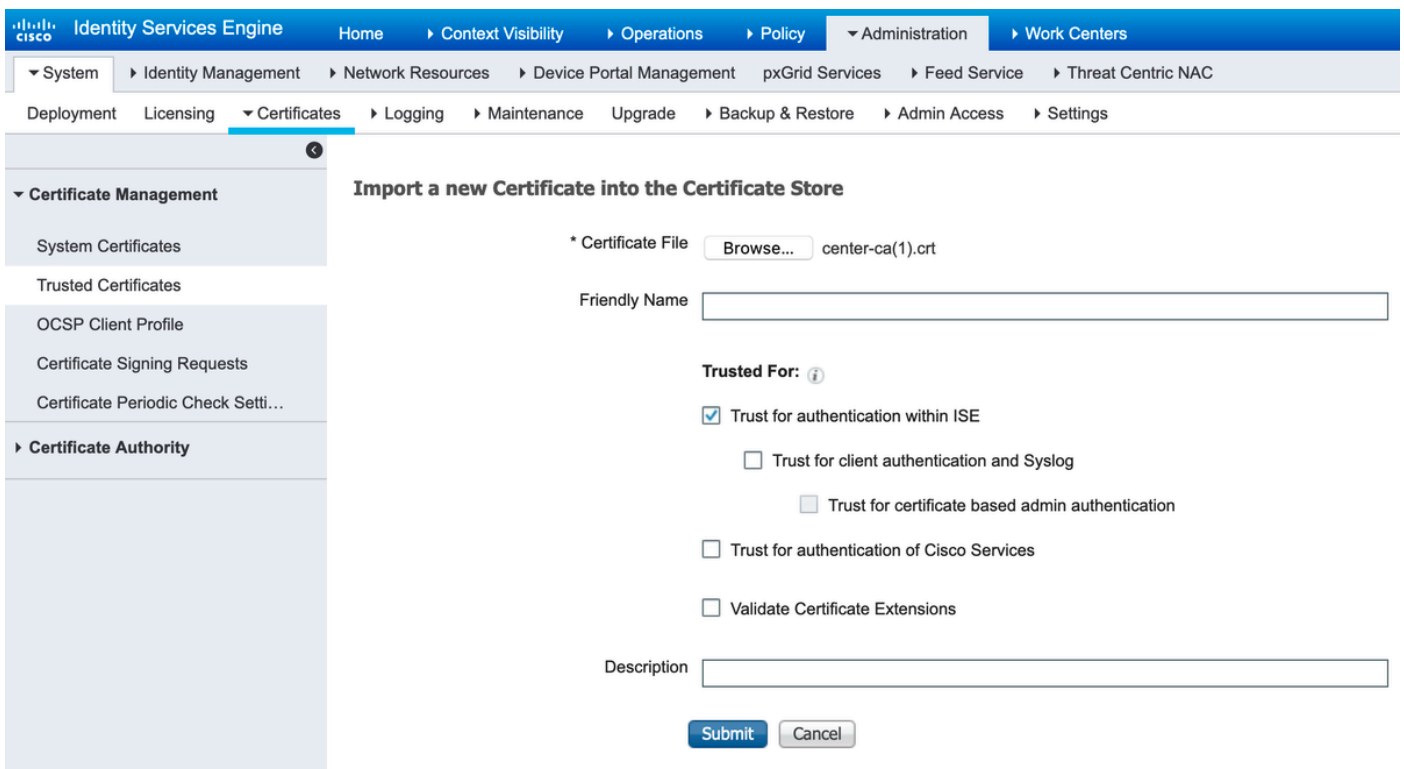
#### 6. Esportazione di un certificato CCV

Selezionare **Admin > pxGrid**. Fare clic su **DOWNLOAD CERTIFICATE**. Questo certificato è utilizzato durante la registrazione di pxGrid, quindi ISE deve considerarlo attendibile.



## 7. Carica il certificato di identità CCV nell'archivio sicuro ISE

Selezionare **Amministrazione > Certificati > Gestione certificati > Certificati attendibili**. Fare clic su **Import**. Fare clic su **Sfoglia** e selezionare il certificato CCV dal Passo 5. Fare clic su **Invia**.



## 8. Genera certificato per CCV

Durante l'integrazione e gli aggiornamenti di pxGrid, CCV richiede il certificato client. Deve essere rilasciato dalla CA interna di ISE, utilizzando **PxGrid\_Certificate\_Template**.

Selezionare **Amministrazione > pxGrid Services > Certificati**. Popolare i campi in base a questa immagine. Il campo Nome comune (CN) è obbligatorio poiché l'obiettivo di ISE CA è il rilascio di un certificato di identità. Immettere il nome host di CCV, il valore del campo CN è critical. Per controllare il nome host di CCV, usare il comando **hostname**. Selezionare PKCS12 come **formato di download del certificato**.

```
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)   - +

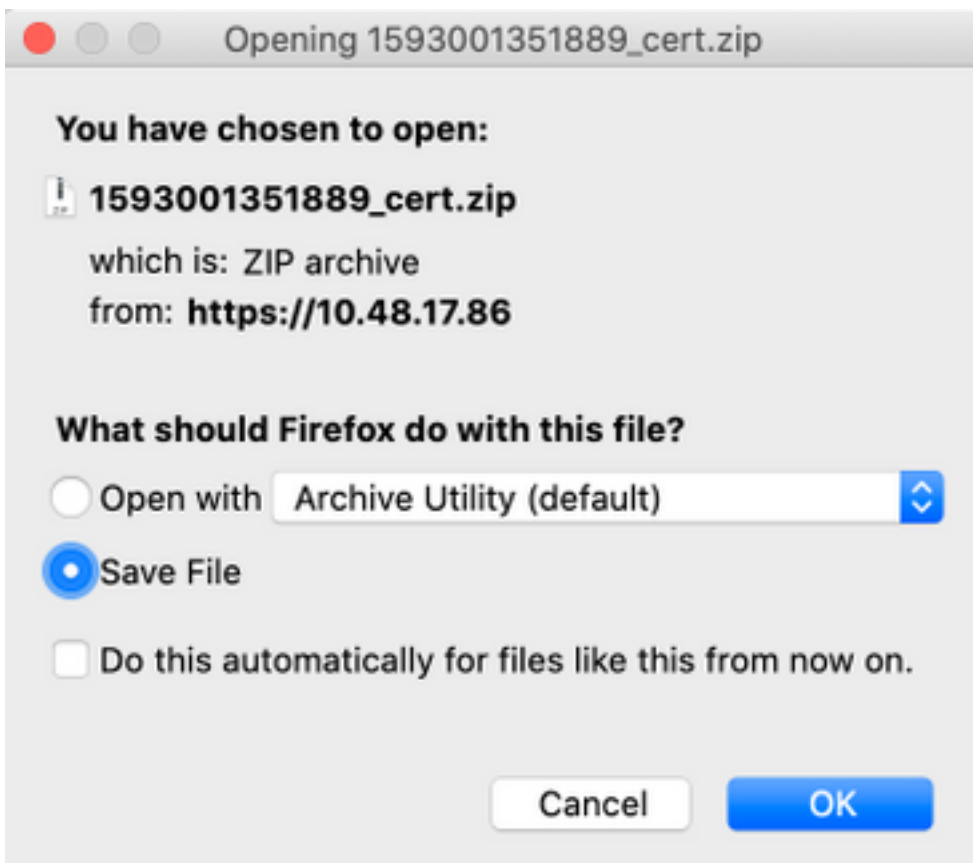
Certificate Download Format \*  ⓘ

Certificate Password \*  ⓘ

Confirm Password \*

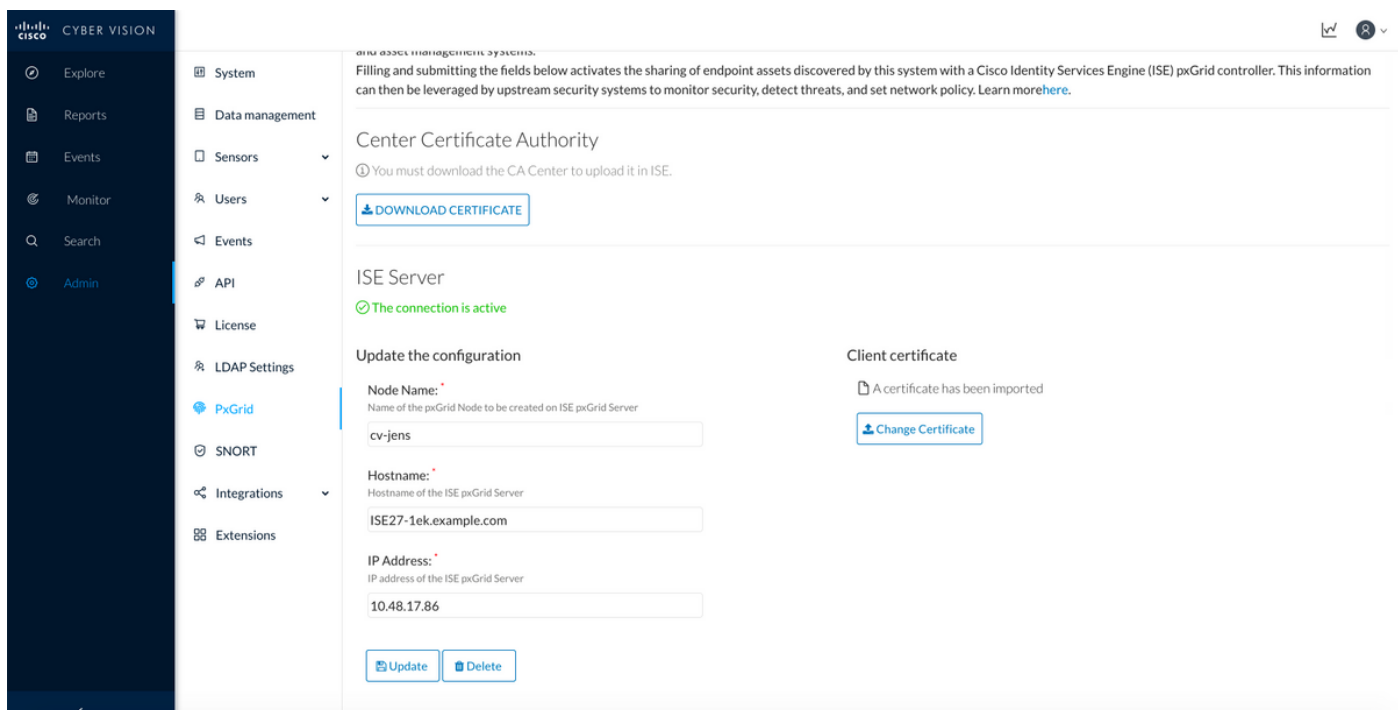
## 9. Scaricare la catena di certificati in formato PKCS12

Quando si installa il certificato nel formato PKCS12, insieme al certificato di identità CCV ISE Internal CA chain viene installato su CCV per garantire che CCV consideri attendibile ISE quando la comunicazione pxGrid viene avviata da ISE, ad esempio, messaggi keepalive pxGrid.



## 10. Configurazione dei dettagli di integrazione ISE su CCV

Selezionare **Admin > pxGrid**. Configure Node Name, questo nome verrà visualizzato su ISE come Nome client in **Administration > pxGrid Services > Web Clients**. Configurare Nome host e Indirizzo IP di ISE pxGrid Node. Verificare che CCV sia in grado di risolvere l'FQDN ISE.



## 11. Caricamento della catena di certificati in CCV e avvio dell'integrazione

Selezionare **Admin > pxGrid**. Fare clic su **Cambia certificato**. Selezionare il certificato rilasciato dalla CA ISE dai passaggi 8-9. Immettere la password dal passaggio 8 e fare clic su **OK**.

Do you want to enter a password?



Ok

Cancel

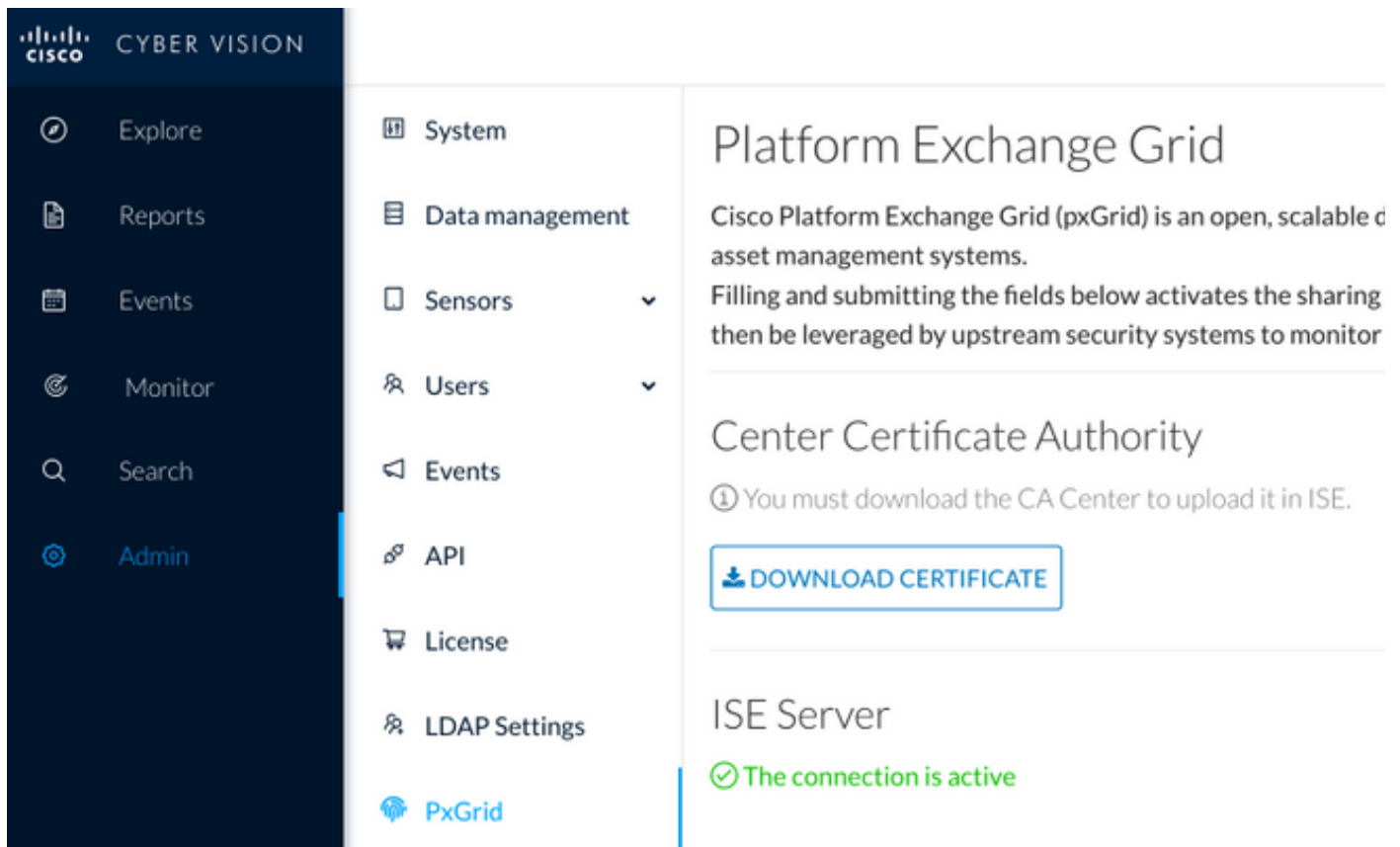
Fare clic su **Update** (Aggiorna) per attivare l'integrazione effettiva CCV - ISE.

## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

## Verifica integrazione CCV

Una volta completata l'integrazione, è possibile confermarla passando a **Admin > pxGrid**. Dovrebbe essere visualizzato il messaggio **La connessione è attiva** in ISE Server.



## Verifica dell'integrazione di ISE

Selezionare **Amministrazione > pxGrid Services > Web Clients**. Confermare che lo stato del client CCV (cv-jens) sia **ON**.

**Nota:** Si prevede che lo stato del client pxGrid CCV sia **Offline** nel menu **All Clients**, in quanto mostra solo lo stato di pxGrid v1.

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

Nota: A causa di [CSCvt78208](#) non vedrete immediatamente CCV con `/topic/com.cisco.ise.endpoint.asset`, verrà mostrato solo alla prima pubblicazione.

## Verifica modifica gruppo CCV

Selezionare **Esplora > Tutti i dati > Elenco componenti**. Fate clic su uno dei componenti e aggiungetelo al gruppo.

The screenshot shows the Cisco Cyber Vision interface. The main view is 'Component list' showing 5 components. The component 'Cisco a0:3a:59' is selected, and its details are shown in the right-hand panel. A 'Component' dialog box is open, showing options to 'Add to group', 'Create a new group', and 'Group1'.

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

Verificare che `/topic/com.cisco.ise.endpoint.asset` sia ora elencato come Pubblicazioni rispetto a CCV.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The main view is 'Web Clients' showing a list of clients. The client 'cv-jens' is selected, and its details are shown in the right-hand panel. The table below shows the list of clients.

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	/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...	/topic/com.cisco.endpoint.asset	10.48.17.88	ON	2020-06-24 10:18:26 UTC	00:04:51:31
ise-mnt-ise27-1ek	ISE27-1ek	ISE27-1ek:39	CN=ISE27-1ek.e...	/topic/com.cisco.ise.se...	/topic/com.cisco.ise.session.internal	10.48.17.86	OFF	2020-06-24 13:53:51 UTC	00:00:58:00
ise-admin-ise27-1ek	ISE27-1ek	ISE27-1ek:41	CN=ISE27-1ek.e...	/topic/com.cisco.ise.se...	/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	/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/wildcard	/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	/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...	/topic/com.cisco.ise.session.internal	10.48.17.86	OFF	2020-06-24 14:52:51 UTC	00:00:17:00
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:46	CN=ISE27-1ek.e...	/topic/distributed	/topic/distributed	10.48.17.86	OFF	2020-06-24 14:53:53 UTC	00:00:02:00
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:47	CN=ISE27-1ek.e...	/topic/distributed	/topic/distributed	10.48.17.86	ON	2020-06-24 14:55:53 UTC	00:00:14:03
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:48	CN=ISE27-1ek.e...	/topic/wildcard	/topic/wildcard	127.0.0.1	ON	2020-06-24 14:57:52 UTC	00:00:12:05
ise-mnt-ise27-2ek	ISE27-1ek	ISE27-1ek:49	No Certificate	/topic/com.cisco.ise.se...	/topic/com.cisco.ise.session.internal	10.48.17.88	ON	2020-06-24 15:01:26 UTC	00:00:08:31

Verificare che Group1 assegnato tramite CCV si rifletta sull'ISE e che i criteri di profilatura siano stati applicati passando a **Context Visibility > Endpoints**. Selezionare l'endpoint aggiornato nel passaggio precedente. Passare alla scheda Attributi. La sezione degli attributi personalizzati deve



riflettere il gruppo appena configurato.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there is a navigation bar with 'Identity Services Engine' and 'Home'. Below it, there are tabs for 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Underneath, there are sub-tabs for 'Endpoints', 'Users', 'Network Devices', and 'Application'. A filter box contains the MAC address '00:F2:8B:A0:3A:59'. The breadcrumb 'Endpoints > 00:F2:8B:A0:3A:59' is visible. The main content area shows the MAC address '00:F2:8B:A0:3A:59' with icons for refresh, edit, and delete. Below this, there is a list of attributes: 'MAC Address: 00:F2:8B:A0:3A:59', 'Username:', 'Endpoint Profile: ekorneyc\_ASSET\_Group1', 'Current IP Address:', and 'Location:'. There are five tabs: 'Applications', 'Attributes' (selected), 'Authentication', 'Threats', and 'Vulnerabilities'. The 'General Attributes' section lists: 'Static Assignment: false', 'Endpoint Policy: ekorneyc\_ASSET\_Group1', 'Static Group Assignment: false', and 'Identity Group Assignment: ekorneyc\_ASSET\_Group1'. The 'Custom Attributes' section has a table with two columns: 'Attribute String' and 'Attribute Value'. The table contains one entry: 'assetGroup' with value 'Group1'. There are 'Filter' and 'Settings' icons to the right of the table.

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**

Attribute String	Attribute Value
assetGroup	Group1

La sezione Altri attributi elenca tutti gli altri attributi delle attività ricevuti dal CCV.

## 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

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

### Abilita debug su ISE

Per abilitare i debug su ISE, selezionare **Amministrazione > Sistema > Registrazione > Configurazione log di debug**. Impostare i seguenti livelli di log:

Persona	Nome componente	Livello log	File da controllare
PAN (opzionale)	profiler	DEBUG	profiler.log
PSN con probe pxGrid abilitato	profiler	DEBUG	profiler.log
PxGrid	pxgrid	TRACCIA	pxgrid-server.log

### Abilita debug su CCV

Per abilitare i debug sulla CCV:

- Creare un file `/data/etc/sbs/pxgrid-agent.conf` con il comando `touch /data/etc/sbs/pxgrid-agent.conf`
- Incollare il contenuto nel file `pxgrid-agent.conf` con l'utilizzo dell'editor `vi` con il comando `vi /data/etc/sbs/pxgrid-agent.conf`

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

- Riavviare `pxgrid-agent` eseguendo il comando `systemctl restart pxgrid-agent`
- Visualizzare i registri con il comando `journalctl -u pxgrid-agent`

## Download in blocco non riuscito

CCV pubblica Bulk Download URL per ISE durante l'integrazione. ISE PSN con probe pxGrid abilitato esegue il download bulk con l'uso di questo URL. Accertarsi che:

- Il nome host nell'URL è risolvibile correttamente dalla prospettiva ISE
- La comunicazione tra PSN sulla porta 8910 e CCV è consentita

`profiler.log` su PSN con probe pxGrid abilitato:

```
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}]]
```

Il download bulk può non riuscire a causa di [CSCvt75422](#), questo errore dovrebbe essere visualizzato in `profiler.log` su ISE per confermarlo. Il difetto è stato risolto 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)
```

## Non tutti gli endpoint vengono creati ad ISE

Ad alcuni endpoint CCV possono essere associati troppi attributi, quindi il database ISE non sarà in grado di gestirli. È possibile verificare la presenza di questi errori nel file `profiler.log` su 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_ENDPOINTTIP" (actual: 660, maximum: 100)
com.cisco.epm.edf2.exceptions.EDF2SQLException: ORA-12899:
value too large for column "CEPM"."EDF_EP_MASTER"."EDF_ENDPOINTTIP" (actual: 660, maximum: 100)
```

## AssetGroup non è disponibile ad ISE

Se AssetGroup non è disponibile su ISE, molto probabilmente il criterio Profiling non è configurato utilizzando gli attributi custom (fare riferimento ai passaggi 2-4. nella parte Configurazioni del documento). Anche per Visibilità contesto, solo per visualizzare gli attributi di gruppo, i criteri di profilatura e altre impostazioni dei passi 2-4 sono obbligatori.

## Gli aggiornamenti del gruppo di endpoint non vengono riflessi su ISE

A causa di [CSCvu80175](#), CCV non pubblica gli aggiornamenti dell'endpoint all'ISE fino a quando CCV non si riavvia subito dopo l'integrazione. È possibile riavviare il CCV una volta completata l'integrazione come soluzione alternativa.

## La rimozione del gruppo dal CCV non comporta la sua rimozione dall'ISE

Questo problema è dovuto al difetto noto su CCV [CSCvu47880](#).L'aggiornamento pxGrid inviato durante la rimozione del gruppo da CCV ha un formato diverso da quello previsto, quindi il gruppo non viene rimosso.

## Il CCV non viene utilizzato dai client Web

Questo problema è dovuto a un difetto noto di ISE [CSCvu47880](#) dove i client passano allo stato OFF seguito da una rimozione completa dai client Web. Il problema è risolto nella patch 2.6 7 e 2.7 patch 2 di ISE.

È possibile confermare la presenza di questi errori in `pxgrid-server.log` su ISE:

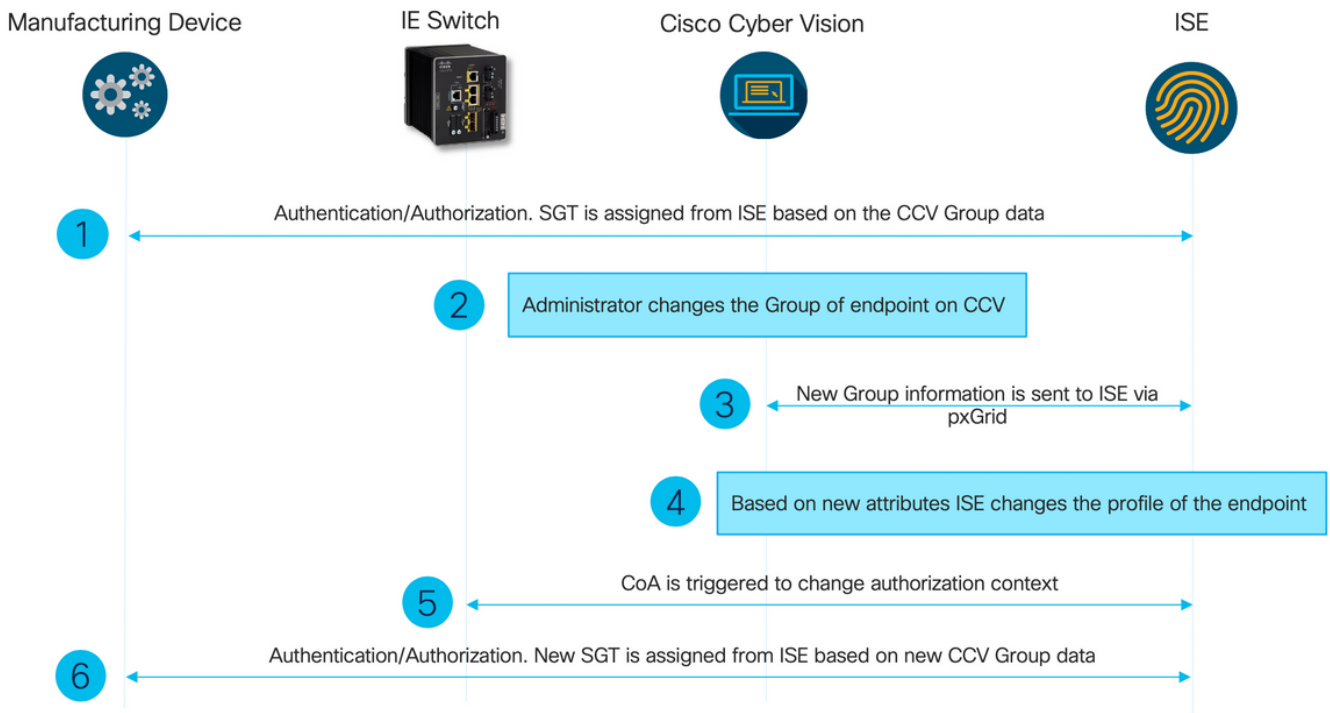
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionID=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726,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

## Integrazione di ISE con CCV TrustSec Use Case

Questa configurazione mostra come l'integrazione di ISE con CCV possa migliorare la sicurezza end-to-end quando TrustSec è in funzione. Questo è solo uno degli esempi di come l'integrazione può essere usata, una volta che l'integrazione è fatta.

**Nota:** La spiegazione della configurazione dello switch TrustSec non rientra nell'ambito di questo articolo, ma è disponibile nell'Appendice.

## Topologia e flusso



## Configurazione

### 1. Configurazione dei tag di gruppo scalabili su ISE

Per ottenere lo scenario d'uso menzionato in precedenza, le proprietà IOT\_Group1\_Asset e IOT\_Group2\_Asset del tag TrustSec sono configurate manualmente in modo da differenziare le risorse CCV di Group1 rispettivamente dal Gruppo2. Passare a **Centri di lavoro > TrustSec > Componenti > Gruppi di sicurezza**. Fare clic su **Add**. Denominare i moduli SGT come mostrato nell'immagine.

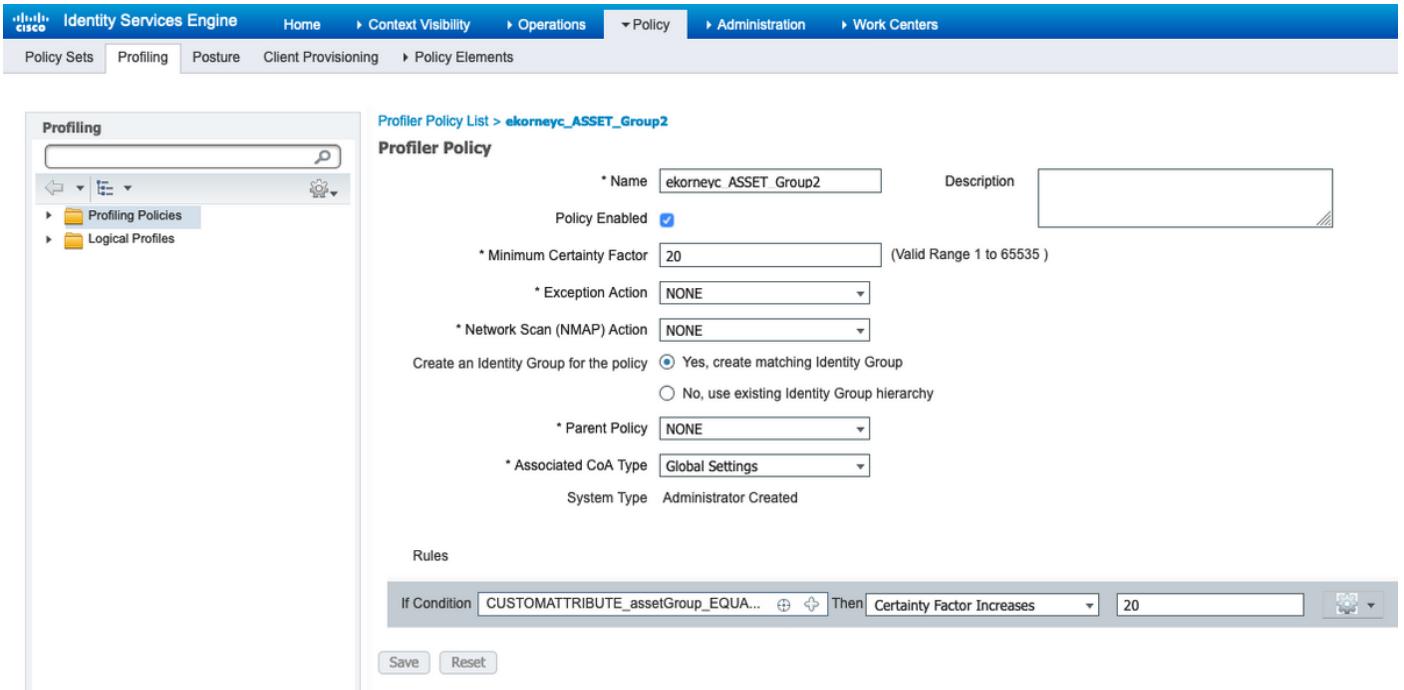
**Security Groups**  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

<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. Configurare i criteri del profiler con attributi personalizzati per il gruppo 2

**Nota:** La configurazione del profilo per il gruppo 1 è stata eseguita nel passo 3. nella prima parte del documento.

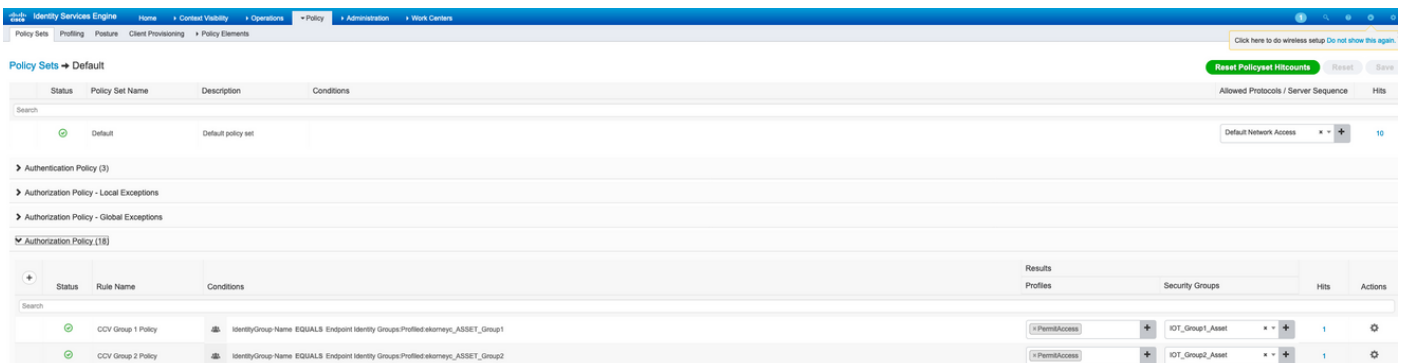
Passare a **Centri di lavoro > Profiler > Criteri di profilatura**. Fare clic su **Add**. Configurare i criteri del profiler in modo simile a questa immagine. L'espressione della condizione utilizzata in questo criterio è **CUSTOMATTRIBUTE:assetGroup EQUALS Group2**.



### 3. Configurare i criteri di autorizzazione per assegnare i moduli SGT in base ai gruppi di identità degli endpoint su ISE

Passare a **Criterio > Set di criteri**. Selezionare **Set di criteri** e configurare i **criteri di autorizzazione** come illustrato nell'immagine. Si noti che, di conseguenza, vengono assegnate le SGT configurate nel passo 1.

Nome regola	Condizioni	Profili	Gruppi di sicurezza
Criteri di gruppo 1 CCV	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ ASSET_Group1	PermitAccess	IOT_Group1_Asset
Criteri di gruppo 2 CCV	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ ASSET_Group2	PermitAccess	IOT_Group2_Asset



# Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

## 1. Gli endpoint vengono autenticati in base al gruppo CCV 1

Su Switch, è possibile verificare che i dati di ambiente includono sia SGT **16-54:IOT\_Group1\_Asset** che **17-54:IOT\_Group2\_Asset**.

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

Gli endpoint vengono autenticati e, di conseguenza, i **Criteri di gruppo 1 CCV** vengono abbinati, il SGT **IOT\_Group1\_Asset** viene assegnato.

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	<span style="color: blue;">●</span>		0	00:F2:8B:A0:3A:59	00:F2:8B: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	<span style="color: green;">■</span>			00:F2:8B:A0:3A:59	00:F2:8B:A0:3A:59	ekomeyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermitAccess	172.16.0.100

Il dettaglio Switch `show authentication sessions interface fa1/7` conferma che i dati di Access-Accept sono stati applicati correttamente.

```
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
```

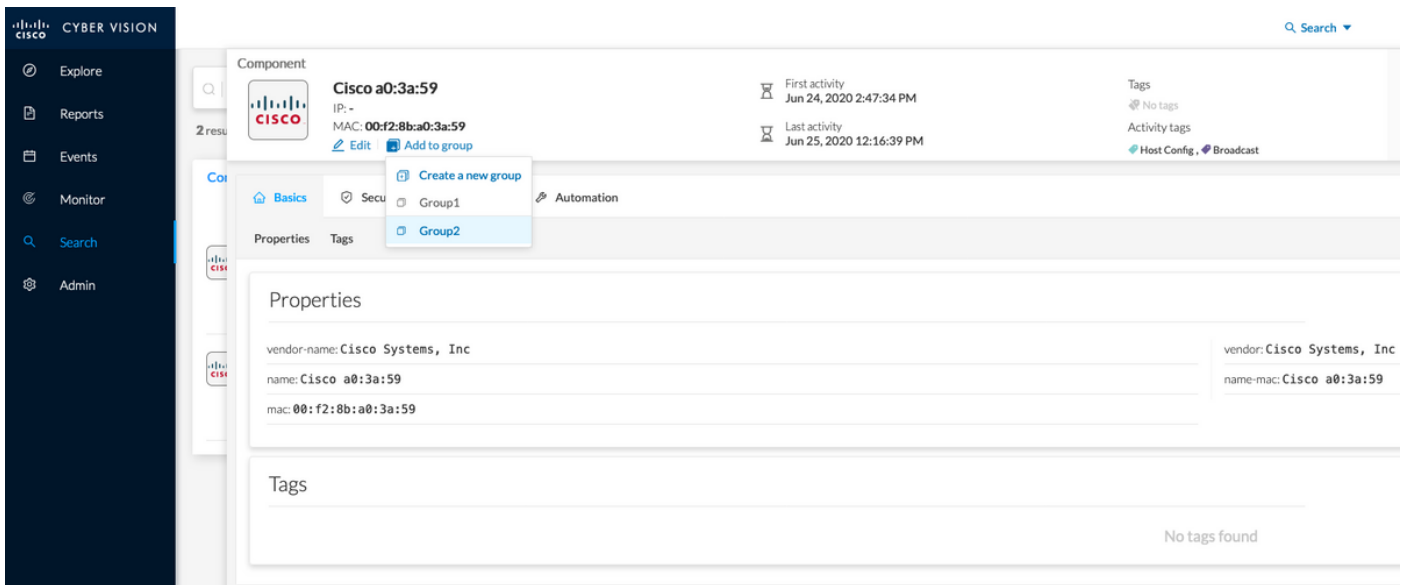
```
KJK_IE4000_10#
```

## 2. L'amministratore modifica il gruppo

Passare a **Cerca**. Incollare l'indirizzo Mac dell'endpoint, fare clic su di esso e **aggiungerlo** al Gruppo 2.

**Nota:** Con CCV, non è possibile modificare il gruppo da 1 a 2 in una sola operazione. È quindi necessario rimuovere prima l'endpoint dal gruppo e quindi assegnare successivamente il gruppo 2.





### 3-6. Effetto della modifica del gruppo di endpoint sul CCV

I punti 4., 5. e 6. sono rappresentati in questa immagine. Grazie alla profilatura, l'endpoint ha modificato il gruppo di identità in ekorneyc\_ASSET\_Group2, come mostrato nel Passaggio 4., causando l'invio di CoA allo switch (Passaggio 5) e la riautenticazione dell'endpoint (Passaggio 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	00F2:8B:AD:3A:59	00F2:8B:AD:3A:59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_Asset/PermitAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59:503 AM	Success			00F2:8B:AD:3A:59	00F2:8B:AD:3A:59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_Asset/PermitAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59:482 AM	Success			00F2:8B:AD:3A:59	00F2:8B:AD:3A:59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_Asset/PermitAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group1

Il dettaglio Switch show authentication session interface fa1/7 conferma che il nuovo SGT è stato assegnato.

```
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#

## Appendice

### Configurazione correlata a Switch TrustSec

**Nota:** Le credenziali Cts non fanno parte di running-config e devono essere configurate con l'utilizzo del comando `id <id> password <password>` delle credenziali CTS in modalità di esecuzione privilegiata.

```
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#