

# Configurar a integração do ISE 2.7 pxGrid CCV

## 3.1.0

### Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de fluxo de alto nível](#)

[Configurações](#)

[1. Ative o teste pxGrid em uma das PSNs](#)

[2. Configurar atributos personalizados de endpoint no ISE](#)

[3. Configurar política de perfil usando atributos personalizados](#)

[4. Ativar atributos personalizados para aplicação de perfil](#)

[5. Configurar a aprovação automática para clientes pxGrid](#)

[6. Exportar certificado CCV](#)

[7. Fazer upload do certificado de identidade CCV para a loja confiável do ISE](#)

[8. Gerar certificado para CCV](#)

[9. Baixar cadeia de certificados no formato PKCS12](#)

[10. Configurar detalhes de integração do ISE no CCV](#)

[11. Fazer upload da cadeia de certificados no CCV e iniciar a integração](#)

[Verificar](#)

[Verificação de integração do CCV](#)

[Verificação de integração do ISE](#)

[Verificar a alteração do grupo CCV](#)

[Troubleshoot](#)

[Habilitar depurações no ISE](#)

[Habilitar depurações no CCV](#)

[Falha no download em massa](#)

[Nem todos os endpoints são criados no ISE](#)

[O AssetGroup não está disponível no ISE](#)

[As atualizações do grupo de endpoints não são refletidas no ISE](#)

[A remoção do grupo do CCV não o está removendo do ISE](#)

[CCV cai dos clientes da Web](#)

[Integração do ISE com o caso de uso do CCV TrustSec](#)

[Topologia e o fluxo](#)

[Configurar](#)

[1. Configurar tags de grupo escaláveis no ISE](#)

[2. Configurar política de perfil com atributos personalizados para o grupo 2](#)

[3. Configurar políticas de autorização para atribuir SGTs com base em grupos de identidade de endpoint no ISE](#)

[Verificar](#)

- [1. Endpoints autenticam com base no grupo 1 do CCV](#)
- [2. O administrador altera o grupo](#)
- [3-6. Efeito da alteração do grupo de endpoints no CCV](#)
- [Appendix](#)
- [Configuração relacionada ao TrustSec do switch](#)

## Introduction

Este documento descreve como configurar e solucionar problemas de integração do Identity Services Engine (ISE) 2.7 com o Cisco Cyber Vision (CCV) 3.1.0 sobre Platform Exchange Grid v2 (pxGrid). O CCV está registrado com o pxGrid v2 como um editor e publica informações sobre atributos de endpoint para o ISE para o dicionário IOTASSET.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- ISE
- Visão cibernética da Cisco

### Componentes Utilizados

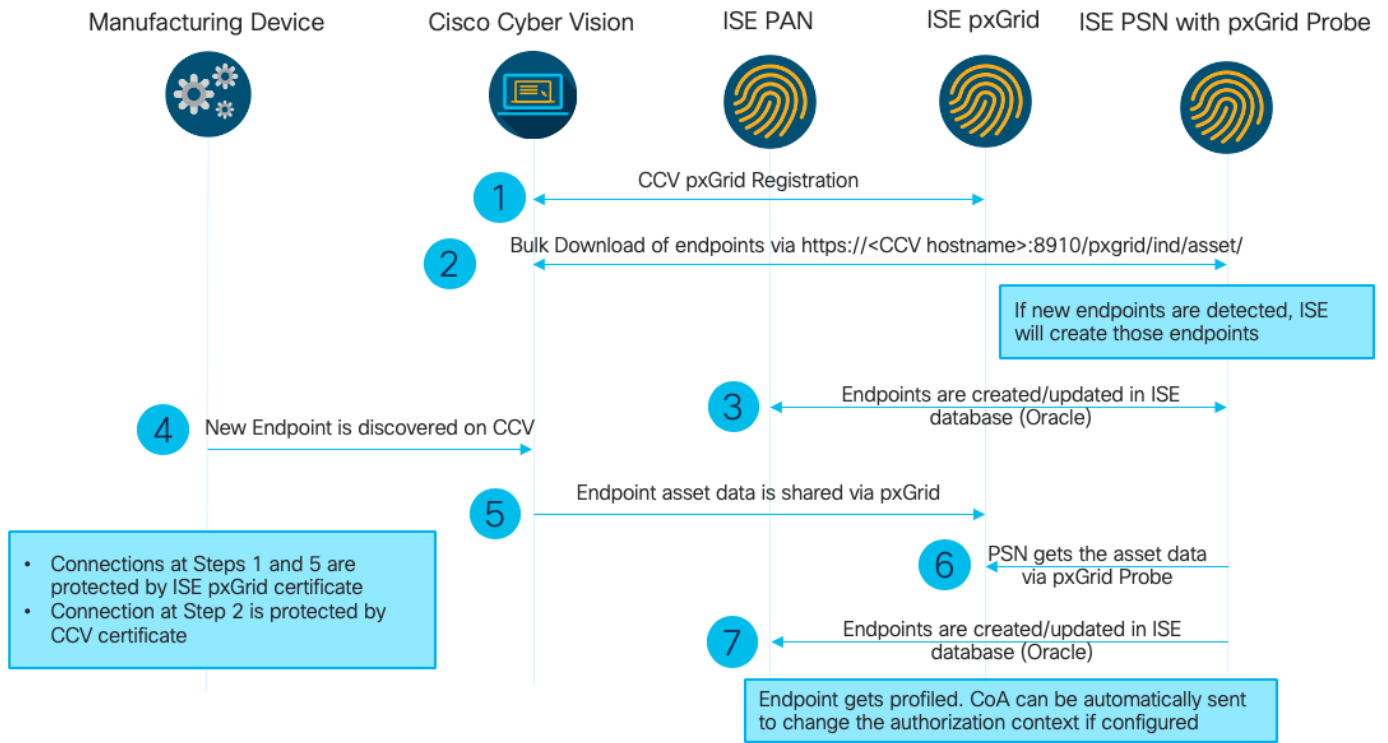
As informações deste documento são baseadas nas seguintes versões de software e de hardware:

- Patch 1 do Cisco ISE versão 2.7
- Cisco Cyber Vision versão 3.1.0
- Switch Ethernet industrial IE-4000-4TC4G-E com s/w 15.2(6)E

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

### Diagrama de fluxo de alto nível



Essa implantação do ISE é usada na configuração.

#### Deployment Nodes

<a href="#">Edit</a> <a href="#">Register</a> <a href="#">Syncup</a> <a href="#">Deregister</a>			
Hostname	Personas	Role(s)	Services
<input type="checkbox"/> ISE27-1ek	Administration, Monitoring, Policy Service, pxGrid	PRI(A), PRI(M)	ALL
<input type="checkbox"/> ISE27-2ek	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION,PROFILER

O ISE 2.7-1ek é o nó de nó administrativo primário (PAN) e o nó pxGrid.

O ISE 2.7-2ek é o Policy Service Node (PSN) com a sonda pxGrid ativada.

Aqui estão as etapas que correspondem ao diagrama mencionado anteriormente.

1. O CCV se registra no assetTopic no ISE via pxGrid versão 2. Registros correspondentes do CCV:

**Note:** Para revisar os registros de pxGrid no CCV, emita o seguinte comando `journal alctl -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. O ISE PSN com sonda pxGrid ativada faz um download em massa dos ativos pxGrid existentes (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. Endpoints são adicionados à PSN com prova pxGrid ativada e PSN envia evento persistente para a PAN para salvar esses endpoints (**profiler.log**). Os endpoints criados no ISE podem ser visualizados nos detalhes do endpoint em Context Visibility.

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

4. Depois de colocar um endpoint em um grupo, o CCV envia mensagem STOMP através da porta 8910 para atualizar o endpoint com os dados do grupo em atributos personalizados. Registros correspondentes do 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. O nó PxGrid recebe a atualização STOMP e encaminha essa mensagem a todos os assinantes, inclui PSNs com prova pxGrid ativada. **pxgrid-server.log** no nó pxGrid.

```

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 com a sonda pxGrid ativada como assinante no tópico do ativo recebe a mensagem do nó pxGrid e atualiza o ponto de extremidade (**profiler.log**). Os endpoints atualizados no ISE podem ser visualizados nos detalhes do endpoint em 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. PSN com prova pxGrid ativada redefine o perfil do ponto de extremidade como uma nova Política correspondente (**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
```

## Configurações

**Note:** As etapas 1 a 4 são necessárias mesmo que você deseje ter apenas visibilidade do assetGroup e da visibilidade de contexto.

### 1. Ative o teste pxGrid em uma das PSNs

Navegue até **Administration > System > Deployment**, selecione ISE node com PSN Persona. Mude para a guia **Configuração de perfil**. Verifique se a sonda **pxGrid** está ativada.



**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. Configurar atributos personalizados de endpoint no ISE

Navegue até **Administration > Identity Management > Settings > Endpoint Custom Attributes**. Configure atributos personalizados (assetGroup) de acordo com esta imagem. O CCV 3.1.0 suporta apenas o **AssetGroup** Attribute Personalizado.

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. Configurar política de perfil usando atributos personalizados

Navegue até **Centros de trabalho > Perfil > Políticas de criação de perfil**. Clique em **Adicionar**. Configure a Política de Perfil semelhante a esta imagem. A expressão de condição usada nesta política é **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. Ativar atributos personalizados para aplicação de perfil

Navegue até **Centros de trabalho > Perfil > Políticas de criação de perfil**. Clique em **Adicionar**. Configure a Política de Perfil semelhante a esta imagem. Certifique-se de que **Enable Custom Attribute for Profying Implementation** esteja ativado.

The screenshot shows the Cisco Identity Services Engine (ISE) Profiler Configuration page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Profiler. The left sidebar shows 'Profiler Settings' and 'NMAP Scan Subnet Exclusions'. The main content area is titled 'Profiler Configuration' and contains the following settings:

- \* CoA Type: Reauth
- Current custom SNMP community strings: \*\*\*\*\* (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

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

#### 5. Configurar a aprovação automática para clientes pxGrid

Navegue até **Administration > pxGrid Services > Settings**. Selecione **Aprovar automaticamente novas contas baseadas em certificados** e clique em **Salvar**. Essa etapa garante que você não precise aprovar o CCV após a integração.

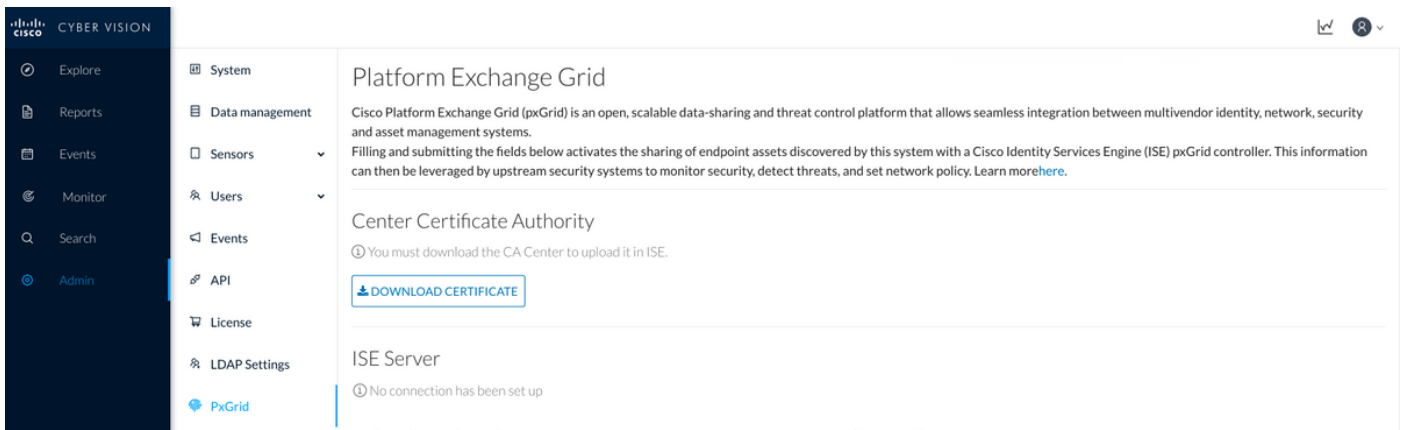
The screenshot shows the Cisco Identity Services Engine (ISE) pxGrid Services Settings page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > pxGrid Services. The left sidebar shows 'All Clients', 'Web Clients', 'Capabilities', 'Live Log', 'Settings', 'Certificates', and 'Permissions'. The main content area is titled 'PxGrid Settings' and contains the following settings:

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

Buttons for 'Use Default' and 'Save' are located at the bottom of the settings area.

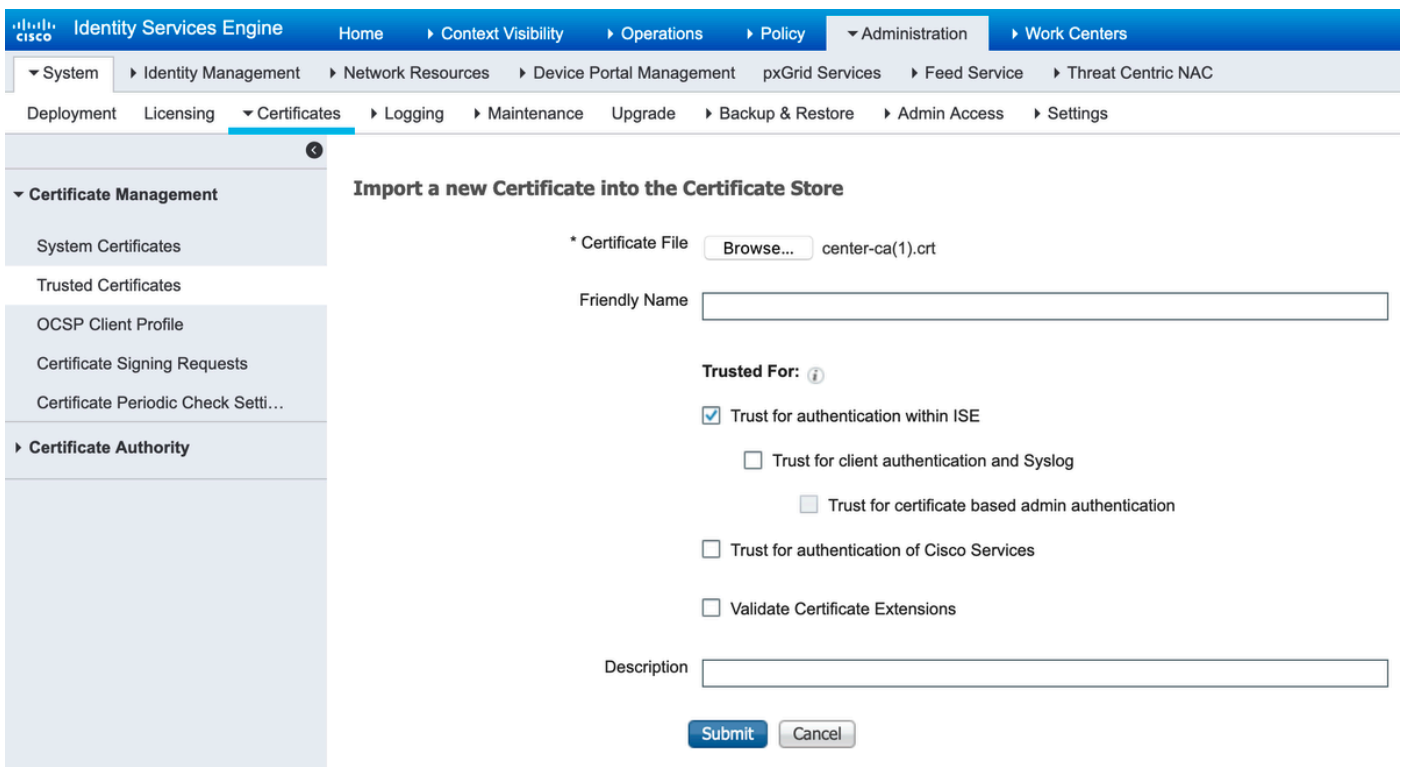
#### 6. Exportar certificado CCV

Navegue até **Admin > pxGrid**. Clique em **DOWNLOAD CERTIFICATE**. Este certificado é usado durante o registro pxGrid, portanto, o ISE deve confiar nele.



## 7. Fazer upload do certificado de identidade CCV para a loja confiável do ISE

Navegue até **Administração > Certificados > Gerenciamento de Certificados > Certificados Confiáveis**. Clique em **Importar**. Clique em **Procurar** e selecione o certificado CCV na Etapa 5. Clique em **Submit**.



## 8. Gerar certificado para CCV

Durante a integração e as atualizações do pxGrid, o CCV precisa do certificado do cliente. Ele deve ser emitido pela CA interna do ISE, usando **PxGrid\_Certificate\_Template**.

Navegue até **Administration > pxGrid Services > Certificados**. Preencha os campos de acordo com esta imagem. O campo Nome Comum (CN) é obrigatório, pois o objetivo da CA do ISE é emitir um certificado de identidade. Você deve inserir o nome do host CCV, o valor do campo CN é crítico. Para verificar o nome do host do CCV, execute o comando **hostname**. Selecione PKCS12 como **formato de download de certificado**.

```
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)   - +

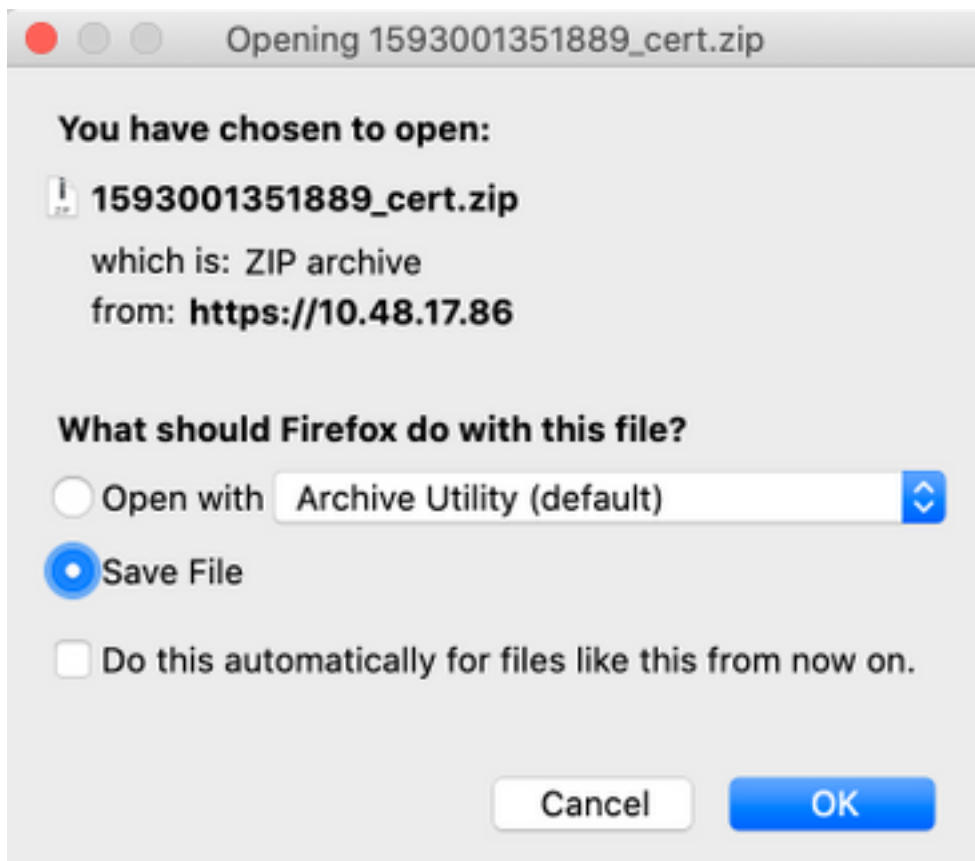
Certificate Download Format \*  ⓘ

Certificate Password \*  ⓘ

Confirm Password \*

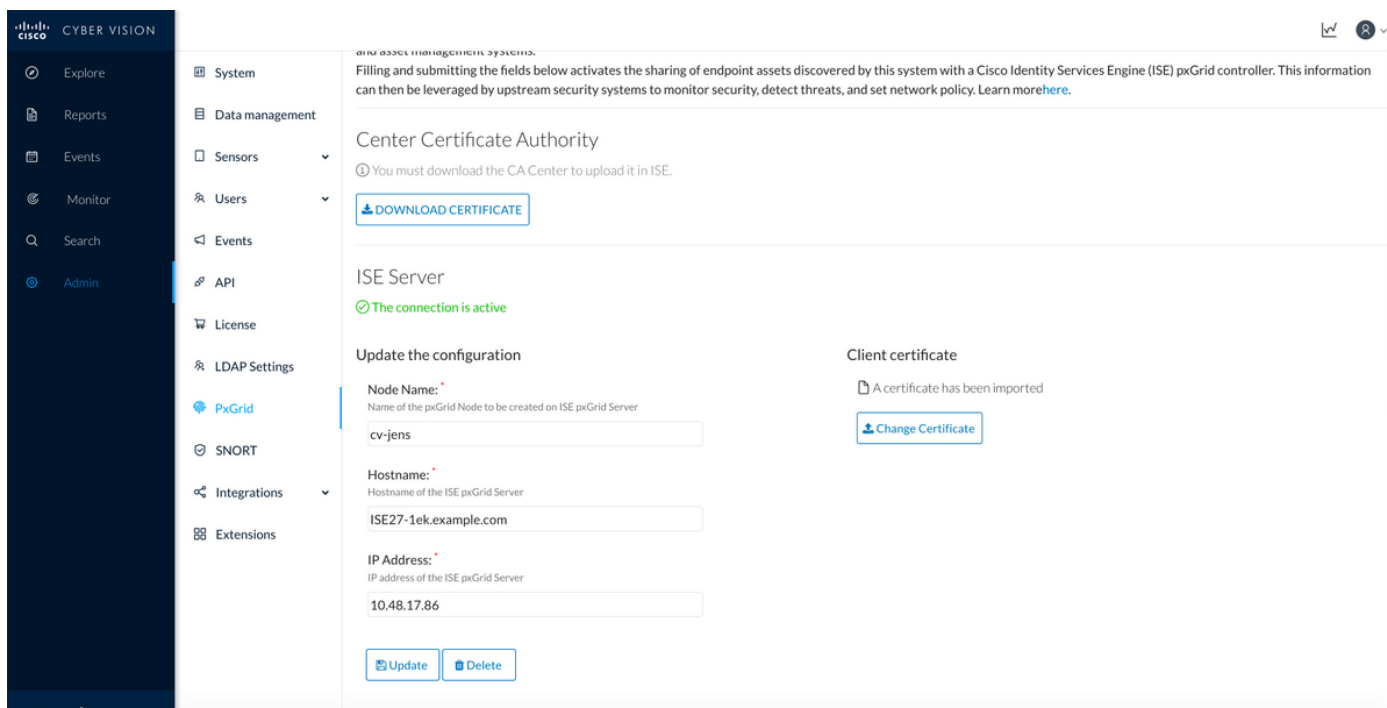
## 9. Baixar cadeia de certificados no formato PKCS12

Quando você instala o certificado no formato PKCS12, juntamente com a cadeia de CA interna ISE do certificado de identidade CCV é instalada no CCV para garantir que o CCV confie no ISE quando a comunicação pxGrid é iniciada no ISE, por exemplo, mensagens de keepalive pxGrid.



## 10. Configurar detalhes de integração do ISE no CCV

Navegue até **Admin > pxGrid**. Configure o nome do nó, esse nome será exibido no ISE como um nome de cliente em **Administration > pxGrid Services > Web Clients**. Configure **Hostname** e **IP Address** de ISE pxGrid Node. Certifique-se de que o CCV possa resolver ISE FQDN.



The screenshot shows the Cisco Cyber Vision Admin interface. The left sidebar contains navigation options: Explore, Reports, Events, Monitor, Search, and Admin. The main content area is titled 'Center Certificate Authority' and 'ISE Server'. The 'Update the configuration' section includes the following fields and values:

- Node Name:** cv-jens
- Hostname:** ISE27-1ek.example.com
- IP Address:** 10.48.17.86

Buttons for 'Update' and 'Delete' are located at the bottom of the configuration section. A 'Client certificate' section on the right indicates 'A certificate has been imported' and includes a 'Change Certificate' button.

## 11. Fazer upload da cadeia de certificados no CCV e iniciar a integração

Navegue até **Admin > pxGrid**. Clique em **Alterar certificado**. Selecione o certificado emitido pela CA do ISE nas Etapas 8 a 9. Insira a senha na Etapa 8. e clique em **OK**.

Do you want to enter a password?

●●●●●●●●

Ok

Cancel

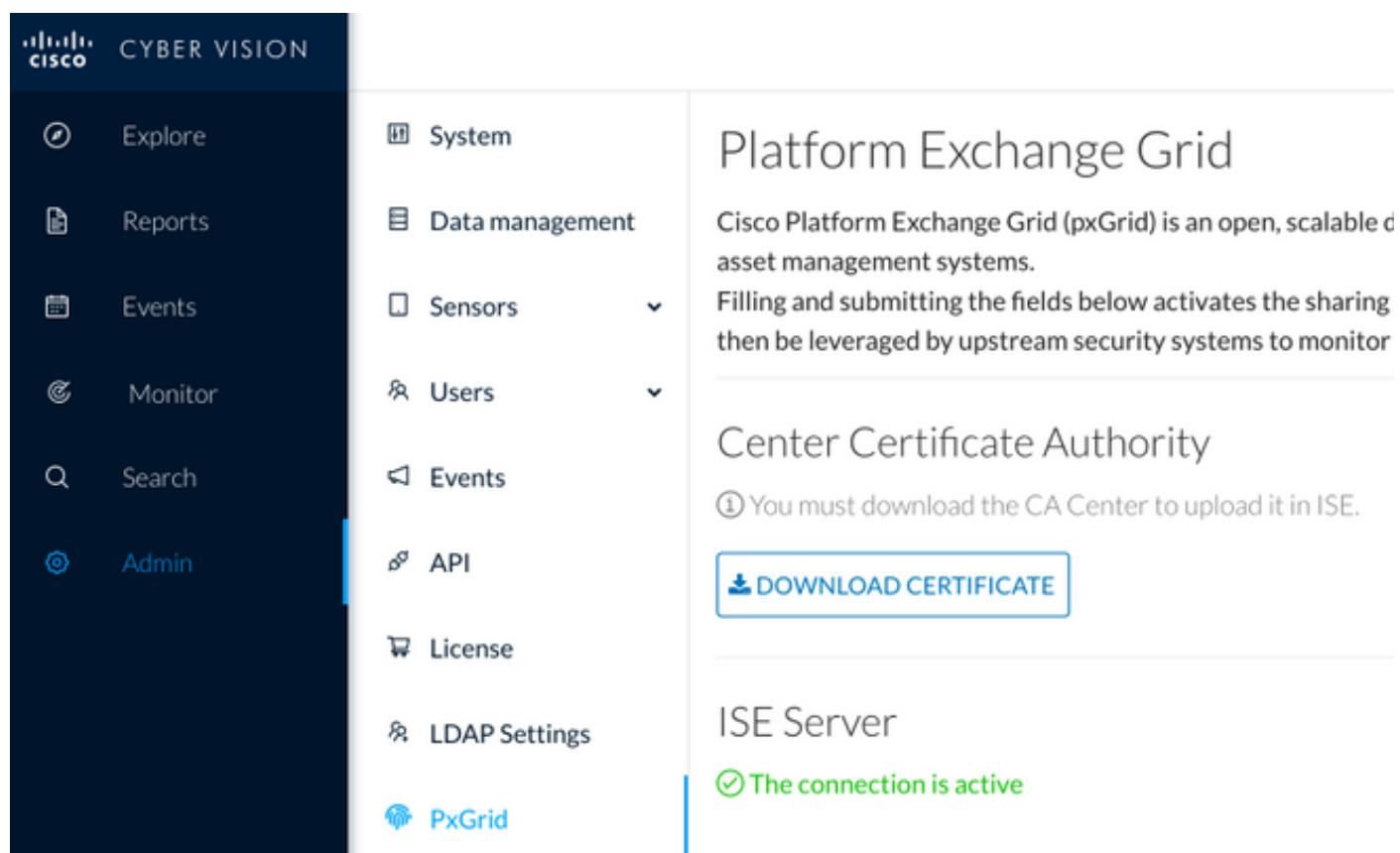
Clique em **Update**, que aciona a integração CCV - ISE real.

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

## Verificação de integração do CCV

Quando a integração estiver concluída, você poderá confirmá-la com êxito navegando até **Admin > pxGrid**. Você deve ver a mensagem **connection is active** em ISE Server.



The screenshot displays the Cisco Cyber Vision Admin interface. The left sidebar contains the following menu items: Explore, Reports, Events, Monitor, Search, and Admin (highlighted). The main content area is titled 'Platform Exchange Grid' and includes the following text: 'Cisco Platform Exchange Grid (pxGrid) is an open, scalable d asset management systems. Filling and submitting the fields below activates the sharing then be leveraged by upstream security systems to monitor'. Below this is the 'Center Certificate Authority' section, which includes a warning icon and the text 'You must download the CA Center to upload it in ISE.' and a 'DOWNLOAD CERTIFICATE' button. At the bottom, the 'ISE Server' status is shown as 'The connection is active' with a green checkmark.

## Verificação de integração do ISE

Navegue até **Administration > pxGrid Services > Web Clients**. Confirme se o status do cliente CCV (cv-jens) está **ON**.

**Note:** Espera-se ver o status do cliente CCV pxGrid como **Offline** no menu **Todos os clientes**, pois ele mostra apenas o status 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...	/topic/com.cisco.ise.co...	127.0.0.1	ON	2020-06-24 10:06:52 UTC	00:04:27:16
ise-mnt-ise27-2ek	ISE27-1ek	ISE27-1ek:24	No Certificate	/topic/com.cisco.ise.se...	/topic/com.cisco.ise.se...	10.48.17.88	ON	2020-06-24 10:18:25 UTC	00:04:15:43
ise-admin-ise27-2ek	ISE27-1ek	ISE27-1ek:25	No Certificate	/topic/com.cisco.endpo...		10.48.17.88	ON	2020-06-24 10:18:26 UTC	00:04:15:43
ise-admin-ise27-1ek	ISE27-1ek	ISE27-1ek:34	CN=ISE27-1ek.e...		/topic/com.cisco.ise.en...	10.48.17.86	OFF	2020-06-24 12:09:50 UTC	00:02:19:00
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:37	CN=ISE27-1ek.e...	/topic/wildcard		127.0.0.1	OFF	2020-06-24 13:02:51 UTC	00:01:08:00
cv-jens	ISE27-1ek	ISE27-1ek:38	CN=center			10.48.43.241	ON	2020-06-24 13:39:12 UTC	00:00:54:56
ise-mnt-ise27-1ek	ISE27-1ek	ISE27-1ek:39	CN=ISE27-1ek.e...	/topic/com.cisco.ise.se...		10.48.17.86	ON	2020-06-24 13:53:51 UTC	00:00:40:17
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:40	CN=ISE27-1ek.e...	/topic/wildcard		127.0.0.1	OFF	2020-06-24 14:11:51 UTC	00:00:18:00
ise-admin-ise27-1ek	ISE27-1ek	ISE27-1ek:41	CN=ISE27-1ek.e...			10.48.17.86	ON	2020-06-24 14:29:51 UTC	00:00:04:17
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:42	CN=ISE27-1ek.e...	/topic/wildcard		127.0.0.1	ON	2020-06-24 14:30:51 UTC	00:00:03:17

**Note:** Devido ao [CSCvt78208](#), você não verá imediatamente o CCV com `/topic/com.cisco.ise.endpoint.asset`, ele será mostrado somente na primeira publicação.

## Verificar a alteração do grupo CCV

Navegue até **Explorar > Todos os dados > Lista de componentes**. Clique em um dos componentes e adicione-o ao grupo.

The screenshot shows the Cisco Cyber Vision interface. The main view is titled 'Component list' and displays a table with 5 components. The component 'Cisco a0:3a:59' is selected, and a context menu is open over it, showing options like 'Add to group', 'Create a new group', 'Group1', and 'Group2'. The interface also shows a sidebar with navigation options like 'Explore', 'Reports', 'Events', 'Monitor', 'Search', and 'Admin'.

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:
01:00:0c:00:00:00	-	May 11, 2020 6:44:15 PM	Jun 24, 2020 4:27:19 PM	-	01:
01:00:0c:cccc:cccc	-	Mar 13, 2020 1:52:23 PM	Jun 24, 2020 4:27:19 PM	-	01:
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:

Verifique se `/topic/com.cisco.ise.endpoint.asset` agora está listado como Publications no CCV.



Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

Click here to do wirel

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions

Rows/Page 25 1



Refresh

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

Confirme se o Grupo1 atribuído via CCV é refletido no ISE e a política de criação de perfil entrou em vigor navegando até **Context Visibility > Endpoints**. Selecione o ponto final atualizado na etapa anterior. Mude para a guia Atributos. A seção de atributos personalizados deve refletir o grupo recém-configurado.

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

[Endpoints](#) > 00:F2:8B:A0:3A:59

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



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

[Applications](#)
**Attributes**
Authentication
Threats
Vulnerabilities

**General Attributes**

Description

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

**Custom Attributes**

▼ Filter ▼
⚙️ ▼

	Attribute String	Attribute Value
×	Attribute String	Attribute Value
	assetGroup	Group1

A seção Outros atributos lista todos os outros atributos de ativos recebidos do 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

## Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

### Habilitar depurações no ISE

Para habilitar depurações no ISE, navegue para **Administration > System > Logging > Debug Log Configuration**. Defina os níveis de log para estes:

Persona	Nome do componente	Nível de log	Arquivo a ser verificado
PAN (opcional)	profiler	DEBUG	profiler.log
PSN com prova pxGrid habilitada	profiler	DEBUG	profiler.log
PxGrid	pxgrid	RASTREAMENTO	pxgrid-server.log

### Habilitar depurações no CCV

Para ativar depurações no CCV:

- Crie um arquivo `/data/etc/sbs/pxgrid-agent.conf` com o comando `touch /data/etc/sbs/pxgrid-agent.conf`
- Cole este conteúdo no arquivo `pxgrid-agent.conf` com o uso do vi editor com o comando `vi /data/etc/sbs/pxgrid-agent.conf`

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

- Reinicie o pxgrid-agent executando o comando `systemctl restart pxgrid-agent`
- Exibir logs com o comando `journal -u pxgrid-agent`

## Falha no download em massa

O CCV publica o URL de download em massa para o ISE durante a integração. O ISE PSN com prova pxGrid ativada executa o Download em massa com o uso deste URL. Assegure que:

- O nome do host na URL pode ser resolvido corretamente da perspectiva do ISE
- A comunicação de PSN na porta 8910 para CCV é permitida

`profiler.log` no PSN com prova pxGrid ativada:

```
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}]]
```

O download em massa pode falhar devido ao [CSCvt75422](#), você deve ver esse erro em `profiler.log` no ISE para confirmá-lo. O defeito é corrigido no 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)
```

## Nem todos os endpoints são criados no ISE

Alguns endpoints no CCV podem ter muitos atributos anexados, portanto o banco de dados do ISE não poderá lidar com isso. Isso pode ser confirmado se você vir esses erros no `profiler.log` no ISE.

```
2020-05-29 00:01:25,228 ERROR [admin-http-pool1][] com.cisco.profiler.api.EDFEndPointHandler -
:::-
Failed to create endpoint 00:06:F6:2A:C4:2B ORA-12899:
```

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

## O AssetGroup não está disponível no ISE

Se AssetGroup não estiver disponível no ISE, muito provavelmente, a política de criação de perfil não está configurada usando Atributos personalizados (consulte as Etapas 2 a 4). na parte Configurações do documento). Mesmo para visibilidade de contexto, apenas para exibir atributos de grupo, políticas de criação de perfil e outras configurações das Etapas 2 a 4 são obrigatórias.

## As atualizações do grupo de endpoints não são refletidas no ISE

Devido ao [CSCvu80175](#), o CCV não publica atualizações de endpoint para o ISE até que o CCV seja reinicializado logo após a integração. Você pode reinicializar o CCV depois que a integração for feita como uma solução alternativa.

## A remoção do grupo do CCV não o está removendo do ISE

Esse problema é observado devido ao defeito conhecido no CCV [CSCvu47880](#). A atualização do pxGrid enviada durante a remoção do grupo do CCV com formato diferente do esperado, portanto, o grupo não é removido.

## CCV cai dos clientes da Web

Esse problema é observado devido ao defeito conhecido no ISE [CSCvu47880](#), onde os clientes fazem a transição para o estado DESLIGADO seguido de remoção completa dos clientes da Web. O problema é resolvido nos 2.6 patch 7 e 2.7 patch 2 do ISE.

Você pode confirmá-lo se vir estes erros em `pxgrid-server.log` no ISE:

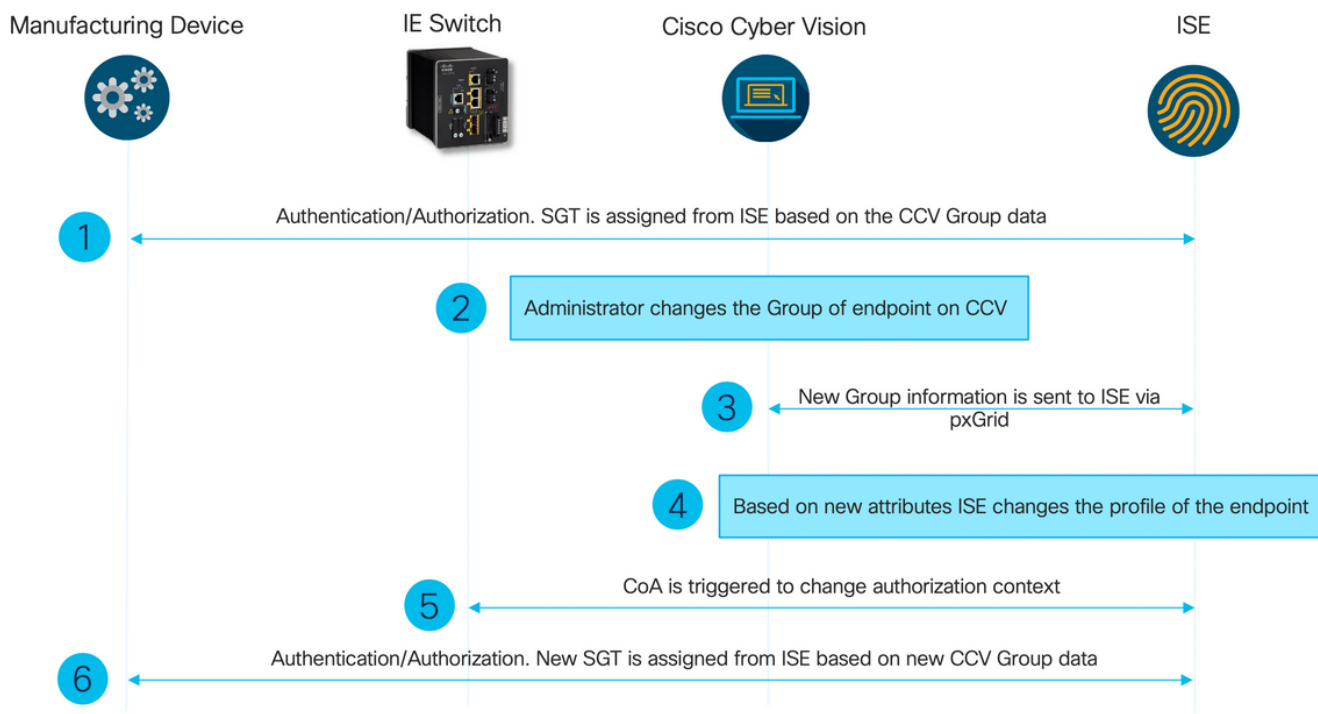
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionId=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726,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

## Integração do ISE com o caso de uso do CCV TrustSec

Esta configuração mostra como a integração do ISE com o CCV pode beneficiar a segurança de ponta a ponta quando o TrustSec está em vigor. Este é apenas um dos exemplos de como a integração pode ser usada, depois que a integração for feita.

**Note:** A explicação da configuração do switch TrustSec está fora do escopo deste artigo, no entanto, ele pode ser encontrado no Apêndice.

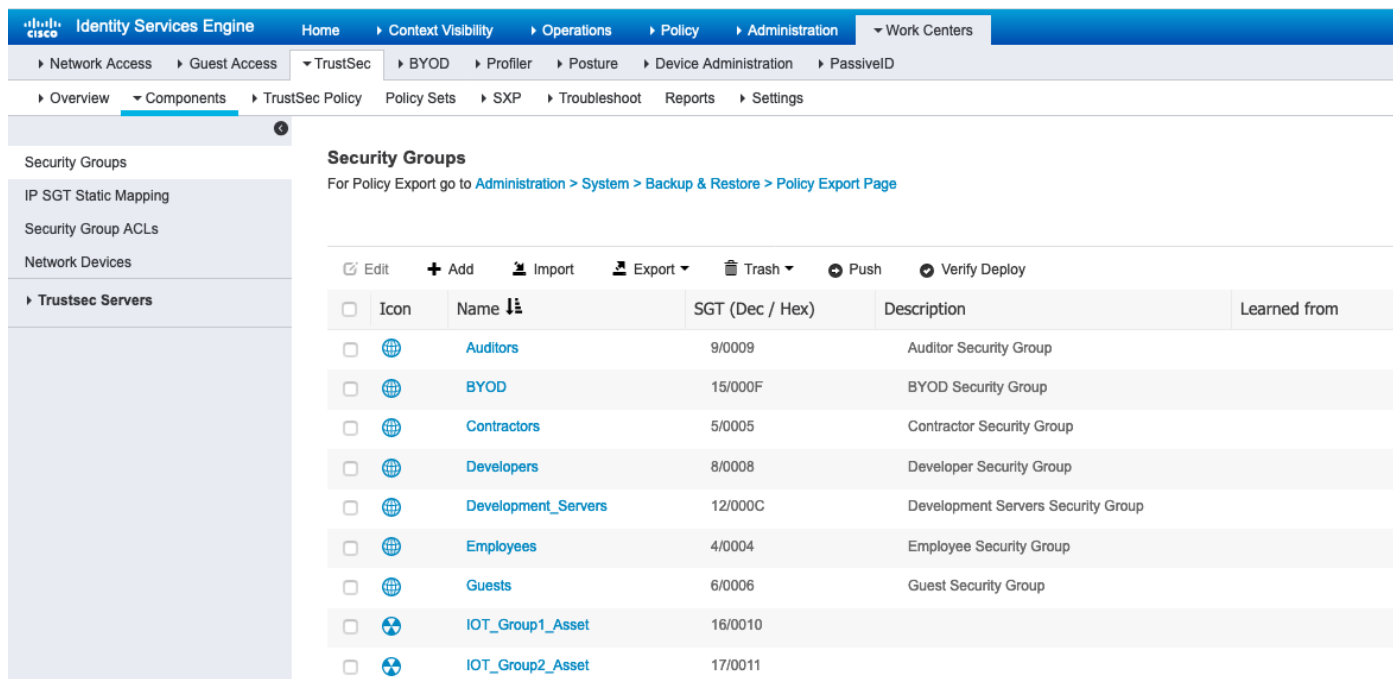
# Topologia e o fluxo



## Configurar

### 1. Configurar tags de grupo escaláveis no ISE

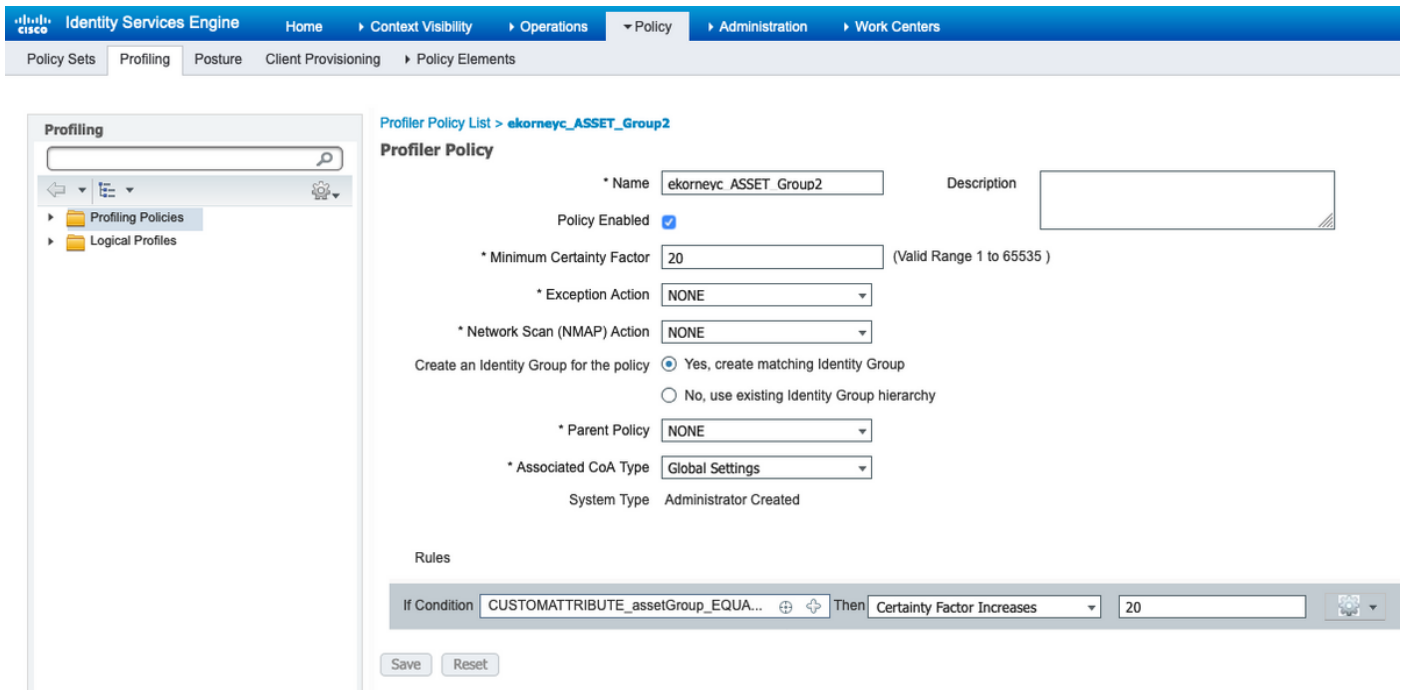
Para obter o caso de uso mencionado anteriormente, o IOT\_Group1\_Asset da tag TrustSec e o IOT\_Group2\_Asset são configurados manualmente para diferenciar os ativos do CCV Group1 do Group2, respectivamente. Navegue até **Centros de trabalho > TrustSec > Componentes > Grupos de segurança**. Clique em **Adicionar**. Nomeie SGTs como mostrado na imagem.



### 2. Configurar política de perfil com atributos personalizados para o grupo 2

**Note:** A configuração de perfil para o Grupo 1 foi feita na Etapa 3. na primeira parte do documento.

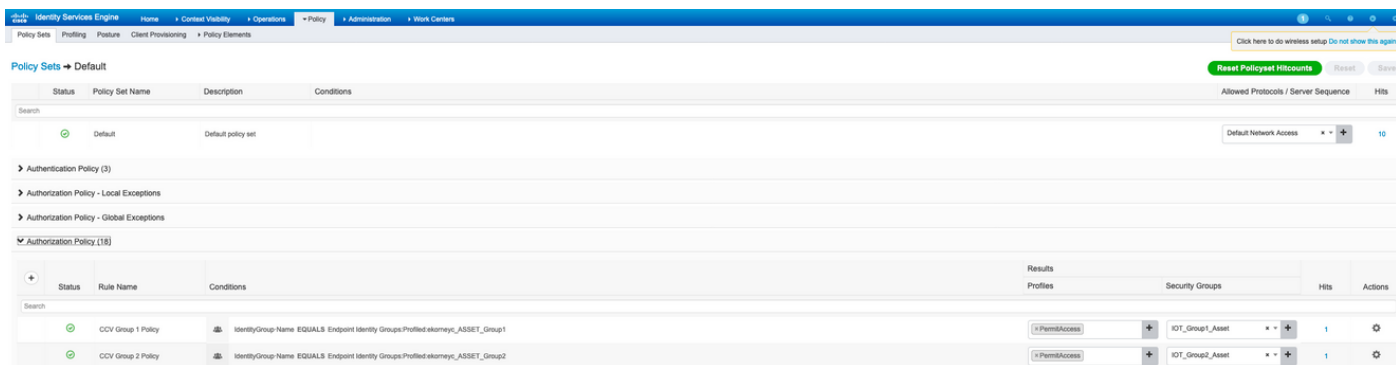
Navegue até **Centros de trabalho > Perfil > Políticas de criação de perfil**. Clique em **Adicionar**. Configure a Política de Perfil semelhante a esta imagem. A expressão de condição usada nesta política é **CUSTOMATTRIBUTE:assetGroup EQUALS Group2**.



### 3. Configurar políticas de autorização para atribuir SGTs com base em grupos de identidade de endpoint no ISE

Navegue até **Política > Conjuntos de políticas**. Selecione **Conjunto de políticas** e configure **Políticas de autorização** de acordo com esta imagem. Observe que, como resultado, o SGT é configurado na Etapa 1. são atribuídos.

Nome da regra	Condições	Perfis	Grupos de segurança
Política do grupo 1 do CCV	IdentidadeGrupo · Nome IGALS Grupo de Identidades do Ponto Final:Perfil:ekorneyc_ASS ET_Group1	PermitAccess	IOT_Group1_Asset
Política do grupo 2 do CCV	IdentidadeGrupo · Nome IGALS Grupo de Identidades do Ponto Final:Perfil:ekorneyc_ASS ET_Group2	PermitAccess	IOT_Group2_Asset



## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

### 1. Endpoints autenticam com base no grupo 1 do CCV

No Switch, você pode ver que os dados do ambiente incluem os **16-54:IOT\_Group1\_Asset** da SGT e **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#

Endpoints são autenticados e, como resultado, a Política do Grupo 1 do CCV é correspondida, SGT IOT\_Group1\_Asset é atribuída.

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

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

Below the statistics is a table of active sessions:

Time	Status	Details	Repeat C...	Identity	Endpoint ID	Endpoint Profile	Authentication Pol...	Authorization Policy	Authorization Profiles	IP Address
Jun 25, 2020 10:37:32.590 AM	<span style="color: blue;">●</span>		0	00F2.8B.A0.3A.59	00F2.8B.A0.3A.59	ekomeyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermitAccess	172.16.0.100
Jun 25, 2020 10:37:31.567 AM	<span style="color: green;">●</span>			00F2.8B.A0.3A.59	00F2.8B.A0.3A.59	ekomeyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermitAccess	172.16.0.100

Os detalhes da interface fa1/7 do switch show authentication confirmam que os dados do Access-Accept foram aplicados com êxito.

```
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
```

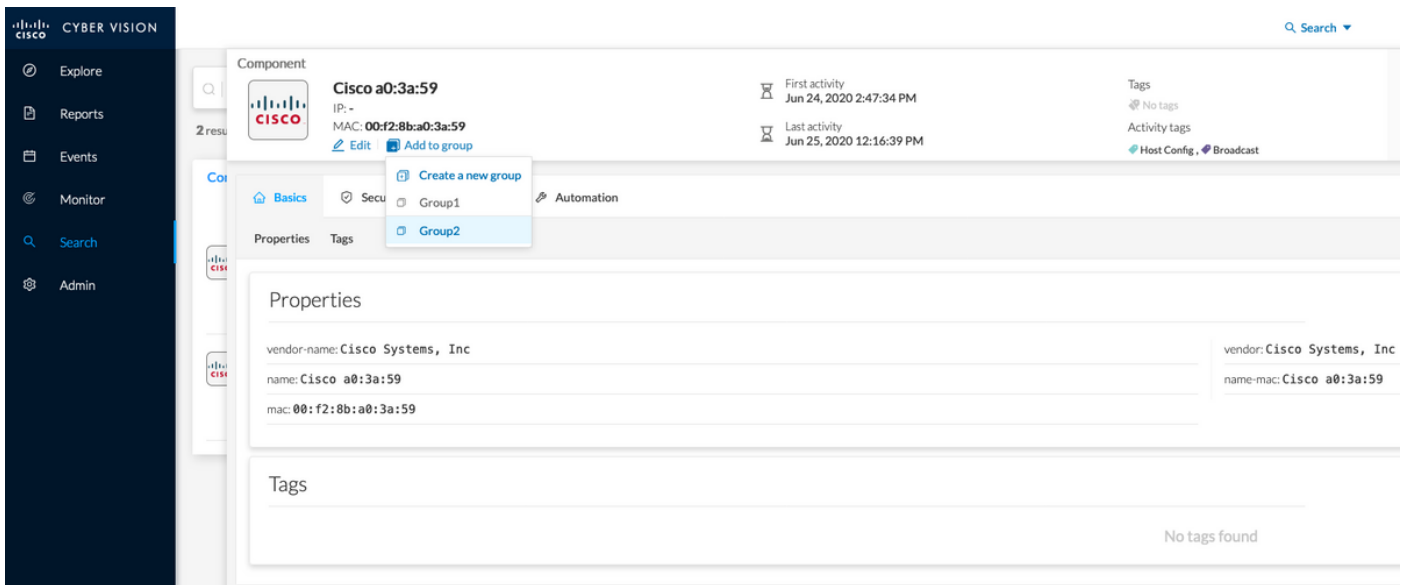
```
mab Authc Success
```

```
KJK_IE4000_10#
```

## 2. O administrador altera o grupo

Navegue até **Pesquisar**. Cole o endereço Mac do Endpoint, clique nele e **adicione-o** ao Grupo 2.

**Note:** No CCV, você não pode alterar o grupo de 1 para 2 de uma só vez. Portanto, você deve remover o Endpoint do grupo primeiro e atribuir o Grupo 2 em seguida.



### 3-6. Efeito da alteração do grupo de endpoints no CCV

Etapas 4, 5, e 6. são refletidos nessa imagem. Graças à criação de perfil, o ponto final alterou o Grupo de Identidades para ekorneyc\_ASSET\_Group2 visto na Etapa 4., o que fez com que o ISE enviase CoA para o switch (Etapa 5) e finalmente a reautenticação do ponto final (Etapa 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	●		0	00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_Asset/PermAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59:503 AM	●			00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_Asset/PermAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59:482 AM	●			00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_Asset/PermAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group1

Os detalhes da interface fa1/7 do switch show authentication confirmam que o novo SGT está atribuído.

```
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#

## Appendix

### Configuração relacionada ao TrustSec do switch

**Note:** As credenciais Cts não fazem parte da configuração atual e devem ser configuradas com o uso do comando `cts credenid <id> password <password>` no modo exec privilegiado.

```
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#