

Configuración de la integración de ISE 2.7 pxGrid CCV 3.1.0

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de flujo de alto nivel](#)

[Configuraciones](#)

[1. Habilitar sonda pxGrid en una de las redes PSN](#)

[2. Configurar atributos personalizados de terminal en ISE](#)

[3. Configurar la política del generador de perfiles mediante atributos personalizados](#)

[4. Habilitar atributos personalizados para la aplicación de perfiles](#)

[5. Configuración de la aprobación automática para clientes pxGrid](#)

[6. Exportar certificado CCV](#)

[7. Cargar certificado de identidad de CCV en almacén de confianza de ISE](#)

[8. Generar certificado para CCV](#)

[9. Descargar cadena de certificado en formato PKCS12](#)

[10. Configurar los detalles de integración de ISE en CCV](#)

[11. Cargar cadena de certificados en CCV e integración de lanzamiento](#)

[Verificación](#)

[Verificación de la integración de CCV](#)

[Verificación de la integración de ISE](#)

[Verificar el cambio de grupo de CCV](#)

[Troubleshoot](#)

[Habilitar depuraciones en ISE](#)

[Habilitar depuración en CCV](#)

[La descarga masiva falla](#)

[No todos los terminales se crean en ISE](#)

[AssetGroup no está disponible en ISE](#)

[Las actualizaciones de grupos de terminales no se reflejan en ISE](#)

[La eliminación del grupo de CCV no lo está eliminando de ISE](#)

[CCV se descarta de clientes web](#)

[Integración de ISE con el caso práctico de CCV TrustSec](#)

[Topología y flujo](#)

[Configurar](#)

[1. Configuración de etiquetas de grupo escalables en ISE](#)

[2. Configuración de la política de perfiles con atributos personalizados para el grupo 2](#)

[3. Configuración de Políticas de Autorización para Asignar SGTs Basadas en Grupos de Identidad de Extremo en ISE](#)

[Verificación](#)

[1. Autenticación de terminales basada en el grupo 1 de CCV](#)

[2. El administrador cambia el grupo](#)

[3-6. Efecto del cambio de grupo de terminales en CCV](#)

[Appendix](#)

[Configuración relacionada con Switch TrustSec](#)

Introducción

Este documento describe cómo configurar y solucionar problemas de integración de Identity Services Engine (ISE) 2.7 con Cisco Cyber Vision (CCV) 3.1.0 sobre Platform Exchange Grid v2 (pxGrid). CCV se registra con pxGrid v2 como editor y publica información sobre atributos de terminales en ISE para IOTASSET Dictionary.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- ISE
- Cisco Cyber Vision

Componentes Utilizados

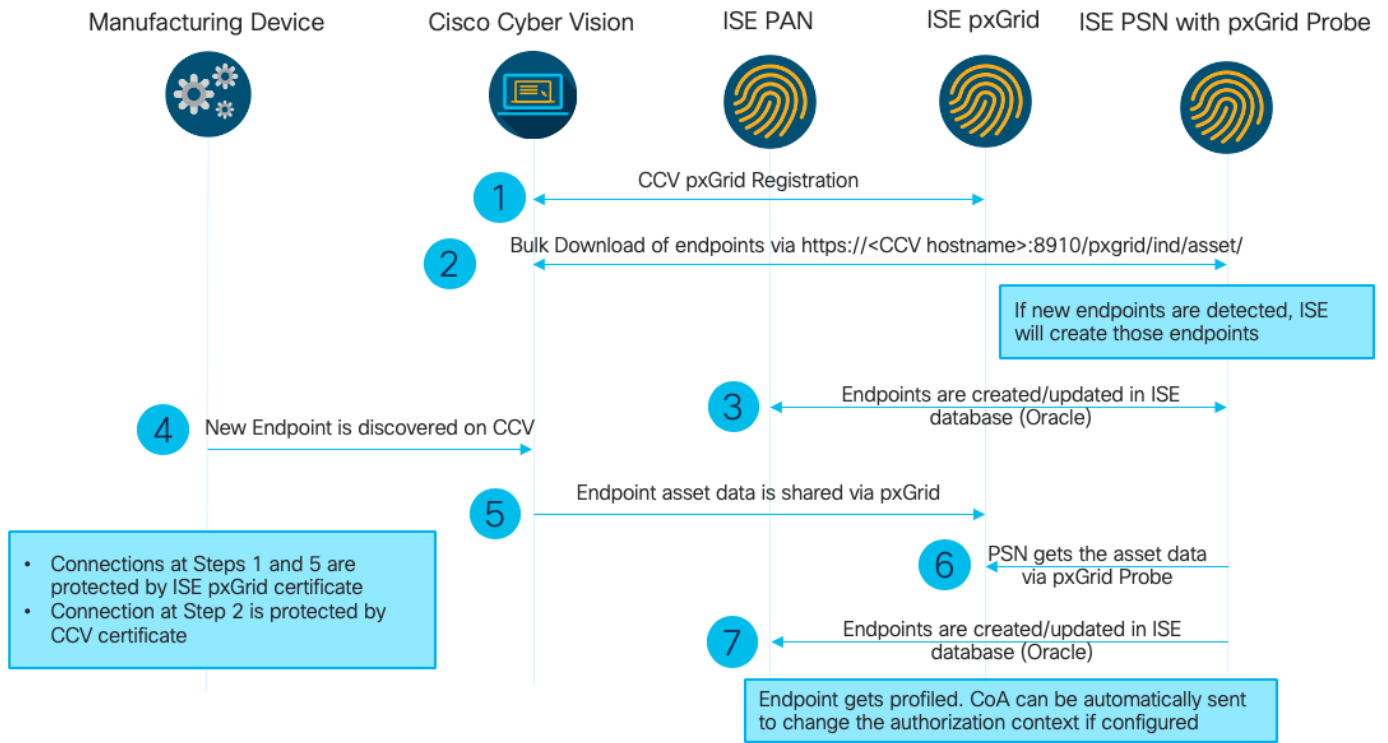
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE versión 2.7 parche 1
- Cisco Cyber Vision versión 3.1.0
- Switch Ethernet industrial IE-4000-4TC4G-E con 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de flujo de alto nivel



Esta implementación de ISE se utiliza en la configuración.

Deployment Nodes

Edit Register Syncup Deregister			
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

ISE 2.7-1ek es el nodo principal de administrador (PAN) y el nodo pxGrid.

ISE 2.7-2ek es un nodo de servicio de políticas (PSN) con la sonda pxGrid habilitada.

Estos son los pasos que corresponden al diagrama mencionado anteriormente.

1. CCV se registra en assetTopic en ISE a través de pxGrid versión 2. Registros correspondientes de CCV:

Nota: Para revisar los registros de pxGrid en CCV, ejecute el siguiente 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 la sonda pxGrid habilitada realiza una descarga masiva de los recursos 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. Los terminales se agregan al PSN con la sonda pxGrid habilitada y PSN envía un evento persistente al PAN para guardar estos terminales (**profiler.log**). Los terminales creados en ISE se pueden ver en los detalles de los terminales en Visibilidad de contexto.

```
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. Después de colocar un punto final en un grupo, CCV envía el mensaje STOMP a través del puerto 8910 para actualizar el punto final con los datos de grupo en atributos personalizados. Registros correspondientes de CCV:

```
root@center:~# journalctl -u pxgrid-agent -f
Jun 24 14:32:04 center pxgrid-agent-start.sh[1216]: pxgrid-agent STOMP SEND
destination=/topic/com.cisco.endpoint.asset
body={"opType":"UPDATE","asset":{"assetId":"ce01ade2-eb6f-53c8-a646-9661b10c976e",
"assetName":"Cisco
a0:3a:59","assetIpAddress":"","assetMacAddress":"00:f2:8b:a0:3a:59","assetVendor":"Cisco
Systems, Inc",
"assetProductId":"","assetSerialNumber":"","assetDeviceType":"","assetSwRevision":"","assetHwRev
ision":"","assetProtocol":"","
"assetCustomAttributes": [{"key":"assetGroup","value":"Group1"}, {"key":"assetCCVGrp","value":"Gro
up1"}]},
"assetConnectedLinks":[]}} [caller=endpoint.go:118]
```

5. PxGrid Node recibe la actualización STOMP y reenvía este mensaje a todos los suscriptores, incluye PSN con la sonda pxGrid habilitada. **pxgrid-server.log** en pxGrid Node.

```
2020-06-24 14:40:13,765 TRACE [Thread-1631][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -
:::::-
stomp=SEND:{content-length=453, destination=/topic/com.cisco.endpoint.asset}
2020-06-24 14:40:13,766 TRACE [Thread-1631][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -
:::::-
session [2b,cv-jens,OPEN] is permitted (cached) to send to
topic=/topic/com.cisco.endpoint.asset:
2020-06-24 14:40:13,766 TRACE [Thread-1631][[]]
cpm.pxgridwebapp.ws.pubsub.SubscriptionThreadedDistributor -:::::-
Distributing stomp frame from=[2b,cv-jens,OPEN], topic=/topic/com.cisco.endpoint.asset,
true:true
2020-06-24 14:40:13,766 TRACE [Thread-1631][[]]
cpm.pxgridwebapp.ws.pubsub.SubscriptionThreadedDistributor -:::::-
Distributing stomp frame from=[2b,cv-jens,OPEN],
topic=/topic/com.cisco.endpoint.asset,to=[19,ise-admin-ise27-2ek,OPEN]
2020-06-24 14:40:13,766 TRACE [Thread-1631][[]]
cpm.pxgridwebapp.ws.pubsub.SubscriptionThreadedDistributor -:::::-
Distributing stomp frame from=[2b,cv-jens,OPEN], topic=/topic/wildcard,to=[2a,ise-fanout-ise27-
1ek,OPEN]
```

6. PSN con la sonda pxGrid habilitada como suscriptor en tema de recursos recibe el mensaje del nodo pxGrid y actualiza el punto final (**profiler.log**). Los terminales actualizados de ISE se pueden ver en los detalles de los terminales en 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 con la sonda pxGrid habilitada vuelve a asignar perfiles al terminal cuando se compara una nueva política (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
```

Configuraciones

Nota: Los pasos 1 a 4 son obligatorios aunque sólo desee tener visibilidad de assetGroup y en Context Visibility.

1. Habilitar sonda pxGrid en una de las redes PSN

Vaya a **Administration > System > Deployment**, seleccione el nodo ISE con PSN Persona. Cambie a la pestaña **Configuración de perfiles**. Asegúrese de que la sonda **pxGrid** esté habilitada.

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 terminal en ISE

Vaya a **Administration > Identity Management > Settings > Endpoint Custom Attributes**. Configure los atributos personalizados (assetGroup) de acuerdo con esta imagen. CCV 3.1.0 sólo admite el atributo **assetGroup** 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 la política del generador de perfiles mediante atributos personalizados

Vaya a **Centros de trabajo > Generador de perfiles > Políticas de perfiles**. Haga clic en **Agregar**. Configure la política del generador de perfiles de forma similar a esta imagen. La expresión de condición utilizada en esta política es **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 > ekorneyc_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. Habilitar atributos personalizados para la aplicación de perfiles

Vaya a **Centros de trabajo > Generador de perfiles > Políticas de perfiles**. Haga clic en **Agregar**. Configure la política del generador de perfiles de forma similar a esta imagen. Asegúrese de que **Habilitar atributo personalizado para la aplicación de perfiles** esté habilitado.

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' with a sub-section for '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: ***** (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. Configuración de la aprobación automática para clientes pxGrid

Vaya a **Administration > pxGrid Services > Settings**. Seleccione **Aprobar automáticamente nuevas cuentas basadas en certificados** y haga clic en **Guardar**. Este paso garantiza que no tendrá que aprobar CCV una vez que se haya realizado la integración.

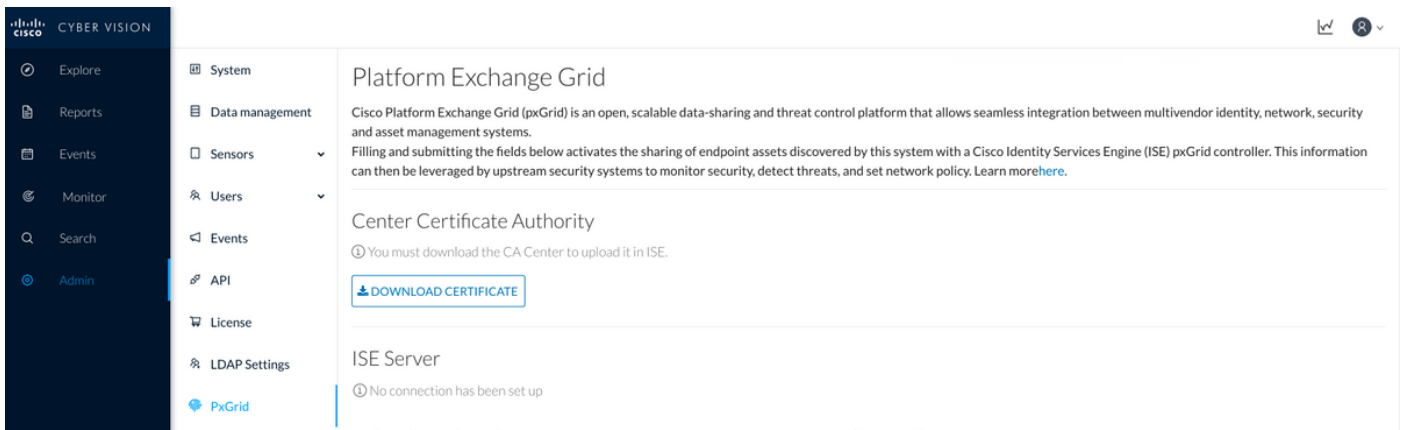
The screenshot shows the Cisco Identity Services Engine (ISE) pxGrid Services Settings page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > pxGrid Services. The left sidebar shows 'All Clients', 'Web Clients', 'Capabilities', 'Live Log', '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

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

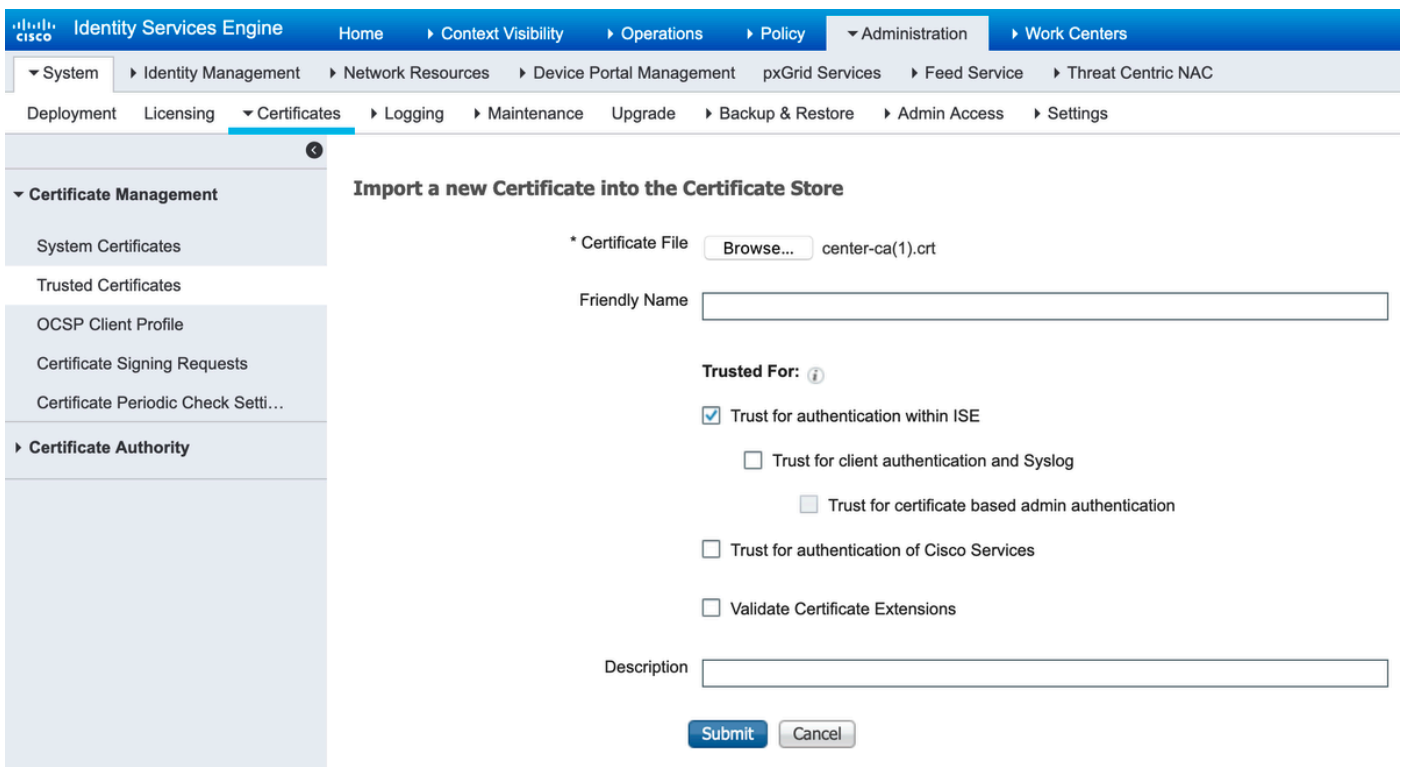
6. Exportar certificado CCV

Vaya a **Admin > pxGrid**. Haga clic en **DESCARGAR CERTIFICADO**. Este certificado se utiliza durante el registro de pxGrid, por lo que ISE debe confiar en él.



7. Cargar certificado de identidad de CCV en almacén de confianza de ISE

Vaya a **Administración > Certificados > Administración de certificados > Certificados de confianza**. Haga clic en **Importar**. Haga clic en **Examinar** y seleccione el certificado de CCV en el Paso 5. Haga clic en **Submit (Enviar)**.



8. Generar certificado para CCV

Durante la integración y las actualizaciones de pxGrid, CCV necesita el certificado de cliente. Debe ser emitido por la CA interna de ISE, usando **PxGrid_Certificate_Template**.

Vaya a **Administration > pxGrid Services > Certificates**. Rellene los campos según esta imagen. El campo Nombre común (CN) es obligatorio, ya que el objetivo de ISE CA es emitir un certificado de identidad. Debe introducir el nombre de host de CCV, el valor del campo CN es crítico. Para verificar el nombre de host de CCV, ejecute el comando **hostname**. Seleccione PKCS12 como **Formato de descarga de certificados**.

```
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) - +

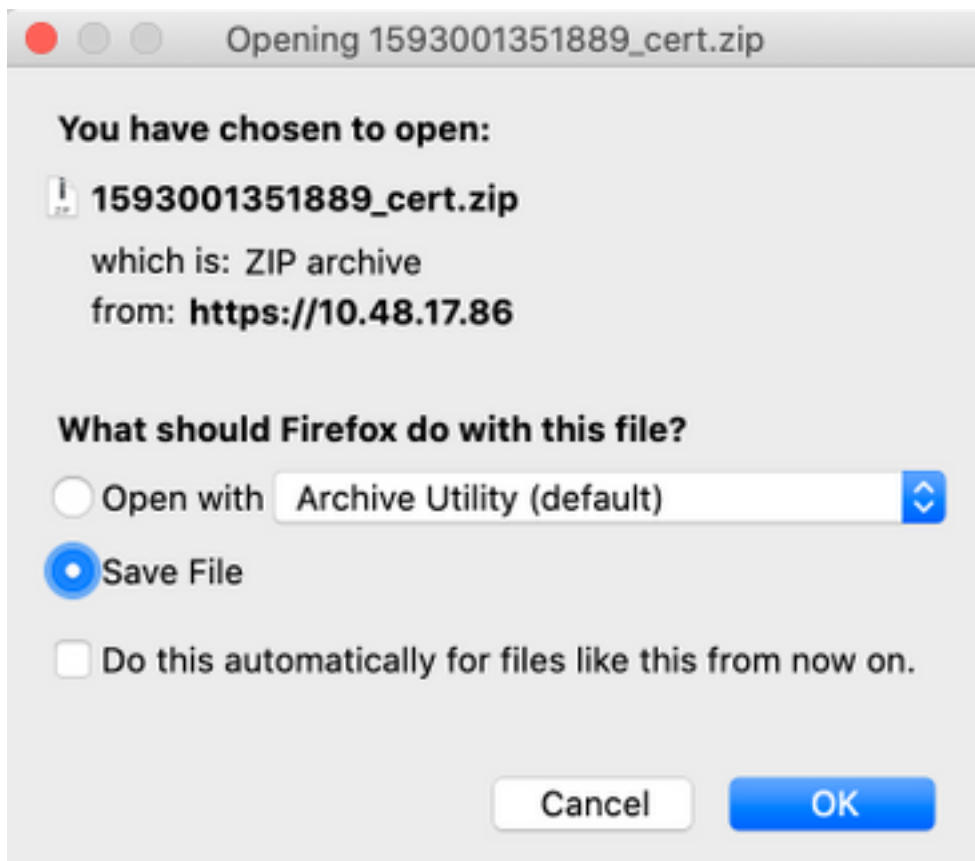
Certificate Download Format * ⓘ

Certificate Password * ⓘ

Confirm Password *

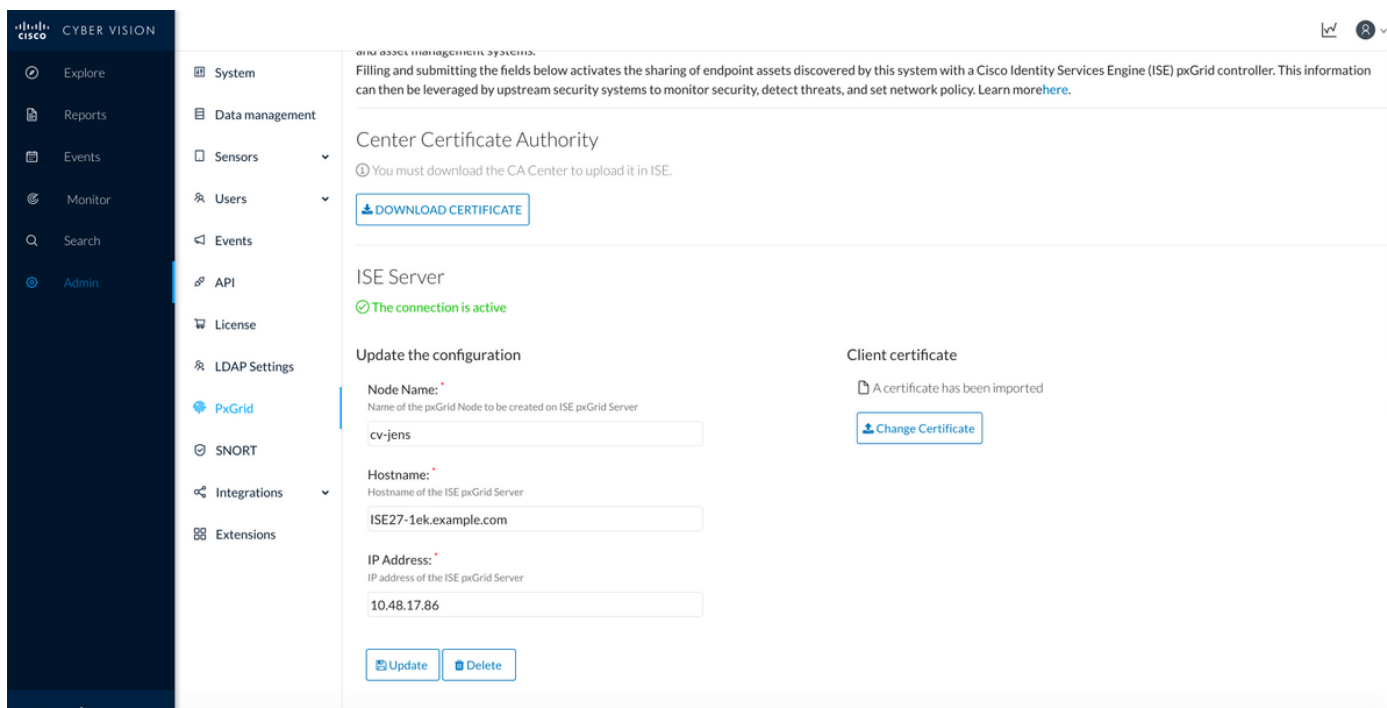
9. Descargar cadena de certificado en formato PKCS12

Cuando instala el certificado en formato PKCS12, junto con el certificado de identidad de CCV, la cadena de CA interna ISE se instala en CCV para asegurarse de que CCV confía en ISE cuando se inicia la comunicación pxGrid desde ISE, por ejemplo, los mensajes de keepalive de pxGrid.



10. Configurar los detalles de integración de ISE en CCV

Vaya a **Admin > pxGrid**. Configure Node Name, este nombre se mostrará en ISE como Client Name at **Administration > pxGrid Services > Web Clients**. Configure **Hostname** y **IP Address** del Nodo PxGrid de ISE. Asegúrese de que CCV pueda resolver el FQDN de ISE.



11. Cargar cadena de certificados en CCV e integración de lanzamiento

Vaya a **Admin > pxGrid**. Haga clic en **Cambiar certificado**. Seleccione el certificado emitido por ISE CA de los pasos 8-9. Introduzca la contraseña del paso 8. y haga clic en **Aceptar**.

Do you want to enter a password?

.....

Ok

Cancel

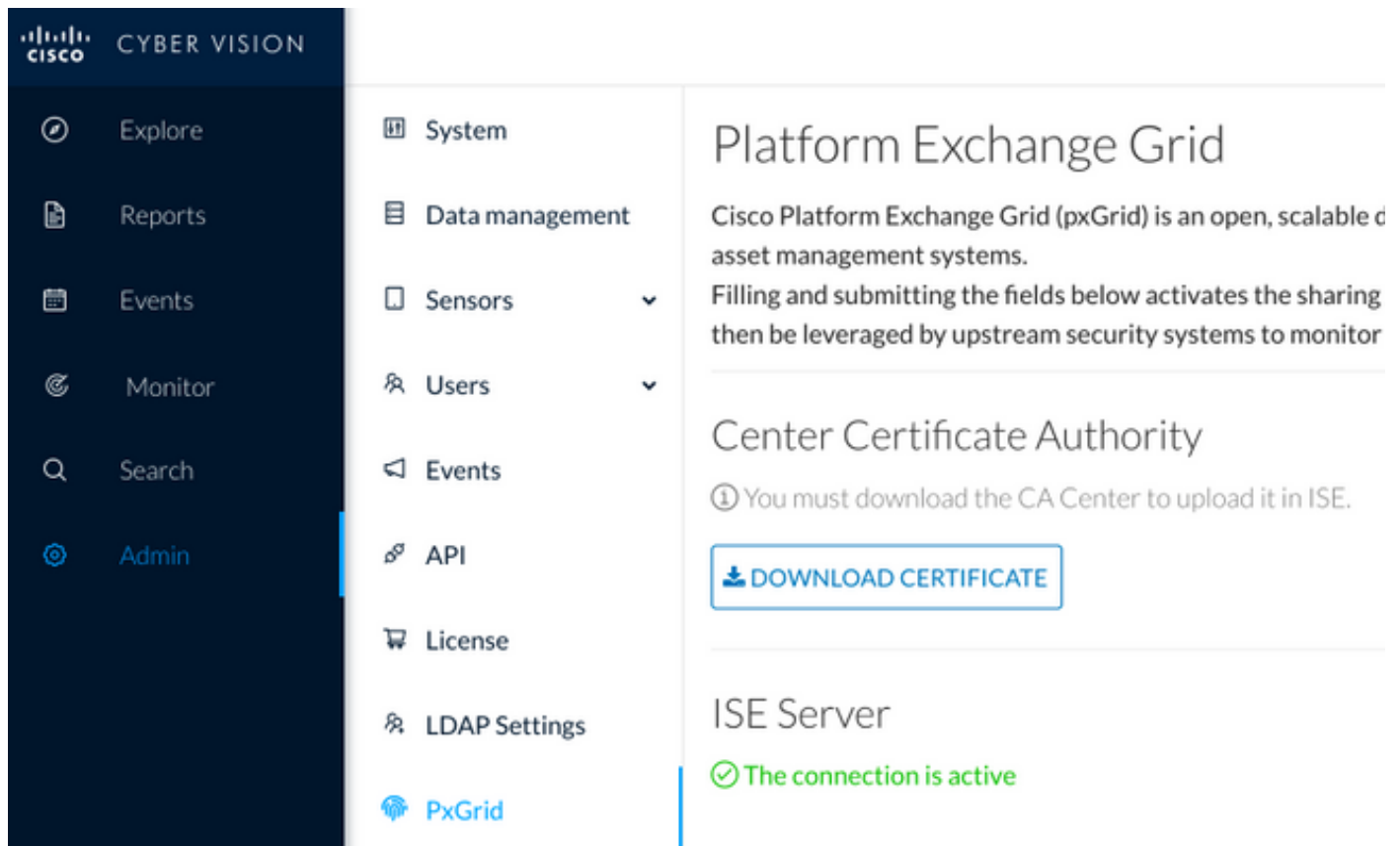
Haga clic en **Update**, que activa la integración real de CCV e ISE.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Verificación de la integración de CCV

Una vez finalizada la integración, puede confirmar que es exitosa navegando a **Admin > pxGrid**. Debería ver **El mensaje de conexión está activa** en ISE Server.



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 'Platform Exchange Grid' and includes a description of pxGrid, a 'Center Certificate Authority' section with a 'DOWNLOAD CERTIFICATE' button, and an 'ISE Server' section with a green checkmark and the text 'The connection is active'.

Verificación de la integración de ISE

Vaya a **Administration > pxGrid Services > Web Clients**. Confirme que el estado de CCV Client (cv-jens) esté **ACTIVADO**.

Nota: Se espera ver el estado del cliente pxGrid de CCV como **Offline** en el **menú Todos los clientes**, ya que muestra solamente el estado de 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

Nota: Debido a [CSCvt78208](#) no verá de inmediato a CCV que tenga /topic/com.cisco.ise.endpoint.asset, se mostrará solamente en la primera publicación.

Verificar el cambio de grupo de CCV

Vaya a Explorar > Todos los datos > Lista de componentes. Haga clic en uno de los componentes y Agréguelo al grupo.

The screenshot shows the Cisco Cyber Vision interface. On the left is a navigation sidebar with options like Explore, Reports, Events, Monitor, Search, and Admin. The main area displays a 'Component list' for the period 'Jun 24, 2020 3:36:22 PM - Jun 24, 2020 4:36:22 PM (1 hr)'. It shows 5 components in a table:

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:

The detailed view on the right shows the 'Cisco a0:3a:59' component with its IP and MAC address. A context menu is open, allowing to 'Add to group', 'Create a new group', or select 'Group1' or 'Group2'. The component's activity tags include 'Host Config' and 'Broadcast', and its properties list 'vendor-name: Cisco Systems, Inc', 'name: Cisco a0:3a:59', and 'mac: 00:f2:8b:a0:3a:59'.

Verifique que /topic/com.cisco.ise.endpoint.asset ahora esté listado como Publications contra 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 que el grupo 1 asignado a través de CCV se refleje en ISE y que la política de definición de perfiles haya entrado en vigor navegando hasta **Visibilidad de contexto > Terminales**. Seleccione el terminal actualizado en el paso anterior. Cambie a la ficha Attributes (Atributos). La sección atributos personalizados debe reflejar el grupo recientemente 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
x	<input type="text" value="Attribute String"/>	<input type="text" value="Attribute Value"/>
	assetGroup	Group1

La sección Otros atributos muestra todos los demás atributos de activos recibidos de 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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Habilitar depuraciones en ISE

Para habilitar las depuraciones en ISE, navegue hasta **Administration > System > Logging > Debug Log Configuration**. Establezca los niveles de registro en los siguientes:

Persona	Nombre del componente	Nivel de registro	Archivo a comprobar
PAN (opcional)	generador de perfiles	DEPURAR	profiler.log
PSN con sonda pxGrid habilitada	generador de perfiles	DEPURAR	profiler.log
PxGrid	pxgrid	TRACE	pxgrid-server.log

Habilitar depuración en CCV

Para habilitar las depuraciones en CCV:

- Cree un archivo `/data/etc/sbs/pxgrid-agent.conf` con el comando `/data/etc/sbs/pxgrid-agent.conf`
- Pegue este contenido en el archivo `pxgrid-agent.conf` con el editor `vi` con el comando `vi /data/etc/sbs/pxgrid-agent.conf`

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

- Reinicie `pxgrid-agent` ejecutando el comando `systemctl restart pxgrid-agent`
- Ver registros con el comando `journalctl -u pxgrid-agent`

La descarga masiva falla

CCV publica la URL de descarga masiva a ISE durante la integración. ISE PSN con la sonda `pxGrid` activada realiza la descarga masiva con el uso de esta URL. Asegúrese de lo siguiente:

- El nombre de host en la URL se puede resolver correctamente desde la perspectiva de ISE
- Se permite la comunicación de PSN en el puerto 8910 a CCV

`profiler.log` en PSN con la sonda `pxGrid` habilitada:

```
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}]]
```

La descarga masiva puede fallar debido a [CSCvt75422](#), debería ver este error en `profiler.log` en ISE para confirmarlo. El defecto se corrige en 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)
```

No todos los terminales se crean en ISE

Algunos terminales de CCV pueden tener demasiados atributos adjuntos, por lo que la base de datos de ISE no podrá gestionarla. Se puede confirmar si ve estos errores en `profiler.log` en 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 no está disponible en ISE

Si AssetGroup no está disponible en ISE, lo más probable es que la política de generación de perfiles no esté configurada utilizando Atributos personalizados (consulte los pasos 2-4). en la parte Configuraciones del documento). Incluso para la visibilidad de contexto, sólo para mostrar atributos de grupo, políticas de definición de perfiles y otras configuraciones de los pasos 2 a 4 son obligatorios.

Las actualizaciones de grupos de terminales no se reflejan en ISE

Debido a [CSCvu80175](#), CCV no publica actualizaciones de terminales en ISE hasta que CCV se reinicie inmediatamente después de la integración. Puede reiniciar CCV una vez que la integración se realice como solución alternativa.

La eliminación del grupo de CCV no lo está eliminando de ISE

Este problema se ve debido al defecto conocido en CCV [CSCvu47880](#). La actualización pxGrid enviada durante la eliminación del grupo de CCV con un formato diferente del esperado, por lo que el grupo no se elimina.

CCV se descarta de clientes web

Este problema se ve debido al defecto conocido en ISE [CSCvu47880](#) donde los clientes pasan al estado OFF seguido de la eliminación completa de los clientes web. El problema se resuelve en el parche 2.6 7 y el parche 2.7 2 de ISE.

Puede confirmarlo si ve estos errores en `pxgrid-server.log` en ISE:

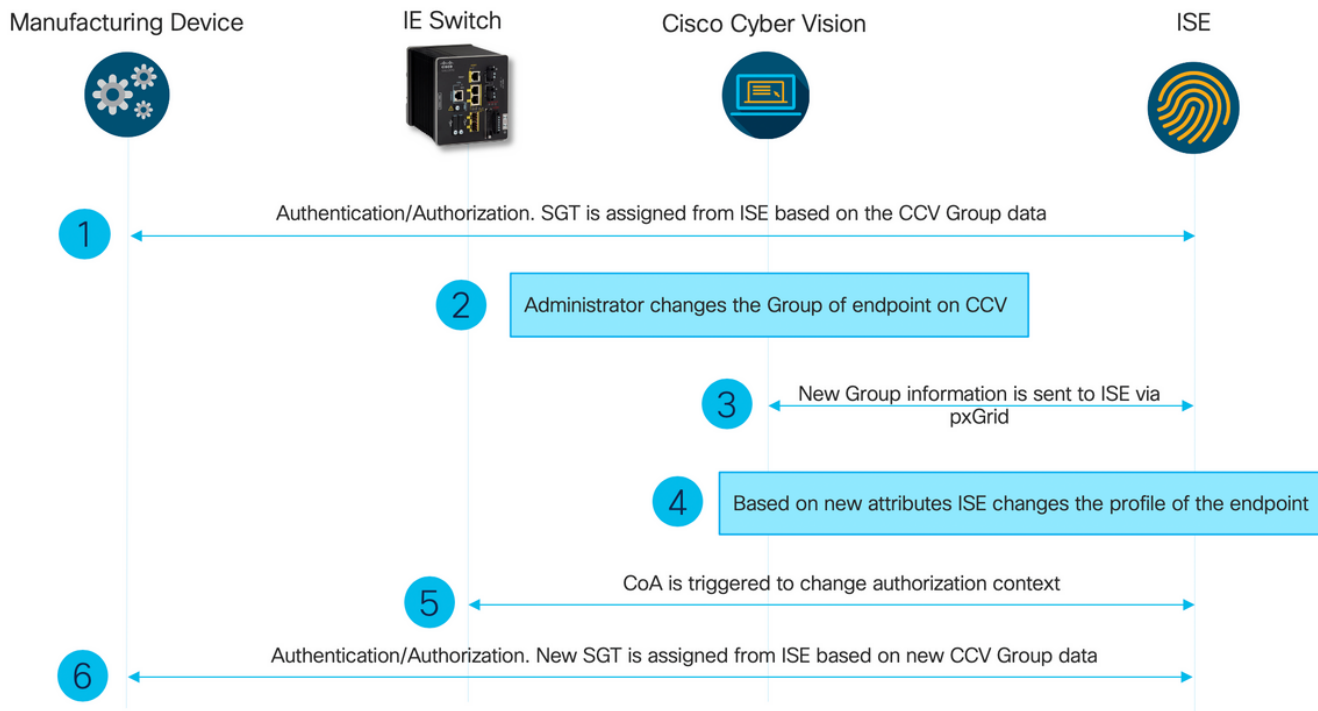
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionId=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726, closeTime=2020-06-26 09:42:28.772,
reason=VIOLATED_POLICY:Did not receive a pong: too slow ... ,
subscriptions=[], publications=[/topic/com.cisco.endpoint.asset]]
```

Integración de ISE con el caso práctico de CCV TrustSec

Esta configuración muestra cómo la integración de ISE con CCV puede beneficiar la seguridad de extremo a extremo cuando TrustSec está en funcionamiento. Este es sólo uno de los ejemplos de cómo se puede utilizar la integración, una vez que se ha hecho.

Nota: La explicación de la configuración del switch TrustSec está fuera del alcance de este artículo, sin embargo, se puede encontrar en el Apéndice.

Topología y flujo



Configurar

1. Configuración de etiquetas de grupo escalables en ISE

Para lograr el caso de uso mencionado anteriormente, IOT_Group1_Asset y IOT_Group2_Asset de la etiqueta TrustSec se configuran manualmente para diferenciar los recursos de CCV de Group1 de Group2 respectivamente. Vaya a **Centros de trabajo > TrustSec > Componentes > Grupos de seguridad**. Haga clic en **Agregar**. Nombre las SGT como se muestra en la imagen.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > TrustSec > Components > TrustSec Policy > Policy Sets > SXP > Troubleshoot > Reports > Settings.

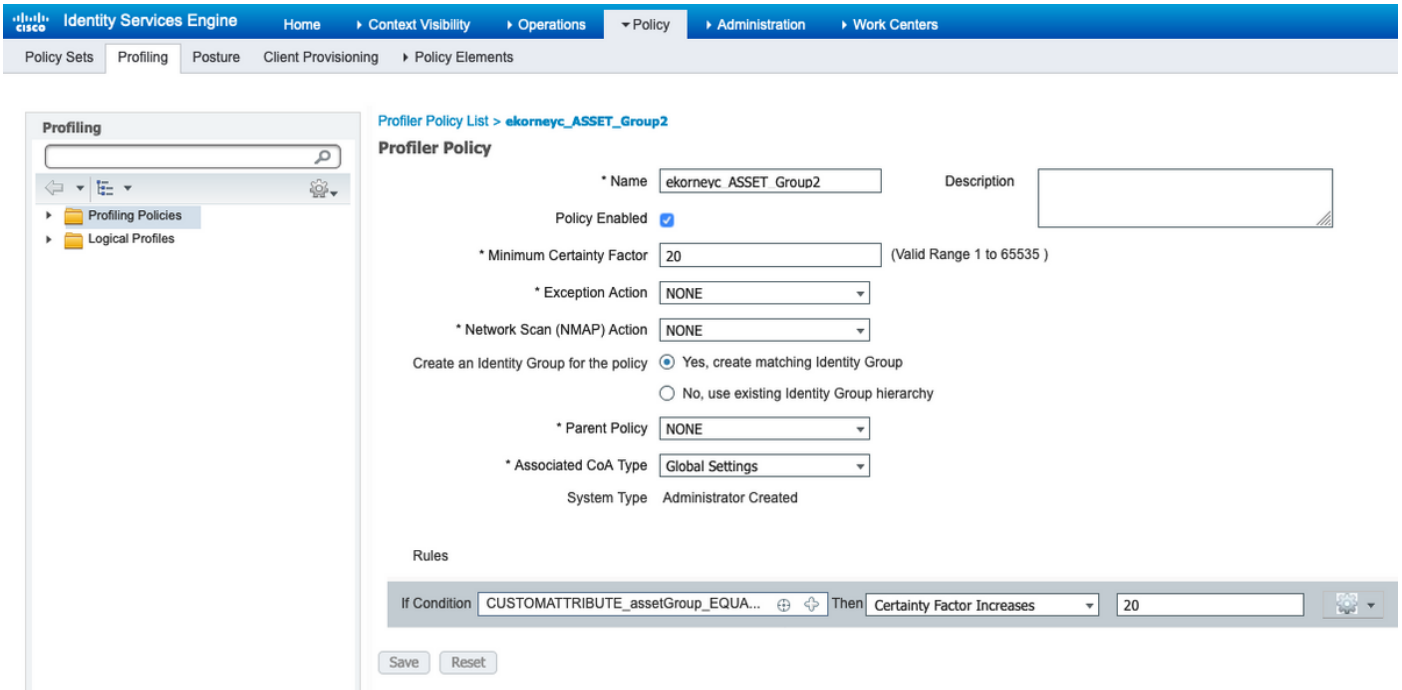
The main content area is titled "Security Groups" and includes a table of configured groups. Below the table are options for Edit, Add, Import, Export, Trash, Push, and Verify Deploy.

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

2. Configuración de la política de perfiles con atributos personalizados para el grupo 2

Nota: La configuración de perfiles para el grupo 1 se realizó en el paso 3. en la primera parte del documento.

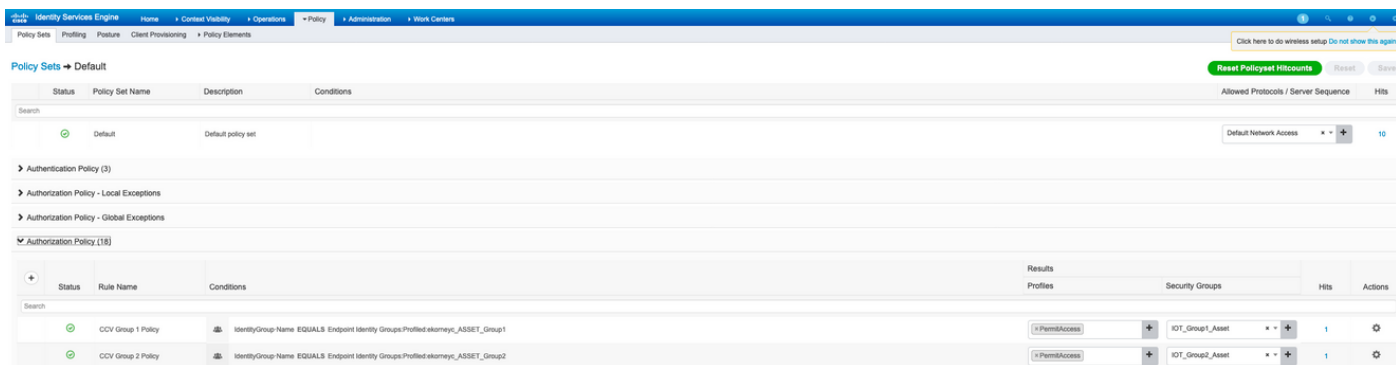
Vaya a **Centros de trabajo > Generador de perfiles > Políticas de perfiles**. Haga clic en **Agregar**. Configure la política del generador de perfiles de forma similar a esta imagen. La expresión de condición utilizada en esta política es **CUSTOMATTRIBUTE:assetGroup EQUALS Group2**.



3. Configuración de Políticas de Autorización para Asignar SGTs Basadas en Grupos de Identidad de Extremo en ISE

Navegue hasta **Política > Conjuntos de Políticas**. Seleccione **Policy Set** y configure **Authorization Policies** según esta imagen. Tenga en cuenta que, como resultado, la SGT se configura en el Paso 1. están asignados.

Nombre de regla	Condiciones	Perfiles	Grupos de seguridad
Política del grupo 1 de CCV	Grupos de identidad de terminales con el nombre de · de grupo de identidad IGUALES:Perfil:ekorneyc_ASSET_Group1	PermitAccess	IOT_Group1_Asset
Política del grupo 2 de CCV	Grupos de identidad de terminales con el nombre de · de grupo de identidad IGUALES:perfiles:ekorneyc_ASSET_Group2	PermitAccess	IOT_Group2_Asset



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

1. Autenticación de terminales basada en el grupo 1 de CCV

En Switch, puede ver que los datos del entorno incluyen **16-54:IOT_Group1_Asset** de SGT y **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#

Los terminales se autentican y, como resultado, la política del grupo 1 de CCV se coteja, se asigna SGT IOT_Group1_Asset.

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

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

Below the statistics is a table of 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	●		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	●			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

El switch show authentication sessions interface fa1/7 detail confirma que los datos de Access-Accept se aplicaron correctamente.

```
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
```

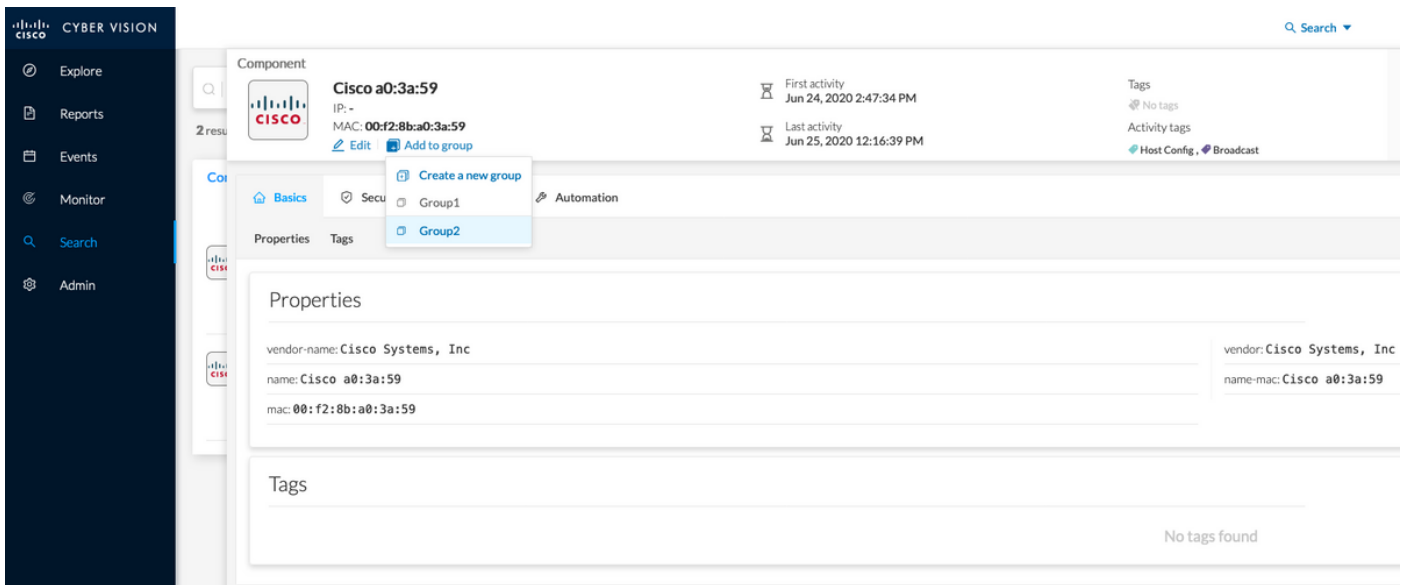
```
mab Authc Success
```

```
KJK_IE4000_10#
```

2. El administrador cambia el grupo

Vaya a **Búsqueda**. Pegue la dirección Mac del terminal, haga clic en él y **Adición** al grupo 2.

Nota: En CCV, no puede cambiar el grupo de 1 a 2 de una vez. Por lo tanto, primero debe quitar el punto final del grupo y asignar el grupo 2 siguiente.



3-6. Efecto del cambio de grupo de terminales en CCV

Pasos 4, 5, y 6, se reflejan en esta imagen. Gracias a la creación de perfiles, el terminal cambió el grupo de identidad a ekorneyc_ASSET_Group2 que se muestra en el paso 4.2, lo que hizo que ISE enviara CoA al switch (paso 5) y finalmente la reautenticación del terminal (paso 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/PermAccess	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/PermAccess	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/PermAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group1

El `show authentication sessions interface fa1/7 detail` confirma que la nueva SGT está asignada.

```
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

Configuración relacionada con Switch TrustSec

Nota: Las credenciales de Cts no forman parte de running-config y deben configurarse con el uso del comando **cts credentials id <id> password <password>** en el modo de exec de privilegios.

```
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#