Configure ISE 2.7 pxGrid CCV 3.1.0 Integration

Contents

Introduction

This document describes how to configure and troubleshoot Identity Services Engine (ISE) 2.7 integration with Cisco Cyber Vision (CCV) 3.1.0 over Platform Exchange Grid v2 (pxGrid). CCV is registered with pxGrid v2 as a publisher and publishes information on endpoint attributes to ISE for IOTASSET Dictionary.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- ISE
- Cisco Cyber Vision

Components Used

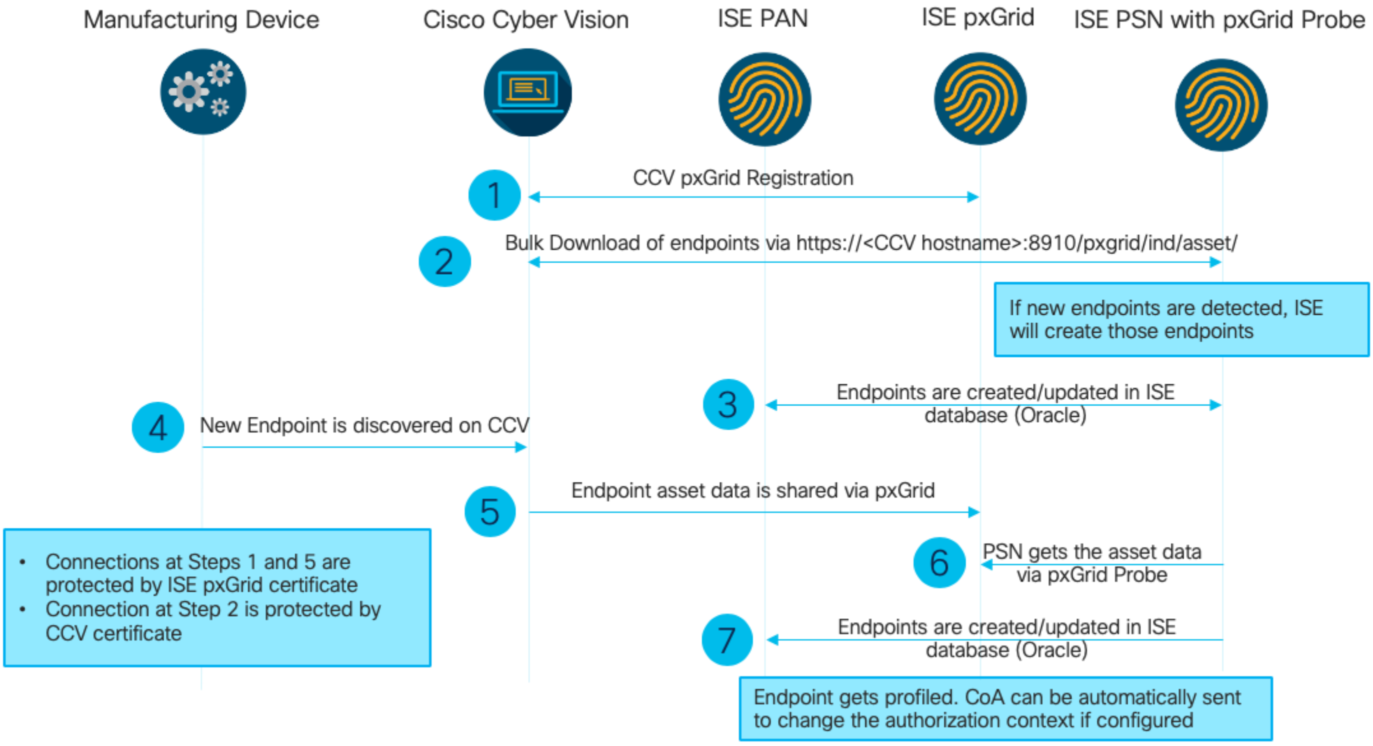
The information in this document is based on the following software and hardware versions:

- Cisco ISE Version 2.7 Patch 1
- Cisco Cyber Vision Version 3.1.0
- Industrial Ethernet Switch IE-4000-4TC4G-E with 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. If your network is live, ensure that you understand the potential impact of any command.

Configure

High-Level Flow Diagram

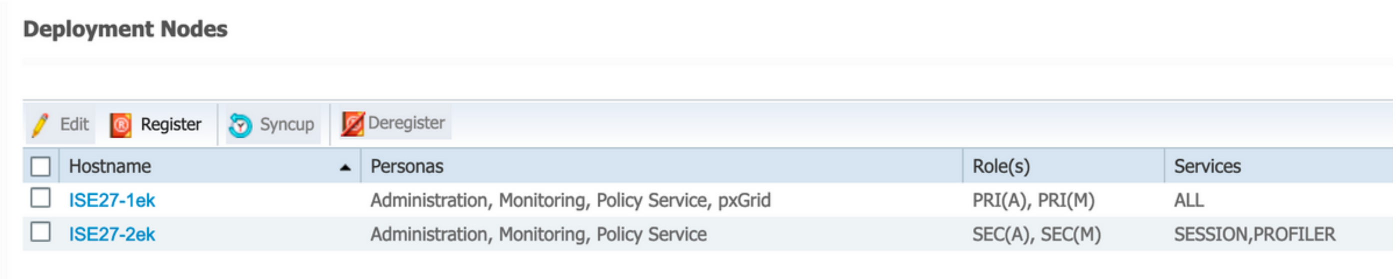

Manufacturing Device
Cisco Cyber Vision
ISE PAN
ISE pxGrid
ISE PSN with pxGrid Probe
1
CCV pxGrid Registration
2
Bulk Download of endpoints via https://<CCV hostname>:8910/pxgrid/ind/asset/
3
Endpoints are created/updated in ISE database (Oracle)
4
New Endpoint is discovered on CCV
5
Endpoint asset data is shared via pxGrid
6
PSN gets the asset data via pxGrid Probe
7
Endpoints are created/updated in ISE database (Oracle)

If new endpoints are detected, ISE will create those endpoints

- Connections at Steps 1 and 5 are protected by ISE pxGrid certificate
- Connection at Step 2 is protected by CCV certificate

Endpoint gets profiled. CoA can be automatically sent to change the authorization context if configured

This ISE deployment is used in the setup.


Deployment Nodes

□	Hostname	Personas	Role(s)	Services
□	ISE27-1ek	Administration, Monitoring, Policy Service, pxGrid	PRI(A), PRI(M)	ALL
□	ISE27-2ek	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION,PROFILER

ISE 2.7-1ek is Primary Admin Node (PAN) node and pxGrid Node.

ISE 2.7-2ek is Policy Service Node (PSN) with pxGrid probe Enabled.

Here are the steps that correspond to the previously mentioned diagram.

1. CCV registers to assetTopic on ISE via pxGrid version 2. Corresponding logs from CCV:

> **Note**: In order to review the pxGrid logs on CCV issue the following command **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 with pxGrid probe enabled does a bulk download of existing pxGrid Assets (**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 are added to the PSN with pxGrid probe enabled and PSN sends persist event to the PAN to save these endpoints (**profiler.log**). Endpoints created on ISE can be viewed in endpoint details under 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
proccessedEndPoint[id=<null>,name=<null>]
MAC: 28:63:36:1E:10:05
Attribute:BYODRegistration value:Unknown
Attribute:DeviceRegistrationStatus value:NotRegistered
Attribute:EndPointPolicy value:Unknown
Attribute:EndPointPolicyID value:
Attribute:EndPointSource value:pxGrid Probe
Attribute:MACAddress value:28:63:36:1E:10:05
Attribute:MatchedPolicy value:Unknown
Attribute:MatchedPolicyID value:
Attribute:NmapSubnetScanID value:0
Attribute:OUI value:Siemens AG
Attribute:PolicyVersion value:0
Attribute:PortalUser value:
Attribute:PostureApplicable value:Yes
Attribute:StaticAssignment value:false
Attribute:StaticGroupAssignment value:false
Attribute:Total Certainty Factor value:0
Attribute:assetDeviceType value:
Attribute:assetHwRevision value:
Attribute:assetId value:01c8f9dd-8538-5eac-a924-d6382ce3df2d
Attribute:assetIpAddress value:192.168.105.150
Attribute:assetMacAddress value:28:63:36:1e:10:05
Attribute:assetName value:Siemens 192.168.105.150
Attribute:assetProductId value:
Attribute:assetProtocol value:ARP, S7Plus
Attribute:assetSerialNumber value:
Attribute:assetSwRevision value:
Attribute:assetVendor value:Siemens AG
Attribute:ip value:192.168.105.150
Attribute:SkipProfiling value:false
```

4. After you place an endpoint into a group, CCV sends STOMP message via port 8910 to update the endpoint with the Group Data in Custom Attributes. Corresponding logs from 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 receives STOMP update and forwards this message to all subscribers, it includes PSNs with pxGrid probe enabled. **pxgrid-server.log** on 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 with pxGrid probe enabled being a subscriber on asset topic receives the message from pxGrid Node and updates the endpoint (**profiler.log**). Updated endpoints on ISE can be viewed in endpoint details under Context Visibility.

```
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-
Parsing push notification response: {"opType":"UPDATE","asset":{"assetId":"ce01ade2-eb6f-53c8-
a646-9661b10c976e",
"assetName":"Cisco
a0:3a:59","assetIpAddress":"","assetMacAddress":"00:f2:8b:a0:3a:59","assetVendor":"Cisco
Systems, Inc",
"assetProductId":"","assetSerialNumber":"","assetDeviceType":"","assetSwRevision":"","assetHwRev
ision":"",
"assetProtocol":"","assetCustomAttributes":[{"key":"assetGroup","value":"Group1"},{"key":"assetC
CVGrp","value":"Group1"}],
"assetConnectedLinks":[]}}
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-
sending endpoint to forwarder{"assetId":"ce01ade2-eb6f-53c8-a646-
9661b10c976e","assetName":"Cisco a0:3a:59","assetIpAddress":"",
"assetMacAddress":"00:f2:8b:a0:3a:59","assetVendor":"Cisco Systems,
Inc","assetProductId":"","assetSerialNumber":"",
"assetDeviceType":"","assetSwRevision":"","assetHwRevision":"","assetProtocol":"",
"assetCustomAttributes":[{"key":"assetGroup","value":"Group1"},{"key":"assetCCVGrp","value":"Gro
up1"}],"assetConnectedLinks":[]}
2020-06-24 14:40:13,768 INFO [Grizzly(2)][] cisco.profiler.infrastructure.probemgr.Forwarder -
::::-
Forwarder Mac 00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,768 DEBUG [forwarder-9][]
```

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

7. PSN with pxGrid probe enabled re-profiles the endpoint as a new Policy is matched (**profiler.log**).

```
2020-06-24 14:40:13,773 INFO [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Classify Mac
00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,777 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Policy Cisco-Device matched
00:F2:8B:A0:3A:59 (certainty 10)
2020-06-24 14:40:13,777 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Policy ekorneyc_ASSET_Group1
matched 00:F2:8B:A0:3A:59 (certainty 20)
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- After analyzing policy
hierarchy: Endpoint:
00:F2:8B:A0:3A:59 EndpointPolicy:ekorneyc_ASSET_Group1 for:20 ExceptionRuleMatched:false
```

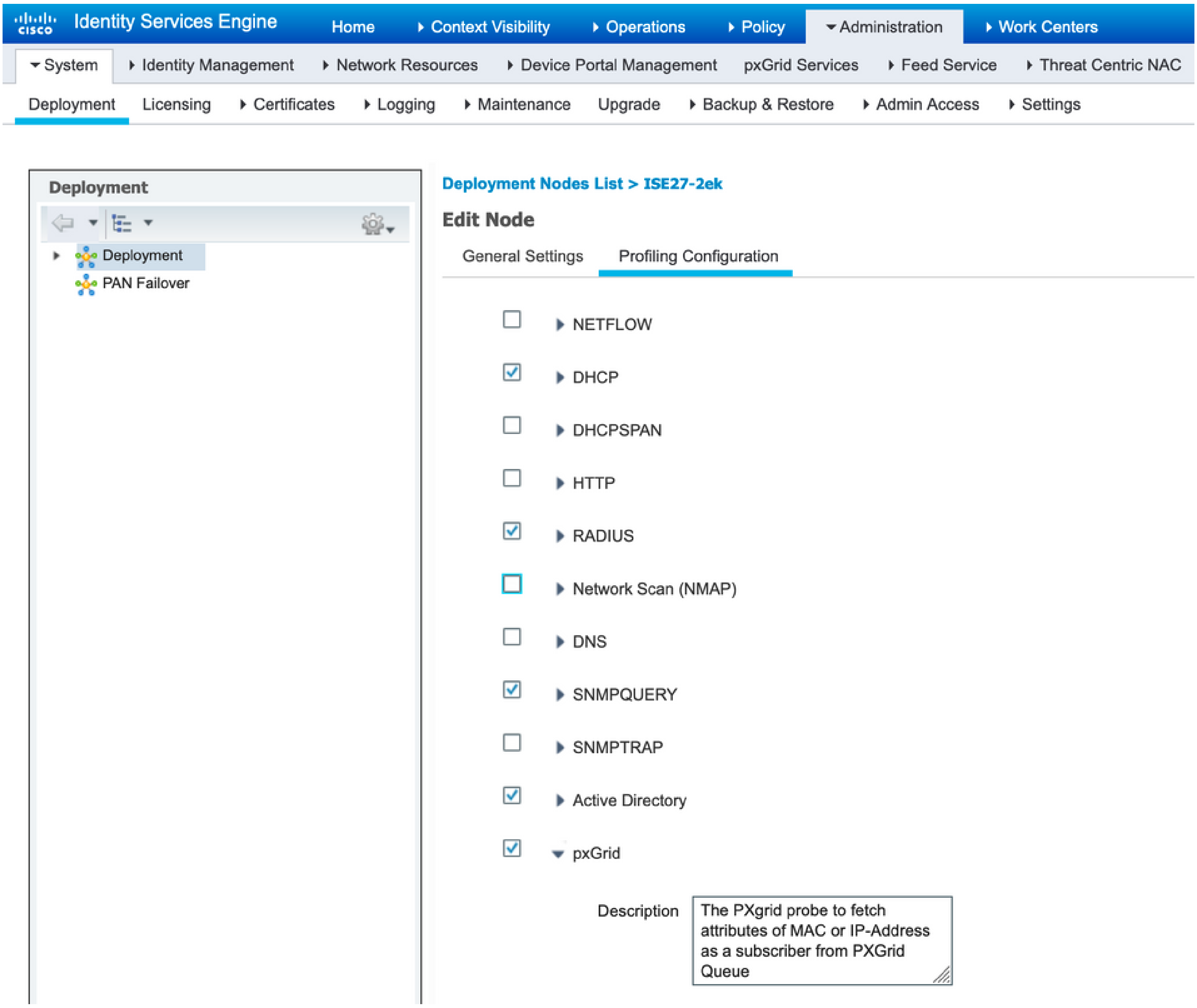
```
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
Matched Policy Changed.
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager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

Configurations

> **Note**: Steps 1 - 4 are required even if you wish to have just visibility of assetGroup and in Context Visibility.

1. Enable pxGrid Probe on One of the PSN's

Navigate to **Administration > System > Deployment**, select ISE node with PSN Persona. Switch to **Profiling Configuration** tab. Ensure that the **pxGrid** probe is enabled.



Deployment Nodes List > ISE27-2ek

Edit Node

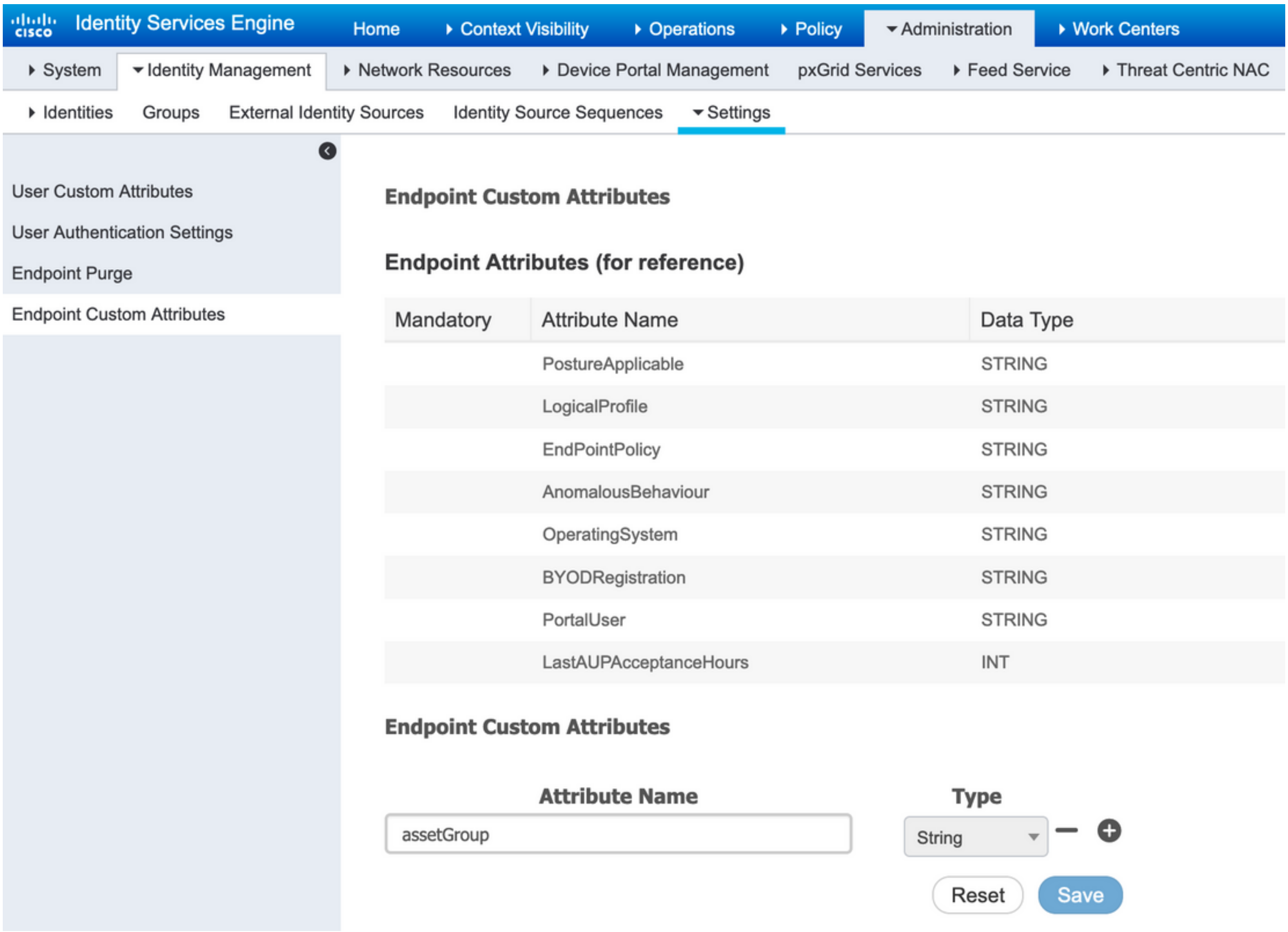
General Settings | Profiling Configuration

- ☐ 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. Configure Endpoint Custom Attributes on ISE

Navigate to **Administration > Identity Management > Settings > Endpoint Custom Attributes**. Configure Custom Attributes (assetGroup) according to this image. CCV 3.1.0 supports only Custom **assetGroup** Attribute.



Endpoint Custom Attributes

Endpoint Attributes (for reference)

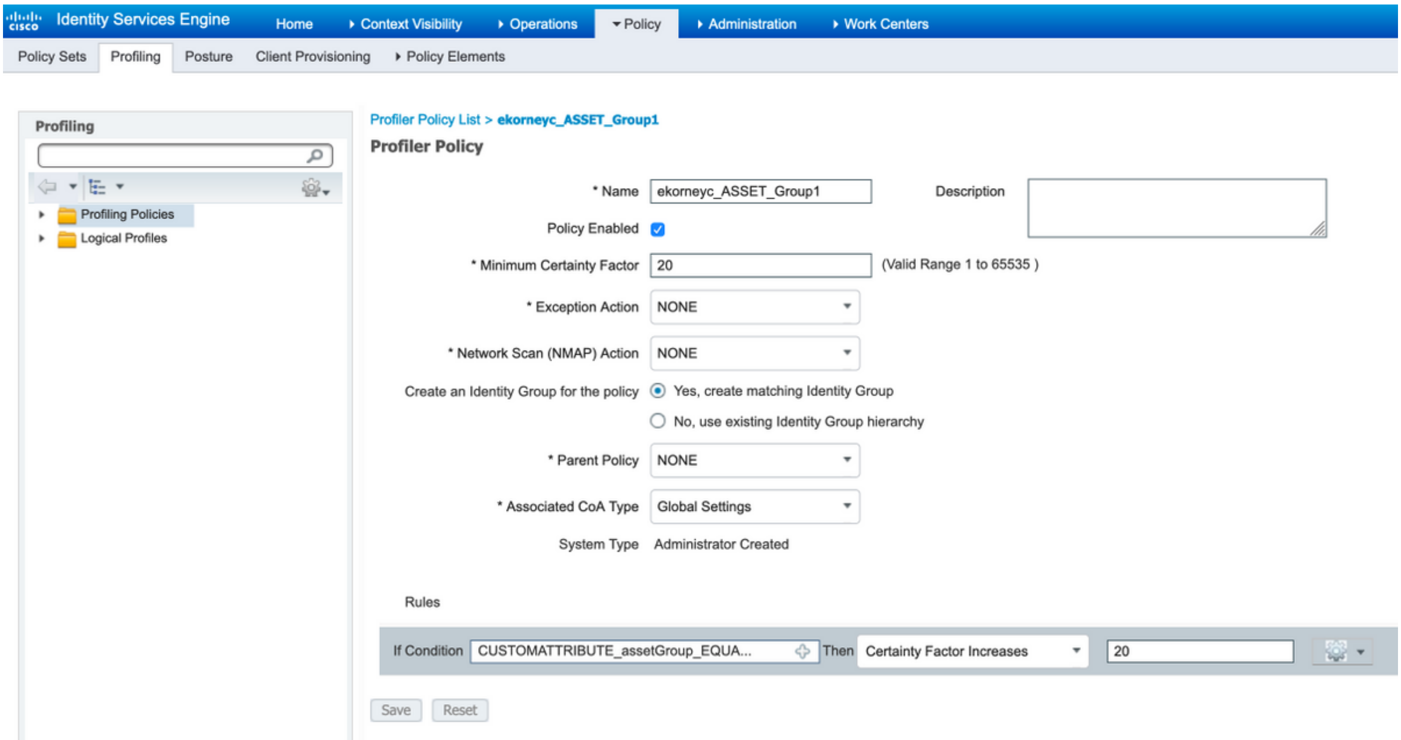
Mandatory	Attribute Name	Data Type
	PostureApplicable	STRING
	LogicalProfile	STRING
	EndPointPolicy	STRING
	AnomalousBehaviour	STRING
	OperatingSystem	STRING
	BYODRegistration	STRING
	PortalUser	STRING
	LastAUPAcceptanceHours	INT

Endpoint Custom Attributes

Attribute Name	Type
assetGroup	String

3. Configure Profiler Policy using Custom Attributes

Navigate to **Work Centers > Profiler > Profiling Policies**. Click on **Add**. Configure Profiler Policy similar to this image. Condition expression used in this policy is **CUSTOMATTRIBUTE:assetGroup EQUALS Group1.**



Profiler Policy List > ekorneyc_ASSET_Group1

Profiler Policy

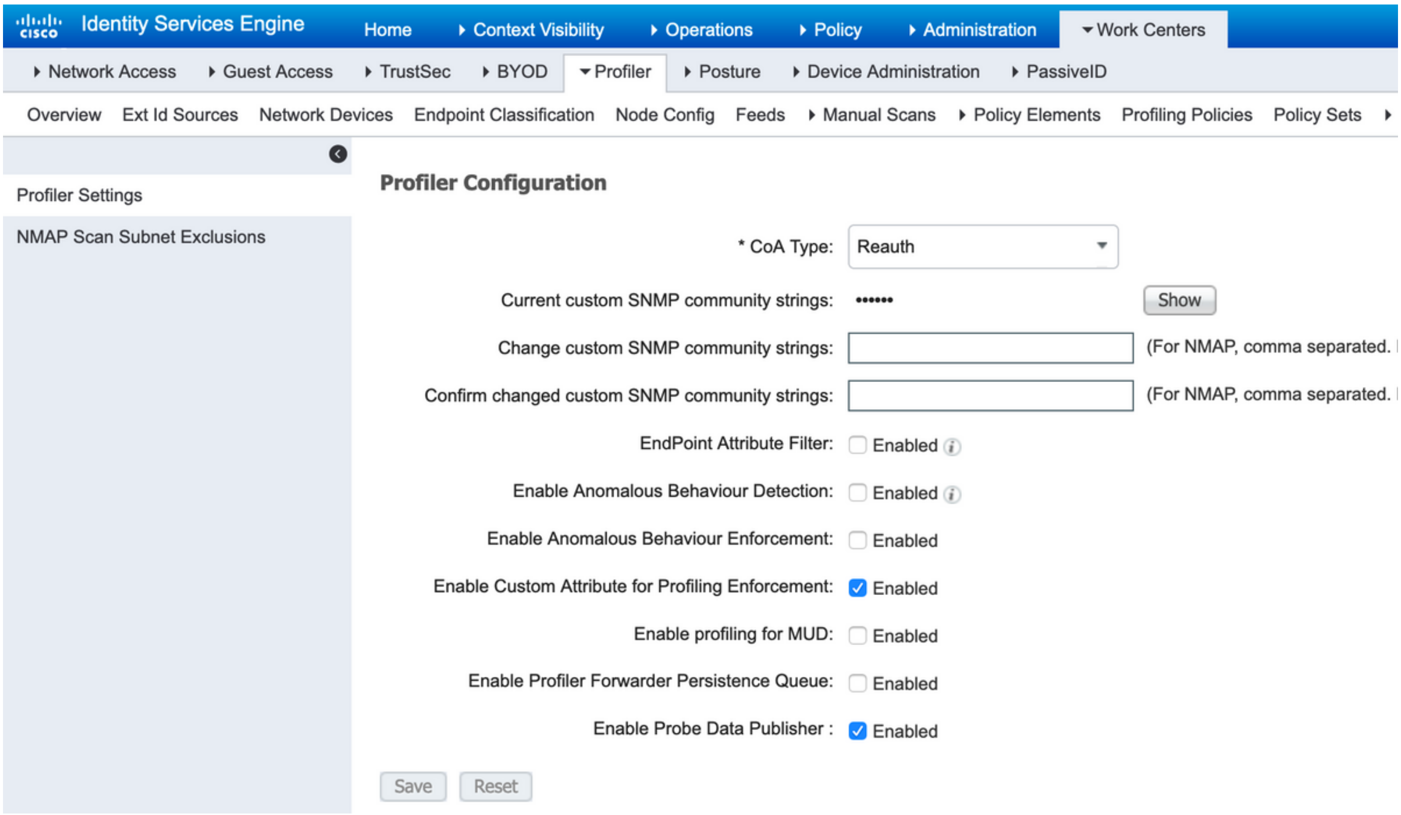
* Name	ekorneyc_ASSET_Group1
Description	
Policy Enabled	☑
* Minimum Certainty Factor	20 (Valid Range 1 to 65535)
* Exception Action	NONE
* Network Scan (NMAP) Action	NONE
Create an Identity Group for the policy	● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy
* Parent Policy	NONE
* Associated CoA Type	Global Settings
System Type	Administrator Created

Rules

If Condition	CUSTOMATTRIBUTE_assetGroup_EQUA...	Then	Certainty Factor Increases	20

4. Enable Custom Attributes for Profiling Enforcement

Navigate to **Work Centers > Profiler > Profiling Policies**. Click on **Add**. Configure Profiler Policy similar to this image. Ensure **Enable Custom Attribute for Profiling Enforcement** is enabled.



Profiler Configuration

* CoA Type: Reauth

Current custom SNMP community strings: ••••••

Change custom SNMP community strings: (For NMAP, comma separated.

Confirm changed custom SNMP community strings: (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

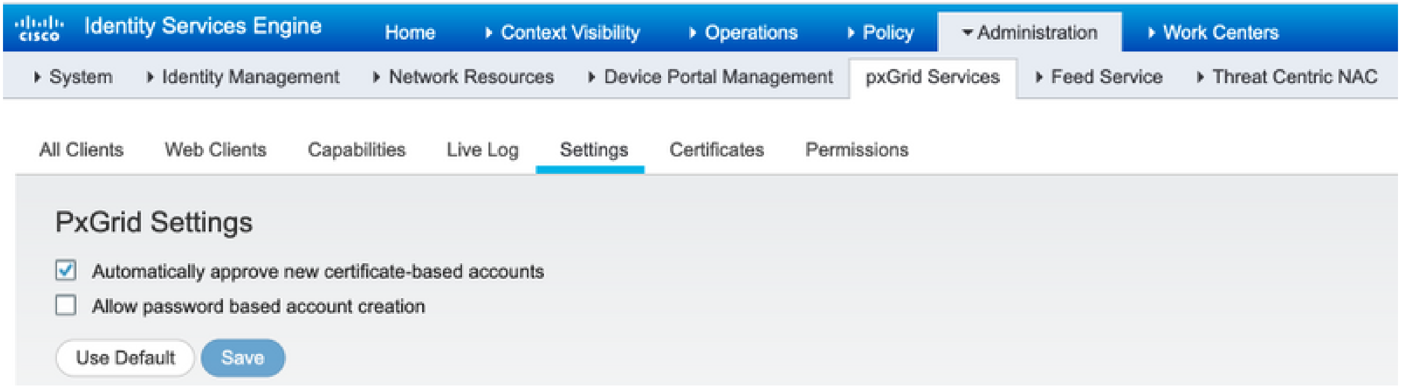
Enable profiling for MUD: □ Enabled

Enable Profiler Forwarder Persistence Queue: □ Enabled

Enable Probe Data Publisher : ☑ Enabled

5. Configure Automatic Approval for pxGrid Clients

Navigate to **Administration > pxGrid Services > Settings**. Select **Automatically approve new certificate-based accounts** and click **Save**. This step ensures that you don't need to approve CCV once the integration is done.



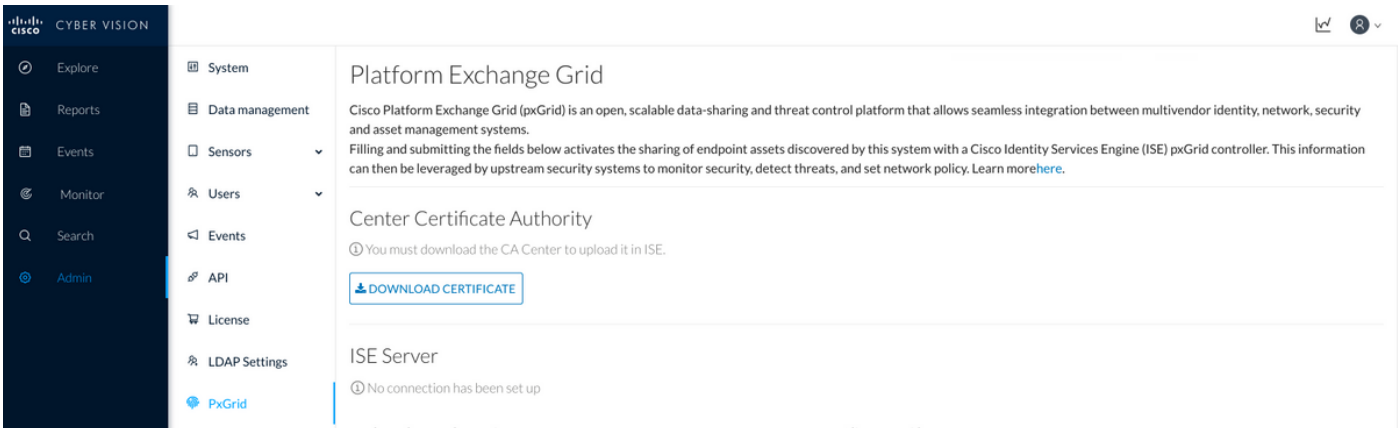
PxGrid Settings

☑ Automatically approve new certificate-based accounts

□ Allow password based account creation

6. Export CCV Certificate

Navigate to **Admin > pxGrid**. Click **DOWNLOAD CERTIFICATE**. This certificate is used during pxGrid registration, so ISE should trust it.



Platform Exchange Grid

Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat control platform that allows seamless integration between multivendor identity, network, security and asset management systems.
Filling and submitting the fields below activates the sharing of endpoint assets discovered by this system with a Cisco Identity Services Engine (ISE) pxGrid controller. This information can then be leveraged by upstream security systems to monitor security, detect threats, and set network policy. Learn morehere.

Center Certificate Authority

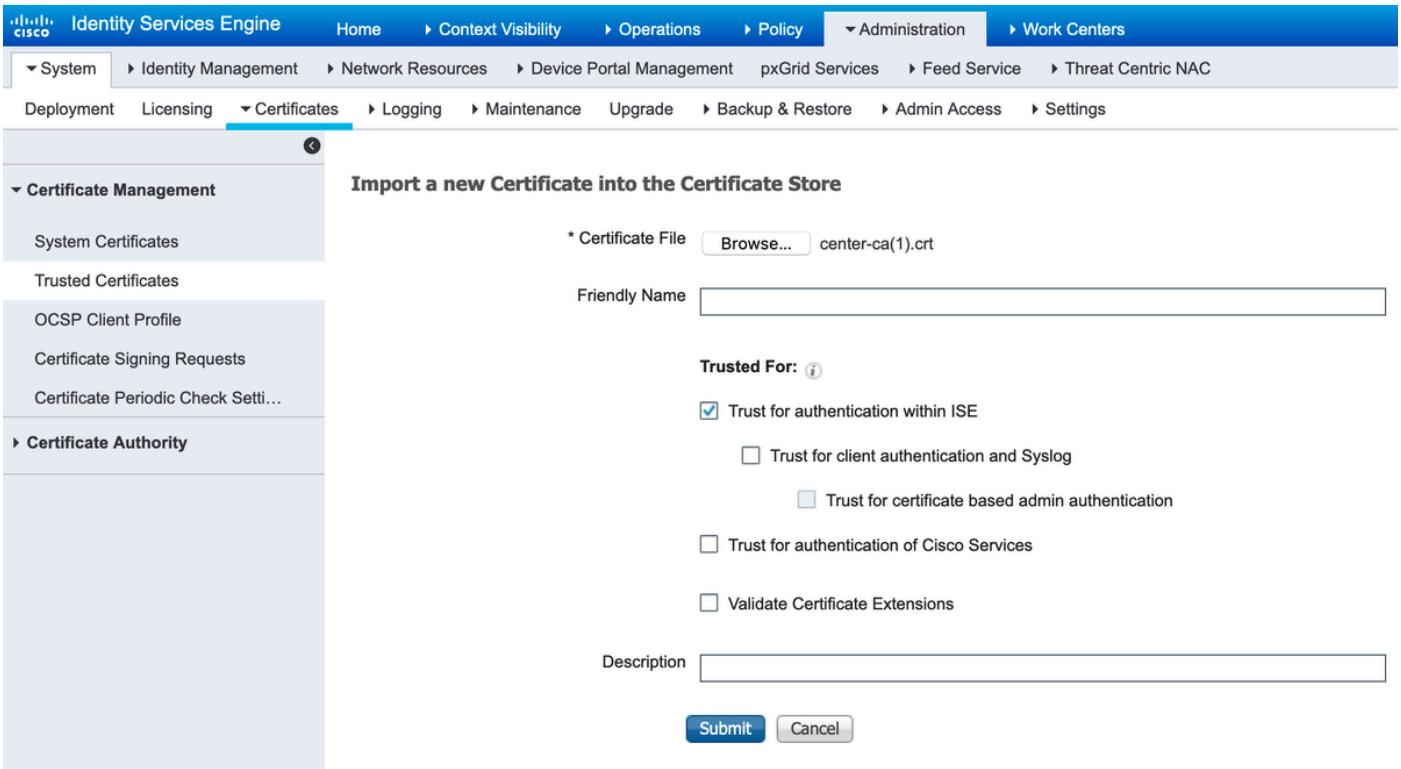
ⓘ You must download the CA Center to upload it in ISE.

ISE Server

ⓘ No connection has been set up

7. Upload CCV Identity Certificate to ISE Trusted Store

Navigate to **Administration > Certificates > Certificate Management > Trusted Certificates**. Click on **Import**. Click on **Browse** and select CCV certificate from Step 5. Click **Submit**.



Import a new Certificate into the Certificate Store

* Certificate File Browse... center-ca(1).crt

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

□ Trust for client authentication and Syslog

□ Trust for certificate based admin authentication

□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

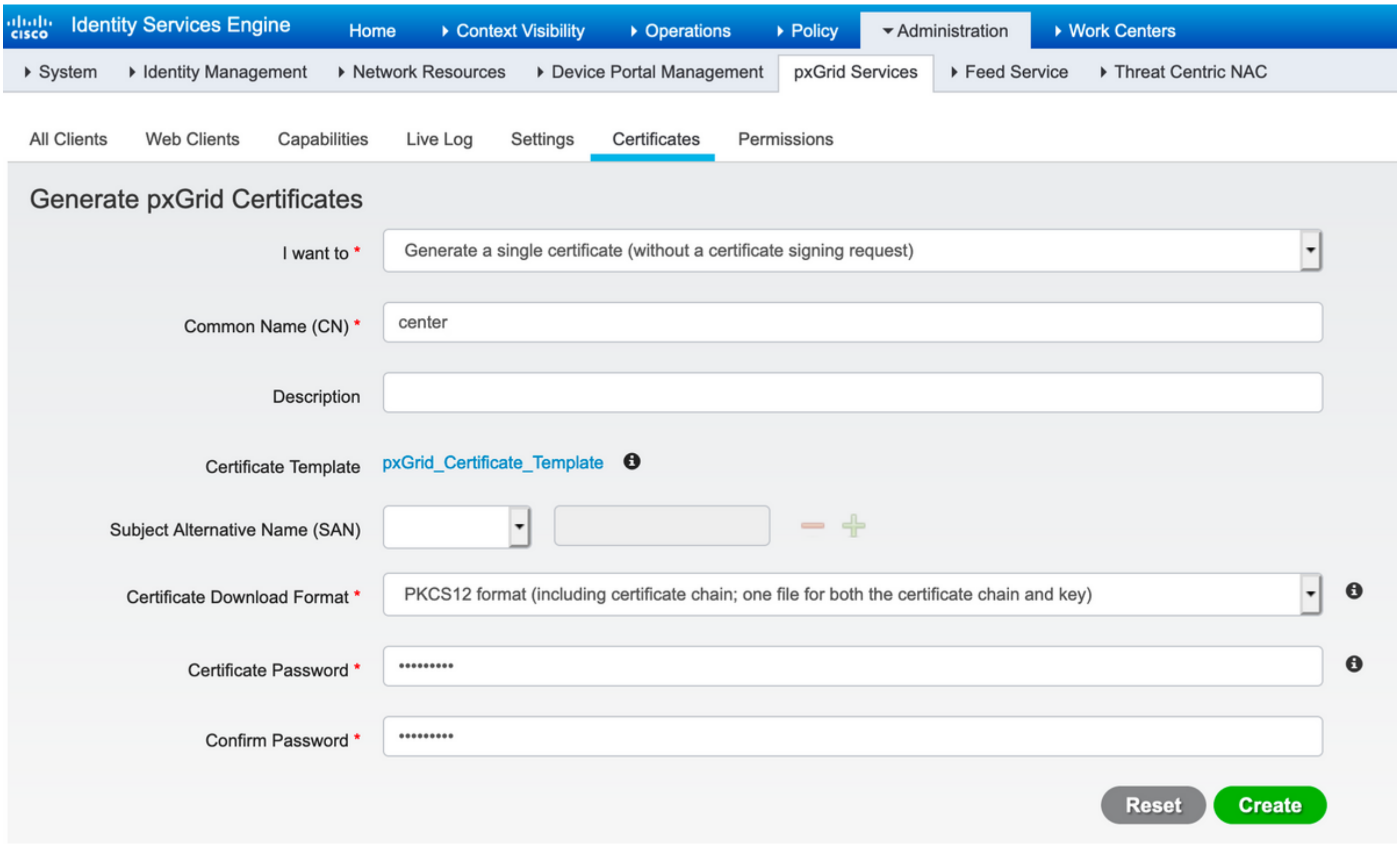
Description

8. Generate Certificate for CCV

During pxGrid Integration and updates, CCV needs the client certificate. It should be issued by ISE internal CA, using **PxGrid_Certificate_Template**.

Navigate to **Administration > pxGrid Services > Certificates**. Populate fields according to this image. Common Name (CN) field is mandatory since the goal of ISE CA is to issue an identity certificate. You should enter the hostname of CCV, CN field value is critical. In order to check the hostname of CCV, issue the **hostname** command. Select PKCS12 as **Certificate Download Format.**

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



Generate pxGrid Certificates

I want to * Generate a single certificate (without a certificate signing request)

Common Name (CN) * center

Description

Certificate Template pxGrid_Certificate_Template

Subject Alternative Name (SAN)

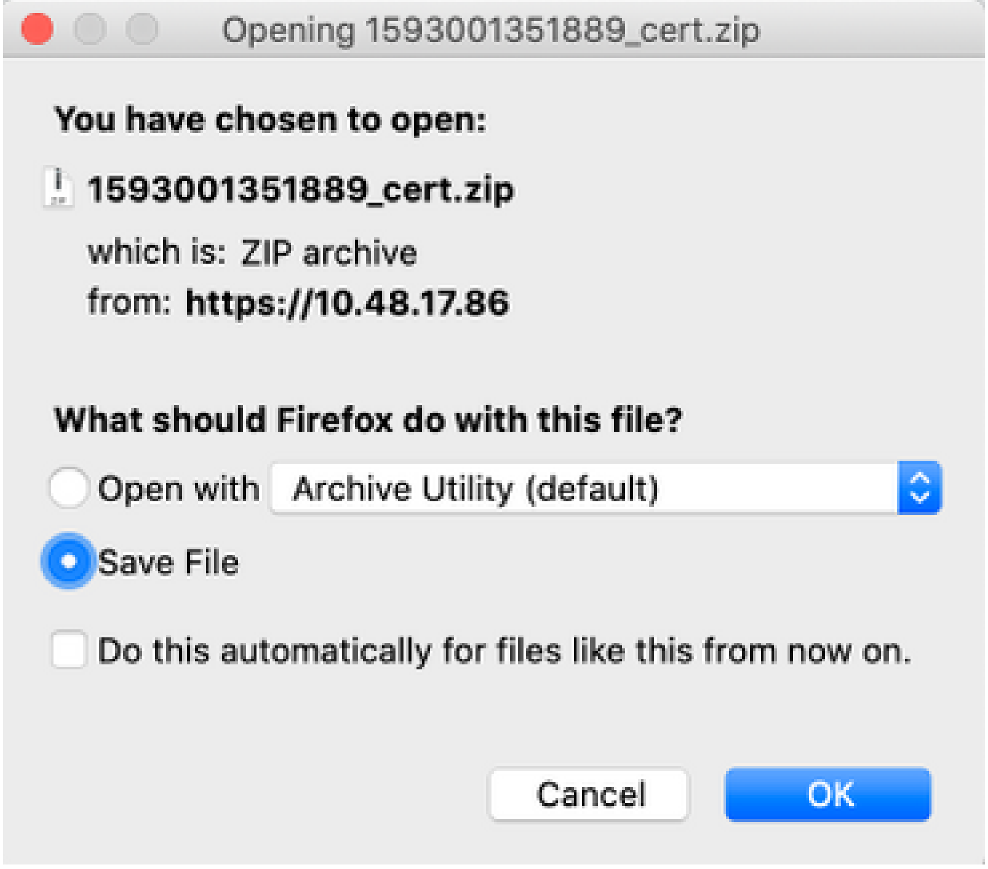
Certificate Download Format * PKCS12 format (including certificate chain; one file for both the certificate chain and key)

Certificate Password * •••••••••

Confirm Password * •••••••••

9. Download Certificate Chain in PKCS12 Format

When you install the certificate in PKCS12 format, along with the CCV identity certificate ISE Internal CA chain is installed on CCV to ensure that CCV trusts ISE when pxGrid communication is initiated from ISE, for example, pxGrid keepalive messages.



Opening 1593001351889_cert.zip

You have chosen to open:

1593001351889_cert.zip

which is: ZIP archive

from: https://10.48.17.86

What should Firefox do with this file?

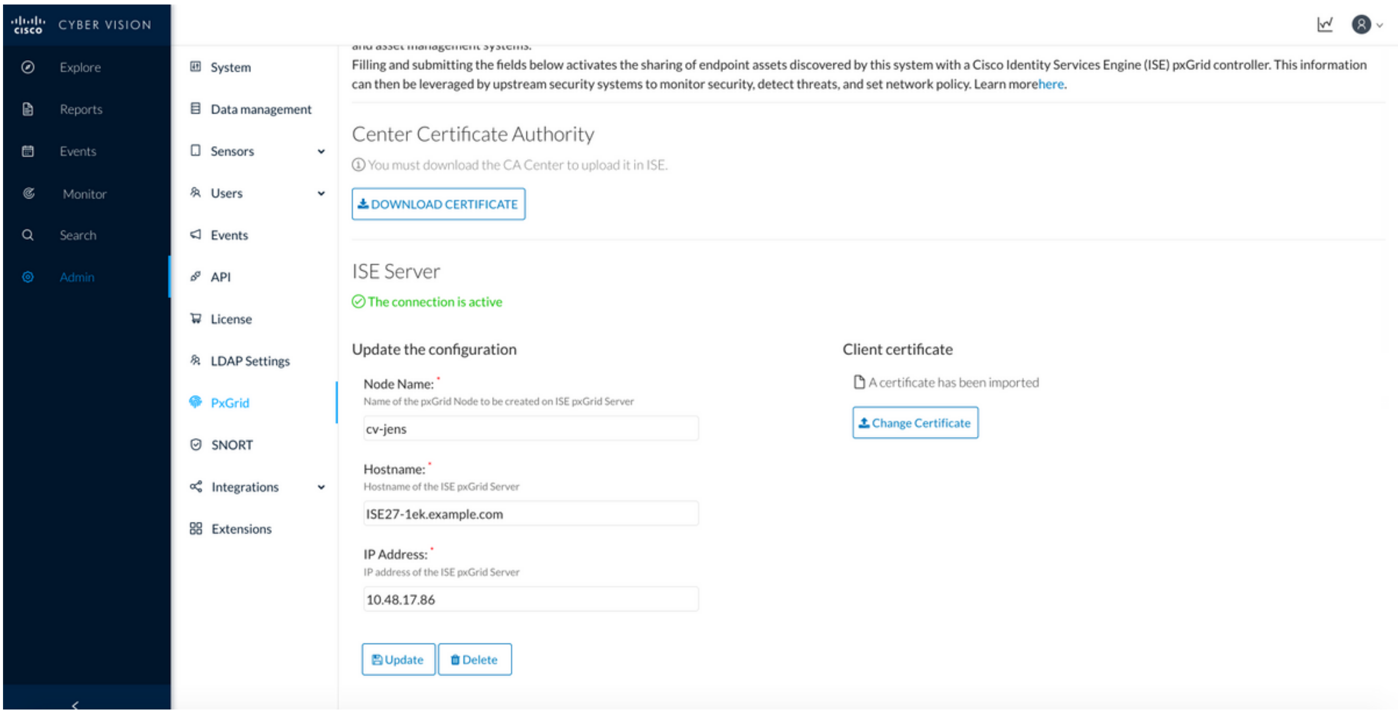
○ Open with Archive Utility (default)

● Save File

□ Do this automatically for files like this from now on.

10. Configure ISE Integration Details on CCV

Navigate to **Admin > pxGrid**. Configure Node Name, this name will be displayed on ISE as a Client Name at **Administration > pxGrid Services > Web Clients.** Configure **Hostname** and **IP Address** of ISE pxGrid Node. Ensure that CCV can resolve ISE FQDN.



and asset management systems.

Filling and submitting the fields below activates the sharing of endpoint assets discovered by this system with a Cisco Identity Services Engine (ISE) pxGrid controller. This information can then be leveraged by upstream security systems to monitor security, detect threats, and set network policy. Learn morehere.

Center Certificate Authority

ⓘ You must download the CA Center to upload it in ISE.

DOWNLOAD CERTIFICATE

ISE Server

The connection is active

Update the configuration

Node Name: *
Name of the pxGrid Node to be created on ISE pxGrid Server
cv-jens

Hostname: *
Hostname of the ISE pxGrid Server
ISE27-1ek.example.com

IP Address: *
IP address of the ISE pxGrid Server
10.48.17.86

Update Delete

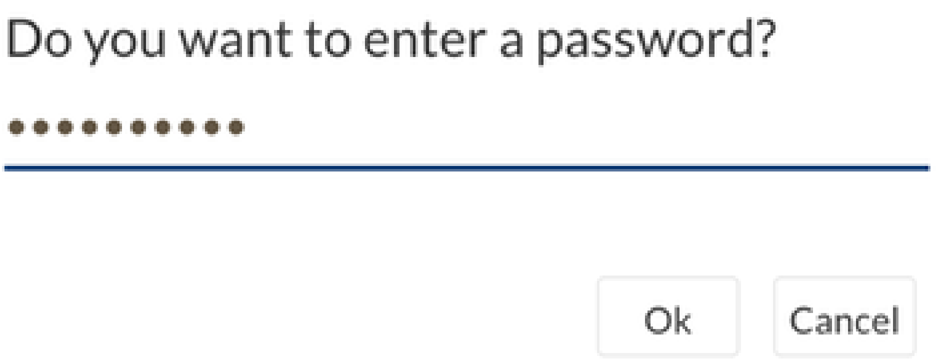
Client certificate

A certificate has been imported

Change Certificate

11. Upload Certificate Chain on CCV and Launch Integration

Navigate to **Admin > pxGrid**. Click on **Change Certificate**. Select certificate issued by ISE CA from Steps 8-9. Enter the password from Step 8. and click **OK.**



Do you want to enter a password?

●●●●●●●●●●

Ok Cancel

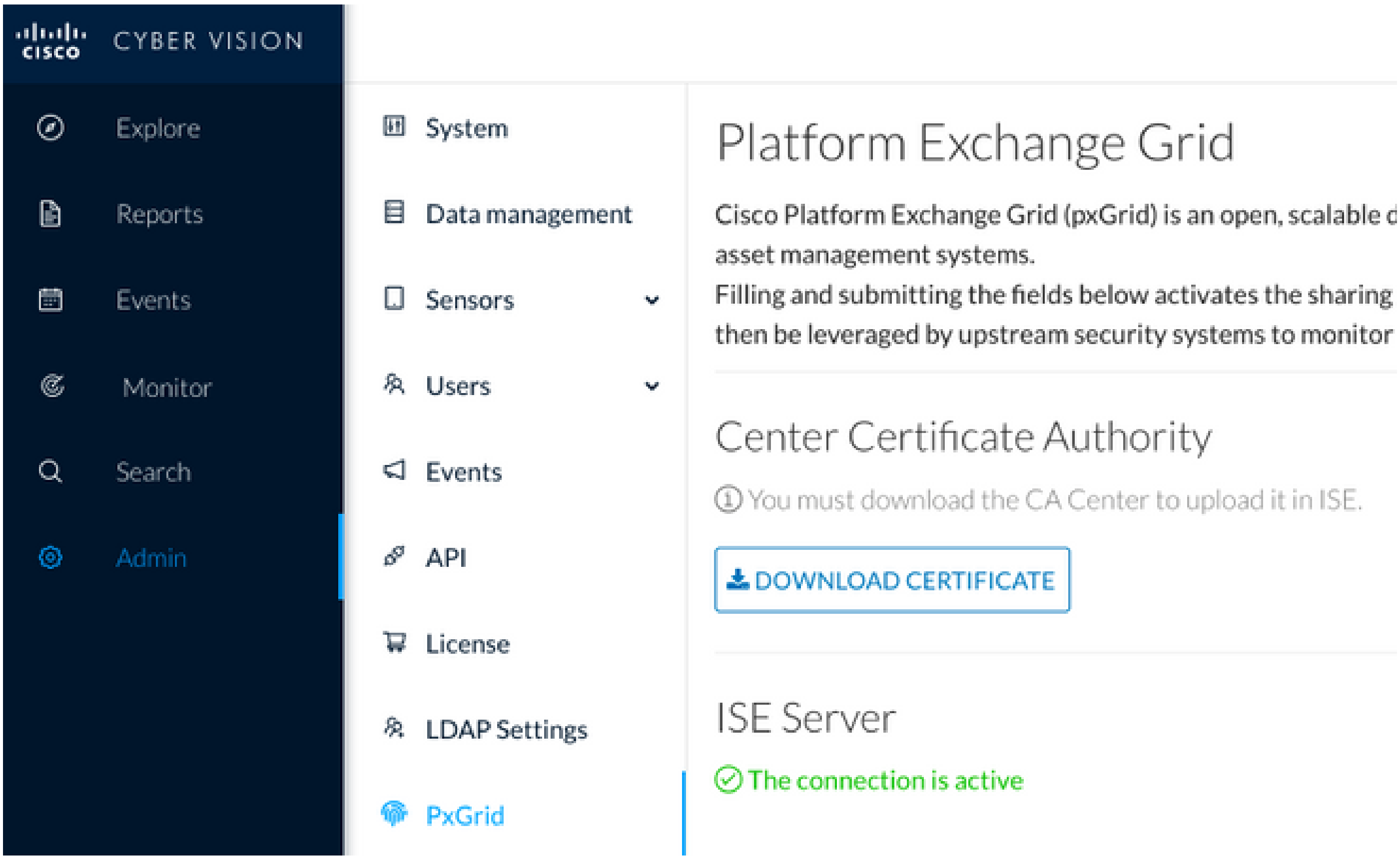
Click on **Update**, which triggers actual CCV - ISE integration.

Verify

Use this section to confirm that your configuration works properly.

CCV Integration Verification

Once the integration is done, you can confirm it is successful by navigating to **Admin > pxGrid**. You should see **The connection is active** message under ISE Server.



Platform Exchange Grid

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

Center Certificate Authority

ⓘ You must download the CA Center to upload it in ISE.

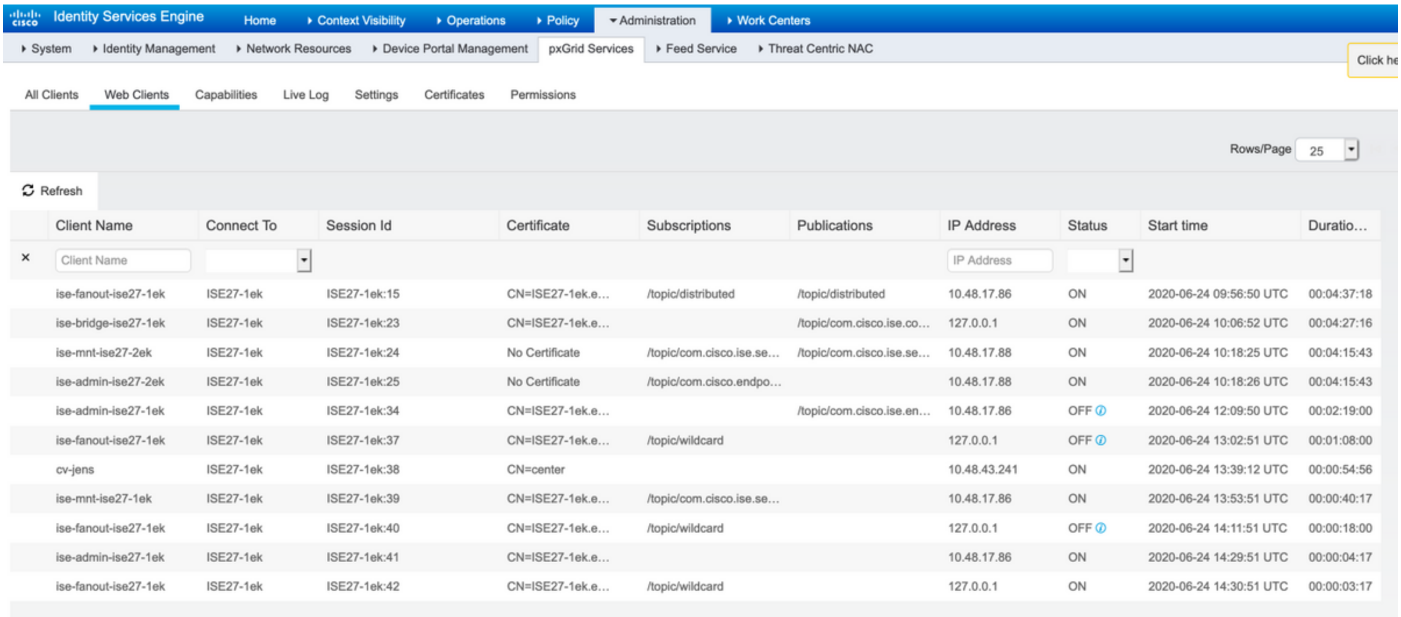
ISE Server

✓ The connection is active

ISE Integration Verification

Navigate to **Administration > pxGrid Services > Web Clients**. Confirm that the status of CCV Client (cv-jens) is **ON.**

> **Note**: It is expected to see the status of CCV pxGrid client as **Offline** in **All Clients** menu, as it shows only pxGrid v1 status.

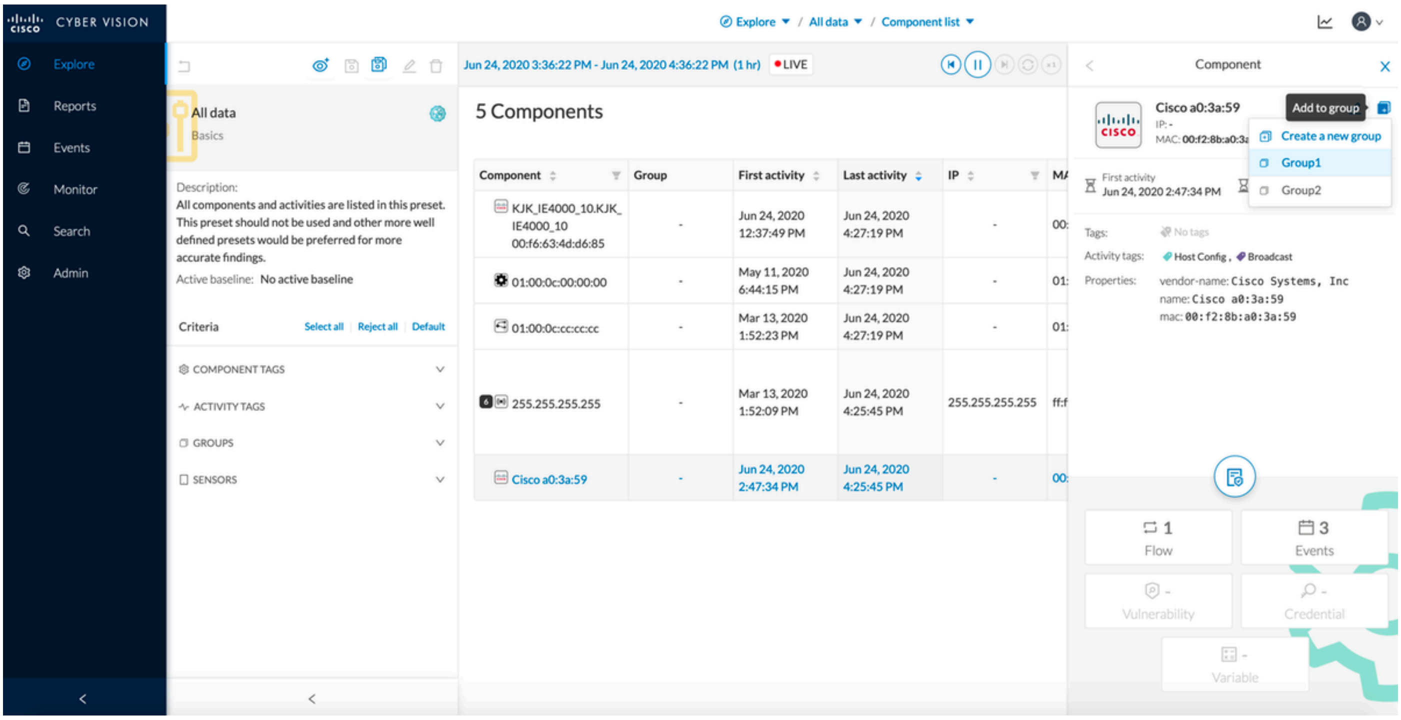


Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duratio…
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:15	CN=ISE27-1ek.e…	/topic/distributed	/topic/distributed	10.48.17.86	ON	2020-06-24 09:56:50 UTC	00:04:37:18
ise-bridge-ise27-1ek	ISE27-1ek	ISE27-1ek:23	CN=ISE27-1ek.e…		/topic/com.cisco.ise.co…	127.0.0.1	ON	2020-06-24 10:06:52 UTC	00:04:27:16
ise-mnt-ise27-2ek	ISE27-1ek	ISE27-1ek:24	No Certificate	/topic/com.cisco.ise.se…	/topic/com.cisco.ise.se…	10.48.17.88	ON	2020-06-24 10:18:25 UTC	00:04:15:43
ise-admin-ise27-2ek	ISE27-1ek	ISE27-1ek:25	No Certificate	/topic/com.cisco.endpo…		10.48.17.88	ON	2020-06-24 10:18:26 UTC	00:04:15:43
ise-admin-ise27-1ek	ISE27-1ek	ISE27-1ek:34	CN=ISE27-1ek.e…		/topic/com.cisco.ise.en…	10.48.17.86	OFF ⓘ	2020-06-24 12:09:50 UTC	00:02:19:00
ise-fanout-ise27-1ek	ISE27-1ek	ISE27-1ek:37	CN=ISE27-1ek.e…	/topic/wildcard		127.0.0.1	OFF ⓘ	2020-06-24 13:02:51 UTC	00:01:08:00
cv-jens	ISE27-1ek	ISE27-1ek:38	CN=center			10.48.43.241	ON	2020-06-24 13:39:12 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: Due to CSCvt78208 you will not immediately see CCV having **/topic/com.cisco.ise.endpoint.asset**, it will be shown only upon first publishing.

Verify CCV Group Change

Navigate to **Explore > All data > Component list**. Click on one of the Components and **Add** it to the Group.



Description:
All components and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.
Active baseline: No active baseline

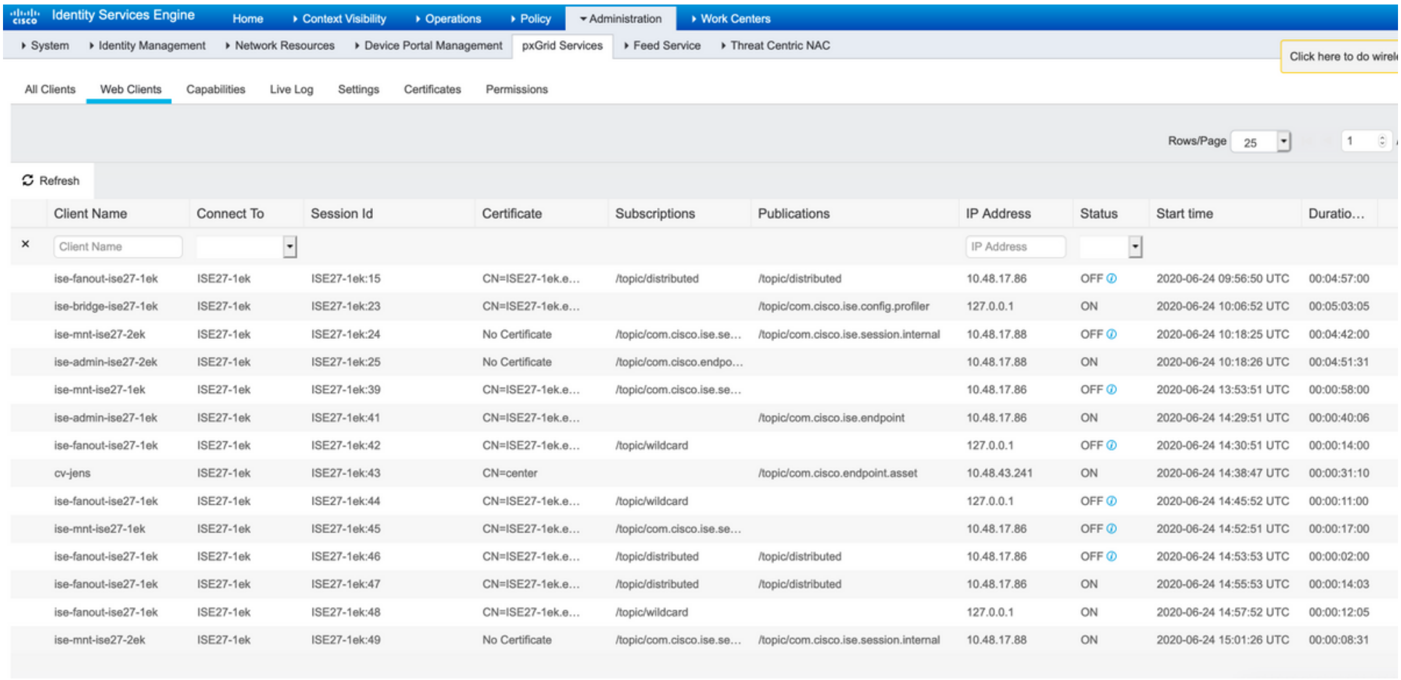
Jun 24, 2020 3:36:22 PM - Jun 24, 2020 4:36:22 PM (1 hr)

5 Components

Component	Group	First activity	Last activity	IP	MA
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:cc:cc:cc	-	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	ff:f
Cisco a0:3a:59	-	Jun 24, 2020 2:47:34 PM	Jun 24, 2020 4:25:45 PM	-	00:

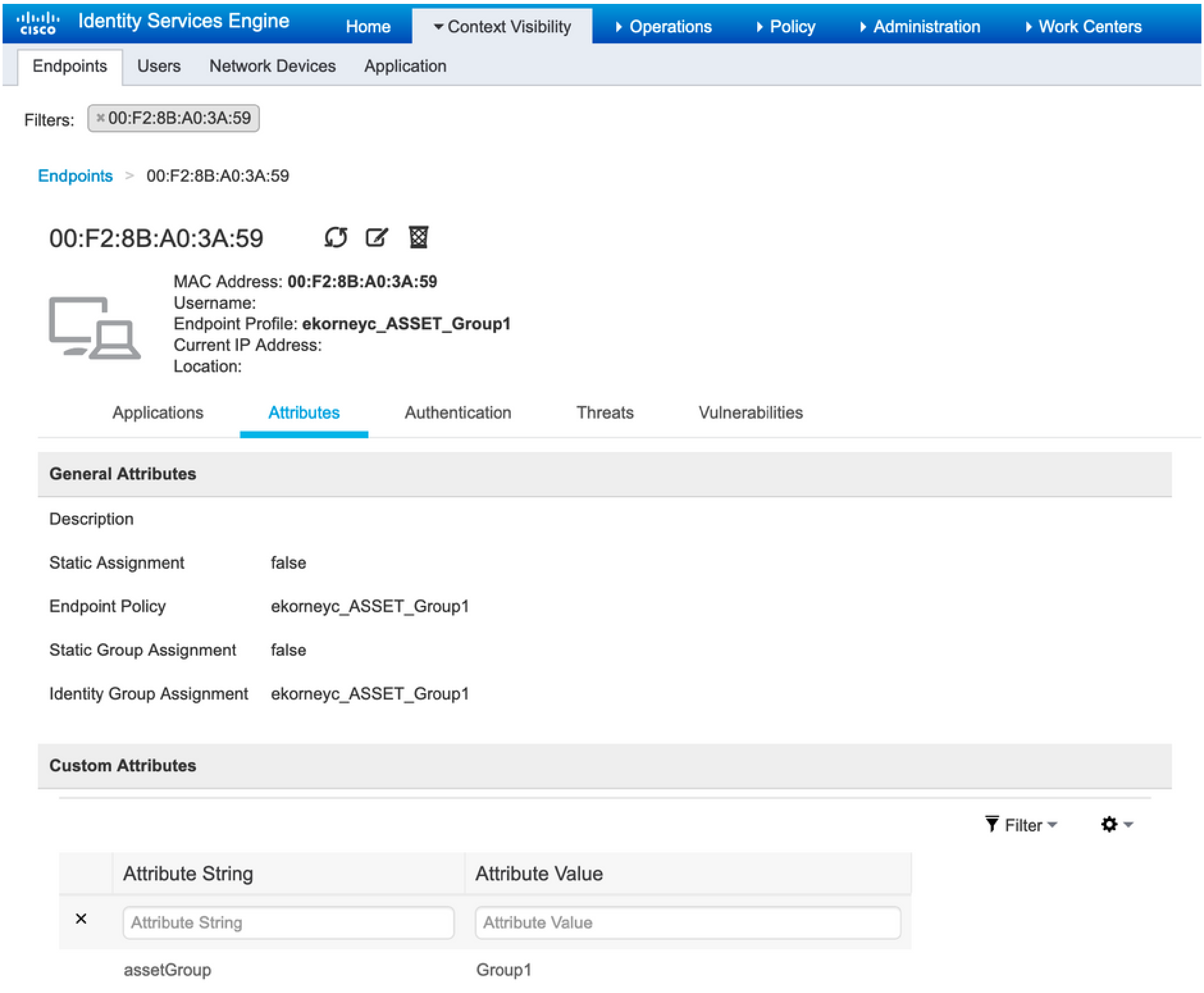
Cisco a0:3a:59
IP: -
MAC: 00:f2:8b:a0:3a
First activity
Jun 24, 2020 2:47:34 PM
Tags: No tags
Activity tags: Host Config, Broadcast
Properties: vendor-name: Cisco Systems, Inc
name: Cisco a0:3a:59
mac: 00:f2:8b:a0:3a:59

Verify that **/topic/com.cisco.ise.endpoint.asset** is now listed as Publications against CCV.



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

Confirm that Group1 assigned via CCV is reflected on ISE and profiling policy took effect by navigating to **Context Visibility > Endpoints**. Select the endpoint updated in the previous step. Switch to the Attributes tab. The custom attributes section should reflect the newly configured Group.



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:

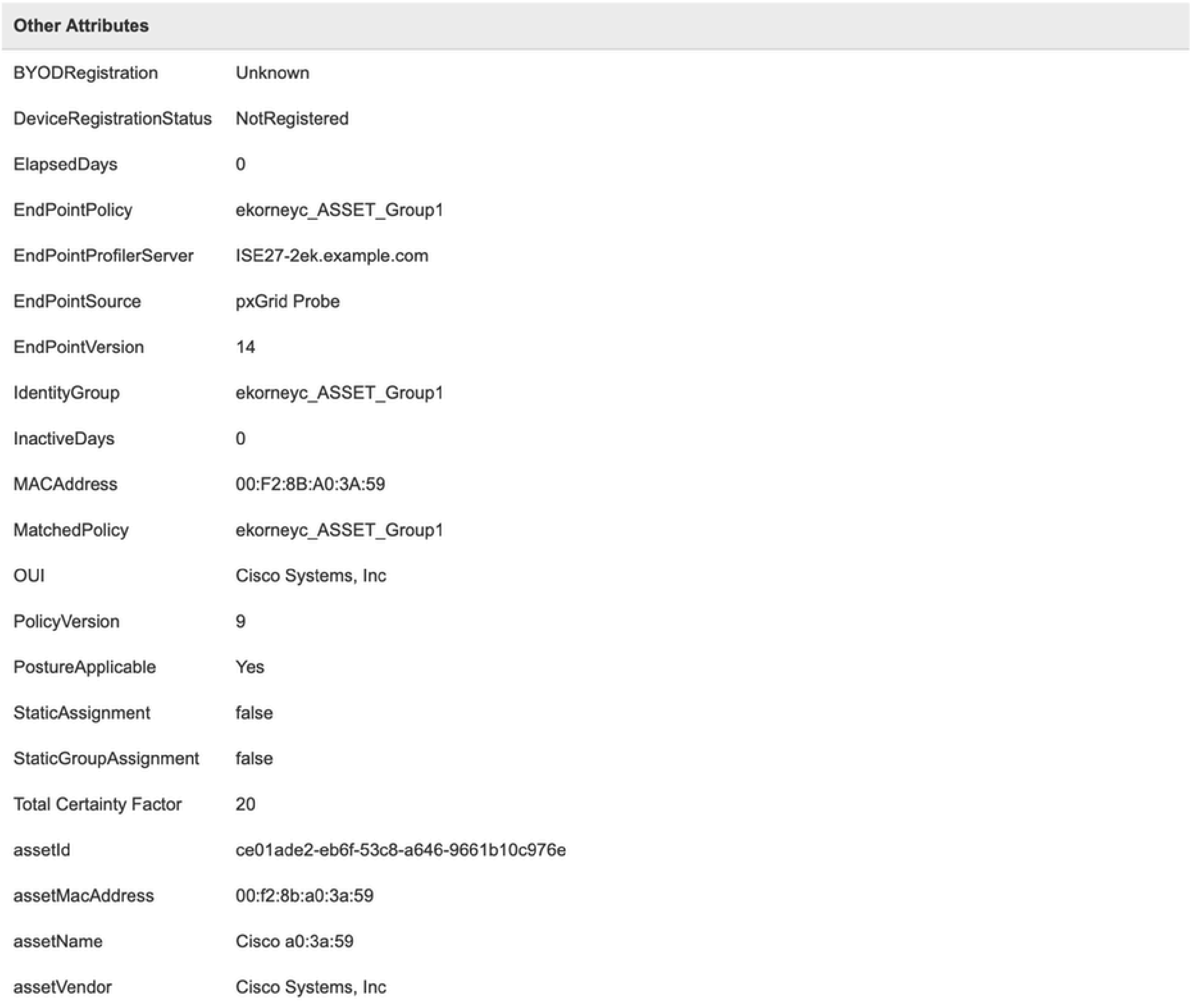
General Attributes

Description	
Static Assignment	false
Endpoint Policy	ekorneyc_ASSET_Group1
Static Group Assignment	false
Identity Group Assignment	ekorneyc_ASSET_Group1

Custom Attributes

Attribute String	Attribute Value
Attribute String	Attribute Value
assetGroup	Group1

The other Attributes section lists all other asset attributes received from 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

This section provides information you can use to troubleshoot your configuration.

Enable Debugs on ISE

In order to enable debugs on ISE, navigate to **Administration > System > Logging > Debug Log Configuration**. Set Log Levels to these:

Persona	Component Name	Log Level	File to check
PAN (optional)	profiler	DEBUG	profiler.log
PSN with pxGrid probe enabled	profiler	DEBUG	profiler.log
PxGrid	pxgrid	TRACE	pxgrid-server.log

Enable Debugs on CCV

In order to enable debugs on CCV:

- Create a file **/data/etc/sbs/pxgrid-agent.conf** with **touch /data/etc/sbs/pxgrid-agent.conf** command
- Paste this content into **pxgrid-agent.conf** file with the use of the **vi** editor with the **vi /data/etc/sbs/pxgrid-agent.conf** command

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

- Restart pxgrid-agent by running the **systemctl restart pxgrid-agent** command
- View logs with the **journalctl -u pxgrid-agent** command

Bulk Download Fails

CCV publishes Bulk Download URL to ISE during the integration. ISE PSN with pxGrid probe enabled performs Bulk Download with the use of this URL. Ensure that:

- The hostname in the URL is correctly resolvable from the ISE perspective
- Communication from PSN on port 8910 to CCV is allowed

profiler.log on PSN with pxGrid probe enabled:

```
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}]]
```

The bulk download can fail due to CSCvt75422, you should see this error in **profiler.log** on ISE to confirm it. The defect is fixed in CCV 3.1.0.

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

Not all Endpoints are Created on ISE

Some endpoints on CCV can have too many attributes attached, hence ISE database will not be able to handle it. It can be confirmed if you see these errors in **profiler.log** on 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)
```

AssetGroup is not Available on ISE

If AssetGroup is not available on ISE, most probably the Profiling policy is not configured using Custom Attributes (refer to Steps 2-4. in the Configurations part of the document). Even for Context Visibility, just to display Group attributes, Profiling policies and other settings from Steps 2-4 are mandatory.

Endpoint Group Updates are Not Reflected on ISE

Due to CSCvu80175, CCV does not publish endpoint updates to ISE until CCV reboots right after the integration. You can reboot CCV once the integration is done as a workaround.

Removing Group from CCV is not Removing it from ISE

This issue is seen due to the known defect on CCV CSCvu47880.The pxGrid update sent during Group removal from CCV having different than expected format, hence the group is not removed.

CCV Drops Off from Web Clients

This issue is seen due to the known defect on ISE CSCvu47880 where clients transition to OFF state followed by complete removal from Web Clients. The issue is resolved in 2.6 patch 7 and 2.7 patch 2 of ISE.

You can confirm it if you see these errors in **pxgrid-server.log** on ISE:

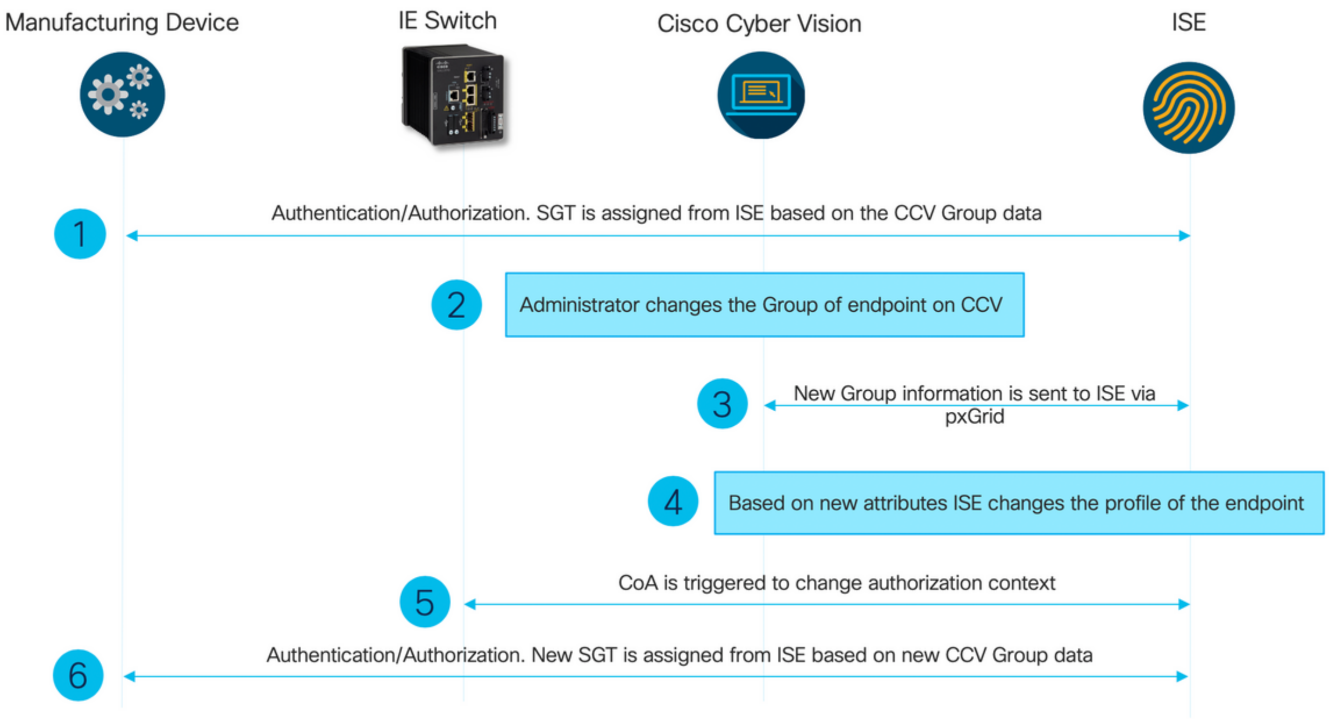
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionID=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726,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

ISE Integration with CCV TrustSec Use Case

This configuration shows how ISE integration with CCV can benefit security end-to-end when TrustSec is in place. This is just one of the examples of how integration can be used, once the integration is done.

> **Note**: TrustSec switch configuration explanation is outside of the scope of this article, however, it can be found in Appendix.

Topology and the Flow

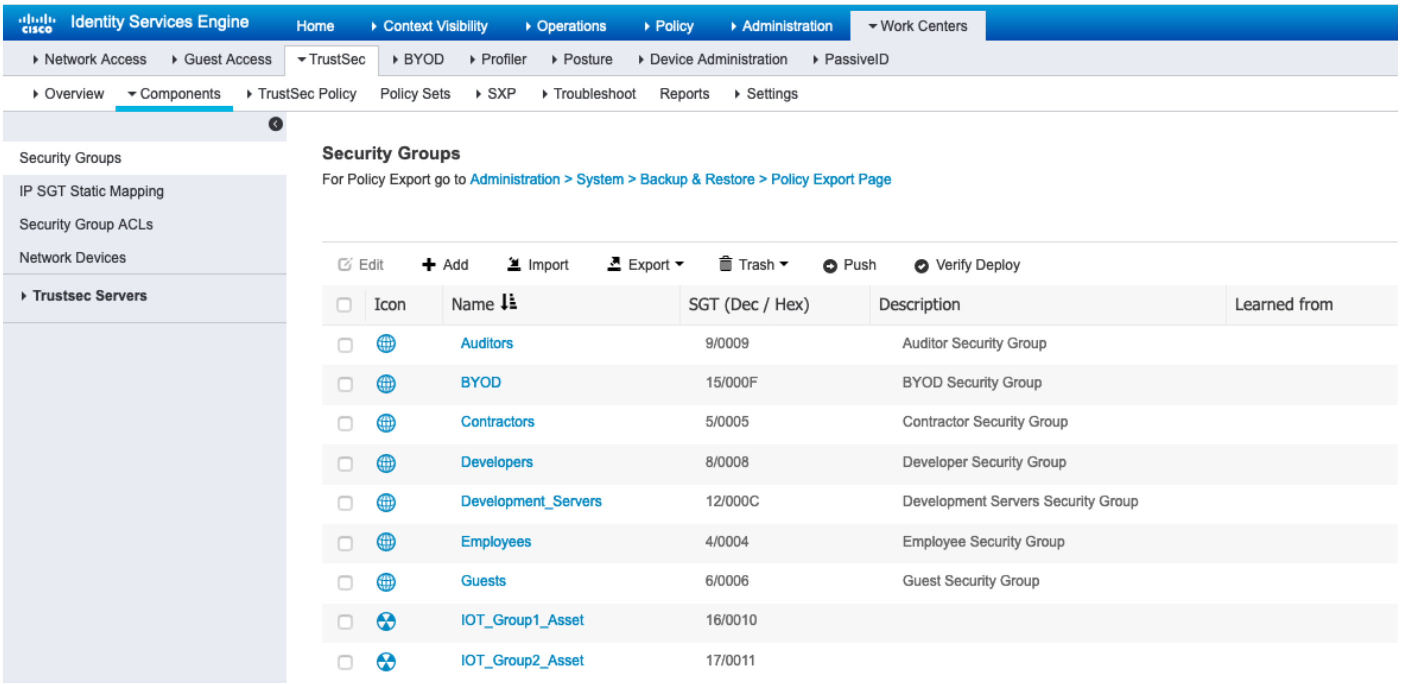


Manufacturing Device
IE Switch
Cisco Cyber Vision
ISE
1
Authentication/Authorization. SGT is assigned from ISE based on the CCV Group data
2
Administrator changes the Group of endpoint on CCV
3
New Group information is sent to ISE via pxGrid
4
Based on new attributes ISE changes the profile of the endpoint
5
CoA is triggered to change authorization context
6
Authentication/Authorization. New SGT is assigned from ISE based on new CCV Group data

Configure

1. Configure Scalable Group Tags on ISE

In order to achieve the use case mentioned previously, the TrustSec Tag's IOT_Group1_Asset and IOT_Group2_Asset are manually configured to differentiate Group1 CCV assets from Group2 respectively. Navigate to **Work Centers > TrustSec > Components > Security Groups**. Click on **Add.** Name SGT's as shown in the image.



Security Groups

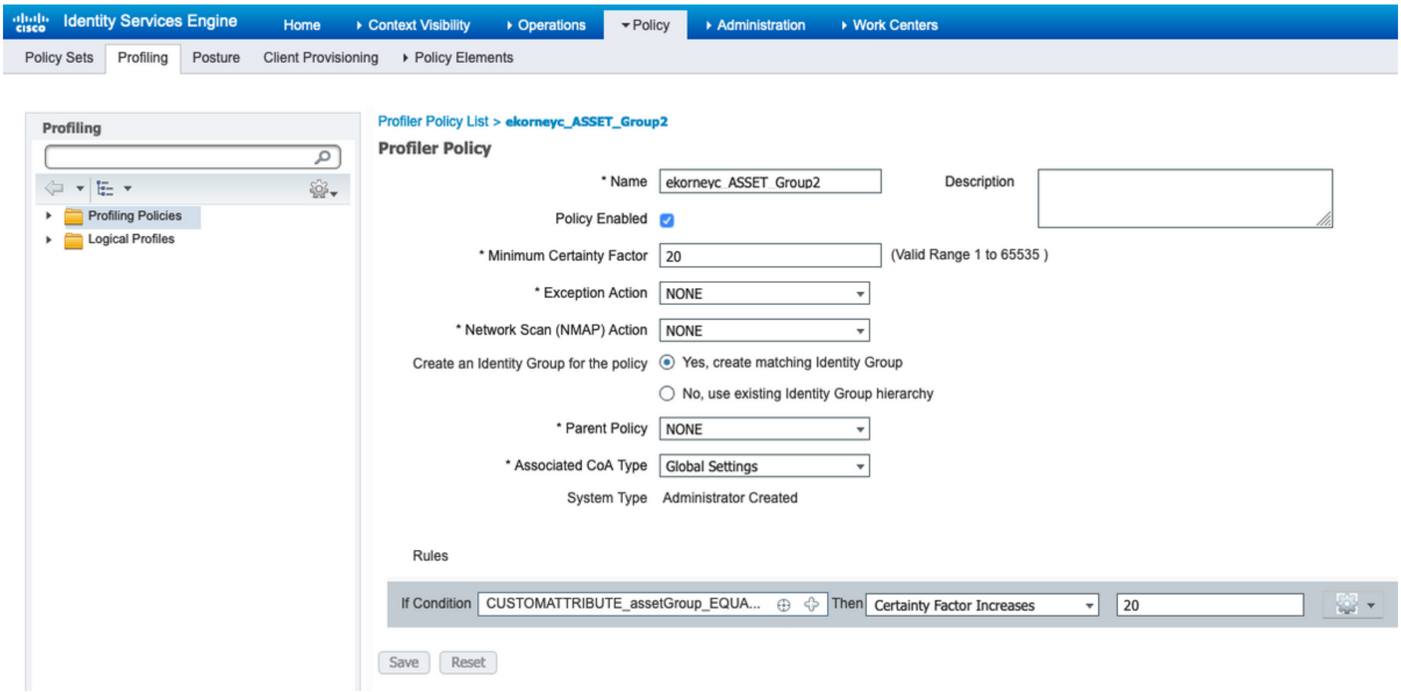
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

	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. Configure Profiler Policy with Custom Attributes for Group 2

Note: Profiling Configuration for Group 1 was done in Step 3. in the first part of the document.

Navigate to **Work Centers > Profiler > Profiling Policies**. Click on **Add**. Configure Profiler Policy similar to this image. Condition expression used in this policy is **CUSTOMATTRIBUTE:assetGroup EQUALS Group2.**



Profiler Policy List > ekorneyc_ASSET_Group2

Profiler Policy

* Name	ekorneyc_ASSET_Group2
Description	
Policy Enabled	☑
* Minimum Certainty Factor	20 (Valid Range 1 to 65535)
* Exception Action	NONE
* Network Scan (NMAP) Action	NONE
Create an Identity Group for the policy	● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy
* Parent Policy	NONE
* Associated CoA Type	Global Settings
System Type	Administrator Created

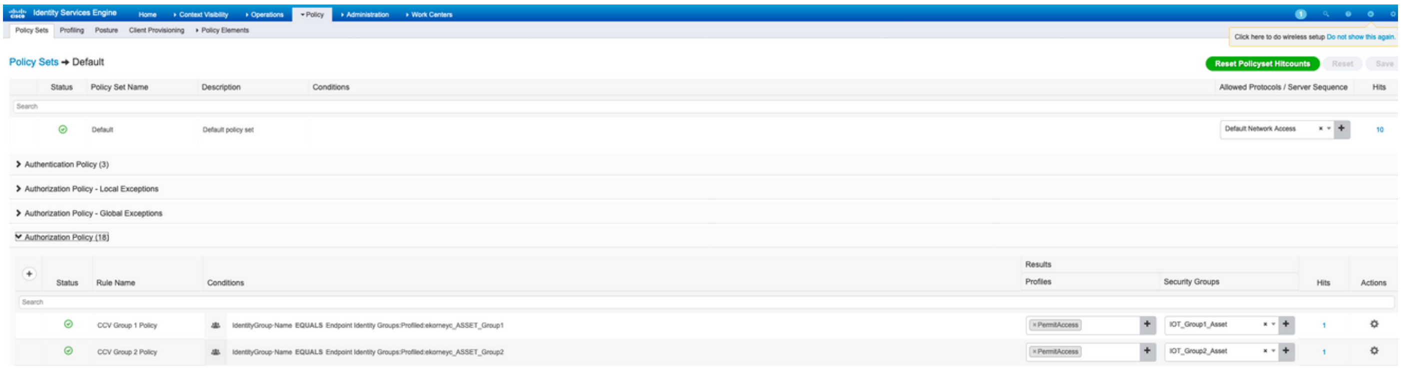
Rules

If Condition CUSTOMATTRIBUTE_assetGroup_EQUA... Then Certainty Factor Increases 20

3. Configure Authorization Policies to Assign SGT's Based on Endpoint Identity Groups on ISE

Navigate to **Policy > Policy Sets**. Select **Policy Set** and configure **Authorization Policies** as per this image. Note that as a result, SGT's configured in Step 1. are assigned.

Rule Name	Conditions	Profiles	Security Groups
CCV Group 1 Policy	IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ASSET_Group1	PermitAccess	IOT_Group1_Asset
CCV Group 2 Policy	IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ASSET_Group2	PermitAccess	IOT_Group2_Asset



Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	10

- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (18)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	CCV Group 1 Policy	IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ASSET_Group1	PermitAccess	IOT_Group1_Asset	1	⚙
✓	CCV Group 2 Policy	IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ASSET_Group2	PermitAccess	IOT_Group2_Asset	1	⚙

Verify

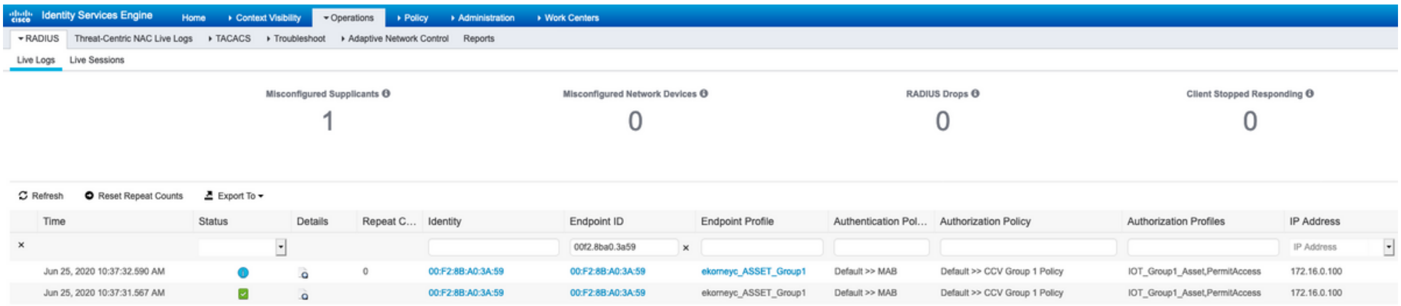
Use this section to confirm that your configuration works properly.

1. Endpoints Authenticate Based on CCV Group 1

On Switch, you can see that environment data includes both SGT's **16-54:IOT_Group1_Asset** and **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 authenticate and as a result, **CCV Group 1 Policy** is matched, SGT **IOT_Group1_Asset** is assigned.



Misconfigured Supplicants: 1

Misconfigured Network Devices: 0

RADIUS Drops: 0

Client Stopped Responding: 0

Time	Status	Details	Repeat C...	Identity	Endpoint ID	Endpoint Profile	Authentication Pol...	Authorization Policy	Authorization Profiles	IP Address
					00f2.8ba0.3a59					IP Address
Jun 25, 2020 10:37:32.590 AM	●		0	00:F2:8B:A0:3A:59	00:F2:8B:A0:3A:59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_Asset,PermitAccess	172.16.0.100
Jun 25, 2020 10:37:31.567 AM	✓			00:F2:8B:A0:3A:59	00:F2:8B:A0:3A:59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_Asset,PermitAccess	172.16.0.100

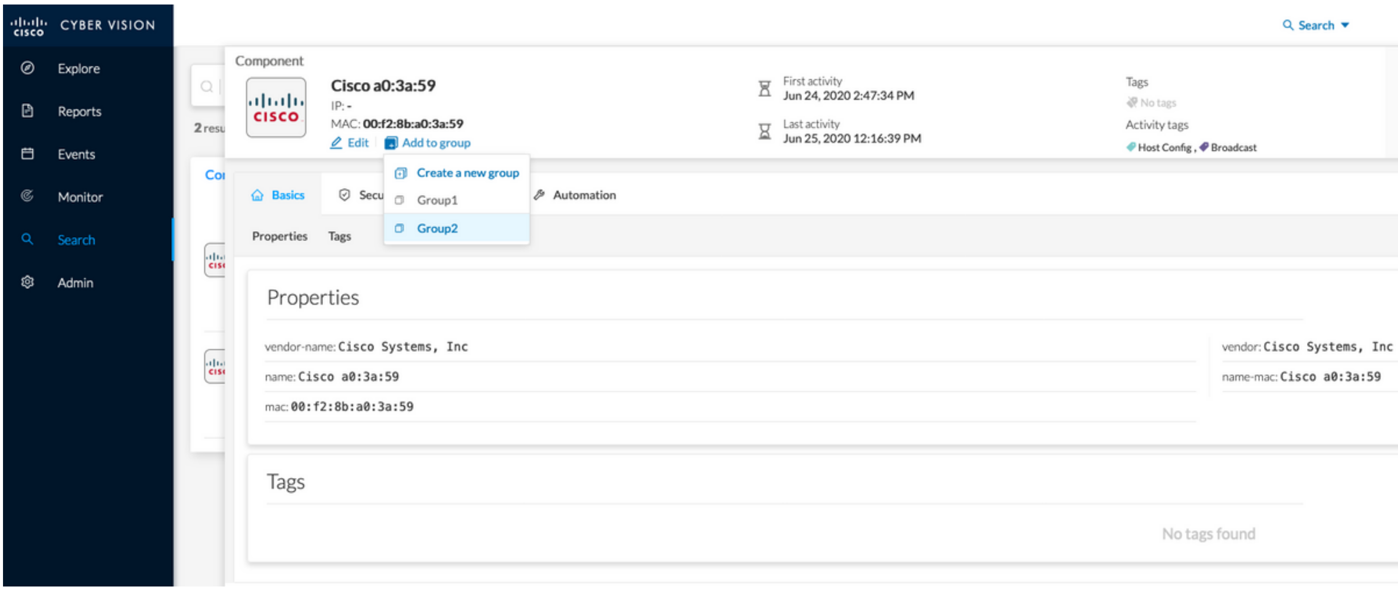
Switch **show authentication sessions interface fa1/7 detail** confirms the Access-Accept data was applied successfully.

```
KJK_IE4000_10#show authentication sessions interface fa1/7 detail
Interface: FastEthernet1/7
MAC Address: 00f2.8ba0.3a59
IPv6 Address: Unknown
IPv4 Address: 172.16.0.100
User-Name: 00-F2-8B-A0-3A-59
Status: Authorized
Domain: DATA
Oper host mode: single-host
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 128s
Common Session ID: 0A302BFD0000001B02BE1E9C
Acct Session ID: 0x00000010
Handle: 0x58000003
Current Policy: POLICY_Fa1/7

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure

Server Policies:
  SGT Value: 16

Method status list:
Method State

mab Authc Success

KJK_IE4000_10#
```

2. Administrator Changes the Group

Navigate to **Search**. Paste the Mac address of the Endpoint, click on it and **Add** it to the Group 2.

> **Note**: On CCV, you can not change the group from 1 to 2 in one go. Hence, you should remove the Endpoint from the group first and assign Group 2 next.



Component

Cisco a0:3a:59
IP: -
MAC: 00:f2:8b:a0:3a:59

First activity
Jun 24, 2020 2:47:34 PM

Last activity
Jun 25, 2020 12:16:39 PM

Tags
No tags

Activity tags
Host Config , Broadcast

Properties

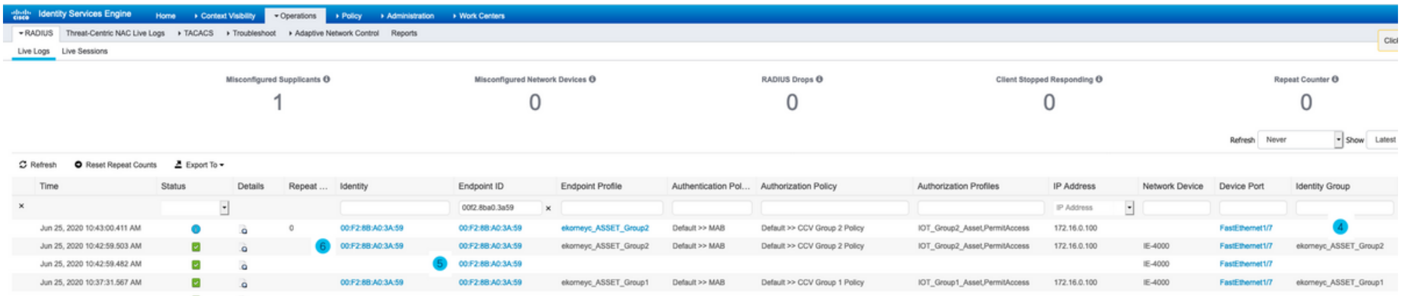
vendor-name: Cisco Systems, Inc
name: Cisco a0:3a:59
mac: 00:f2:8b:a0:3a:59
vendor: Cisco Systems, Inc
name-mac: Cisco a0:3a:59

Tags

No tags found

3-6. Effect of Endpoint Group Change on CCV

Steps 4., 5. and 6. are reflected in this image. Thanks to profiling, endpoint changed Identity Group to ekorneyc_ASSET_Group2 seen in Step 4., which caused ISE to send CoA to the switch (Step 5) and finally endpoint reauthentication (Step 6).



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
1	0	0	0	0

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Pol...	Authorization Policy	Authorization Profiles	IP Address	Network Device	Device Port	Identity Group
					00f2.8ba0.3a59					IP Address			
Jun 25, 2020 10:43:00.411 AM	●		0	00:F2:8B:A0:3A:59	00:F2:8B:A0:3A:59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_Asset,PermitAccess	172.16.0.100		FastEthernet1/7	
Jun 25, 2020 10:42:59.503 AM	☑			00:F2:8B:A0:3A:59	00:F2:8B:A0:3A:59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_Asset,PermitAccess	172.16.0.100	IE-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59.482 AM	☑				00:F2:8B:A0:3A:59						IE-4000	FastEthernet1/7	
Jun 25, 2020 10:37:31.567 AM	☑			00:F2:8B:A0:3A:59	00:F2:8B:A0:3A:59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_Asset,PermitAccess	172.16.0.100	IE-4000	FastEthernet1/7	ekorneyc_ASSET_Group1

Switch **show authentication sessions interface fa1/7 detail** confirms that the new SGT is assigned.

```
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

Switch TrustSec Related Configuration

> **Note**: Cts credentials are not part of running-config and should be configured with the use of **cts credentials id <id> password <password>** command in privilege exec mode.

```
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#
```