

ISE 2.7 pxGrid CCV 3.1.0統合の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[概要フロー図](#)

[設定](#)

- [1. PSNの1つでpxGridプローブを有効にする](#)
- [2. ISEでのエンドポイントカスタム属性の設定](#)
- [3.カスタム属性を使用したプロファイラポリシーの構成](#)
- [4.プロファイル適用のカスタム属性の有効化](#)
- [5. pxGridクライアントの自動承認の設定](#)
- [6. CCV証明書のエクスポート](#)
- [7. CCV ID証明書のISE信頼ストアへのアップロード](#)
- [8. CCVの証明書の生成](#)
- [9. PKCS12形式での証明書チェーンのダウンロード](#)
- [10. CCVでのISE統合の詳細の設定](#)
- [11. CCVへの証明書チェーンのアップロードと統合の開始](#)

[確認](#)

[CCV統合の検証](#)

[ISE統合の検証](#)

[CCVグループの変更の確認](#)

[トラブルシューティング](#)

[ISEでのデバッグの有効化](#)

[CCVでのデバッグの有効化](#)

[一括ダウンロードの失敗](#)

[すべてのエンドポイントがISEで作成されるわけではありません](#)

[AssetGroupがISEで使用できない](#)

[エンドポイントグループの更新がISEに反映されない](#)

[CCVからグループを削除してもISEからグループを削除できない](#)

[WebクライアントからのCCVドロップ](#)

[CCV TrustSecによるISE統合の使用例](#)

[トポロジとフロー](#)

[設定](#)

- [1. ISEでのスケラブルグループタグの設定](#)
- [2.グループ2のカスタム属性を使用したプロファイラポリシーの設定](#)
- [3. ISE上のエンドポイントIDグループに基づいてSGTを割り当てる認可ポリシーの設定](#)

[確認](#)

- [1. CCVグループ1に基づいてエンドポイントを認証](#)
- [2.管理者によるグループの変更](#)

[3-6.エンドポイントグループ変更のCCVへの影響](#)

[付録](#)

[スイッチTrustSec関連の設定](#)

概要

このドキュメントでは、Platform Exchange Grid v2(pxGrid)上でCisco Cyber Vision(CCV)3.1.0とIdentity Services Engine(ISE)2.7の統合を設定およびトラブルシューティングする方法について説明します。CCVはpxGrid v2にパブリッシャとして登録され、エンドポイント属性に関する情報をIOTASSETディクショナリ用にISEに公開します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- ISE
- Cisco Cyber Vision

使用するコンポーネント

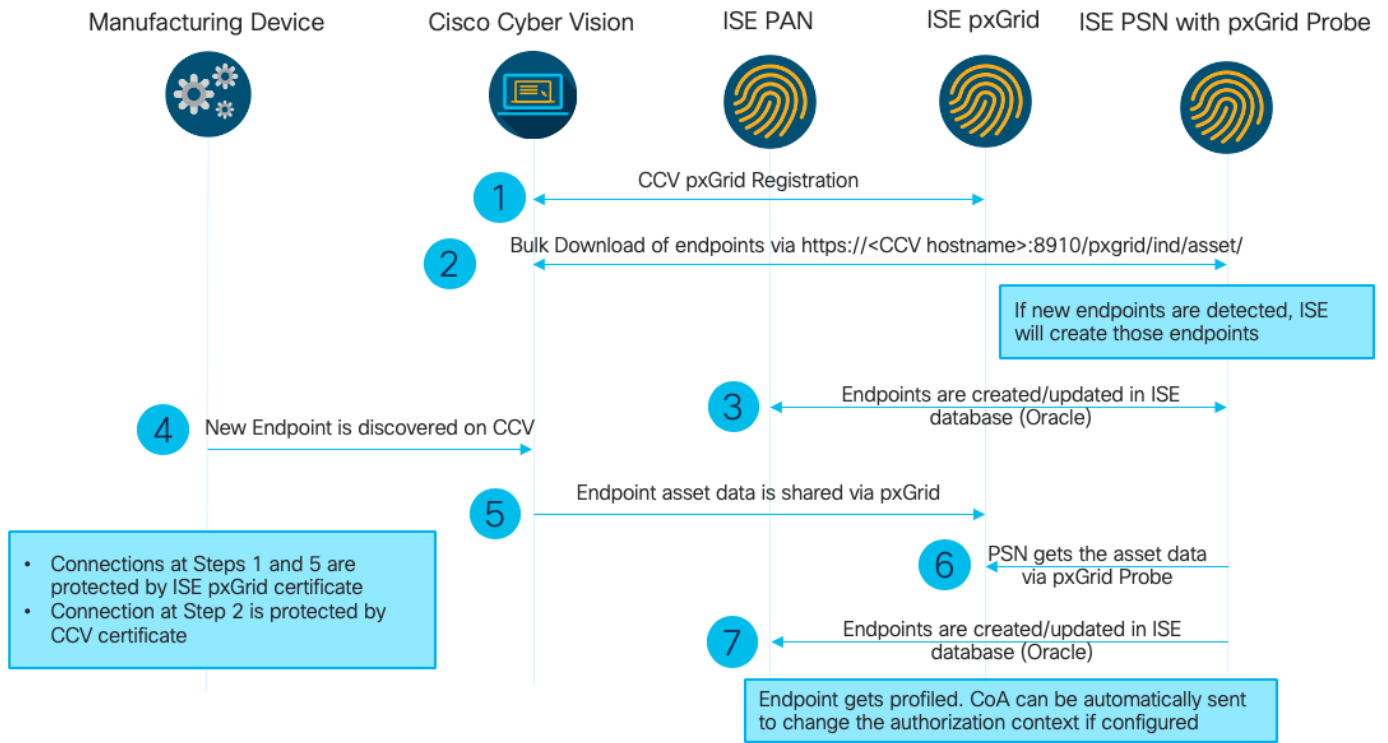
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ISEバージョン2.7パッチ1
- Cisco Cyber Visionバージョン3.1.0
- Industrial EthernetスイッチIE-4000-4TC4G-E(s/w 15.2(6)E)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

概要フロー図



このISE導入は、セットアップで使用されます。

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はプライマリ管理ノード(PAN)ノードおよびpxGridノードです。

ISE 2.7-2ekは、pxGridプローブが有効なポリシーサービスノード(PSN)です。

上記の図に対応する手順を次に示します。

1. pxGridバージョン2経由でISEのassetTopicにCCVが登録されます。CCVからの対応するログ：

注：CCVのpxGridログを確認するには、次のコマンドjournalctl -u pxgrid-agentを発行します。

```
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. pxGridプロンプトを有効にしたISE PSNは、既存のpxGridアセット(profiler.log)を一括ダウンロードします。

```
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.エンドポイントがpxGridプローブを有効にしてPSNに追加され、PSNはpersistイベントをPANに送信して、これらのエンドポイント(**profiler.log**)を保存します。ISEで作成されたエンドポイントは、[Context Visibility]の下のエンドポイントの詳細で表示できます。

```
2020-06-24 13:41:37,677 DEBUG [ProfilerINDSsubscriberBulkRequestPool-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 [ProfilerINDSsubscriberBulkRequestPool-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 [ProfilerINDSsubscriberBulkRequestPool-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 [ProfilerINDSsubscriberBulkRequestPool-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.エンドポイントをグループに配置した後、CCVはポート8910経由でSTOPメッセージを送信し、カスタム属性のグループデータを使用してエンドポイントを更新します。CCVからの対応するログ:

```
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ノードはSTOP更新を受信し、このメッセージをすべての加入者に転送します。これにはPxGridプロンプが有効なPSNが含まれます。PxGridノード上のpxgrid-server.log

```
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. pxGridプロンプが有効なPSNがアセットトピックのサブスクリバである場合、PxGridノードからメッセージを受信し、エンドポイント(**profiler.log**)を更新します。ISE上の更新されたエンドポイントは、[Context Visibility]の下のエンドポイントの詳細で表示できます。

```
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. pxGridプローブを有効にしたPSNは、新しいポリシーが一致したときにエンドポイントを再プロファイルします(**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
```

設定

注：assetGroupとContext Visibilityだけを表示したい場合でも、ステップ1～4が必要です。

1. PSNの1つでpxGridプローブを有効にする

[Administration] > [System] > [Deployment]に移動し、[ISE node with PSN Persona]を選択します。
[プロファイルの設定]タブに切り替えます。pxGridプローブが有効になっていることを確認します。

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. ISEでのエンドポイントカスタム属性の設定

[Administration] > [Identity Management] > [Settings] > [Endpoint Custom Attributes]に移動します。このイメージに従ってカスタム属性(assetGroup)を設定します。CCV 3.1.0はカスタム assetGroupアトリビュートのみをサポートします。

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: - +
 Reset Save

3.カスタム属性を使用したプロファイラポリシーの構成

[Work Centers] > [Profiler] > [Profiling Policies] に移動します。[Add] をクリックします。次の図に似たプロファイラポリシーを設定します。このポリシーで使用される条件式は **CUSTOMATTRIBUTE:assetGroup EQUALS Group1** です。

Profiler Policy List > ekornecyc_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:

Save Reset

4. プロファイル適用のカスタム属性の有効化

[Work Centers] > [Profiler] > [Profiling Policies] に移動します。[Add] をクリックします。次の図に似たプロファイルポリシーを設定します。プロファイル適用のカスタム属性の有効化が有効になっていることを確認します。

The screenshot shows the 'Profiler Configuration' page in the Cisco Identity Services Engine. The left sidebar contains 'Profiler Settings' and 'NMAP Scan Subnet Exclusions'. The main content area includes the following settings:

- * CoA Type: Reauth (dropdown menu)
- Current custom SNMP community strings: ***** (with a 'Show' button)
- Change custom SNMP community strings: [text input] (For NMAP, comma separated.)
- Confirm changed custom SNMP community strings: [text input] (For NMAP, comma separated.)
- EndPoint Attribute Filter: Enabled ⓘ
- Enable Anomalous Behaviour Detection: Enabled ⓘ
- Enable Anomalous Behaviour Enforcement: Enabled
- Enable Custom Attribute for Profiling Enforcement: Enabled
- Enable profiling for MUD: Enabled
- Enable Profiler Forwarder Persistence Queue: Enabled
- Enable Probe Data Publisher: Enabled

At the bottom, there are 'Save' and 'Reset' buttons.

5. pxGridクライアントの自動承認の設定

[Administration] > [pxGrid Services] > [Settings]に移動します。[Automatically approve new certificate-based accounts]を選択し、[Save]をクリックします。この手順により、統合が完了したらCCVを承認する必要がなくなります。

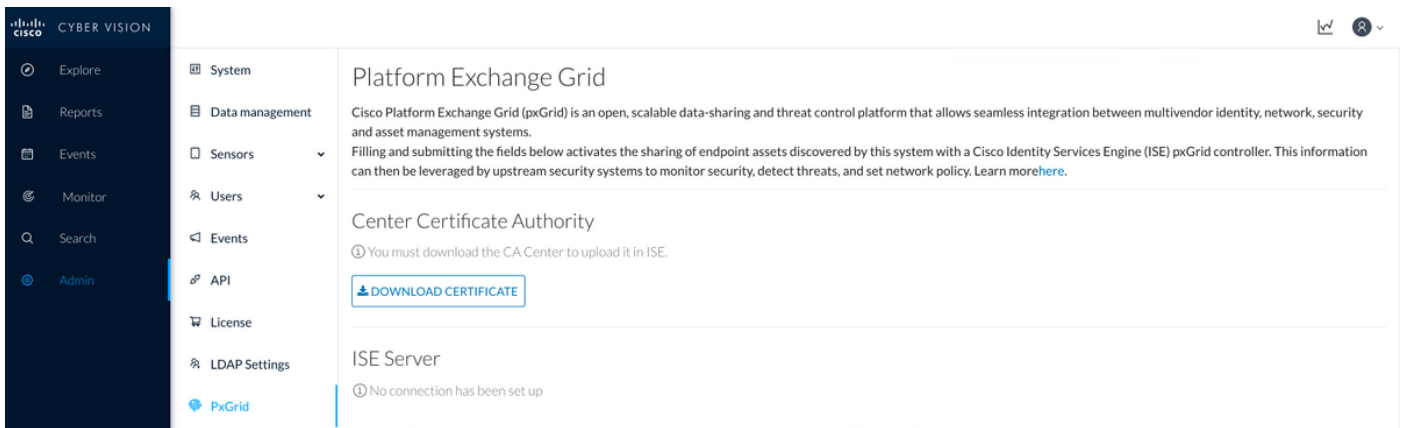
The screenshot shows the 'PxGrid Settings' page in the Cisco Identity Services Engine. The left sidebar contains 'All Clients', 'Web Clients', 'Capabilities', 'Live Log', 'Settings', 'Certificates', and 'Permissions'. The main content area includes the following settings:

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

At the bottom, there are 'Use Default' and 'Save' buttons.

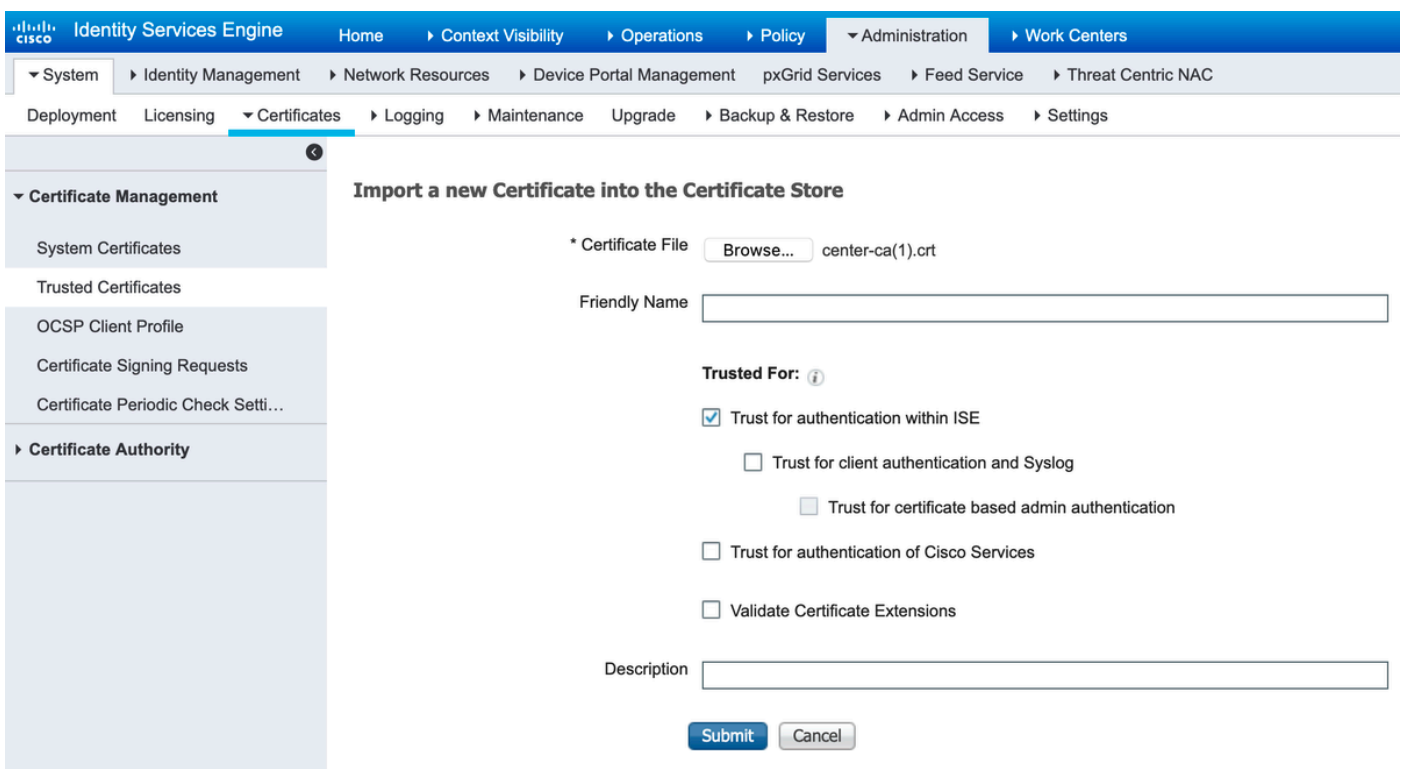
6. CCV証明書のエクスポート

[Admin] > [pxGrid]に移動します。[Download certificate] をクリックします。この証明書はpxGridの登録時に使用されるため、ISEはこれを信頼する必要があります。



7. CCV ID証明書のISE信頼ストアへのアップロード

[Administration] > [Certificates] > [Certificate Management] > [Trusted Certificates]に移動します。
 [インポート]をクリックします。[Browse]をクリックし、ステップ5からCCV証明書を選択します。
 。[Submit]をクリックします。



8. CCVの証明書の生成

pxGridの統合とアップデートの際、CCVにはクライアント証明書が必要です。
 PxGrid_Certificate_Templateを使用して、ISE内部CAから発行する必要があります。

[Administration] > [pxGrid Services] > [Certificates]に移動します。この図に従ってフィールドに入力します。ISE CAの目的はID証明書を発行することであるため、[Common Name (CN)]フィールドは必須です。CCVのホスト名を入力する必要があります。CNフィールドの値は重要です。CCVのホスト名を確認するには、hostnameコマンドを発行します。[Certificate Download Format]として[PKCS12]を選択します。

```
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) - +

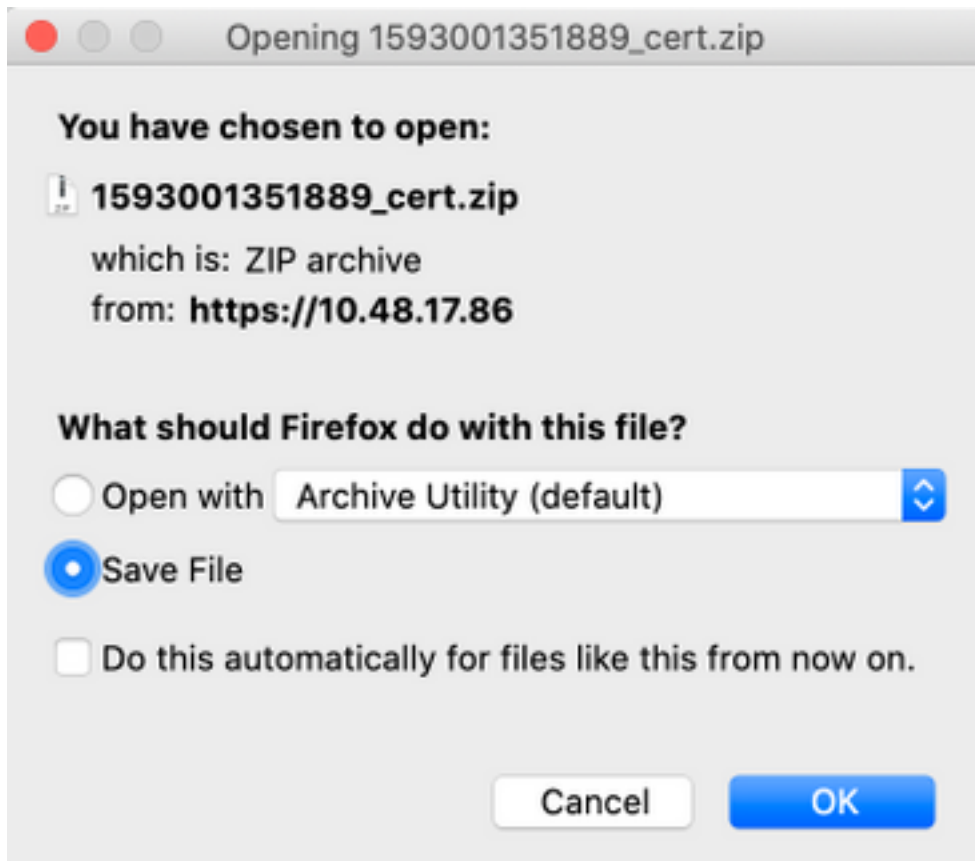
Certificate Download Format * ⓘ

Certificate Password * ⓘ

Confirm Password *

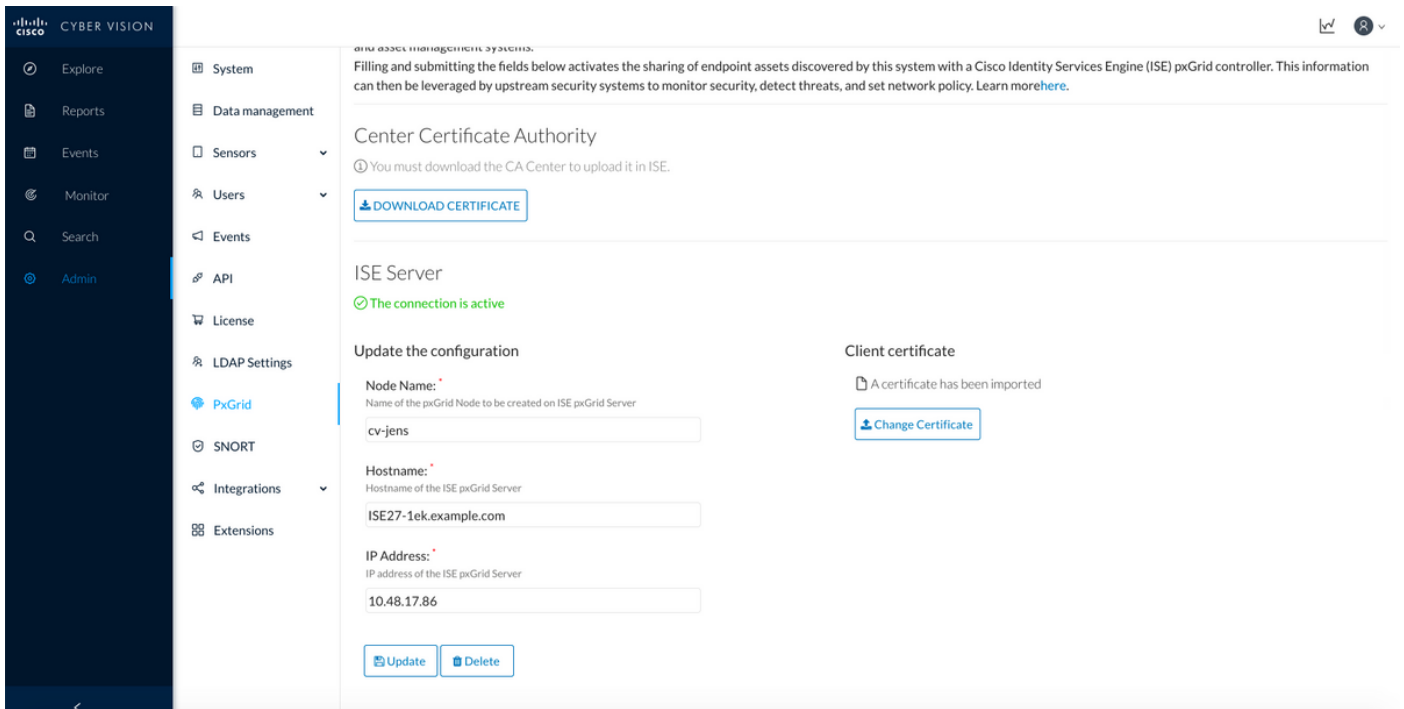
9. PKCS12形式での証明書チェーンのダウンロード

PKCS12形式で証明書をインストールすると、CCV ID証明書ISE内部CAチェーンとともにCCVにインストールされ、pxGrid通信がISEから開始されたときにCCVがISEを信頼します（pxGridキープアライブメッセージなど）。



10. CCVでのISE統合の詳細の設定

[Admin] > [pxGrid]に移動します。ノード名を設定します。この名前は、[Administration] > [pxGrid Services] > [Web Clients]で[Client Name]としてISEに表示されます。ISE pxGridノードのホスト名とIPアドレスを設定します。CCVがISE FQDNを解決できることを確認します。



11. CCVへの証明書チェーンのアップロードと統合の開始

[Admin] > [pxGrid]に移動します。[Change Certificate]をクリックします。ステップ8 ~ 9からISE CAによって発行された証明書を選択します。ステップ8のパスワードを入力し、[OK]をクリックします。

Do you want to enter a password?

●●●●●●●●

Ok Cancel

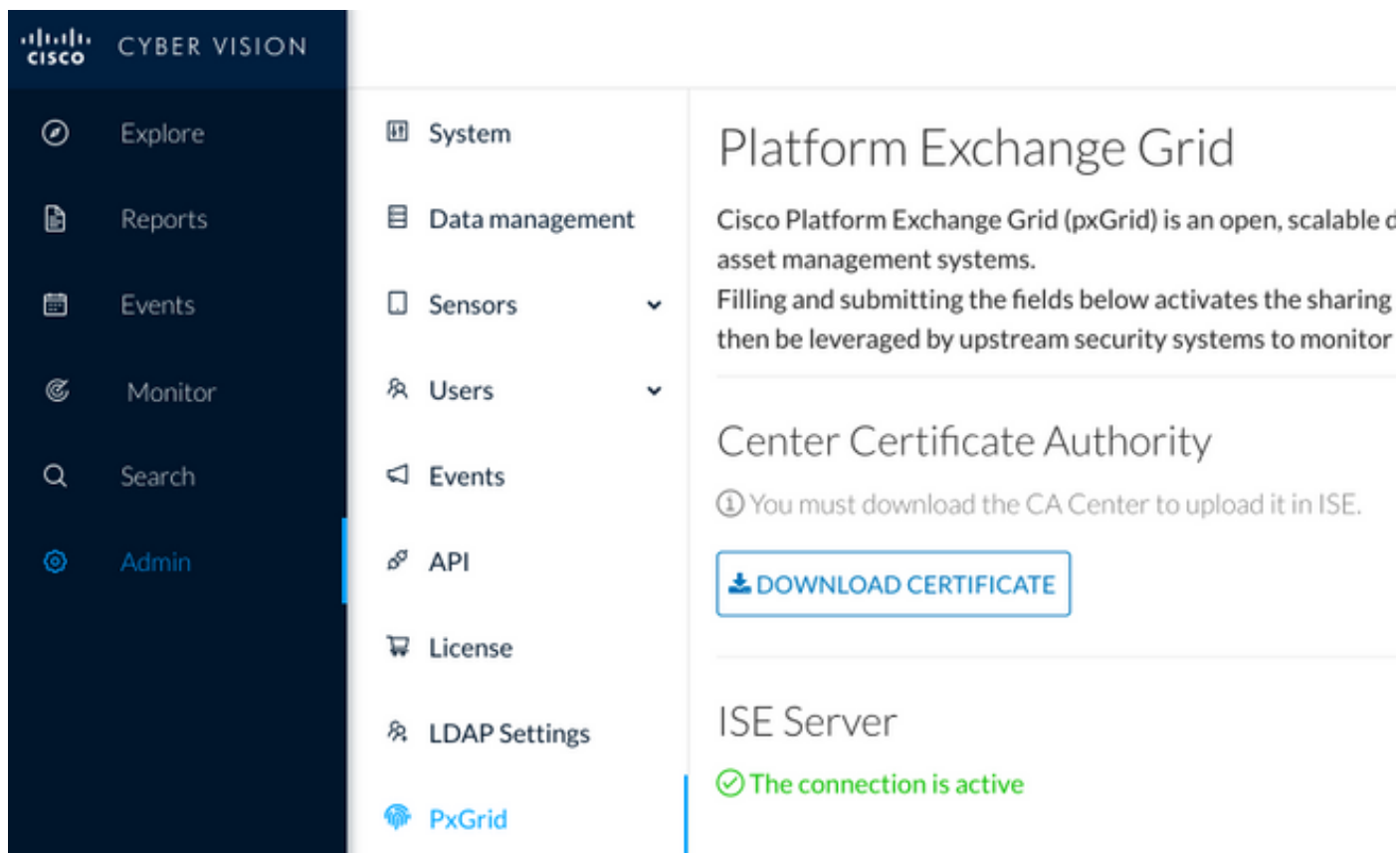
[Update]をクリックします。これにより、実際のCCV - ISE統合がトリガーされます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

CCV統合の検証

統合が完了したら、[Admin] > [pxGrid]の順に選択して、統合が正常に完了したことを確認できます。ISEサーバの下に「The connection is active」というメッセージが表示されます。



ISE統合の検証

[Administration] > [pxGrid Services] > [Web Clients]に移動します。CCVクライアント(cv-jens)のステータスがONであることを確認します。

注：CCV pxGridクライアントのステータスは、[すべてのクライアント(All Clients)]メニューで[オフライン(Offline)]と表示されます。これは、pxGrid v1のステータスだけが表示されるためです。

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duration
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

注：CSCvt78208により、/topic/com.cisco.ise.endpoint.assetを持つCCVがすぐに表示されないため、最初の公開時にのみ表示されます。

CCVグループの変更の確認

[探索] > [すべてのデータ] > [コンポーネントリスト]に移動します。いずれかのコンポーネントをクリックし、グループに追加します。

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 list of 5 components. The component 'Cisco a0:3a:59' is selected, and a context menu is open over it, showing options to 'Add to group', 'Create a new group', 'Group1', and 'Group2'. The component details panel on the right shows information for 'Cisco a0:3a:59', including IP, MAC, and activity tags.

/topic/com.cisco.ise.endpoint.assetがCCVに対するパブリケーションとしてリストされていることを確認します。

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

CCVを介して割り当てられたGroup1がISEに反映され、[Context Visibility] > [Endpoints]に移動してプロファイリングポリシーが有効になったことを確認します。前の手順で更新したエンドポイントを選択します。[Attributes]タブに切り替えます。カスタム属性セクションには、新しく設定されたグループが反映されている必要があります。

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
×	<input type="text" value="Attribute String"/>	<input type="text" value="Attribute Value"/>
	assetGroup	Group1

その他のアトリビュート(Attributes)セクションには、CCVから受信した他のすべてのアセットアトリビュートがリストされます。

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

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ISEでのデバッグの有効化

ISEでデバッグを有効にするには、[Administration] > [System] > [Logging] > [Debug Log Configuration]に移動します。ログレベルを次のように設定します。

ペルソナ	コンポーネント名	ログレベル	チェックするファイル
PAN (オプション)	プロファイラ	デバッグ	profiler.log
pxGridプローブが有効なPSN	プロファイラ	デバッグ	profiler.log
pxGrid	pxgrid	トレース	pxgrid-server.log

CCVでのデバッグの有効化

CCVでデバッグを有効にするには、次の手順を実行します。

- touch /data/etc/sbs/pxgrid-agent.confコマンドを使用して、ファイル/data/etc/sbs/pxgrid-agent.confを作成します
- この内容をpxgrid-agent.confファイルに貼り付けるには、vi /data/etc/sbs/pxgrid-agent.confコマンドでviエディタを使用します

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

- systemctl restart pxgrid-agentコマンドを実行して、pxgrid-agentを再起動します
- journalctl -u pxgrid-agentコマンドを使用してログを表示する

一括ダウンロードの失敗

CCVは、統合時に一括ダウンロードURLをISEに公開します。pxGridプロンプトが有効なISE PSNは、このURLを使用して一括ダウンロードを実行します。次の点を確認します。

- URLのホスト名は、ISEの観点から正しく解決できます
- ポート8910のPSNからCCVへの通信が許可される

pxGridプロンプトが有効になっているPSNのprofiler.log:

```
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}]]
CSCvt75422が原因で一括ダウンロードが失敗する場合があります、ISEのprofiler.logにこのエラーが表示され、確認できます。この不具合はCCV 3.1.0で修正されています。
```

```
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)
```

すべてのエンドポイントがISEで作成されるわけではありません

CCV上の一部のエンドポイントにアタッチされている属性が多すぎるため、ISEデータベースでは処理できません。ISEのprofiler.logに次のエラーが表示される場合に確認できます。

```
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がISEで使用できない

AssetGroupがISEで使用できない場合、ほとんどの場合、プロファイルポリシーはカスタム属性を使用して設定されていません (ドキュメントの「設定」の部分のステップ2 ~ 4を参照)。コンテキストの可視性の場合でも、グループ属性、プロファイリングポリシー、およびその他の設定をステップ2 ~ 4で表示する必要があります。

エンドポイントグループの更新がISEに反映されない

CSCvu80175が原因では、統合の直後にCCVがリポートするまで、CCVはエンドポイントのアップデートをISEに公開しません。統合が完了したら、CCVをリポートできます。

CCVからグループを削除してもISEからグループを削除できない

この問題は、CCV [CSCvu47880](#)の既知の不具合が原因で発生します。予期された形式と異なるCCVからのグループの削除時にpxGridアップデートが送信されるため、グループは削除されません。

WebクライアントからのCCVドロップ

この問題は、ISE [CSCvu47880](#)の既知の不具合で、クライアントがOFF状態に移行した後、Webクライアントから完全に削除された場合に発生します。この問題は、ISEの2.6パッチ7および2.7パッチ2で解決されています。

ISEのpxgrid-server.logに次のエラーが表示された場合は、このエラーを確認できます。

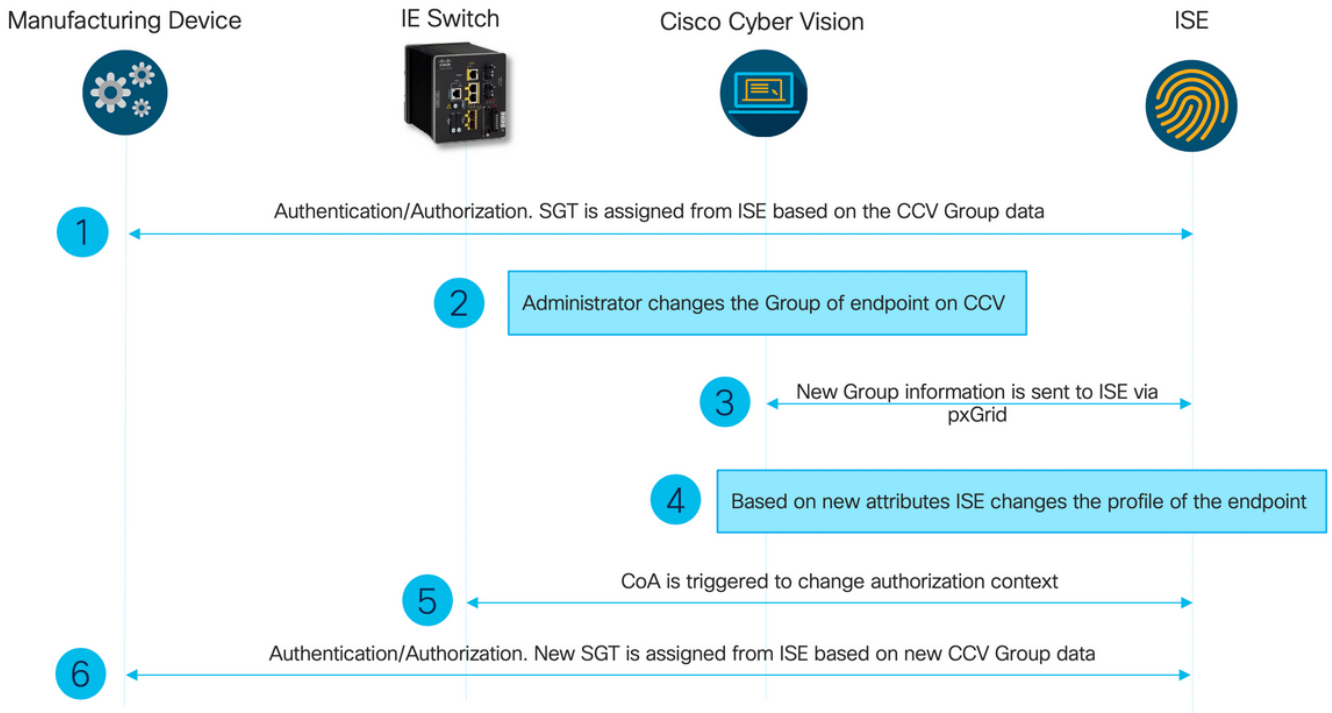
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionId=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726,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

CCV TrustSecによるISE統合の使用例

この設定は、TrustSecが導入されている場合に、ISEとCCVの統合がエンドツーエンドのセキュリティにどのように役立つかを示します。これは、統合が完了した後の統合方法の例の1つにすぎません。

注：TrustSecスイッチの設定の説明は、この記事の範囲外ですが、付録で確認できます。

トポロジとフロー



設定

1. ISEでのスケーラブルグループタグの設定

前述の使用例を達成するために、TrustSecタグのIOT_Group1_AssetおよびIOT_Group2_Assetは、それぞれGroup1 CCVアセットをGroup2と区別するように手動で設定されています。[ワークセンター]> [TrustSec]> [コンポーネント]> [セキュリティグループ]に移動します。[Add] をクリックします。図に示すように、SGTに名前を付けます。

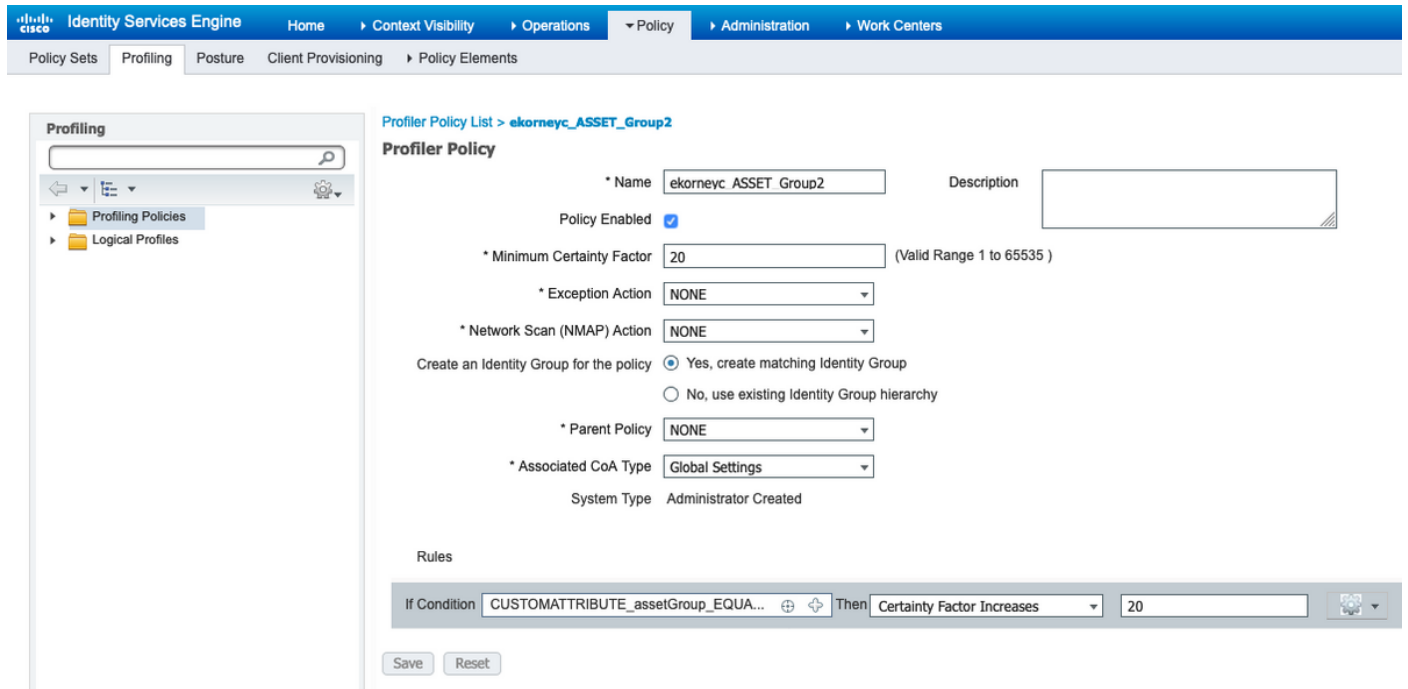
Icon	Name	SGT (Dec / Hex)	Description	Learned from
	Auditors	9/0009	Auditor Security Group	
	BYOD	15/000F	BYOD Security Group	
	Contractors	5/0005	Contractor Security Group	
	Developers	8/0008	Developer Security Group	
	Development_Servers	12/000C	Development Servers Security Group	
	Employees	4/0004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

2. グループ2のカスタム属性を使用したプロファイルポリシーの設定

注：グループ1のプロファイル設定は、ドキュメントの最初の部分のステップ3で行いまし

た。

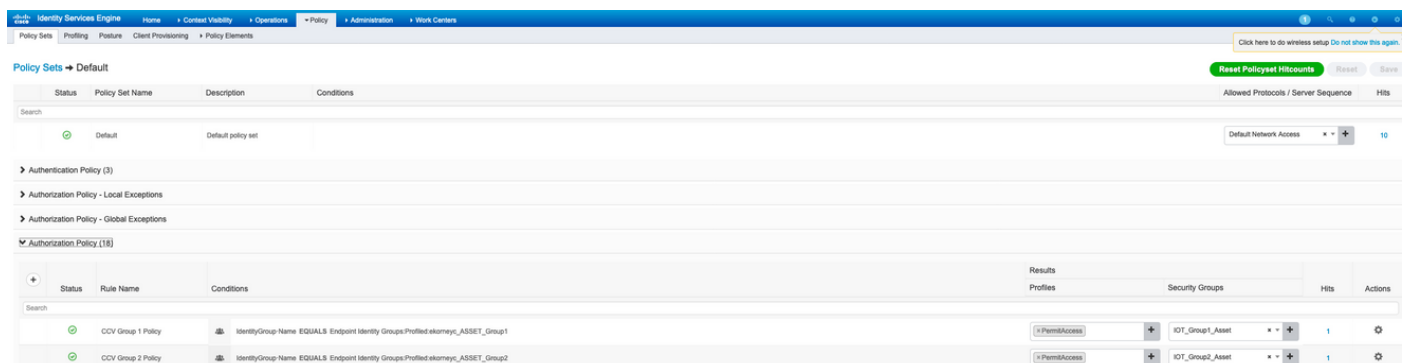
[Work Centers] > [Profiler] > [Profiling Policies] に移動します。[Add] をクリックします。次の図に似たプロファイルポリシーを設定します。このポリシーで使用される条件式は **CUSTOMATTRIBUTE:assetGroup EQUALS Group2** です。



3. ISE上のエンドポイントIDグループに基づいてSGTを割り当てる認可ポリシーの設定

[Policy] > [Policy Sets]に移動します。ポリシーセットを選択し、このイメージに従って認可ポリシーを設定します。その結果、ステップ1.で設定したSGTが割り当てられることに注意してください。

ルール名	条件	プロファイル	セキュリティグループ
CCVグループ1ポリシー	IdentityGroup・ Name EQUALSエンドポイント IDグループ : プロファイル : ekorneyc_ASSET_Group1	PermitAccess	IOT_Group1_Asset
CCVグループ2ポリシー	IdentityGroup・ Name EQUALSエンドポイント IDグループ : プロファイル : ekorneyc_ASSET_Group2	PermitAccess	IOT_Group2_Asset



確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. CCVグループ1に基づいてエンドポイントを認証

スイッチでは、環境データにSGTの16-54:IOT_Group1_Assetと17-54:IOT_Group2_Assetの両方が含まれていることがわかります。

```
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#
```

エンドポイントが認証され、その結果、CCV Group 1 Policyが一致し、SGT IOT_Group1_Assetが割り当てられます。

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

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	00:F2:8B:A0:3A:59	00:F2:8B:A0:3A:59	ekomeyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermitAccess	172.16.0.100
Jun 25, 2020 10:37:31.567 AM	■			00:F2:8B:A0:3A:59	00:F2:8B:A0:3A:59	ekomeyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermitAccess	172.16.0.100

スイッチのshow authentication sessions interface fa1/7 detailは、Access-Acceptデータが正常に適用されたことを確認します。

```
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
```

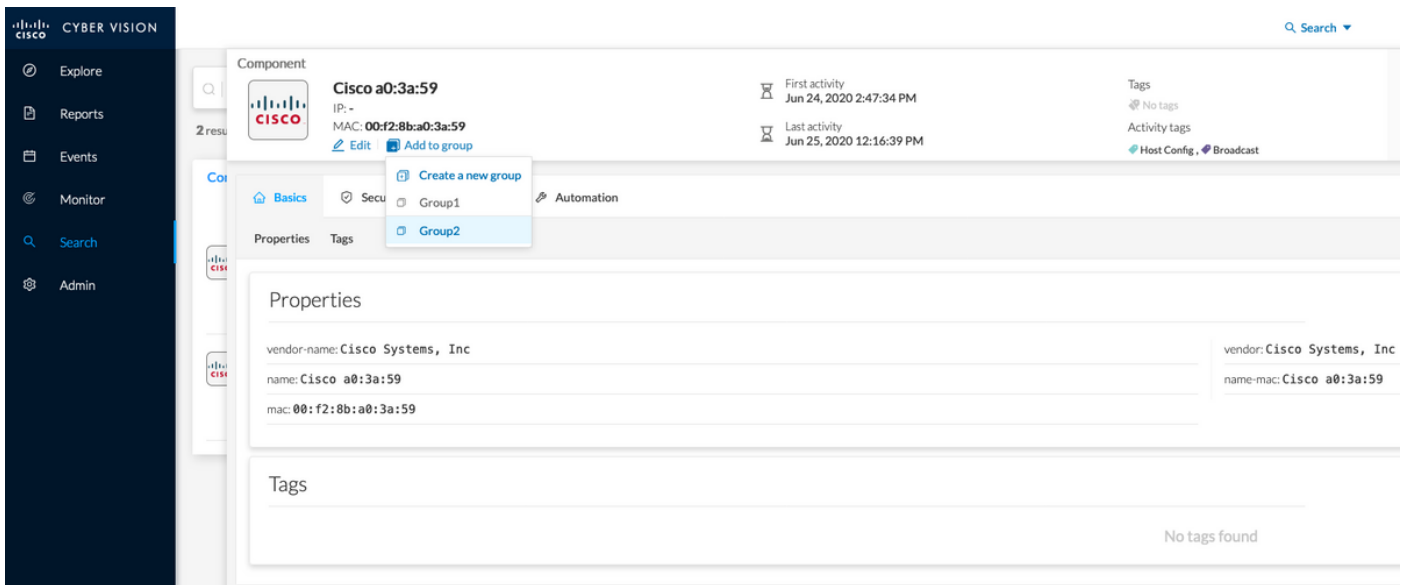
mab Authc Success

```
KJK_IE4000_10#
```

2.管理者によるグループの変更

[検索]にナビゲートします。エンドポイントのMACアドレスを貼り付け、クリックしてグループ2に追加します。

注：CCVでは、グループを1回で1から2に変更することはできません。したがって、まずグループからエンドポイントを削除し、次にグループ2を割り当てる必要があります。



3-6.エンドポイントグループ変更のCCVへの影響

手順4.、5.、および6.はこのイメージに反映されます。プロファイリングにより、エンドポイントは手順4で確認したアイデンティティグループをekorneyc_ASSET_Group2に変更しました。これにより、ISEはスイッチにCoAを送信し（手順5）、最後にエンドポイントの再認証を行いました（手順6）。

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Profile	Authentication Pol.	Authorization Policy	Authorization Profiles	IP Address	Network Device	Device Port	Identity Group
Jun 25, 2020 10:43:00.411 AM	●		0	00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_AssetPermitAccess	172.16.0.100	FastEthernet1/7		
Jun 25, 2020 10:42:59.503 AM	●		0	00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy	IOT_Group2_AssetPermitAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group2
Jun 25, 2020 10:42:59.482 AM	●		0	00F28BAC3A59	00F28BAC3A59	ekorneyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy	IOT_Group1_AssetPermitAccess	172.16.0.100	E-4000	FastEthernet1/7	ekorneyc_ASSET_Group1

スイッチのshow authentication sessions interface fa1/7 detailは、新しいSGTが割り当てられていることを確認します。

```
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#

付録

スイッチTrustSec関連の設定

注：Ctsクレデンシャルはrunning-configの一部ではなく、特権EXECモードでcts credentials id <id> password <password>コマンドを使用して設定する必要があります。

```
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#