McAfee Data Exchange Layer(DXL) Broker and Cisco Platform Exchange Grid (pxGrid) Integration using Cisco Identity Services Engine (ISE)

Authors: John Eppich, Cisco, Kris Leonard, McAfee, Jagathish Poornalingam, McAfee

Table of Contents

About this Document

This document is for Cisco Engineers, McAfee Engineers, partners and customers deploying McAfee Data Exchange Layer (DXL) Broker 4.0., McAfee ePolicy Orchestrator (ePO 5.9) with Cisco Platform Exchange Grid (pxGrid) using Cisco Identity Services Engine (ISE 2.3).

This document illustrates the steps required to configure the use cases below.

This document also includes the following use cases:

- An Eicar Virus is detected on the endpoint, McAfee ePO generates an automated response where the McAfee DXL broker triggers an ISE pxGrid Adaptive Network Control (ANC) mitigation action, quarantining the endpoint in ISE.

  This is a basic use case and illustrates the integration between McAfee DXL broker and Cisco ISE pxGrid node.

- The McAfee DXL broker python client receives ISE ANC "quarantined policy" notifications through Cisco pxGrid and McAfee ePO assigns a policy tag of "quarantined" to the endpoint when a violation in the ISE ANC policy occurs. Once this endpoint has been tagged by McAfee ePO, McAfee ePO can take manual action as defied by the McAfee ePO admin.

  This use case is more advanced and is optional.

- The endpoint does not have the McAfee agent installed, ISE posture will detect this, and deem the endpoint non-compliant. A remediation link will be provided to the end-user via ePO to download and install the application. Once ISE detects that the McAfee ePO is installed, the endpoint is now compliant and granted full network access.

  This use case is more advanced and is optional

- An employee-owned laptop goes through the organization's on-boarding process to satisfy the organization's BYOD initiative. The EPO admin can then install on the endpoint centrally or manually by the by the end-user.

  This use case is more advanced and is optional

It is assumed that McAfee ePO 5.9 along with the Cisco pxGrid extensions, McAfee DXL broker 4.0, and Cisco ISE 2.3 are installed. If running Cisco ISE versions 2.0 through 2.2 please refer to the References sections to configure ISE authorization and IS ANC policies. These policies are GUI driven in ISE 2.3.

Cisco ISE is installed in a stand-alone deployment. If ISE is installed in a productional environment, please see *How to Configure pxGrid in ISE Production Environments* under References.

There is also a McAfee KB article available for integrating McAfee DXL with other versions of Cisco ISE: *How to Use Data Exchange Layer with Cisco Platform Exchange Grid (pxGrid* under References. Also there are additional references to configuring Cisco pxGrid with different versions of ISE under References.

Solution Overview

McAfee ePolicy Orchestrator (ePO) centrally manages endpoints, networks, data and compliance solutions. McAfee ePolicy is the foundation of the McAfee Security Management Solution. McAfee ePolicy Orchestrator provides multiple views and configuration into the deployment process of the McAfee Solutions and endpoint management. It provides a streamlined approach for deploying McAfee software.

The McAfee Data Exchange Layer (DXL) broker uses a DXL communication fabric and provides for an adaptive ecosystem by allowing a real-time, bidirectional communications fabric allowing connected security solutions to share relevant data between endpoints, network and other security systems. The McAfee DXL broker is managed through McAfee EPO. DXL clients that want to communicate over the DXL fabric must be registered and authorized by the McAfee DXL broker. DXL clients can subscribe to published services to access Topics of information.

Cisco Identity Services Engine (ISE) is a security policy management and identity access management solution. ISE provides centralized management of IEEE 802.1X authentications, gust management, posture, client provisioning and TrustSec policies.
ISE also simplifies access control and security compliance for wired, wireless, and VPN connectivity and supports corporate security policy initiatives such as BYOD.

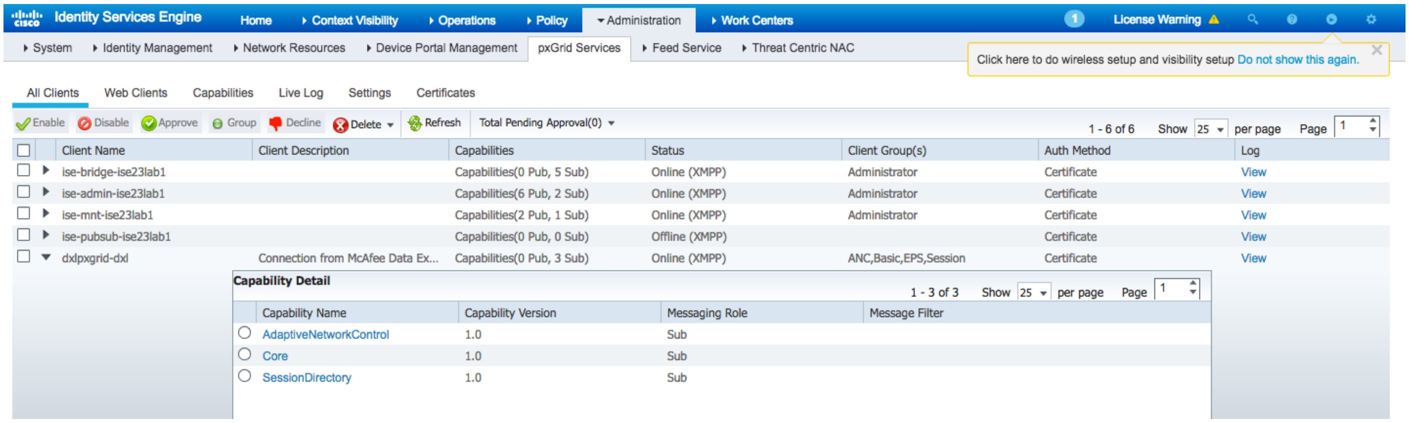
Cisco Platform Exchange Grid (pxGrid) enables multivendor, cross platform network system collaboration among parts of the IT infrastructure such as security monitoring and system detection, network policy platforms, asset and virtually configuration management identity and access management platforms and other IT solutions. pxGrid uses a pub/sub model to publish the contextual information from ISE. pxGrid clients connect and register to the ISE pxGrid node and subscribe to these session topics.   pxGrid also provides the ability for pxGrid client solutions to enforce their security policies by enforcing Adaptive Network Control (ANC) mitigation actions.

Technical Details

All DXL clients or McAfee ecosystem partners connect to the McAfee DXL broker using certificates for mutual authentication, likewise, do all of the pxGrid clients or Cisco ecosystem partners connect to the ISE pxGrid node.

Starting with Cisco ISE 2.1, you can use the ISE internal CA to generate certificates for both the McAfee DXL broker and the Cisco ISE pxGrid node. In this document we will be using Cisco ISE 2.3 and the ISE internal CA for generating the certificates. Once the DXL broker certificates have been generated, the public private key-pair will be uploaded into the McAfee DXL broker's keystore. The ISE internal root certificate will be uploaded into the McAfee DXL broker's rootstore. The ISE pxGrid node, will have the pxGrid signed by the ISE internal CA as default. (*This occurs in ISE 2.2 and above)*

The Cisco ISE pxGrid node contains session information from authenticated ISE sessions and provides the McAfee DXL broker with the ability to perform Adaptive Network Control (ANC) mitigation actions based on Threat Events detected on the endpoint by McAfee Security Product solutions such as McAfee EnterpriseVirusScan. These Threat Events are configured as part of ePO's Automatic Threat Response Policy. ANC mitigations actions are based on the ISE Adaptive Network Control polices and control network access and are based on an organization's security policy. ANC actions can be Quarantine, Port-Shut, or Terminate, where Quarantine can be configured to limit or monitor network access.

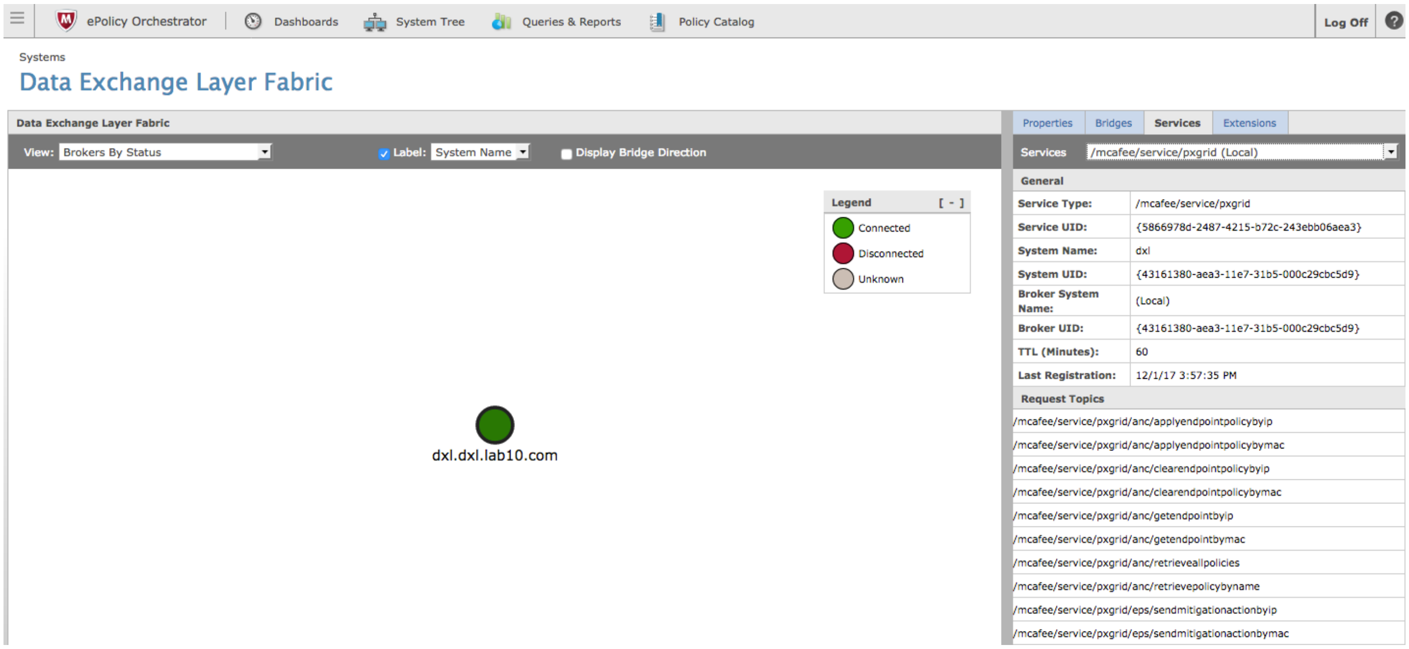


☐	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
☐	ise-bridge-ise23lab1		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-admin-ise23lab1		Capabilities(6 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-mnt-ise23lab1		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-pubsub-ise23lab1		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View
☐	dxlpxgrid-dxl	Connection from McAfee Data Ex...	Capabilities(0 Pub, 3 Sub)	Online (XMPP)	ANC,Basic,EPS,Session	Certificate	View

Capability Detail

	Capability Name	Capability Version	Messaging Role	Message Filter
○	AdaptiveNetworkControl	1.0	Sub	
○	Core	1.0	Sub	
○	SessionDirectory	1.0	Sub	

The McAfee DXL broker will be configured to query the ISE pxGrid node for performing Adaptive Network Control (ANC) mitigation actions, sending mitigation actions, and obtain endpoint information by MAC address or IP address. The McAfee broker will also be configured to receive ISE pxGrid notifications for subscribing to pxGrid sessions and ANC policy related notifications.   The ISE pxGrid ANC attributes can be seen under the DXL broker "Services" menu. These attributes constitute the ANC operations that are available in the ANC policies.



Data Exchange Layer Fabric

Data Exchange Layer Fabric

View: Brokers By Status ☑ Label: System Name □ Display Bridge Direction

Services: /mcafee/service/pxgrid (Local)

General

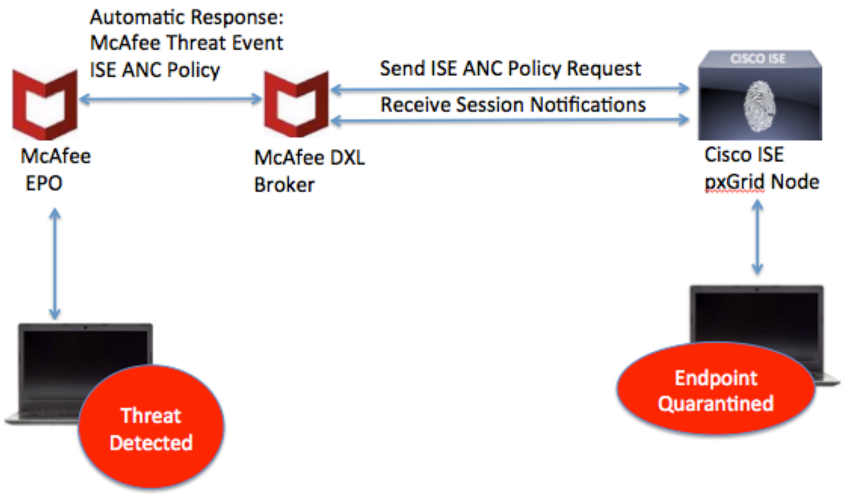
Service Type:	/mcafee/service/pxgrid
Service UID:	{5866978d-2487-4215-b72c-243ebb06aea3}
System Name:	dxl
System UID:	{43161380-aea3-11e7-31b5-000c29cbc5d9}
Broker System Name:	(Local)
Broker UID:	{43161380-aea3-11e7-31b5-000c29cbc5d9}
TTL (Minutes):	60
Last Registration:	12/1/17 3:57:35 PM

Request Topics

```
/mcafee/service/pxgrid/anc/applyendpointpolicybyip
/mcafee/service/pxgrid/anc/applyendpointpolicybymac
/mcafee/service/pxgrid/anc/clearendpointpolicybyip
/mcafee/service/pxgrid/anc/clearendpointpolicybymac
/mcafee/service/pxgrid/anc/getendpointbyip
/mcafee/service/pxgrid/anc/getendpointbymac
/mcafee/service/pxgrid/anc/retrieveallpolicies
/mcafee/service/pxgrid/anc/retrievepolicybyname
/mcafee/service/pxgrid/eps/sendmitigationactionbyip
/mcafee/service/pxgrid/eps/sendmitigationactionbymac
```

The McAfee DXL Broker and Cisco ISE pxGrid Workflow is as follows: a threat is detected on the endpoint, an Automatic Response Policy is configured on McAfee ePO and is triggered on the received threat event. This event is then sent to the McAfee DXL Broker, which then sends an ISE ANC policy request to the ISE pxGrid node for enforcement based on the organization's security policy. In the example below, the endpoint is quarantined based on the ISE ANC policy which is defined in the McAfee ePO Automatic Response Policy. The ISE authorization profiles determine network access. In the example below, the endpoint is quarantined and given limited network access based on the ISE authorization profile.

McAfee DXL Broker and ISE pxGrid Workflow



Cisco ISE Identity Service Engine Configuration

In this section, we enable pxGrid operation on ISE. Adaptive Network Control (ANC) Policies are also created that will be used to enforce mitigation actions on the endpoint, such as Quarantine, Shutdown and Port Bounce. These ANC policies will be used in McAfee's ePO when configuring the automated responses.

Since ISE 2.3 is used in this document, ANC policies are GUI driven. With versions of ISE 2.0 through 2.2, these policies will need to be created manually, please see https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_01100.html

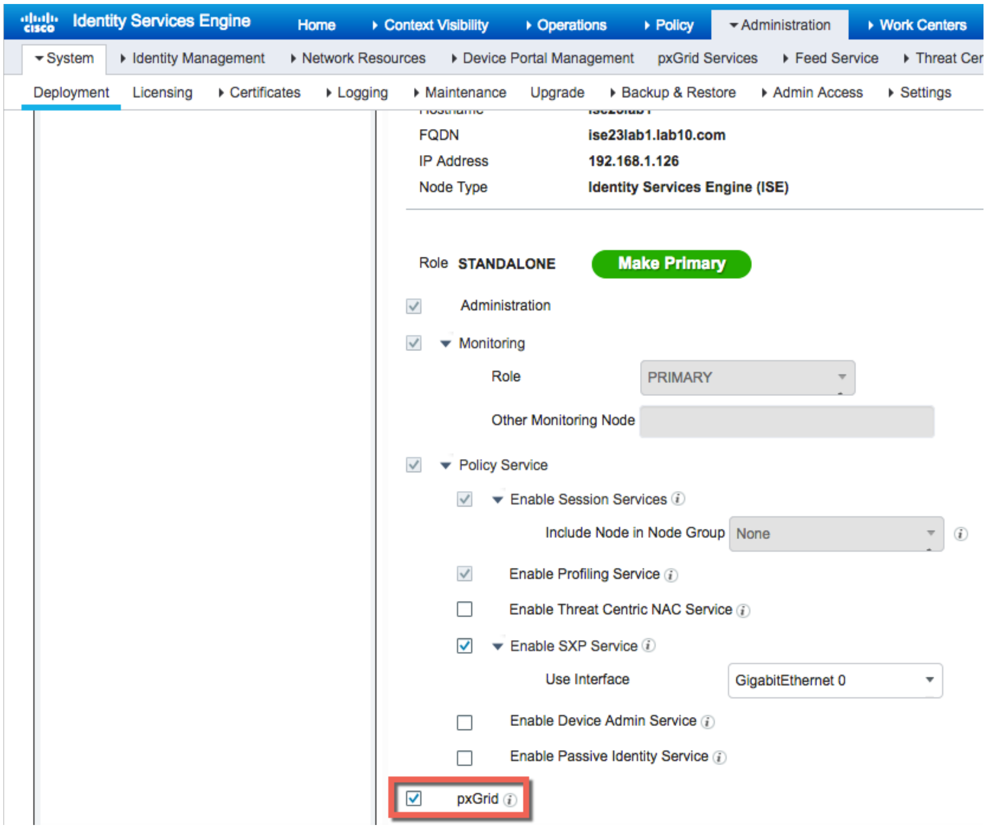
Enabling ISE pxGrid

The ISE pxGrid node needs to be enabled. Before enabling the ISE pxGrid node, it is required that all the necessary certificates have been installed. In this guide, we are using ISE 2.3, which includes the ISE internal Certificate. The pxGrid certificate is signed by the internal CA by default. The end-user will also use the ISE internal CA to create and generate the Certificates for the McAfee DXL broker.

If you are using Cisco ISE 2.0/2.1/2.2, please see refer to the appropriate Certificate Guides under References

Note: If this is a productional ISE deployment or using an external CA server, please see *How to Configure in an ISE Production Environment* under References. In this example, we will use the ISE internal CA only.

Step 1 Select **Administration->System->Deployment->edit the ISE node->enable pxGrid**



FQDN ise23lab1.lab10.com

IP Address 192.168.1.126

Node Type Identity Services Engine (ISE)

Role STANDALONE

☑ Administration

☑ Monitoring

Role PRIMARY

Other Monitoring Node

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

☑ Enable SXP Service

Use Interface GigabitEthernet 0

□ Enable Device Admin Service

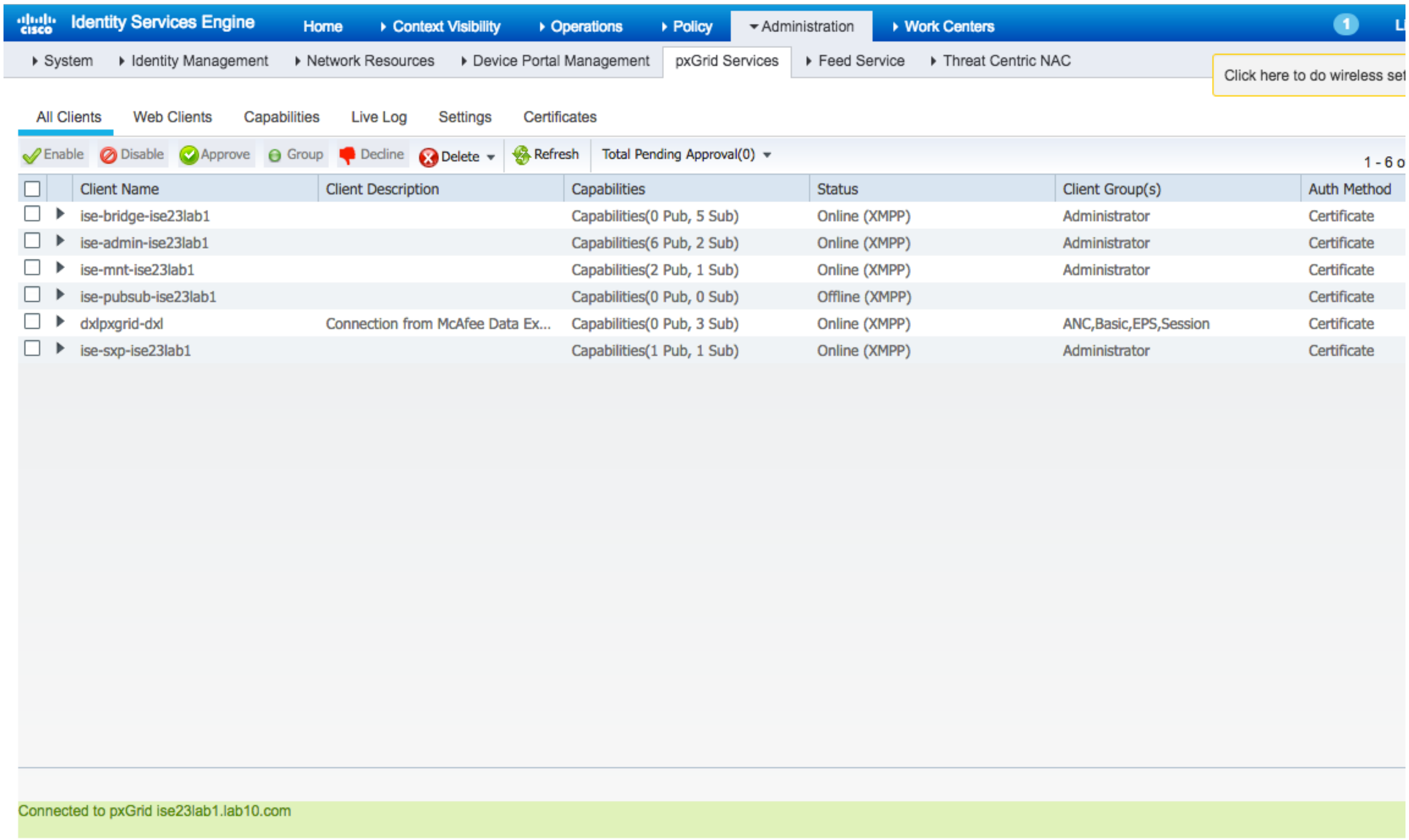
□ Enable Passive Identity Service

☑ pxGrid

Step 2 Select **Save**

Step 3 Select **Administration->pxGrid Services** and verify that the pxGrid published nodes appear and that there is pxGrid node connectivity

Note: In the screenshot below, the McAfee DLX broker (i.e. dxlpxgrid-dxl) client has already registered.



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
□	▸	ise-bridge-ise23lab1		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate
□	▸	ise-admin-ise23lab1		Capabilities(6 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate
□	▸	ise-mnt-ise23lab1		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate
□	▸	ise-pubsub-ise23lab1		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
□	▸	dxlpxgrid-dxl	Connection from McAfee Data Ex...	Capabilities(0 Pub, 3 Sub)	Online (XMPP)	ANC,Basic,EPS,Session	Certificate
□	▸	ise-sxp-ise23lab1		Capabilities(1 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate

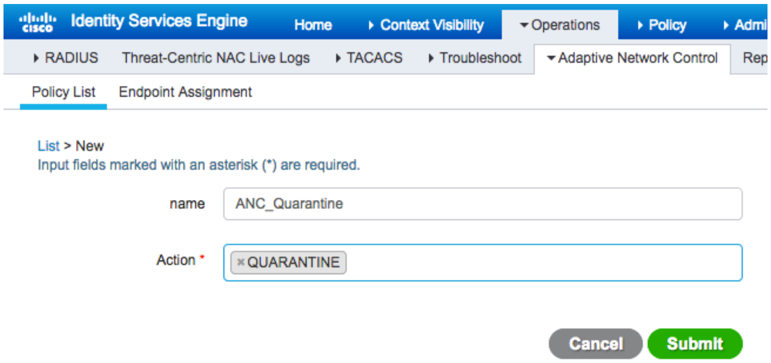
Connected to pxGrid ise23lab1.lab10.com

Configuring Adaptive Network Control (ANC) Policies

These ANC policies provide mitigative actions such as Quarantine, Port Bounce and Shutdown. It is important to note that quarantine is simply a Change of Authorization (CoA) on a switch and is defined by the authorization profile. For example, if you do no not want to enforce any actions by limiting network access, a Cisco Security Group Tag of Quarantine can be applied, so the action is monitored in ISE.

Creating ISE ANC Policies

Step 1 Select **Operations->Adaptive Network Control->Policy List->Add**



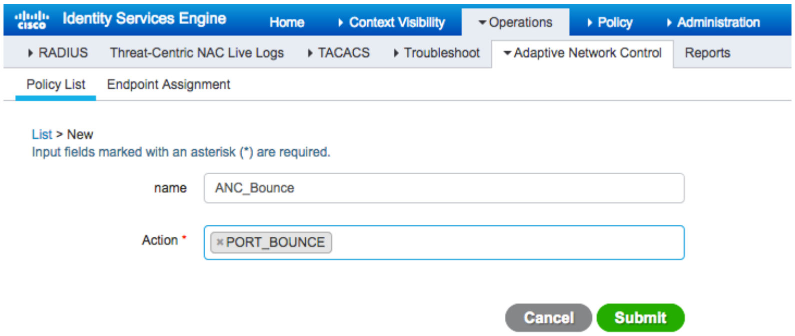
List > New
Input fields marked with an asterisk (*) are required.

name: ANC_Quarantine

Action *: QUARANTINE

Step 2 Select **Submit**

Step 3 Select **Operations->Adaptive Network Control->Policy List->Add**



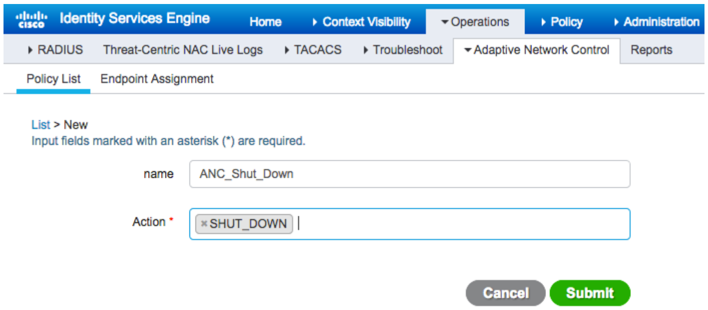
List > New
Input fields marked with an asterisk (*) are required.

name: ANC_Bounce

Action *: PORT_BOUNCE

Step 4 Select **Submit**

Step 5 Select **Operations->Adaptive Network Control->Policy List->Add**

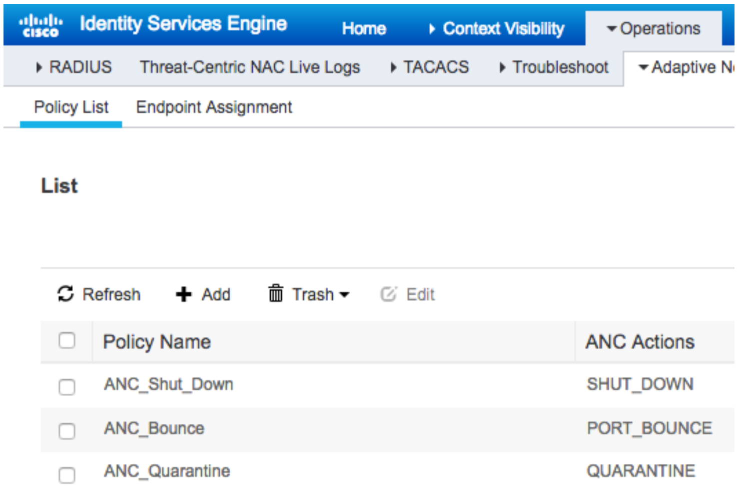


List > New
Input fields marked with an asterisk (*) are required.

name: ANC_Shut_Down

Action *: SHUT_DOWN

Step 6 Select **Submit**
You should see:



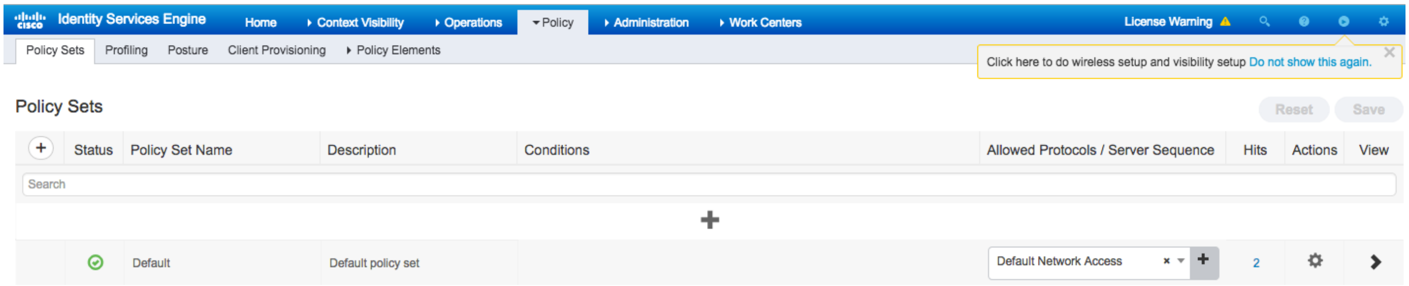
List

□	Policy Name	ANC Actions
□	ANC_Shut_Down	SHUT_DOWN
□	ANC_Bounce	PORT_BOUNCE
□	ANC_Quarantine	QUARANTINE

Adding ISE ANC Policies to Authorization Policy

The Policy Sets in ISE 2.3 and above reflect the Authorization policy. From ISE 2.0 through these would be added directly to the authorization policy, please see: https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010011.html

Step 1 Select **Policy->Policy Sets**
You should see:

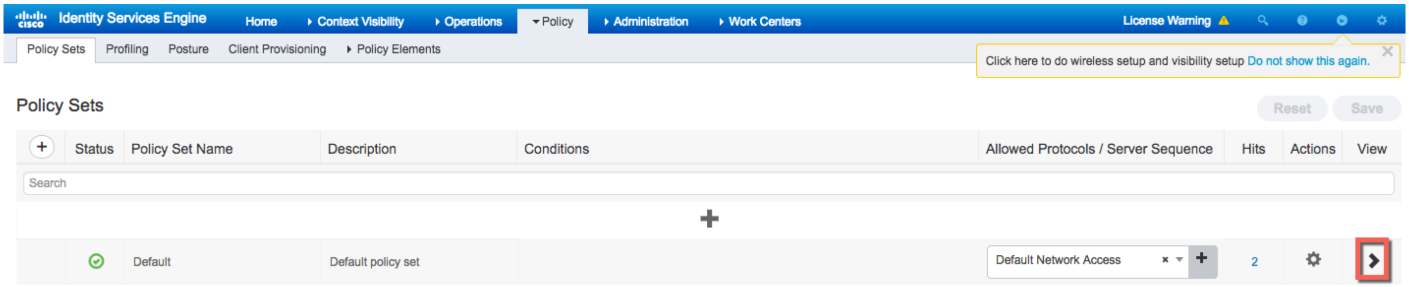


Click here to do wireless setup and visibility setup Do not show this again.

Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	✓	Default	Default policy set		Default Network Access	2	⚙	>

Step 2 Select " >" below

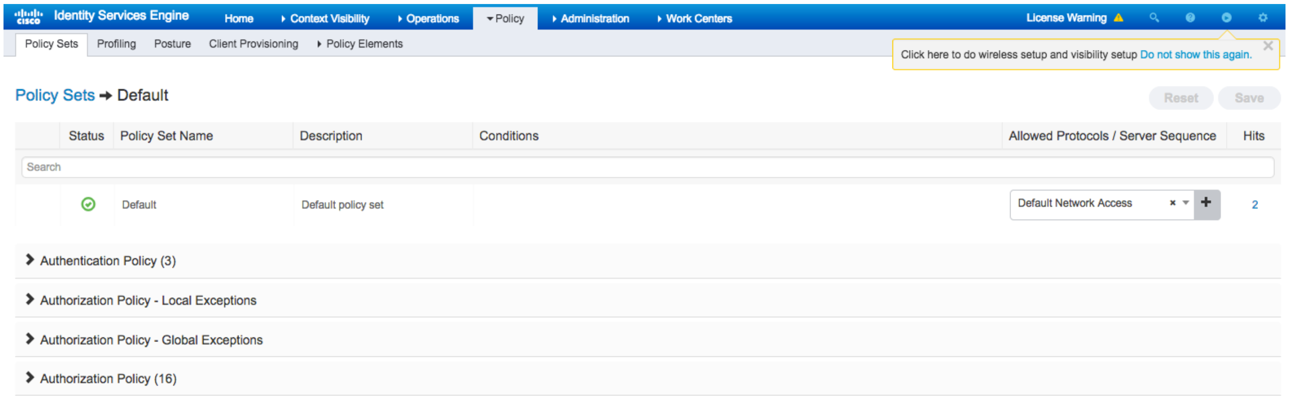


Click here to do wireless setup and visibility setup Do not show this again.

Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	✓	Default	Default policy set		Default Network Access	2	⚙	>

You should see:

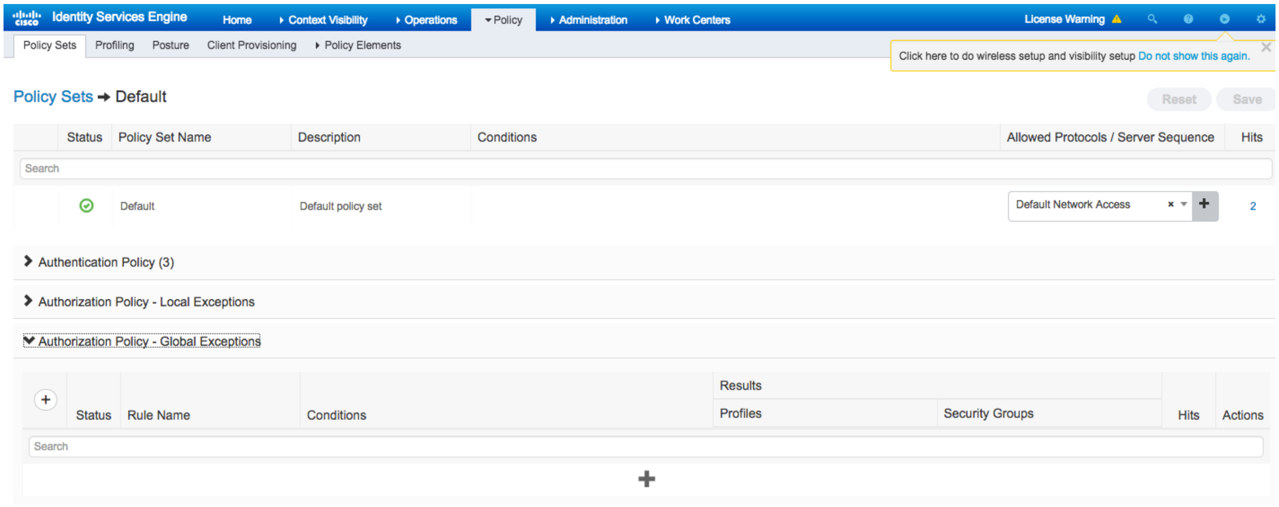


Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	2

- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (16)

Step 3 Select **Authorization Policy –> Global Exceptions**
You should see:



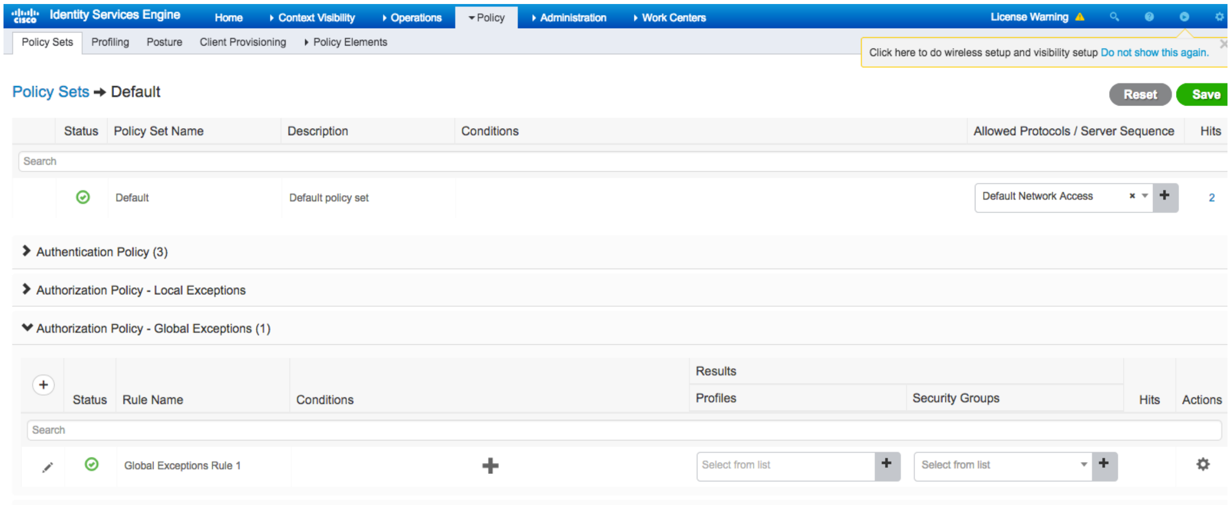
Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	2

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

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions

Step 4 Select "+""
You should see:



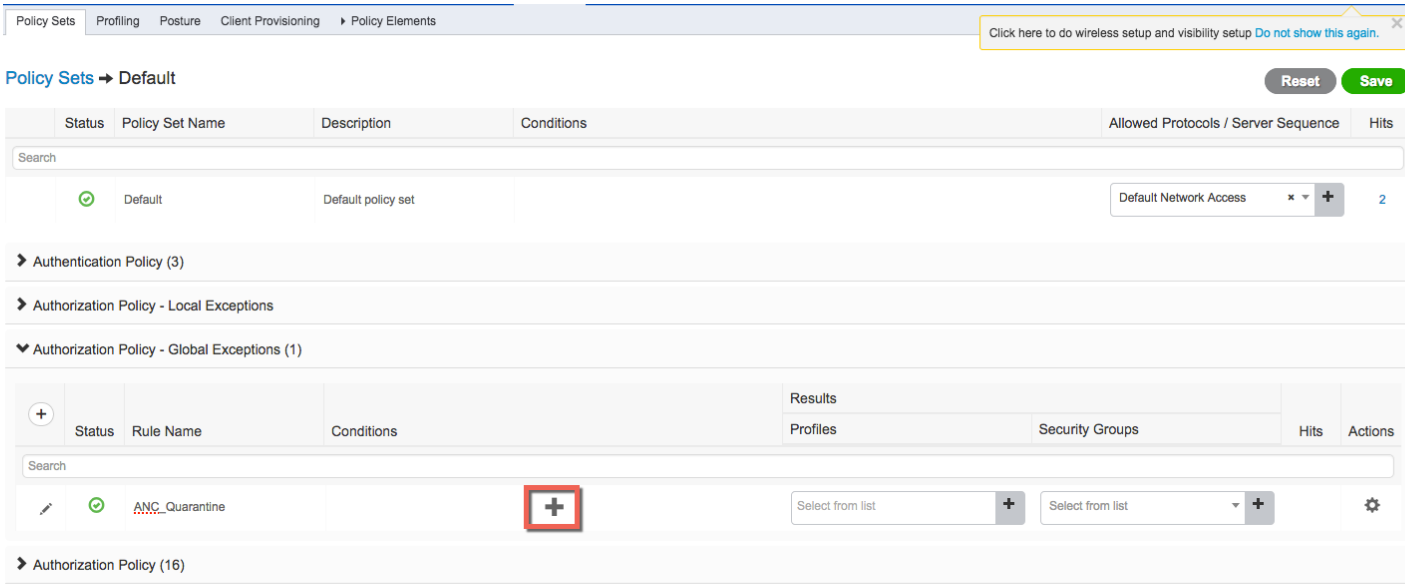
Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	2

- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions (1)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	Global Exceptions Rule 1	+	Select from list	Select from list		

Step 5 Under **"Rule Name"** type **ANC_Quarantine**, select **"+"**


Policy Sets
Profiling
Posture
Client Provisioning
Policy Elements
Click here to do wireless setup and visibility setup Do not show this again.
Reset
Save

Policy Sets → Default

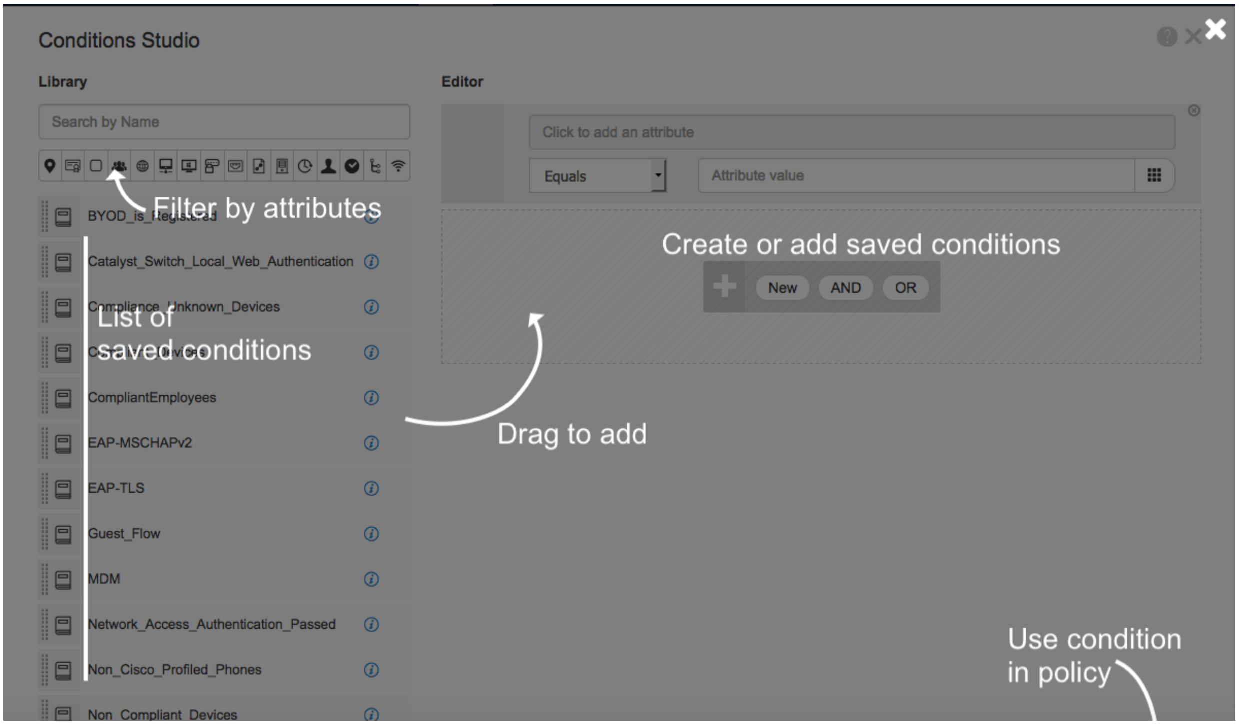
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	2

- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions (1)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	ANC_Quarantine	+	Select from list	Select from list		⚙

- Authorization Policy (16)

Step 6 You should see:


Conditions Studio

Library

Filter by attributes

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- CompliantEmployees
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MDM
- Network_Access_Authentication_Passed
- Non_Cisco_Profiled_Phones
- Non_Compliant_Devices

List of saved conditions

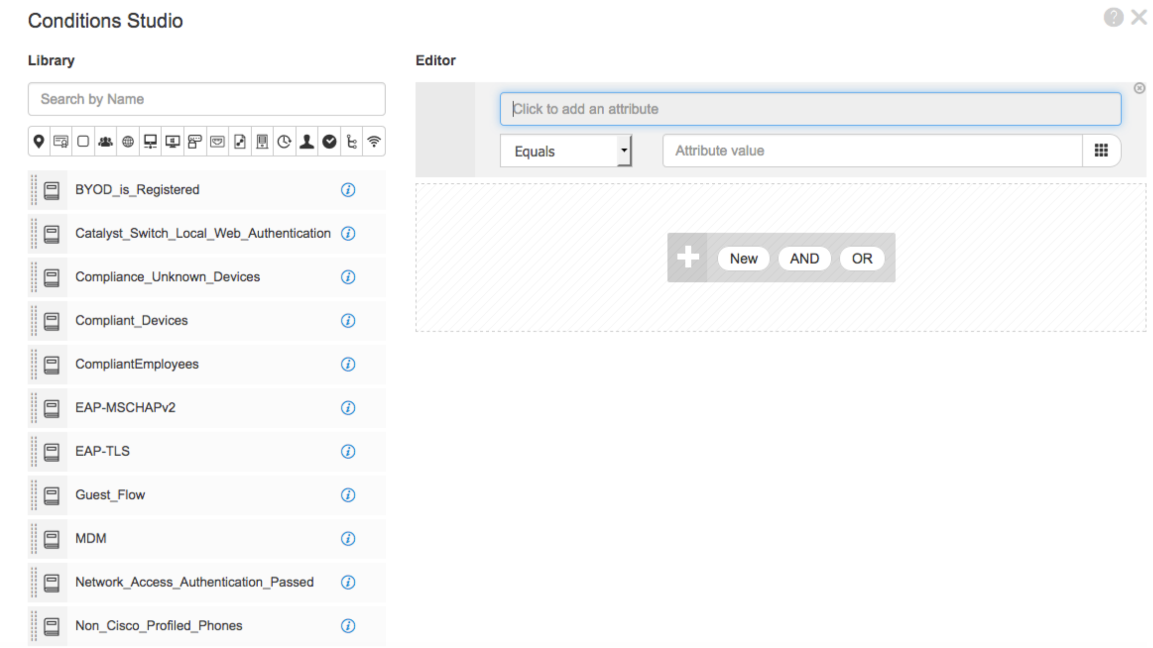
Editor

Create or add saved conditions

Drag to add

Use condition in policy

Step 7 Close the dialog box by click on "**x**"
You should see:



Conditions Studio

Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Compliant_Devices

CompliantEmployees

EAP-MSCHAPv2

EAP-TLS

Guest_Flow

MDM

Network_Access_Authentication_Passed

Non_Cisco_Profiled_Phones

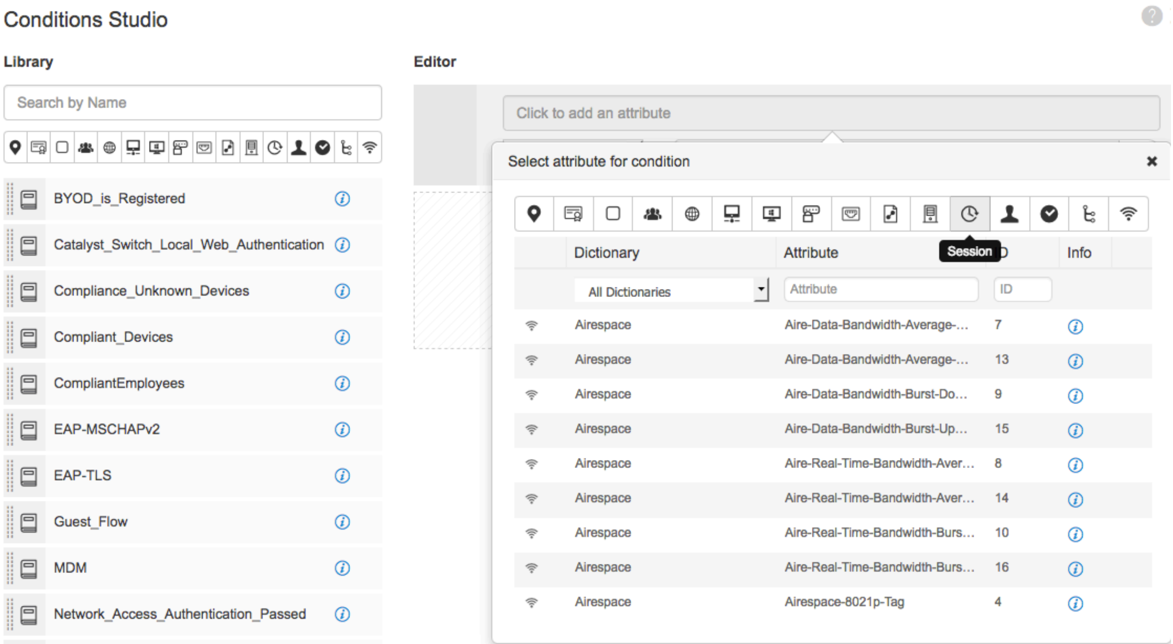
Editor

Click to add an attribute

Equals

Attribute value

Step 8 Under Editor, "**Click to add an attribute**", select "**Session**"



Conditions Studio

Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Compliant_Devices

CompliantEmployees

EAP-MSCHAPv2

EAP-TLS

Guest_Flow

MDM

Network_Access_Authentication_Passed

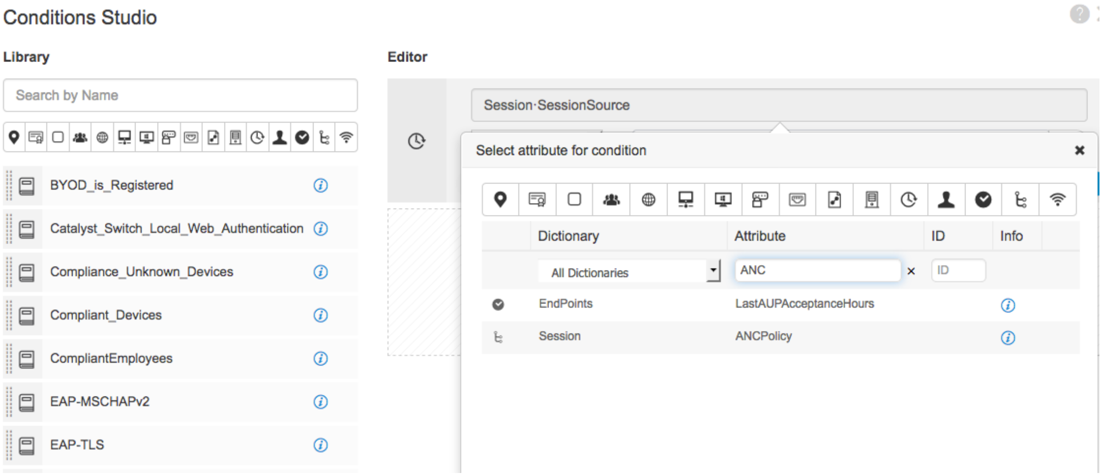
Editor

Click to add an attribute

Select attribute for condition

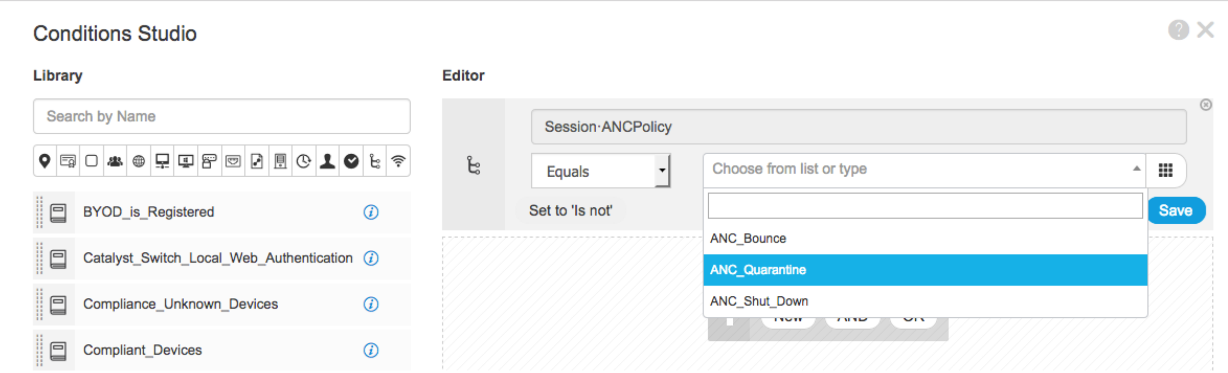
Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
Airespace	Aire-Data-Bandwidth-Average-...	7	ⓘ
Airespace	Aire-Data-Bandwidth-Average-...	13	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Do...	9	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Up...	15	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Aver...	8	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Aver...	14	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Burs...	10	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Burs...	16	ⓘ
Airespace	Airespace-8021p-Tag	4	ⓘ

Step 9 In the attribute field, type in "**ANC**"

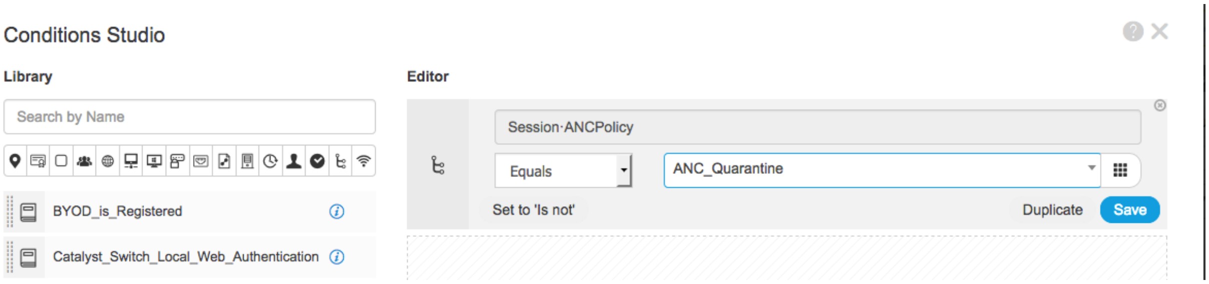


Step 10 Select "**ANCPolicy**"

Step 11 From the drop down select "**ANC Quarantine**"

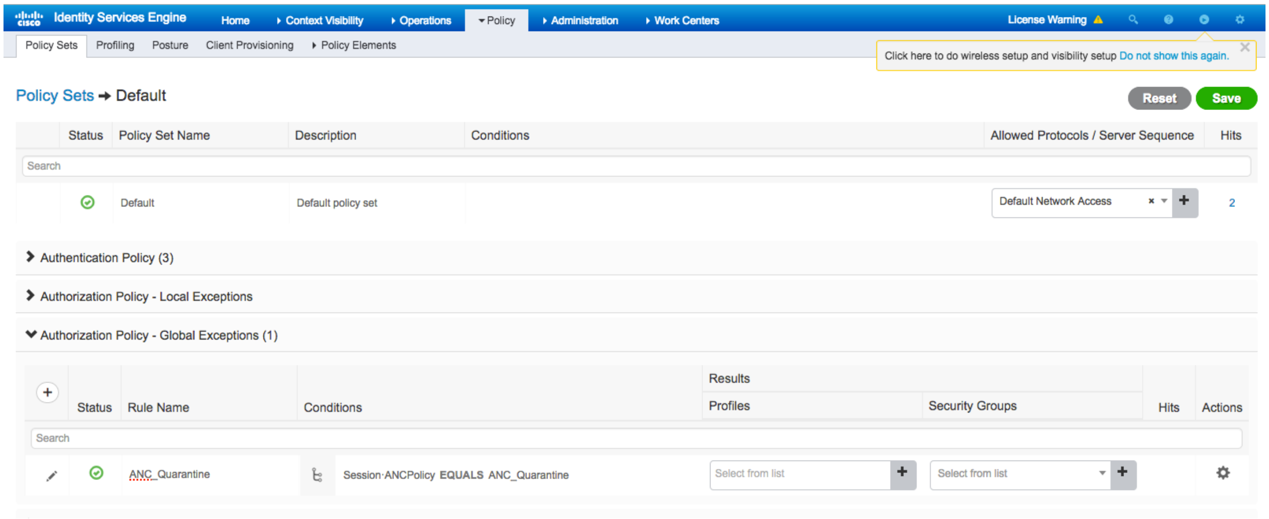


Step 12 Select **Save**



Step 13 Select "**Close**" when the Save Session window appears

Step 14 Select "**Use**"
You should see:



Click here to do wireless setup and visibility setup Do not show this again.

Policy Sets → Default

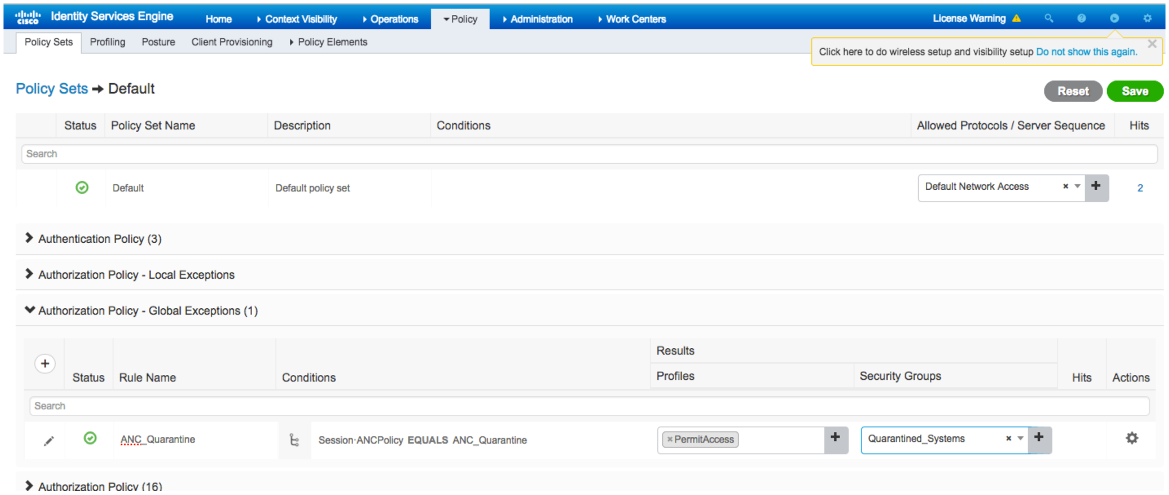
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	2

- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions (1)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	ANC_Quarantine	Session·ANCPolicy EQUALS ANC_Quarantine	Select from list	Select from list		

Step 15 Under **Profiles**, select "**Permit Access**"

Step 16 Under **Security Groups**, select **Quarantined Systems**



Click here to do wireless setup and visibility setup Do not show this again.

Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	2

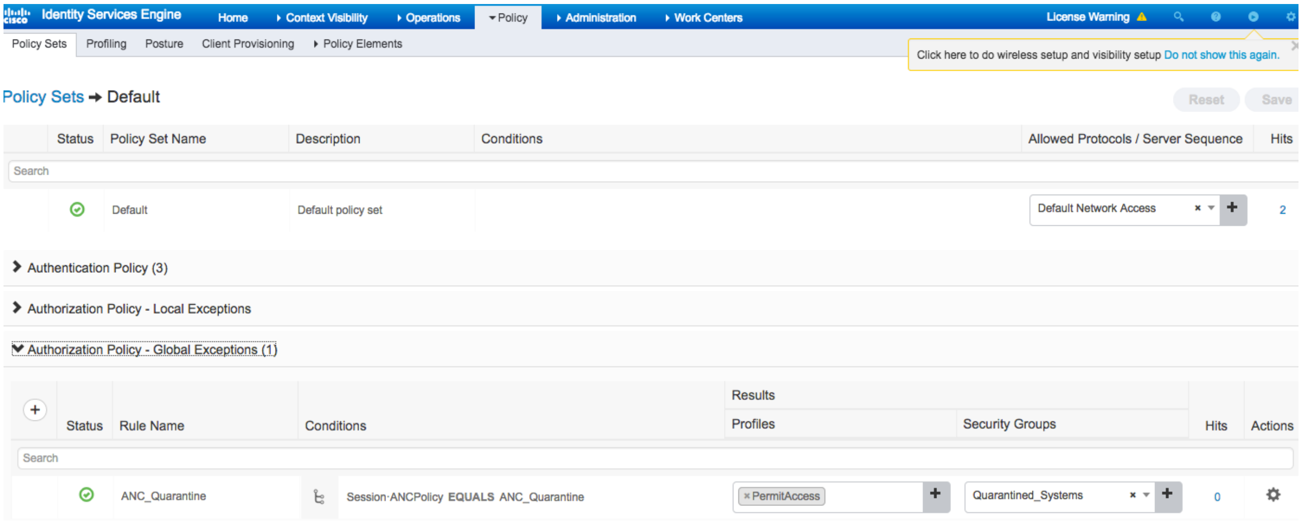
- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions (1)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	ANC_Quarantine	Session·ANCPolicy EQUALS ANC_Quarantine	× PermitAccess	Quarantined_Systems		

- Authorization Policy (16)

Step 17 Select **Save**

Step 18 Select **Authorization Policy ->Global Exceptions (1)**
You should see:



Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	2

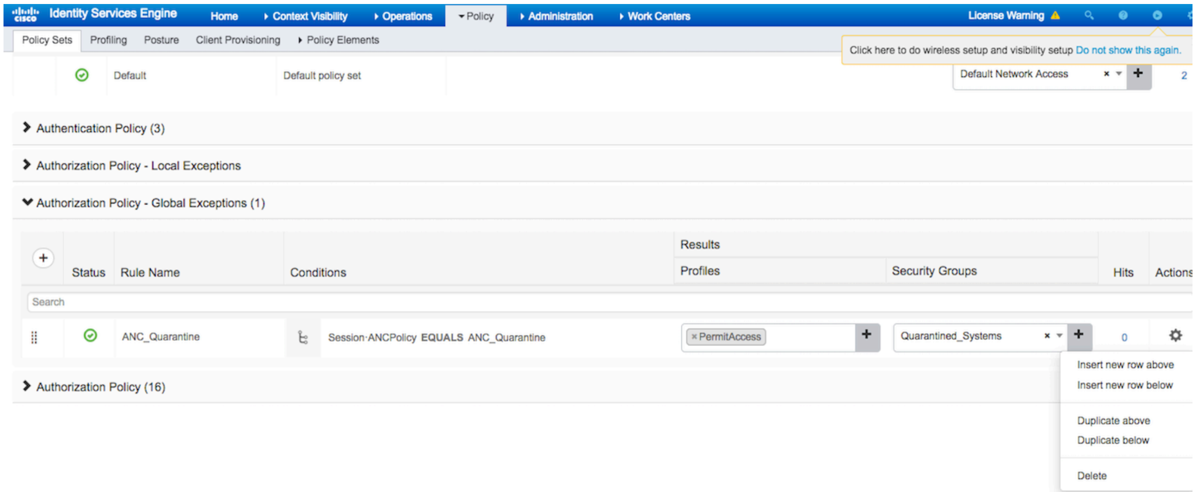
> Authentication Policy (3)

> Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions (1)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	ANC_Quarantine	Session·ANCPolicy EQUALS ANC_Quarantine	PermitAccess	Quarantined_Systems	0	⚙

Step 19 Under **Actions**, select the "**Gear**" button



Status	Policy Set Name	Description	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set	Default Network Access	2

> Authentication Policy (3)

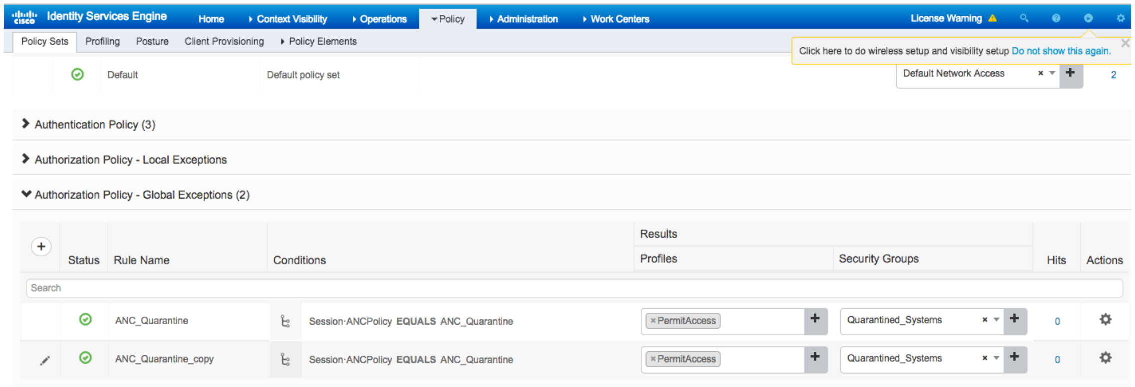
> Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions (1)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	ANC_Quarantine	Session·ANCPolicy EQUALS ANC_Quarantine	PermitAccess	Quarantined_Systems	0	⚙

> Authorization Policy (16)

Step 20 Select "**Duplicate Below**"
You should see:



Status	Policy Set Name	Description	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set	Default Network Access	2

> Authentication Policy (3)

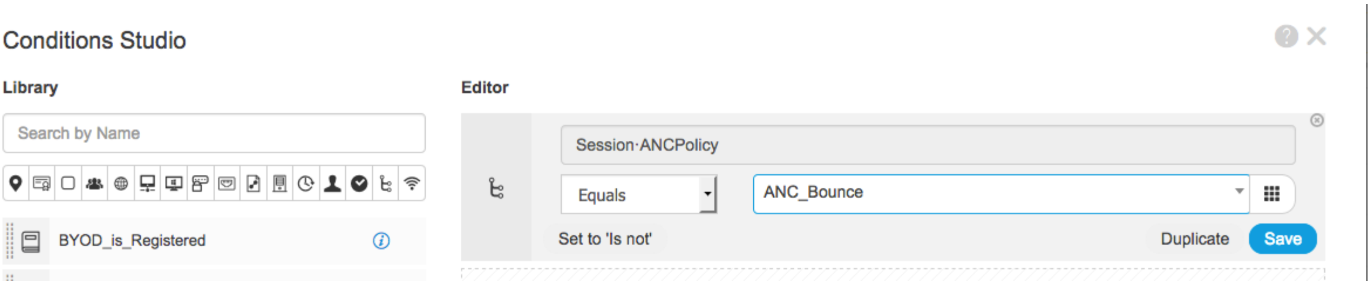
> Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions (2)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	ANC_Quarantine	Session·ANCPolicy EQUALS ANC_Quarantine	PermitAccess	Quarantined_Systems	0	⚙
✓	ANC_Quarantine_copy	Session·ANCPolicy EQUALS ANC_Quarantine	PermitAccess	Quarantined_Systems	0	⚙

Step 21 Change the **ANC_Quarantine_copy** to ANC_Bounce

Step 22 Select "**Session:Policy EQUALS ANC_Quarantine**" change to ANC Bounce



Session·ANCPolicy

Equals: ANC_Bounce

Step 23 Select **Save**

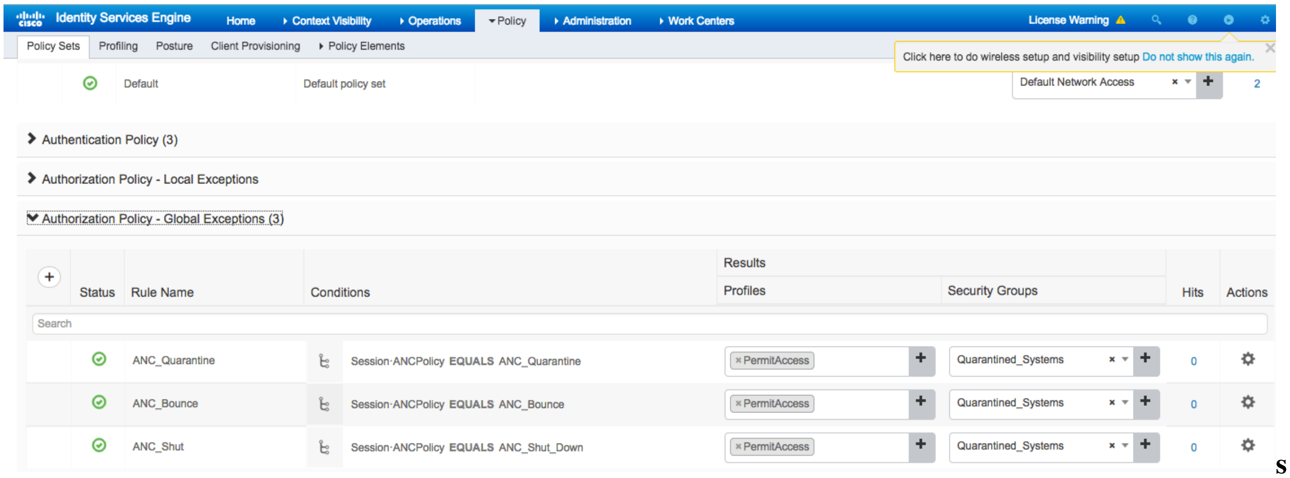
Step 24 **Close** the Save Condition box

Step 25 Select **Use**

Step 26 Follow steps 22-30 to create the policy for **ANC_Shut**

Step 27 Select **Save**

You should see:



Default | Default policy set | Default Network Access | 2

Authentication Policy (3)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions (3)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	ANC_Quarantine	Session·ANCPolicy EQUALS ANC_Quarantine	PermitAccess	Quarantined_Systems	0	⚙
✓	ANC_Bounce	Session·ANCPolicy EQUALS ANC_Bounce	PermitAccess	Quarantined_Systems	0	⚙
✓	ANC_Shut	Session·ANCPolicy EQUALS ANC_Shut_Down	PermitAccess	Quarantined_Systems	0	⚙

s

McAfee DXL Broker and ISE Configuration

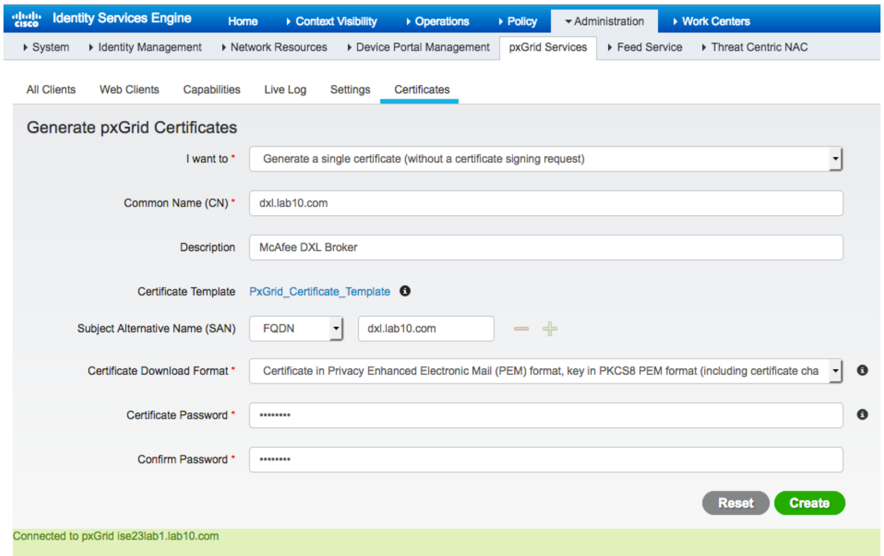
This section describes the pxGrid client and McAfee DXL Broker certificate generation process. If you are using other versions of ISE please see *References* for the appropriate versions of ISE.

Generating McAfee pxGrid Client Certificates using ISE 2.2 and above

ISE 2.2 features an Internal Certificate Authority (CA) for pxGrid operation and pxGrid client certificate generation. This provides an easier way to deploy pxGrid client certificates without having to use openssl to generate the private key and CSR request. If using versions of Cisco ISE 2.0/2.1/2.2 please refer to the appropriate guides under *References*.

Note: in ISE productional environments, there will be an external CA root certificate, this certificate will need to be imported in the McAfee DXL broker truststore. This document will use the ISE internal CA only, which can be used in Proof Of Concept (PoC) environments.

Step 1 Generate the McAfee DXL broker certificate
Select **Administration->pxGrid Services->Certificates**



Generate pxGrid Certificates

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

Common Name (CN) * dxl.lab10.com

Description McAfee DXL Broker

Certificate Template PxGrid_Certificate_Template

Subject Alternative Name (SAN) FQDN dxl.lab10.com

Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

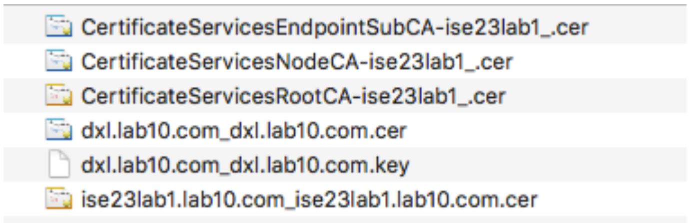
Certificate Password * ••••••••

Confirm Password * ••••••••

Connected to pxGrid ise23lab1.lab10.com

Step 2 Select **Create**

Step 3 A zipped file containing the certs (i.e 1509039174713.cert) will be generated
The contents of the zipped are shown below:

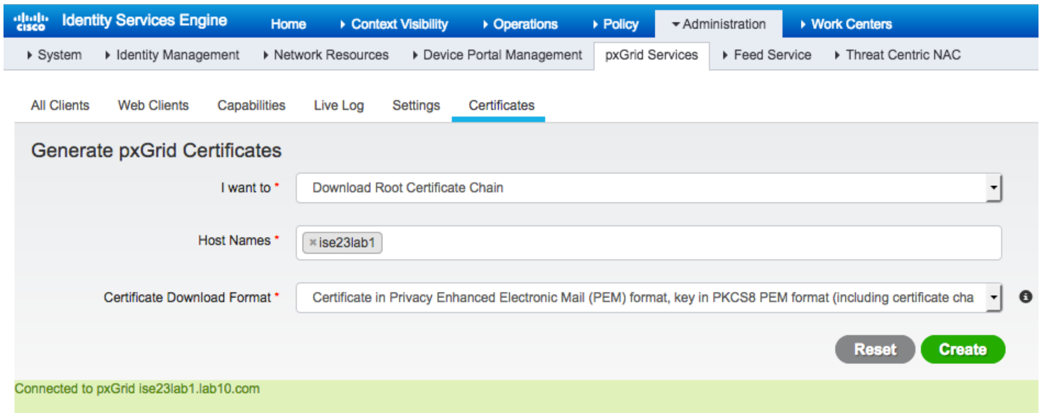


CertificateServicesEndpointSubCA-ise23lab1_.cer
CertificateServicesNodeCA-ise23lab1_.cer
CertificateServicesRootCA-ise23lab1_.cer
dxl.lab10.com_dxl.lab10.com.cer
dxl.lab10.com_dxl.lab10.com.key
ise23lab1.lab10.com_ise23lab1.lab10.com.cer

Step 4 Copy the certificate zipped file (i.e 1509039174713.cert) file to the McAfee dxlbroker **/var/McAfee/dxlbroker/ipe/cisco/keystore directory**

Note: You can Windows SCP to copy the certificate zipped file over to the McAfee dxlbroker keystore directory

Step 5 Download ISE Root Certificate,
Select **Administration->pxGrid Client->Certificates**



Generate pxGrid Certificates

I want to * Download Root Certificate Chain

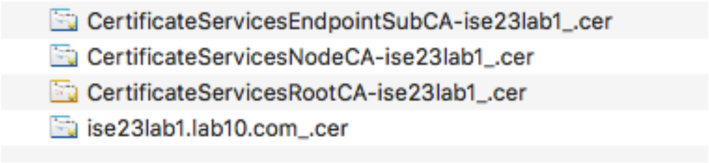
Host Names * ise23lab1

Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Connected to pxGrid ise23lab1.lab10.com

Step 6 Select **Create**

Step 7 A zipped file containing the certs (i.e 1508705614727.cert) will be generated
The contents of the zipped are shown below:



CertificateServicesEndpointSubCA-ise23lab1_.cer
CertificateServicesNodeCA-ise23lab1_.cer
CertificateServicesRootCA-ise23lab1_.cer
ise23lab1.lab10.com_.cer

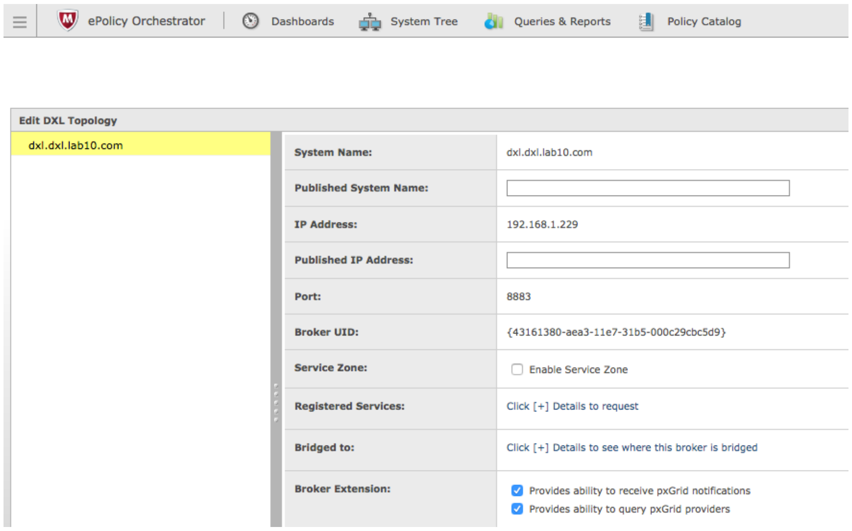
Step 8 Copy the certificate zipped file (i.e.1508705614727.cert) file to the McAfee dxlbroker **/var/McAfee/dxlbroker/ipe/cisco/truststore** directory

Note: You can Windows SCP to copy the certificate zipped file over to the McAfee dxlbroker keystore directory

Configuring McAfee DXL Broker ISE pxGrid Connection

In this section, the McAfee DXL broker extension is configured to query pxGrid providers and receive pxGrid notifications. The McAfee DXL and ISE pxGrid node connection parameters are configured, along with the ISE pxGrid notifications.

Step 1 From EPO, select **Menu->Configuration->Server Settings->DXL Topology->edit->Broker Extension->Enable->both "Provides ability to receive pxGrid notifications" and "Provides ability to query pxGrid providers"**



Edit DXL Topology

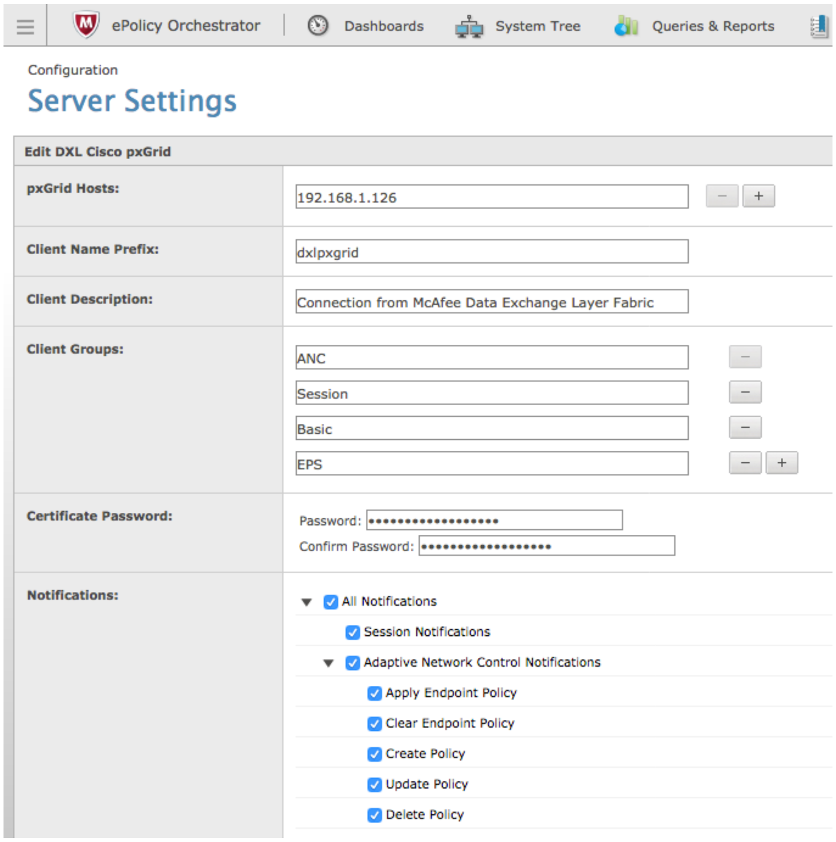
dxl.dxl.lab10.com

System Name:	dxl.dxl.lab10.com
Published System Name:	
IP Address:	192.168.1.229
Published IP Address:	
Port:	8883
Broker UID:	{43161380-aea3-11e7-31b5-000c29cbc5d9}
Service Zone:	☐ Enable Service Zone
Registered Services:	Click [+] Details to request
Bridged to:	Click [+] Details to see where this broker is bridged
Broker Extension:	☑ Provides ability to receive pxGrid notifications ☑ Provides ability to query pxGrid providers

Step 2 Select **Save**

Step 3 From EPO, select **Menu->Configuration->Server Settings->DXL Cisco pxGrid->Edit** and enter the **IP address** of the ISE pxGrid node under **pxGrid Hosts**, provide the **hostname** of the McAfee DXL broker under **Client Name Prefix**, add description under **Description**, add the **ANC**, **Session**, **Basic**, **EPS** groups under **Client Groups**, add the password of the generated McAfee DXL certificate under **Certificate Password** and select all of the notifications.

Note: You can leave the Session Notification Subnet Filter blank

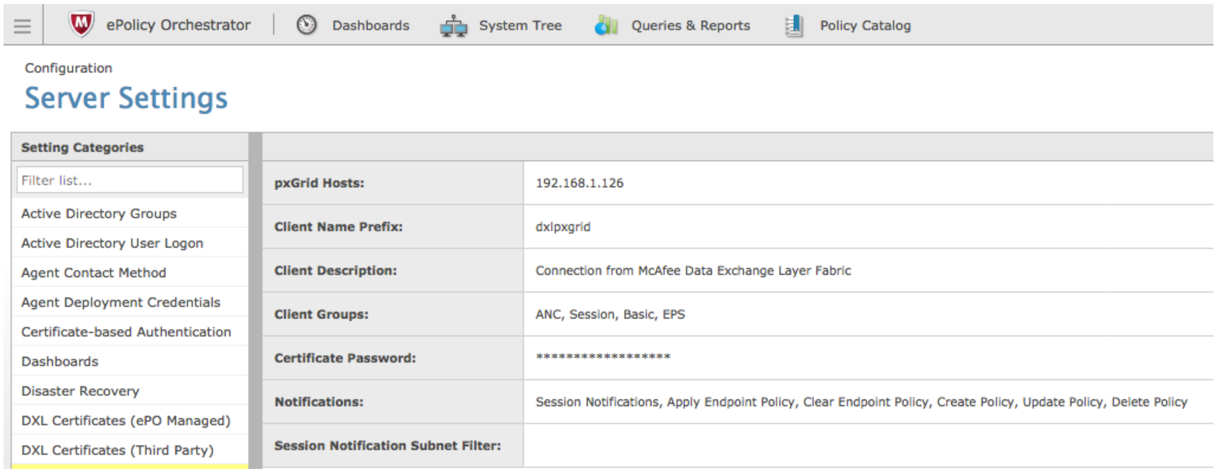


Edit DXL Cisco pxGrid

pxGrid Hosts:	192.168.1.126 − +
Client Name Prefix:	dxlpxgrid
Client Description:	Connection from McAfee Data Exchange Layer Fabric
Client Groups:	ANC − Session − Basic − EPS − +
Certificate Password:	Password: •••••••••••••••••• Confirm Password: ••••••••••••••••••
Notifications:	☑ All Notifications ☑ Session Notifications ☑ Adaptive Network Control Notifications ☑ Apply Endpoint Policy ☑ Clear Endpoint Policy ☑ Create Policy ☑ Update Policy ☑ Delete Policy

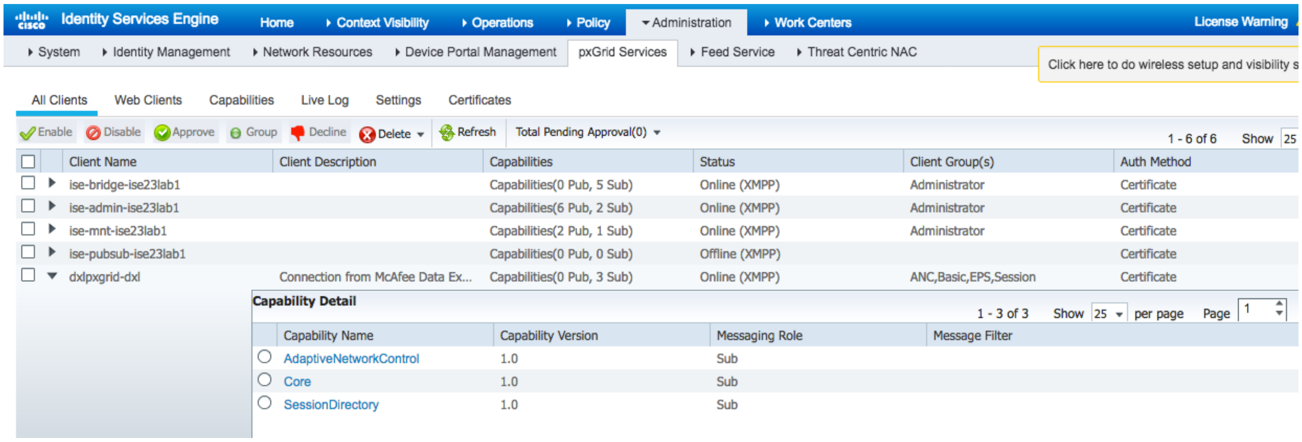
Step 4 Select **Save**

You should see:



pxGrid Hosts:	192.168.1.126
Client Name Prefix:	dxlpxgrid
Client Description:	Connection from McAfee Data Exchange Layer Fabric
Client Groups:	ANC, Session, Basic, EPS
Certificate Password:	******************
Notifications:	Session Notifications, Apply Endpoint Policy, Clear Endpoint Policy, Create Policy, Update Policy, Delete Policy
Session Notification Subnet Filter:	

Step 5 Verify that the McAfee DXL broker has successfully connected and registered with the ISE pxGrid node. Select **Administration-pxGrid Services**



☐	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
☐	▸ ise-bridge-ise23lab1		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate
☐	▸ ise-admin-ise23lab1		Capabilities(6 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate
☐	▸ ise-mnt-ise23lab1		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate
☐	▸ ise-pubsub-ise23lab1		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate
☐	▾ dxlpxgrid-dxl	Connection from McAfee Data Ex...	Capabilities(0 Pub, 3 Sub)	Online (XMPP)	ANC,Basic,EPS,Session	Certificate

Capability Detail

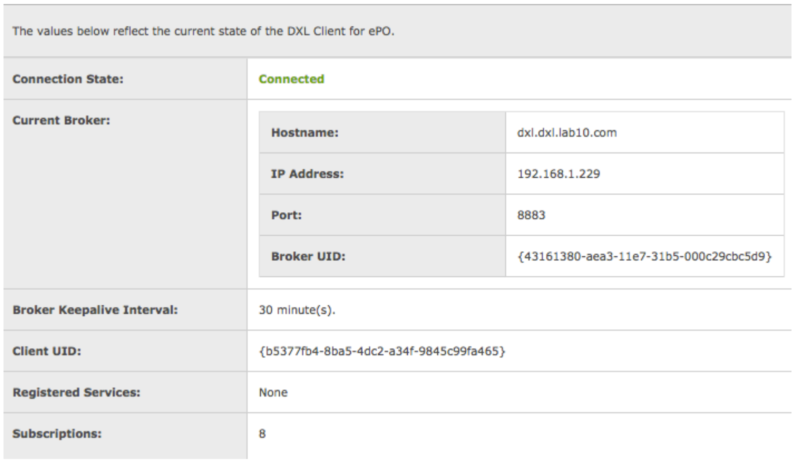
1 - 3 of 3 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	AdaptiveNetworkControl	1.0	Sub	
○	Core	1.0	Sub	
○	SessionDirectory	1.0	Sub	

Configuring McAfee ePO Automatic Responses

The McAfee ePO Automatic Response policy will be configured to retrieve the existing ISE ANC policies in the response. The McAfee ePO admin will select the desired ANC policy that the McAfee DXL broker will take action upon when the Threat Event occurs.

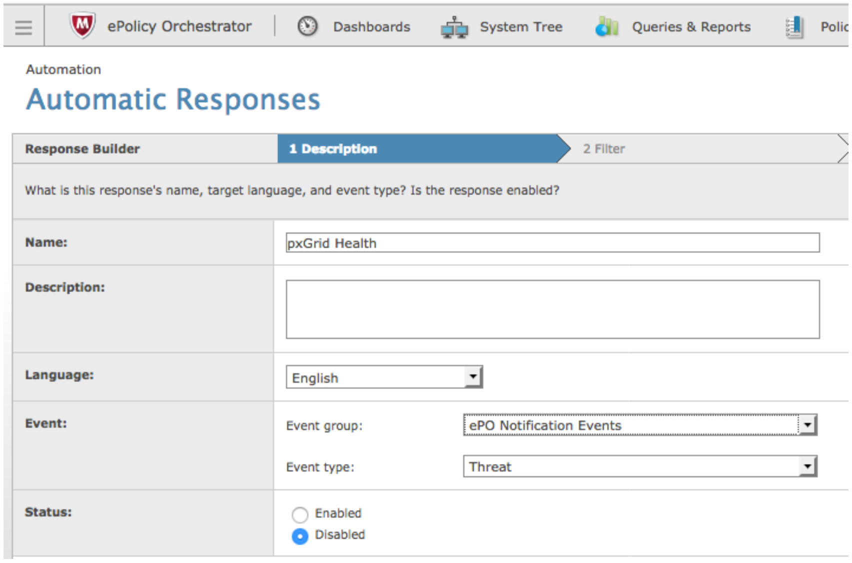
Step 1 Verify McAfee DXL Broker is connected to McAfee EPO
Select **Menu->Server Settings->DXL Client for EPO**



The values below reflect the current state of the DXL Client for ePO.

Connection State:	Connected
Current Broker:	**Hostname:** dxl.dxl.lab10.com **IP Address:** 192.168.1.229 **Port:** 8883 **Broker UID:** {43161380-aea3-11e7-31b5-000c29cbc5d9}
Broker Keepalive Interval:	30 minute(s).
Client UID:	{b5377fb4-8ba5-4dc2-a34f-9845c99fa465}
Registered Services:	None
Subscriptions:	8

Step 2 Select **Menu->Automation->Automatic Responses->New Response->**add **pxGrid Health** under **Name,** select **ePO Notification Events** under **Event group**, select **Threat** under **Event Type**



Automation

Automatic Responses

What is this response's name, target language, and event type? Is the response enabled?

Name: pxGrid Health

Description:

Language: English

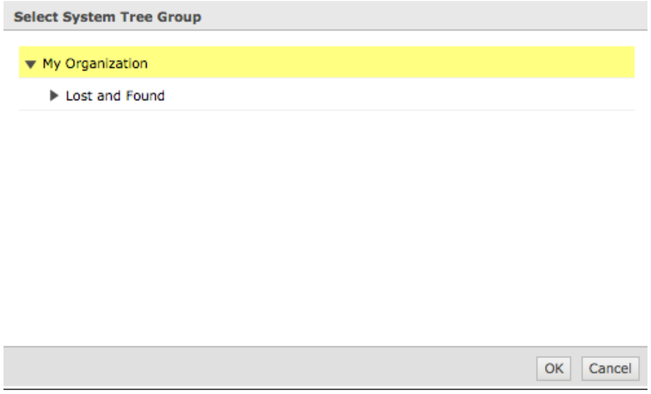
Event: Event group: ePO Notification Events
Event type: Threat

Status: ○ Enabled ● Disabled

Step 3 Select **Next**

Step 4 Select ->"**…**" under **Value**

Step 5 Select ->**My Organization**



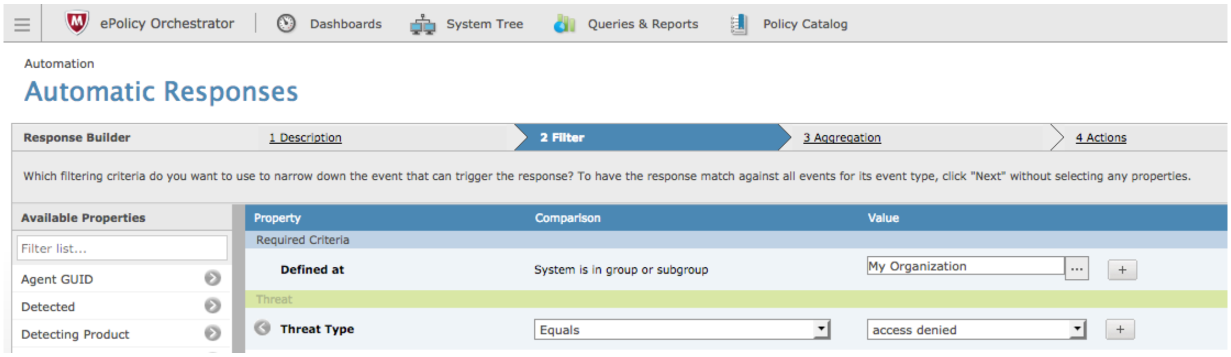
Select System Tree Group

▼ My Organization

▶ Lost and Found

Step 6 Select **OK**

Step 7 Under **Available Properties,** select **Threat Type:Equals:access denied**



Automation

Automatic Responses

Which filtering criteria do you want to use to narrow down the event that can trigger the response? To have the response match against all events for its event type, click "Next" without selecting any properties.

Available Properties

Agent GUID

Detected

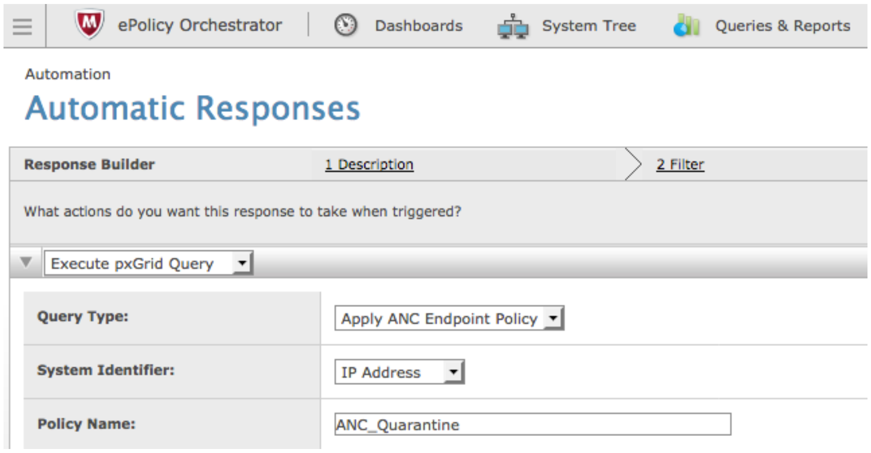
Detecting Product

Property	Comparison	Value
Required Criteria		
Defined at	System is in group or subgroup	My Organization
Threat		
Threat Type	Equals	access denied

Step 8 Select **Next**

Step 9 Keep the defaults for **Aggregation,** select **Next**

Step 10 Under **Actions**, select **Execute pxGrid query**, select **Apply ANC Endpoint Policy** under **Query Type:,** select **IP Address** under **System Identifier**, and select the existing ISE ANC policy under **Policy Name**



Automation

Automatic Responses

Response Builder — 1 Description — 2 Filter

What actions do you want this response to take when triggered?

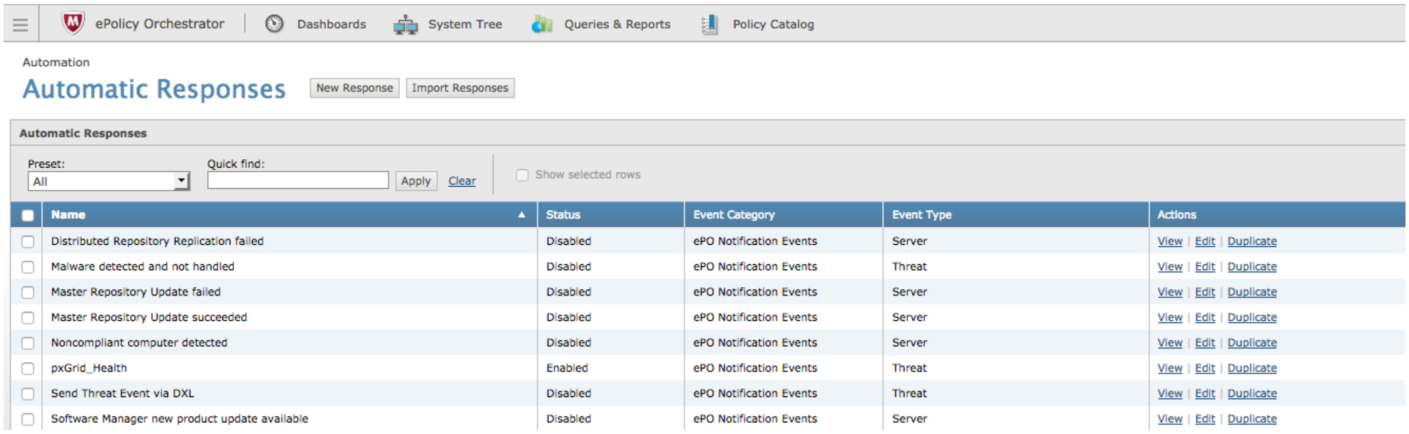
Execute pxGrid Query

Query Type:	Apply ANC Endpoint Policy
System Identifier:	IP Address
Policy Name:	ANC_Quarantine

Step 11 Select **Save**

Step 12 Select **pxGrid Health->Actions->Enable Responses**

Step 13 Should see pxGrid Health Automated Response as Enabled



Automation

Automatic Responses

Automatic Responses

Preset: All   Quick find:

Name	Status	Event Category	Event Type	Actions
Distributed Repository Replication failed	Disabled	ePO Notification Events	Server	View | Edit | Duplicate
Malware detected and not handled	Disabled	ePO Notification Events	Threat	View | Edit | Duplicate
Master Repository Update failed	Disabled	ePO Notification Events	Server	View | Edit | Duplicate
Master Repository Update succeeded	Disabled	ePO Notification Events	Server	View | Edit | Duplicate
Noncompliant computer detected	Disabled	ePO Notification Events	Server	View | Edit | Duplicate
pxGrid_Health	Enabled	ePO Notification Events	Threat	View | Edit | Duplicate
Send Threat Event via DXL	Disabled	ePO Notification Events	Threat	View | Edit | Duplicate
Software Manager new product update available	Disabled	ePO Notification Events	Server	View | Edit | Duplicate

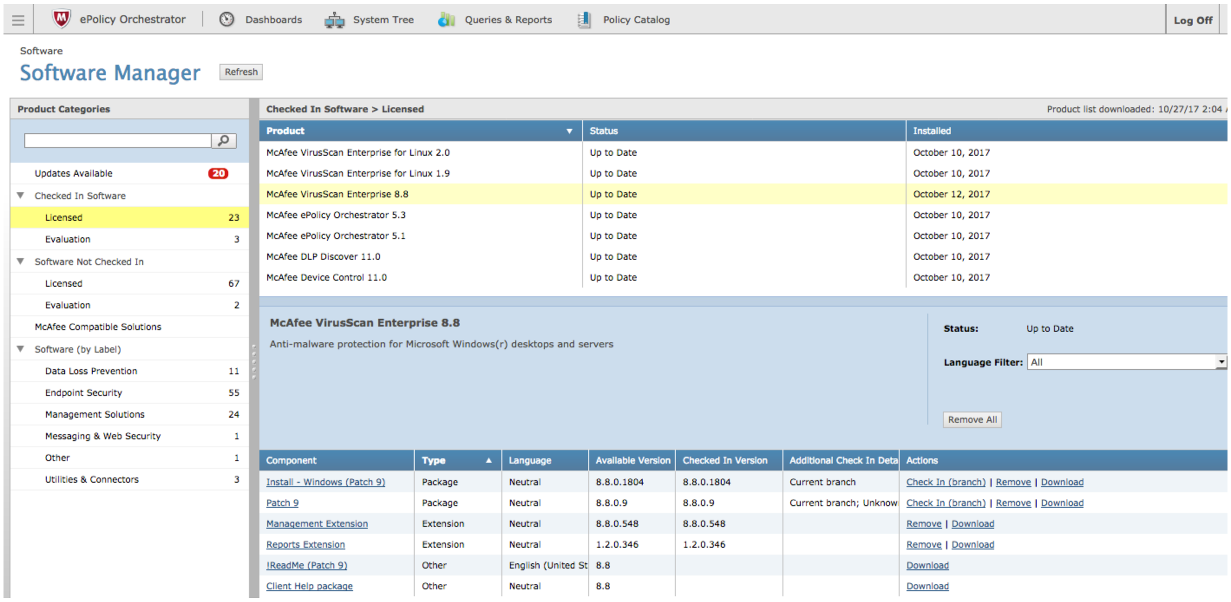
Deploy McAfee Enterprise Virusscan 8.8 through McAfee ePO.

In this section, McAfee Enterprise Virruscan 8.8 is deployed through McAfee EPO. You will need to have McAfee properly licensed.

Step 1 Select **Menu->Software Manager->Software Not Checked In->Evaluation->McAfee Virrusscan8.8->Management Extension->Check-In->enter information->Save->Accept License->Ok**

Step 2 Select **Menu->Software Manager->Checked In Software->Evaluation->McAfee Virrusscan8.8->Reports Extension->Check-In-> Accept License->Ok**

Step 3 Select **Software Manager->Checked In Software->Licensed->McAfee Virusscan8.8->Install-Windows (Patch9)-Check-In->Accept License->Ok**



Software

Software Manager

Product Categories

Updates Available	20
▼ Checked In Software	
Licensed	23
Evaluation	3
▼ Software Not Checked In	
Licensed	67
Evaluation	2
McAfee Compatible Solutions	
▼ Software (by Label)	
Data Loss Prevention	11
Endpoint Security	55
Management Solutions	24
Messaging & Web Security	1
Other	1
Utilities & Connectors	3

Checked In Software > Licensed   Product list downloaded: 10/27/17 2:04

Product	Status	Installed
McAfee VirusScan Enterprise for Linux 2.0	Up to Date	October 10, 2017
McAfee VirusScan Enterprise for Linux 1.9	Up to Date	October 10, 2017
McAfee VirusScan Enterprise 8.8	Up to Date	October 12, 2017
McAfee ePolicy Orchestrator 5.3	Up to Date	October 10, 2017
McAfee ePolicy Orchestrator 5.1	Up to Date	October 10, 2017
McAfee DLP Discover 11.0	Up to Date	October 10, 2017
McAfee Device Control 11.0	Up to Date	October 10, 2017

McAfee VirusScan Enterprise 8.8

Anti-malware protection for Microsoft Windows(r) desktops and servers

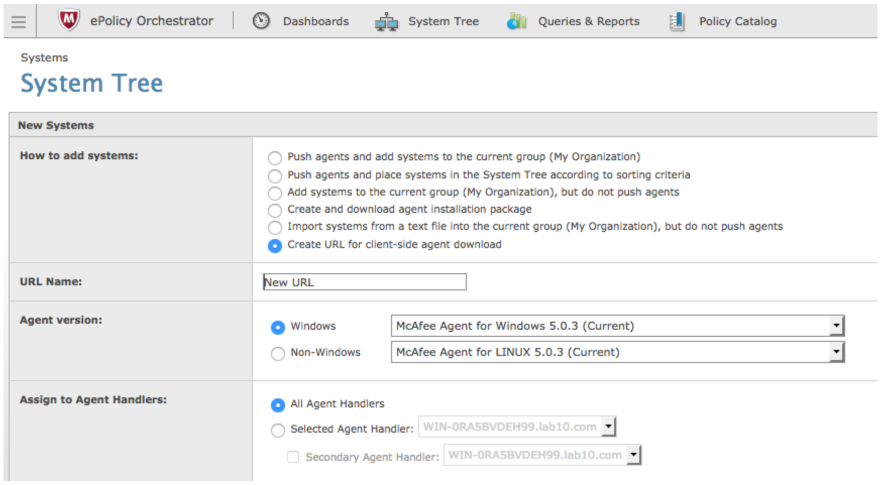
Status: Up to Date

Language Filter: All

Remove All

Component	Type ▲	Language	Available Version	Checked In Version	Additional Check In Deta	Actions
Install - Windows (Patch 9)	Package	Neutral	8.8.0.1804	8.8.0.1804	Current branch	Check In (branch) | Remove | Download
Patch 9	Package	Neutral	8.8.0.9	8.8.0.9	Current branch; Unknow	Check In (branch) | Remove | Download
Management Extension	Extension	Neutral	8.8.0.548	8.8.0.548		Remove | Download
Reports Extension	Extension	Neutral	1.2.0.346	1.2.0.346		Remove | Download
!ReadMe (Patch 9)	Other	English (United St	8.8			Download
Client Help package	Other	Neutral	8.8			Download

Step 4 Select **System Tree->New Systems->Create URL for agent-side download**



Systems

System Tree

New Systems

How to add systems:
- ○ Push agents and add systems to the current group (My Organization)
- ○ Push agents and place systems in the System Tree according to sorting criteria
- ○ Add systems to the current group (My Organization), but do not push agents
- ○ Create and download agent installation package
- ○ Import systems from a text file into the current group (My Organization), but do not push agents
- ● Create URL for client-side agent download

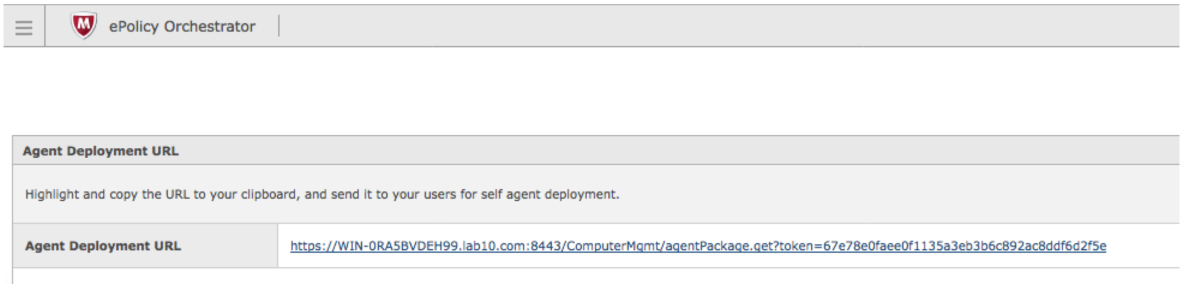
URL Name: New URL

Agent version:
- ● Windows: McAfee Agent for Windows 5.0.3 (Current)
- ○ Non-Windows: McAfee Agent for LINUX 5.0.3 (Current)

Assign to Agent Handlers:
- ● All Agent Handlers
- ○ Selected Agent Handler: WIN-0RA5BVDEH99.lab10.com
- □ Secondary Agent Handler: WIN-0RA5BVDEH99.lab10.com

Step 5 Select **OK**

You should see:



Agent Deployment URL

Highlight and copy the URL to your clipboard, and send it to your users for self agent deployment.

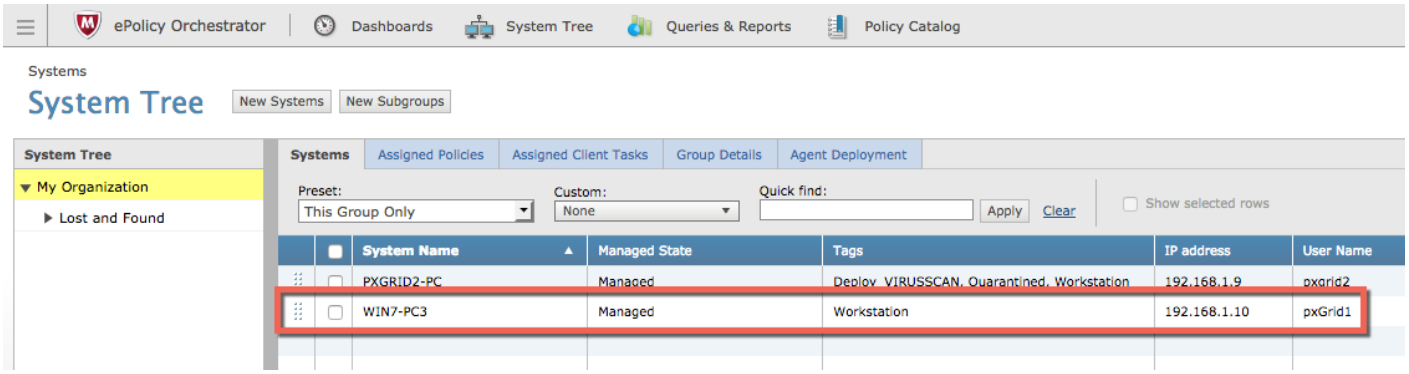
Agent Deployment URL: https://WIN-0RA5BVDEH99.lab10.com:8443/ComputerMgmt/agentPackage.get?token=67e78e0faee0f1135a3eb3b6c892ac8ddf6d2f5e

Step 6 Select **OK**

Step 7 Go to the desired PC and download the link, this will download McAfeeSmartInstall.exe

Step 8 Run **McAfeeSmartInstall.exe**

Step 9 Select **System Tree** to view the installed system.



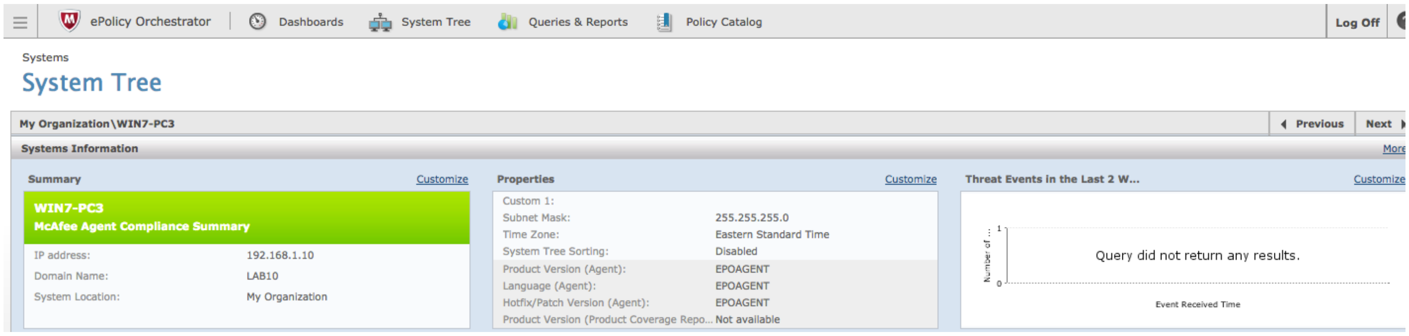
Preset: This Group Only

Custom: None

Quick find:

	System Name	Managed State	Tags	IP address	User Name
□	PXGRID2-PC	Managed	Deploy_VIRUSSCAN, Quarantined, Workstation	192.168.1.9	pxgrid2
□	WIN7-PC3	Managed	Workstation	192.168.1.10	pxGrid1

Step 10 Click on WIN7-PC3 to view the status of the EPO agent



My Organization\WIN7-PC3

Systems Information

Summary

WIN7-PC3
McAfee Agent Compliance Summary

IP address:	192.168.1.10
Domain Name:	LAB10
System Location:	My Organization

Properties

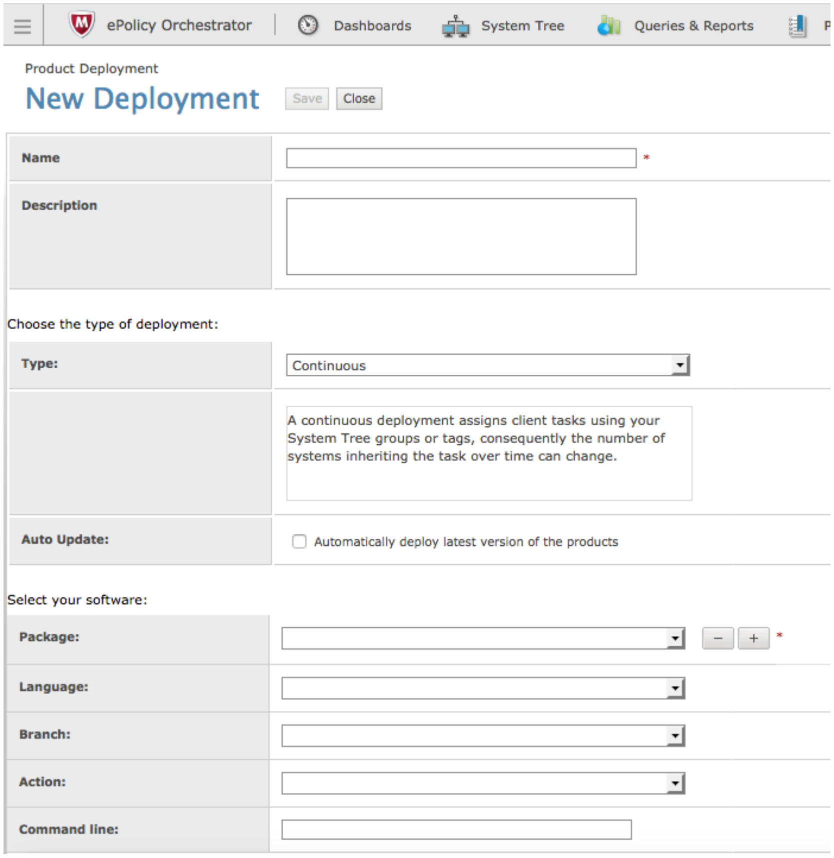
Custom 1:	
Subnet Mask:	255.255.255.0
Time Zone:	Eastern Standard Time
System Tree Sorting:	Disabled
Product Version (Agent):	EPOAGENT
Language (Agent):	EPOAGENT
Hotfix/Patch Version (Agent):	EPOAGENT
Product Version (Product Coverage Repo...	Not available

Threat Events in the Last 2 W...

Query did not return any results.

Step 11 Select **Close**

Step 12 Select **Menu->Software->product deployment->New Deployment**
You should see:



Product Deployment

New Deployment

Name *

Description

Choose the type of deployment:

Type: Continuous

A continuous deployment assigns client tasks using your System Tree groups or tags, consequently the number of systems inheriting the task over time can change.

Auto Update: □ Automatically deploy latest version of the products

Select your software:

Package: *

Language:

Branch:

Action:

Command line:

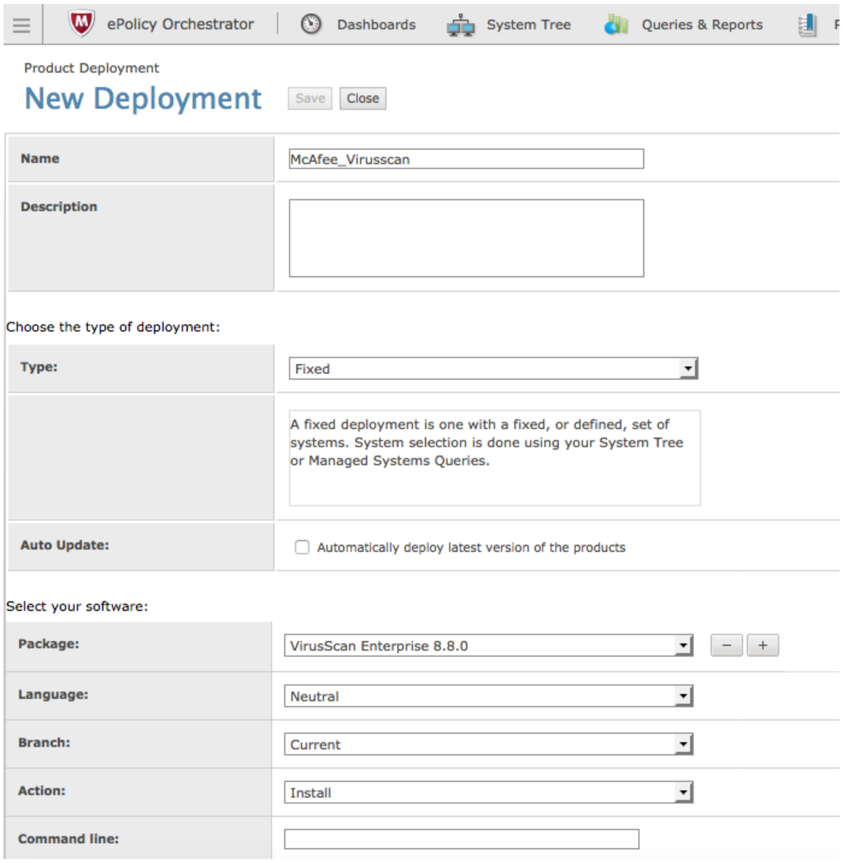
Step 13 Provide the Name, (i.e.) **McAfee_Virusscan**

Step 14 Under "**Type**", select **Fixed**

Step 15 Under "**Package**", select **Virusscan 8.8**

Step 16 Under "**Action**", select **Install**

Step 17 You should see:



Product Deployment

New Deployment

Name	McAfee_Virusscan
Description	

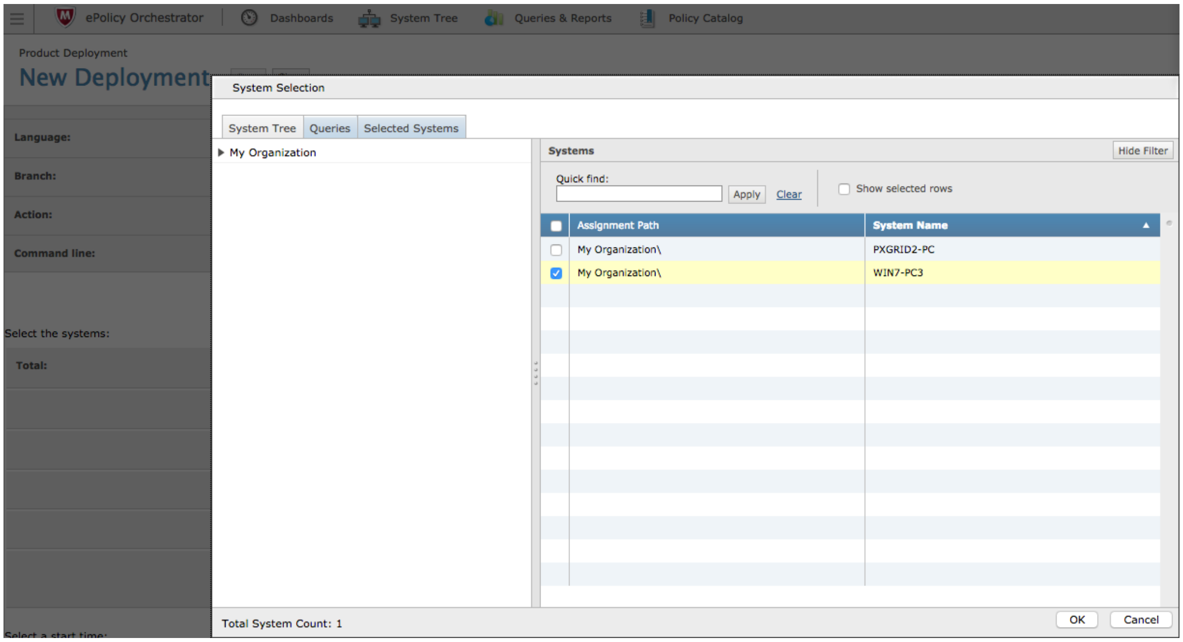
Choose the type of deployment:

Type:	Fixed
	A fixed deployment is one with a fixed, or defined, set of systems. System selection is done using your System Tree or Managed Systems Queries.
Auto Update:	□ Automatically deploy latest version of the products

Select your software:

Package:	VirusScan Enterprise 8.8.0
Language:	Neutral
Branch:	Current
Action:	Install
Command line:	

Step 18 Under "**Select the Systems**"**-> Select Systems,** select the desired system



System Selection

Systems

☐	Assignment Path	System Name ▲
☐	My Organization\	PXGRID2-PC
☑	My Organization\	WIN7-PC3

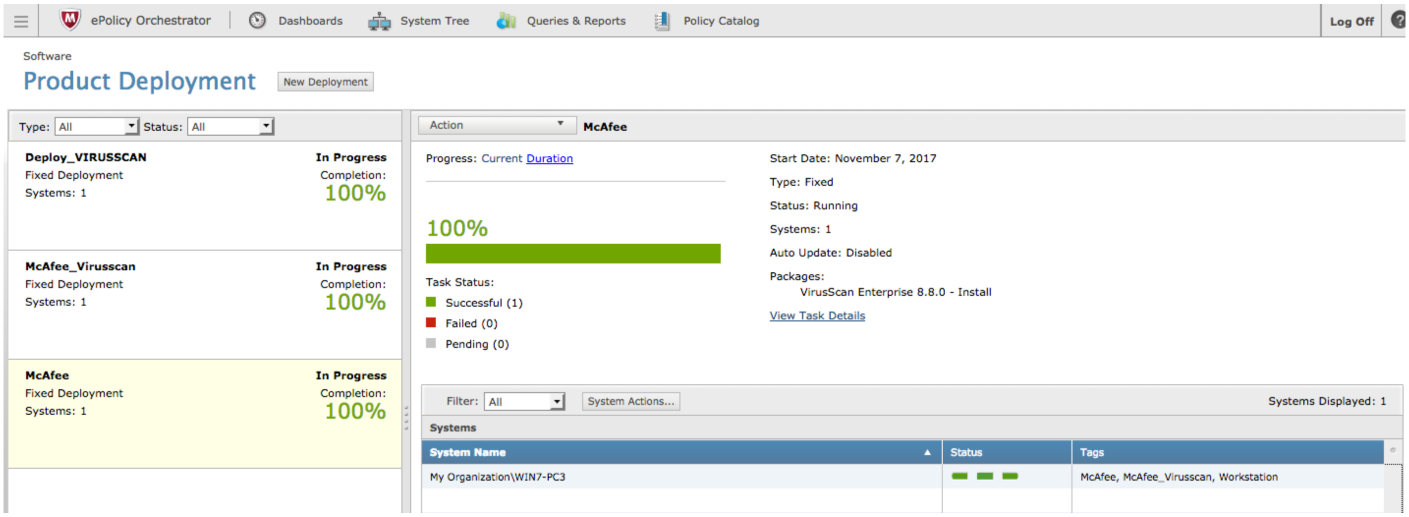
Total System Count: 1

Step 19 Select **OK**

Step 20 Select **Save**

Step 21 On desired system, select **McAfee agent**, **enforce new policies**

Step 22 To verify in ePO, refresh



Product Deployment

Type: All Status: All

Deploy_VIRUSSCAN — Fixed Deployment — Systems: 1 — In Progress — Completion: 100%

McAfee_Virusscan — Fixed Deployment — Systems: 1 — In Progress — Completion: 100%

McAfee — Fixed Deployment — Systems: 1 — In Progress — Completion: 100%

McAfee

Progress: Current Duration

100%

Task Status:
- Successful (1)
- Failed (0)
- Pending (0)

Start Date: November 7, 2017
Type: Fixed
Status: Running
Systems: 1
Auto Update: Disabled
Packages:
VirusScan Enterprise 8.8.0 - Install
View Task Details

Systems Displayed: 1

Systems

System Name	Status	Tags
My Organization\WIN7-PC3	▬ ▬ ▬	McAfee, McAfee_Virusscan, Workstation

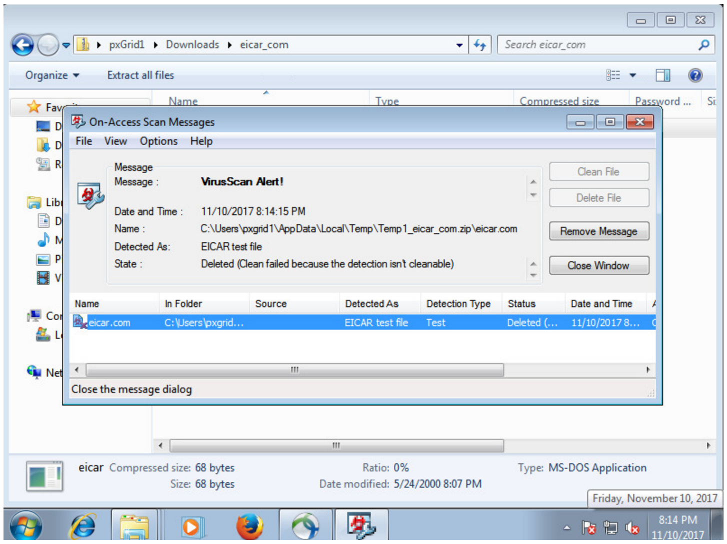
Testing

Here we use eicar to trigger a McAfee epO Threat event based on the Automatic response we created. The DXL broker will perform the ANC mitigated action, and ISE will quarantine the endpoint.

Step 1 Run eicar test, McAfee Virusscan will trigger an event
Enter: www.eicar.org/85-0/Download.html into browser

Step 2 Download and save file eicar_com.zip file locally

Step 3 Click on the eicar file you should see the alert



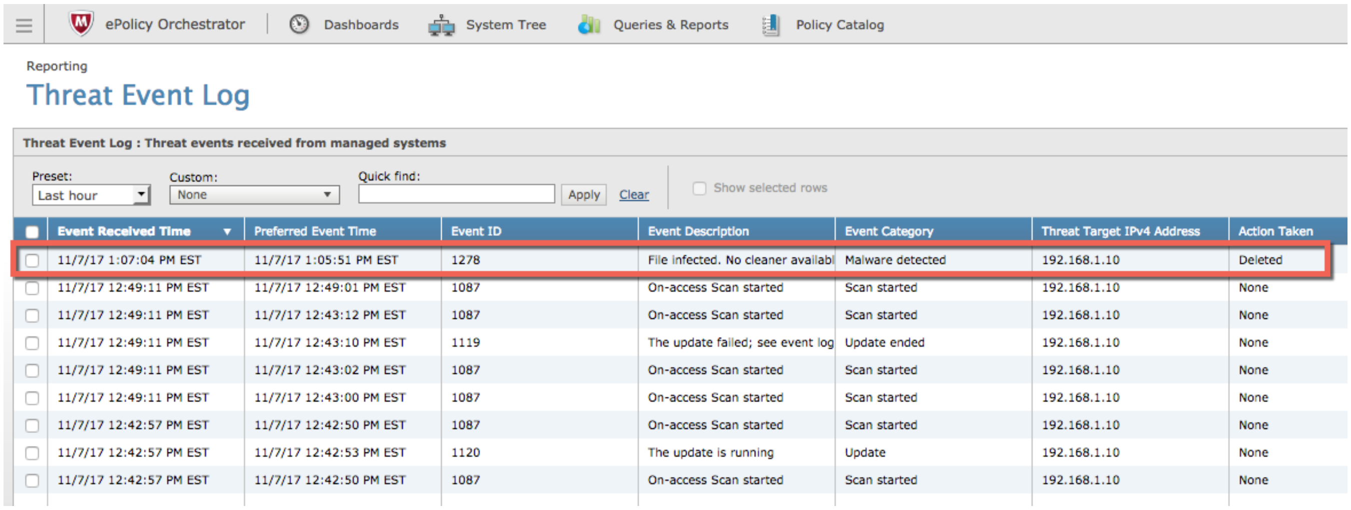
Message
Message : **VirusScan Alert!**
Date and Time : 11/10/2017 8:14:15 PM
Name : C:\Users\pxgrid1\AppData\Local\Temp\Temp1_eicar_com.zip\eicar.com
Detected As: EICAR test file
State : Deleted (Clean failed because the detection isn't cleanable)

Name	In Folder	Source	Detected As	Detection Type	Status	Date and Time
eicar.com	C:\Users\pxgrid...		EICAR test file	Test	Deleted (...	11/10/2017 8...

Close the message dialog

eicar Compressed size: 68 bytes Size: 68 bytes Ratio: 0% Date modified: 5/24/2000 8:07 PM Type: MS-DOS Application

Step 4 In EPO, select **Menu->Reporting->Threat Event Log**
You will the detected malware:



Reporting

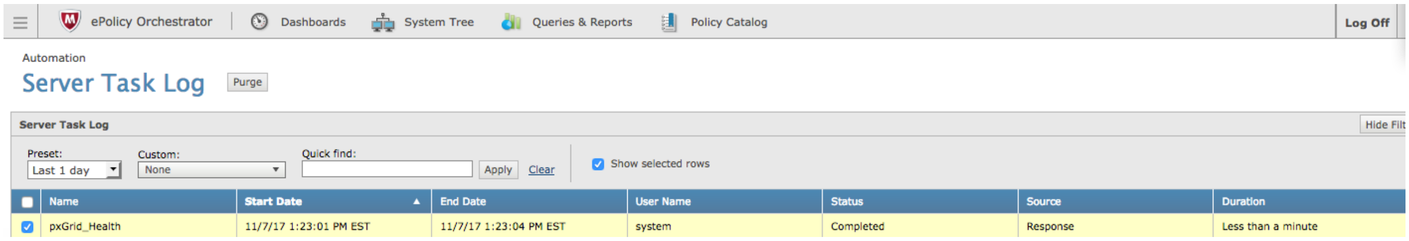
Threat Event Log

Threat Event Log : Threat events received from managed systems

Preset: Last hour | Custom: None | Quick find: | Apply | Clear | □ Show selected rows

□	Event Received Time	Preferred Event Time	Event ID	Event Description	Event Category	Threat Target IPv4 Address	Action Taken
□	11/7/17 1:07:04 PM EST	11/7/17 1:05:51 PM EST	1278	File infected. No cleaner availabl	Malware detected	192.168.1.10	Deleted
□	11/7/17 12:49:11 PM EST	11/7/17 12:49:01 PM EST	1087	On-access Scan started	Scan started	192.168.1.10	None
□	11/7/17 12:49:11 PM EST	11/7/17 12:43:12 PM EST	1087	On-access Scan started	Scan started	192.168.1.10	None
□	11/7/17 12:49:11 PM EST	11/7/17 12:43:10 PM EST	1119	The update failed; see event log	Update ended	192.168.1.10	None
□	11/7/17 12:49:11 PM EST	11/7/17 12:43:02 PM EST	1087	On-access Scan started	Scan started	192.168.1.10	None
□	11/7/17 12:49:11 PM EST	11/7/17 12:43:00 PM EST	1087	On-access Scan started	Scan started	192.168.1.10	None
□	11/7/17 12:42:57 PM EST	11/7/17 12:42:50 PM EST	1087	On-access Scan started	Scan started	192.168.1.10	None
□	11/7/17 12:42:57 PM EST	11/7/17 12:42:53 PM EST	1120	The update is running	Update	192.168.1.10	None
□	11/7/17 12:42:57 PM EST	11/7/17 12:42:50 PM EST	1087	On-access Scan started	Scan started	192.168.1.10	None

Step 5 Select **Menu->Automation->Server Task Log->pxGrid health-> Status Completed->Subtasks->Execute pxGrid Query->Log Messages**



Automation

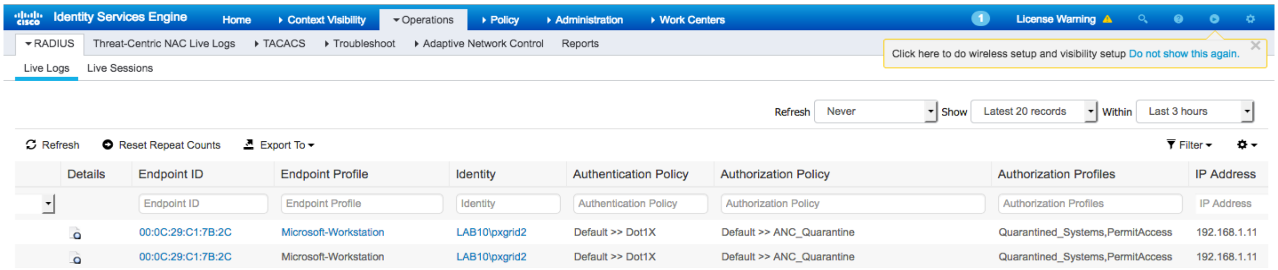
Server Task Log | Purge

Server Task Log | Hide Filt

Preset: Last 1 day | Custom: None | Quick find: | Apply | Clear | ☑ Show selected rows

□	Name	Start Date	End Date	User Name	Status	Source	Duration
☑	pxGrid_Health	11/7/17 1:23:01 PM EST	11/7/17 1:23:04 PM EST	system	Completed	Response	Less than a minute

Step 6 To See the ISE Radius Live Logs see quarantine
Select **Operations->RADIUS->Live Logs**

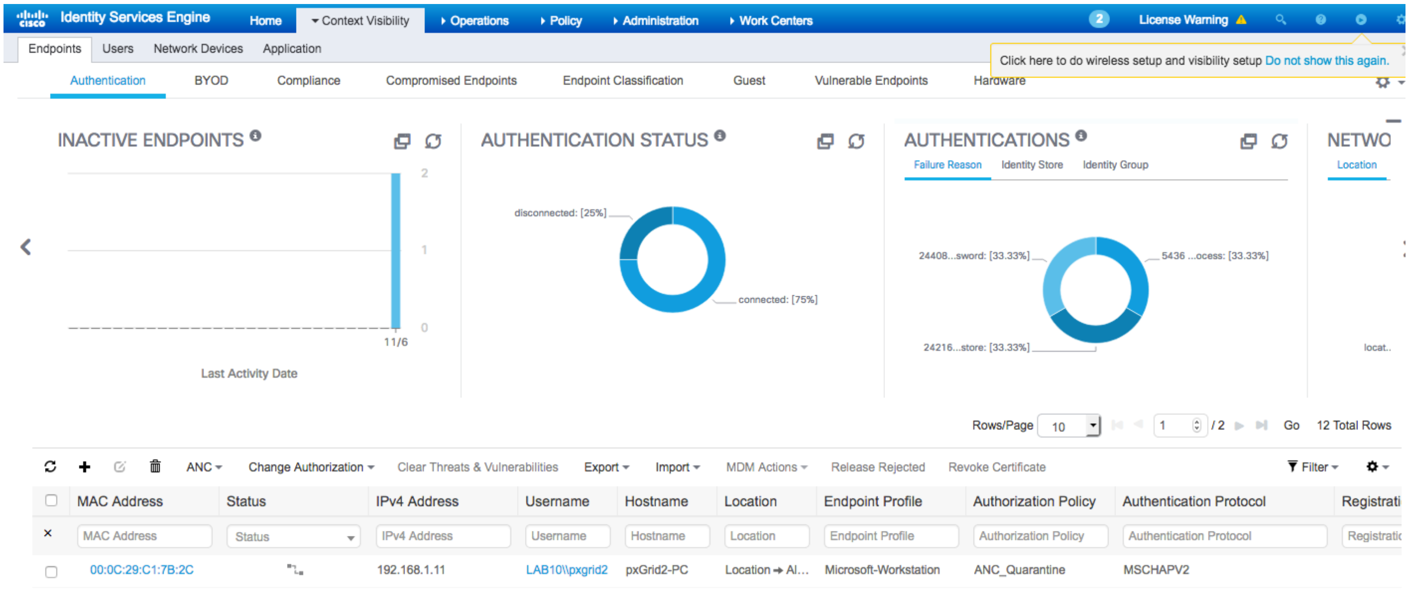


Click here to do wireless setup and visibility setup Do not show this again.

Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

Details	Endpoint ID	Endpoint Profile	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
	00:0C:29:C1:7B:2C	Microsoft-Workstation	LAB10\pxgrid2	Default >> Dot1X	Default >> ANC_Quarantine	Quarantined_Systems,PermitAccess	192.168.1.11
	00:0C:29:C1:7B:2C	Microsoft-Workstation	LAB10\pxgrid2	Default >> Dot1X	Default >> ANC_Quarantine	Quarantined_Systems,PermitAccess	192.168.1.11

Step 7 Select **Context Visibility->Endpoints**
You should also see the quarantined endpoint



MAC Address	Status	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Authorization Policy	Authentication Protocol	Registrati
00:0C:29:C1:7B:2C		192.168.1.11	LAB10\\pxgrid2	pxGrid2-PC	Location → Al...	Microsoft-Workstation	ANC_Quarantine	MSCHAPV2	

Python Clients (optional)

OpenDXL Python client scripts (https://github.com/opendxl/opendxl-pxgrid-client-python) can be used to perform more specific ISE pxGrid operations on the McAfee DXL broker. We will cover two examples, sending notification requests to the ISE pxGrid node, i.e. applying endpoint to an ISE ANC policy. The second example is for the OpenDXL Python client to a listen to an ISE pxGrid notification, that has an ISE ANC policy "quarantined_policy" assigned to it, and also a McAfee ePO Quarantined Tag. Once this notification is received, this endpoint can be managed by McAfee ePO based on the Quarantine Tag.

Send requests to the Cisco ISE pxGrid node

Step 1 Install DXL 4.0.0 extensions, install a DXL Broker, complete steps to bridge DXL and to configure the Cisco pxGrid in the previous sections.

Step 2 Download and install python 2.7.14 (https://www.python.org/downloads/windows/), on a windows laptop.

Note: Run "pip –V" to check the pip installer

```
C:\Python27>pip -V
 pip 9.0.1 from c:\python27\lib\site-packages (python 2.7)
```

Step 3 Install python wheel package

```
C:\Python27>pip install wheel
 Collecting wheel
   Downloading wheel-0.30.0-py2.py3-none-any.whl (49kB)
     100% |################################| 51kB 358kB/s
 Installing collected packages: wheel
 Successfully installed wheel-0.30.0
```

Step 4 Install the Cisco pxGrid DXL Python Client (https://github.com/opendxl/opendxl-pxgrid-client-python

```
C:\Python27>pip install dxlciscopxgridclient
 Collecting dxlciscopxgridclient
   Downloading dxlciscopxgridclient-0.1.2-py2.7-none-any.whl
 Requirement already satisfied: dxlbootstrap in c:\python27\lib\site-packages
(from dxlciscopxgridclient)
 Requirement already satisfied: dxlclient in c:\python27\lib\site-packages
(from dxlciscopxgridclient)
 Requirement already satisfied: asn1crypto in c:\python27\lib\site-packages
(from dxlclient->dxlciscopxgridclient)
 Requirement already satisfied: oscrypto in c:\python27\lib\site-packages (from
dxlclient->dxlciscopxgridclient)
 Requirement already satisfied: configobj in c:\python27\lib\site-packages
(from dxlclient->dxlciscopxgridclient)
 Requirement already satisfied: requests in c:\python27\lib\site-packages (from
dxlclient->dxlciscopxgridclient)
 Requirement already satisfied: six in c:\python27\lib\site-packages (from
dxlclient->dxlciscopxgridclient)
 Requirement already satisfied: chardet<3.1.0,>=3.0.2 in c:\python27\lib\site-
packages (from requests->dxlclient->dxlciscopxgridclient)
Requirement already satisfied: certifi>=2017.4.17 in c:\python27\lib\site-
packages (from requests->dxlclient->dxlciscopxgridclient)
 es (from requests->dxlclient->dxlciscopxgridclient)
 Requirement already satisfied: urllib3<1.23,>=1.21.1 in c:\python27\lib\site-
packages (from requests->dxlclient->dxlciscopxgridclient)
 Requirement already satisfied: idna<2.7,>=2.5 in c:\python27\lib\site-packages
(from requests->dxlclient->dxlciscopxgridclient)
 Installing collected packages: dxlciscopxgridclient
 Successfully installed dxlciscopxgridclient-0.1.2
```

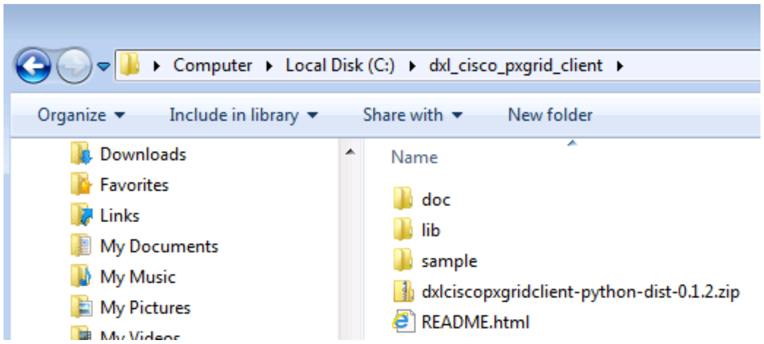
Step 5 Check the openssl version in python
Open a "Python shell" and type the following 2 statements:

```
import ssl
ssl OPENSSL_VERSION
should see "OpenSSL 1.0.2k Jan 2017"
```

Note: The version must be 1.0.1 or greater. Unfortunately, even the latest versions of OSX (Mac) still have version 0.9.8 installed. If you wish to use the Python SDK with OSX, one possible workaround is to use a third party package manager (such as Brew) to install a compatible Python and OpenSSL version.

Step 6 Download the latest Cisco pxGrid DXL Python Client here: https://github.com/opendxl/opendxl-pxgrid-client-python/releases.

Step 7 Create a folder (i.e. dxl_cisco_pxgrid_client) and extract the contents of the Cisco pxGrid DXL Python Client that you just downloaded.



Step 8 Change directories to the “sample” directory under the contents you just unzipped

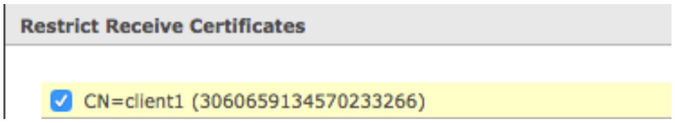
Step 9 Provision certificates for the Cisco pxGrid DXL Python Client to use: python –m dxclient provisionconfig . <YOUR EPO SERVER IP ADDRESS> client1

```
C:\dxl_cisco_pxgrid_client\sample>python -m dxlclient provisionconfig .
192.168.1.15
 1.15 client1
 Enter server username:
 Enter server password:
 INFO: Saving csr file to .\client.csr
 INFO: Saving private key file to .\client.key
 INFO: Saving DXL config file to .\dxlclient.config
 INFO: Saving ca bundle file to .\ca-bundle.crt
 INFO: Saving client certificate file to .\client.crt
```

Note: The “client1” text can be any name and will be used in the scripts later. The username and password will not be shown while typing; can use the –u username and –p password arguments to denote the admin username and password of the EPO Server.

Note: For more information on provisioning an OpenDXL Python Client see the documentation here: https://opendxl.github.io/opendxl-client-python/pydoc/basiccliprovisioning.html

Step 10 Need to authorize DXL Broker to send and receive pxGrid notifications
Select **Menu->Configuration->Server Settings-DXL Topic Authorization->Edit->DXL Cisco pxGrid Queries->Actions->Restrict send certificates-> select the certificate with a CN=client1 or whatever name you used in Step 8**

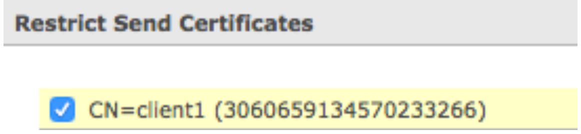


Restrict Receive Certificates

☑ CN=client1 (3060659134570233266)

Step 11 Select **OK**

Step 12 Select **Menu->Configuration->Server Settings-DXL Topic Authorization->Edit->DXL Cisco pxGrid Queries->Actions->Restrict receive certificates-> select the certificate with the CN=client1 or whatever name you used in Step 8**



Restrict Send Certificates

☑ CN=client1 (3060659134570233266)

Step 13 Select **OK**

Step 14 Select **Save**

Step 15 To apply an ANC endpoint policy by IP address in ISE edit the **basic_anc_apply_endpoint_policy_by_ip_example.py** example under the directory "**dxl_cisco_pxgrid_client\sample\basic**" directory and change the **HOST_IP variable** to have an **IP address** of a system that is in Cisco ISE. Provide the ISE configured ANC policy i.e. ANC_Quarantine.

Note: For more information see https://opendxl.github.io/opendxl-pxgrid-client-python/pydoc/basicancapplyendpointpolicybyipexample.html

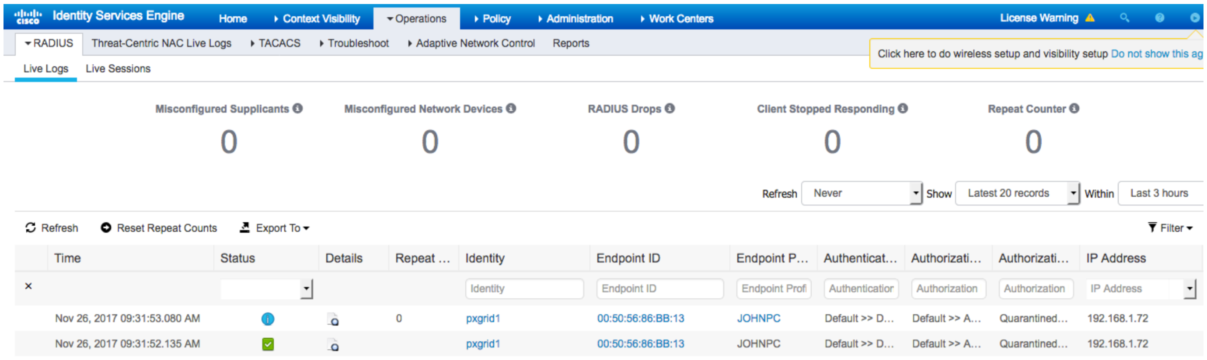
```
import os
import sys

from dxlbootstrap.util import MessageUtils
from dxlclient.client_config import DxlClientConfig
from dxlclient.client import DxlClient

root_dir = os.path.dirname(os.path.abspath(__file__))
sys.path.append(root_dir + "/../..")
sys.path.append(root_dir + "/..")

from dxlciscopxgridclient.client import CiscoPxGridClient

# Import common logging and configuration
from common import *

# Configure local logger
logging.getLogger().setLevel(logging.ERROR)
logger = logging.getLogger(__name__)

# Create DXL configuration from file
config = DxlClientConfig.create_dxl_config_from_file(CONFIG_FILE)

# IP address of the endpoint for which to apply the policy
HOST_IP = "192.168.1.72"

# Create the client
with DxlClient(config) as dxl_client:

    # Connect to the fabric
    dxl_client.connect()

    logger.info("Connected to DXL fabric.")
    # Create client wrapper
    client = CiscoPxGridClient(dxl_client)

    try:
        # Invoke 'apply endpoint policy by IP' method on service
        resp_dict = client.anc.apply_endpoint_policy_by_ip(HOST_IP,
                                                           "ANC_Quarantine")

        # Print out the response (convert dictionary to JSON for pretty
        # printing)
        print("Response:\n{0}".format(
            MessageUtils.dict_to_json(resp_dict, pretty_print=True)))
    except Exception as ex:
        # An exception should be raised if the 'quarantine_policy' has already
        # been applied to the endpoint, the 'quarantine_policy' has not been
        # created, or if no session has been established for the endpoint.
        print(str(ex))
```

Please make sure you have your ISE ANC policies defined and have been added to the ISE global exception authorization policy sets. Please see **Configuring Adaptive Network Control (ANC) Policies** under **Cisco Identity Services Engine**

Step 16 Run the basic_anc_apply_endpoint_policy_by_ip_example.py example. You should see a response of success if the IP address was assigned to the ANC policy.

```
 C:\dxl_cisco_pxgrid_client\sample\basic>python
basic_anc_apply_endpoint_policy_by_ip_example.py
 Response:
 {
     "ancStatus": "success"
 }

 C:\dxl_cisco_pxgrid_client\sample\basic>
```

Step 17 Log in to Cisco ISE and verify that the ANC policy has been applied to the IP address
Select **Operations->RADIUS->RADIUS->Live Logs**

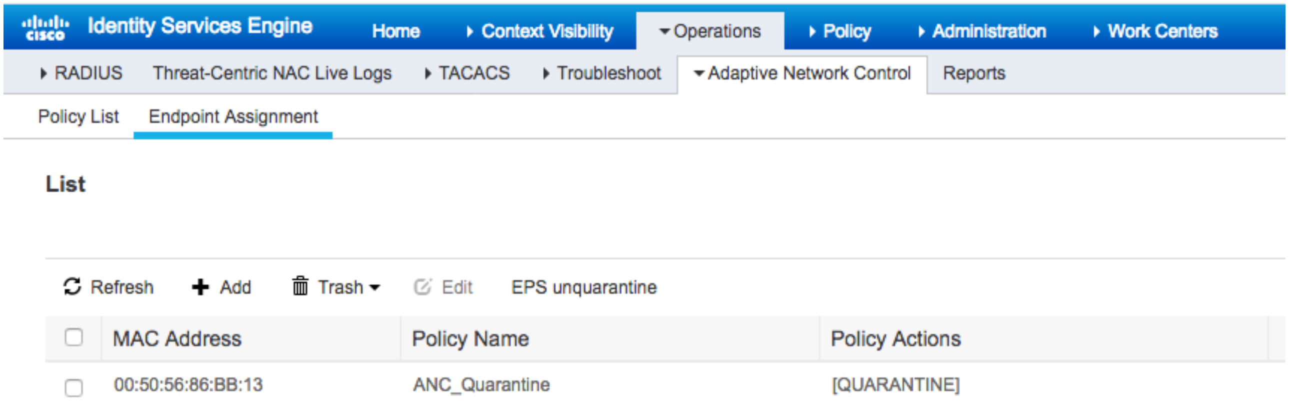


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Never   Show: Latest 20 records   Within: Last 3 hours

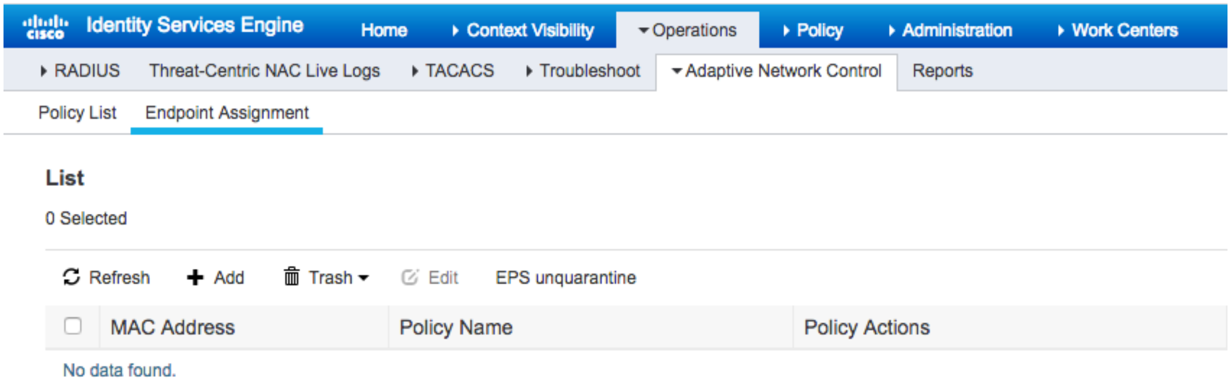
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address
Nov 26, 2017 09:31:53.080 AM	●		0	pxgrid1	00:50:56:86:BB:13	JOHNPC	Default >> D...	Default >> A...	Quarantined...	192.168.1.72
Nov 26, 2017 09:31:52.135 AM	✓			pxgrid1	00:50:56:86:BB:13	JOHNPC	Default >> D...	Default >> A...	Quarantined...	192.168.1.72

Step 18 To view the ISE ANC Policy
Select **Operations->Adaptive Network Control->Endpoint Assignment**



☐	MAC Address	Policy Name	Policy Actions
☐	00:50:56:86:BB:13	ANC_Quarantine	[QUARANTINE]

Step 19 To clear or Unquarantine in Cisco ISE
Select->**Operations->Adaptive Network Control->Endpoint Assignment->select MAC Address->Trash**



☐	MAC Address	Policy Name	Policy Actions

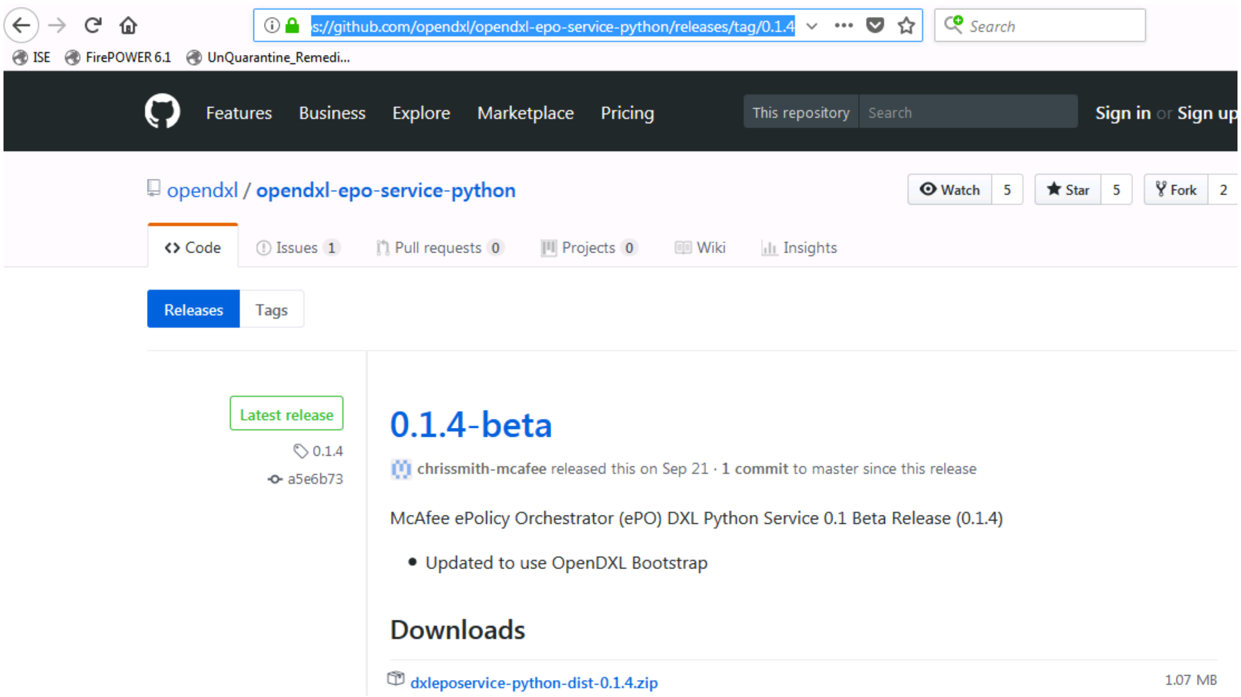
No data found.

Receive notifications from Cisco ISE pxGrid node

Step 1 Create folder dxl_epo_service

Step 2 Change directory to \dxl_epo_service

Step 3 Install ePO DXL Python Service - https://github.com/opendxl/opendxl-epo-service-python/wiki



0.1.4-beta

chrissmith-mcafee released this on Sep 21 · 1 commit to master since this release

McAfee ePolicy Orchestrator (ePO) DXL Python Service 0.1 Beta Release (0.1.4)

- Updated to use OpenDXL Bootstrap

Downloads

dxleposervice-python-dist-0.1.4.zip 1.07 MB

Step 4 Download the latest McAfee Python Client https://github.com/opendxl/opendxl-client-python and run "**python setup.py install**"

```
C:\dxl_epo_service\dxlclient-python-sdk-4.0.0.416\lib\dxlclient-
4.0.0.416\dxlclient-4.0.0.416>python setup.py install

 running install
 running bdist_egg
 running egg_info
 creating dxlclient.egg-info
 writing requirements to dxlclient.egg-info\requires.txt
 writing dxlclient.egg-info\PKG-INFO
 writing top-level names to dxlclient.egg-info\top_level.txt
 writing dependency_links to dxlclient.egg-info\dependency_links.txt
 writing manifest file 'dxlclient.egg-info\SOURCES.txt'
 reading manifest file 'dxlclient.egg-info\SOURCES.txt'
 writing manifest file 'dxlclient.egg-info\SOURCES.txt'
 installing library code to build\bdist.win32\egg
 running install_lib
 running build_py
 creating build
 creating build\lib
 creating build\lib\dxlclient
 copying dxlclient\broker.py -> build\lib\dxlclient
 copying dxlclient\callbacks.py -> build\lib\dxlclient
 copying dxlclient\client.py -> build\lib\dxlclient
 copying dxlclient\client_config.py -> build\lib\dxlclient
 copying dxlclient\exceptions.py -> build\lib\dxlclient
 copying dxlclient\message.py -> build\lib\dxlclient
 copying dxlclient\service.py -> build\lib\dxlclient
 copying dxlclient\_callback_manager.py -> build\lib\dxlclient
 copying dxlclient\_dxl_utils.py -> build\lib\dxlclient
 copying dxlclient\_global_settings.py -> build\lib\dxlclient
 copying dxlclient\_product_props.py -> build\lib\dxlclient
 copying dxlclient\_request_manager.py -> build\lib\dxlclient
 copying dxlclient\_thread_pool.py -> build\lib\dxlclient
 copying dxlclient\_uuid_generator.py -> build\lib\dxlclient
 copying dxlclient\__init__.py -> build\lib\dxlclient
 copying dxlclient\__main__.py -> build\lib\dxlclient
.
.
.
Using c:\python27\lib\site-packages
 Finished processing dependencies for dxlclient==4.0.0.416
```

Step 5 You should see:

```
C:\dxl_epo_service\dxlclient-python-sdk-4.0.0.416\lib\dxlclient-
4.0.0.416\dxlclient-4.0.0.416>dir

  Volume in drive C has no label.
  Volume Serial Number is A49A-C23E

Directory of C:\dxl_epo_service\dxlclient-python-sdk-4.0.0.416\lib\dxlclient-
4.0.0.416\dxlclient-4.0.0.416

 11/26/2017  12:18 PM    <DIR>          .
 11/26/2017  12:18 PM    <DIR>          ..
 11/26/2017  12:18 PM    <DIR>          build
 11/26/2017  12:18 PM    <DIR>          dist
 11/26/2017  12:17 PM    <DIR>          dxlclient
 11/26/2017  12:18 PM    <DIR>          dxlclient.egg-info
 11/26/2017  12:17 PM            15,053 LICENSE
 11/26/2017  12:17 PM             1,890 PKG-INFO
 11/26/2017  12:17 PM             1,157 README
 11/26/2017  12:17 PM                64 setup.cfg
 11/26/2017  12:17 PM             1,891 setup.py
               5 File(s)         20,055 bytes
               6 Dir(s)   5,706,948,608 bytes free
```

Step 6 Install the ePO DXL Python Service - https://github.com/opendxl/opendxl-epo-service-python/wiki

Note: if this has been previously you will see the following messages:

```
C:\dxl_epo_service>pip install dxleposervice

Requirement already satisfied: dxleposervice in c:\python27\lib\site-packages
Requirement already satisfied: dxlbootstrap>=0.1.3 in c:\python27\lib\site-
packages (from dxleposervice)
Requirement already satisfied: requests in c:\python27\lib\site-packages (from
dxleposervice)
Requirement already satisfied: dxlclient in c:\python27\lib\site-packages (from
dxleposervice)
Requirement already satisfied: chardet<3.1.0,>=3.0.2 in c:\python27\lib\site-
packages (from requests->dxleposervice)
Requirement already satisfied: certifi>=2017.4.17 in c:\python27\lib\site-
packages (from requests->dxleposervice)
Requirement already satisfied: urllib3<1.23,>=1.21.1 in c:\python27\lib\site-
packages (from requests->dxleposervice)
Requirement already satisfied: idna<2.7,>=2.5 in c:\python27\lib\site-packages
(from requests->dxleposervice)
Requirement already satisfied: asn1crypto in c:\python27\lib\site-packages
(from dxlclient->dxleposervice)
Requirement already satisfied: oscrypto in c:\python27\lib\site-packages (from
dxlclient->dxleposervice)
Requirement already satisfied: configobj in c:\python27\lib\site-packages (from
dxlclient->dxleposervice)
Requirement already satisfied: six in c:\python27\lib\site-packages (from
dxlclient->dxleposervice)
```

Step 7 Connect to EPO Server, to provision the certificates. eposervice1 can be any name and will be used in the scripts later

Note: The username and password will not be shown while typing; can use the –u username and –p password arguments to denote the admin username and password of the EPO Server.

```
C:\dxl_epo_service\dxleposervice-python-dist-0.1.4\lib\dxleposervice-
0.1.4\dxleposervice-0.1.4>python -m dxlclient provisionconfig . 192.168.1.15
eposervice1
 Enter server username:
 Enter server password:
 INFO: Saving csr file to .\client.csr
 INFO: Saving private key file to .\client.key
 INFO: Saving DXL config file to .\dxlclient.config
 INFO: Saving ca bundle file to .\ca-bundle.crt
 INFO: Saving client certificate file to .\client.crt
```

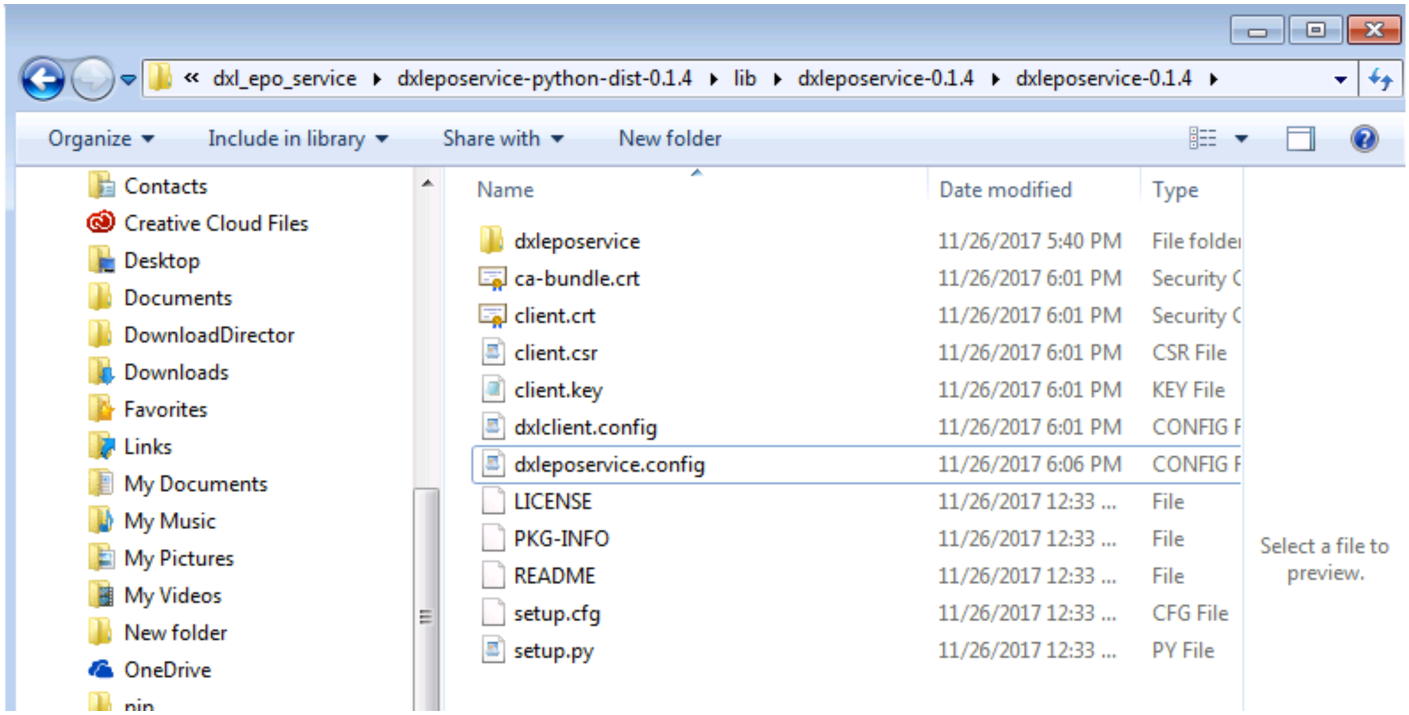
Step 8 Run dxleposervice script

Note: This will fail the first time but it will generate the required configuration file dxleposervice.config.

```
 C:\dxl_epo_service\dxleposervice-python-dist-0.1.4\lib\dxleposervice-
0.1.4\dxleposervice-0.1.4>python -m dxleposervice .

 2017-11-26 17:40:44,953 dxlbootstrap.app INFO     Running application ...
 2017-11-26 17:40:44,953 dxleposervice.app INFO     On 'run' callback.
 2017-11-26 17:40:44,954 dxlbootstrap.app INFO     Configuration file
'dxlclient.  config' not found, creating...
2017-11-26 17:40:44,957 dxlbootstrap.app INFO     Configuration file
'dxleposervice.config' not found, creating...
 2017-11-26 17:40:44,957 dxleposervice.app INFO     On 'load configuration'
callback.
2017-11-26 17:40:44,959 dxleposervice.app INFO     Attempting to determine GUID
 for ePO server: epo1 ...
 2017-11-26 17:40:44,961 dxleposervice._epo ERROR    Error attempting to lookup
GUID for ePO server: epo1
2017-11-26 17:40:44,961 root         ERROR    Error occurred, exiting
 Traceback (most recent call last):
   File "C:\dxl_epo_service\dxleposervice-python-dist-0.1.4\lib\dxleposervice-
0.1.4\dxleposervice-0.1.4\dxleposervice\__main__.py", line 69, in <module>
     app.run()
File "C:\Python27\lib\site-packages\dxlbootstrap\app.py", line 255, in run
     self._load_configuration()
File "C:\Python27\lib\site-packages\dxlbootstrap\app.py", line 217, in _load_c
 Onfiguration self.on_load_configuration(config)
File "dxleposervice\app.py", line 168, in on_load_configuration
     unique_id = epo.lookup_guid()
File "dxleposervice\_epo.py", line 54, in lookup_guid {}, output="json")
File "dxleposervice\_epo.py", line 113, in invoke_command self._save_token()
File "dxleposervice\_epo.py", line 143, in _save_token
     self._token =
self._parse_response(self._send_request('core.getSecurityToken
 '))
File "dxleposervice\_epo.py", line 137, in _send_request verify=self._verify)
File "C:\Python27\lib\site-packages\requests\sessions.py", line 521, in get
     return self.request('GET', url, **kwargs)
File "C:\Python27\lib\site-packages\requests\sessions.py", line 508, in reques
 t resp = self.send(prep, **send_kwargs)
File "C:\Python27\lib\site-packages\requests\sessions.py", line 618, in send
     r = adapter.send(request, **kwargs)
File "C:\Python27\lib\site-packages\requests\adapters.py", line 508, in send
     raise ConnectionError(e, request=request)
ConnectionError: HTTPSConnectionPool(host='%3cepo-server-hostname-or-ip-
address%3e', port=8443): Max retries exceeded with url:
/remote/core.getSecurityToken (Caused by
NewConnectionError('<urllib3.connection.VerifiedHTTPSConnection object
 at 0x02D62170>: Failed to establish a new connection: [Errno 11004]
getaddrinfo failed',))
```

```
2017-11-26 17:40:44,966 dxlbootstrap.app INFO     Destroying application ...
```

Step 9 Edit **\dxl_epo_service\dxleposervice-python-dist-0.1.4\lib\ dxleposervice-python-dist-0.1.4\ dxleposervice-python-dist-0.1.4\dxleposervice.config**



Name	Date modified	Type
dxleposervice	11/26/2017 5:40 PM	File folder
ca-bundle.crt	11/26/2017 6:01 PM	Security C
client.crt	11/26/2017 6:01 PM	Security C
client.csr	11/26/2017 6:01 PM	CSR File
client.key	11/26/2017 6:01 PM	KEY File
dxlclient.config	11/26/2017 6:01 PM	CONFIG F
dxleposervice.config	11/26/2017 6:06 PM	CONFIG F
LICENSE	11/26/2017 12:33 ...	File
PKG-INFO	11/26/2017 12:33 ...	File
README	11/26/2017 12:33 ...	File
setup.cfg	11/26/2017 12:33 ...	CFG File
setup.py	11/26/2017 12:33 ...	PY File

Step 10 Under [epo1] modify the following:
host to be the ip address of ePO
user to be the username of ePO
password to be the password of ePO
verifycertificate = no , this will make it so the script will no verify ePO's certificate. In a production environment it is not recommended to set "Verifycertificate=no" but for testing purposes it is okay.

Note: For more information on configuration on the DXL ePO Service visit https://opendxl.github.io/opendxl-epo-service-python/pydoc/configuration.html

```

###############################################################################
 ## General Section

###############################################################################

 [General]

 # The list of ePO servers to expose to the DXL fabric delimited by commas.
 #
 # For example: epo1,epo2,epo3
 #
```

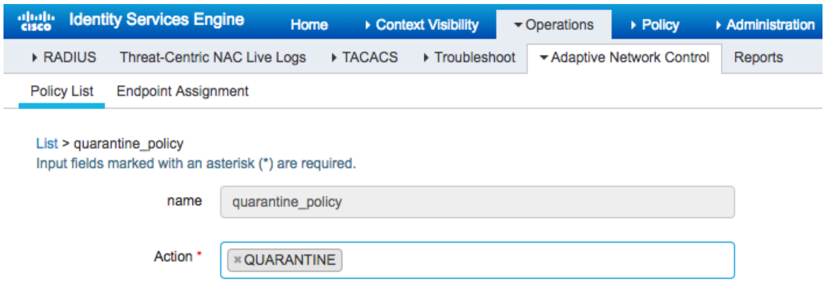
```
# For each ePO name specified, a corresponding section must be defined within
# this configuration file that provides detailed information about the server.
epoNames=epo1


###############################################################################
## ePO section (one section for each name specified in "epoNames")

###############################################################################

[epo1]

# The ePO server hostname or IP address
host=192.168.1.15

# The ePO server communication port (optional, defaults to 8443)
;port=8443

# The name of the user used to login to the ePO server
user=admin

# The password associated with the user used to login to the ePO server
password=Richard08

# A unique identifier used to identify the ePO server on the DXL fabric.
# (optional, if not specified defaults to the GUID of the ePO server)
#
# This unique identifier will be the last portion of the request topic that
# is associated with the ePO server on the fabric.
#
# For example: /mcafee/service/epo/remote/epo1
;uniqueId=epo1

# Whether to verify that the hostname in the ePO's certificate matches the ePO
# server being connected to and that the certificate was signed by a valid
# authority. (optional, enabled by default)
verifyCertificate=no

# A path to a CA Bundle file containing certificates of trusted CAs.
# The CA Bundle is used to ensure that the ePO server being connected to
# was signed by a valid authority.
# (optional, only applicable if "verifyCertificate" is "yes")
;verifyCertBundle=<path-to-bundle-file-or-directory>


###############################################################################
## Settings for the incoming request message pool

###############################################################################

[IncomingMessagePool]

# The queue size for incoming DXL messages (will block when queue is full)
# (optional, defaults to 1000)
;queueSize=1000

# The number of threads available to handle incoming DXL messages
# (optional, defaults to 10)
;threadCount=10
```

Step 11 Run the DXL Python Service

```
C:\dxl_epo_service\dxleposervice-python-dist-0.1.4\lib\dxleposervice-
0.1.4\dxleposervice-0.1.4>python -m dxleposervice .

 2017-11-26 18:12:10,010 dxlbootstrap.app INFO     Running application ...
 2017-11-26 18:12:10,010 dxleposervice.app INFO     On 'run' callback.
 2017-11-26 18:12:10,013 dxleposervice.app INFO     On 'load configuration'
callback.
 2017-11-26 18:12:10,013 dxleposervice.app INFO     Attempting to determine
GUID for ePO server: epo1 ...
 2017-11-26 18:12:10,641 dxleposervice.app INFO     GUID '{b5377fb4-8ba5-4dc2-
a34f-9845c99fa465}' found for ePO server: epo1
 2017-11-26 18:12:10,644 dxleposervice.app INFO     Request topic
'/mcafee/service/epo/remote/{b5377fb4-8ba5-4dc2-a34f-9845c99fa465}' associated
with ePO server: e/epo/remote/{b5377fb4-8ba5-4dc2-a34f-9845c99fa465}'
associated with ePO server:epo1
 2017-11-26 18:12:10,648 dxlbootstrap.app INFO     Incoming message
configuration  : queueSize=1000, threadCount=10
 2017-11-26 18:12:10,650 dxlbootstrap.app INFO     Message callback
configuration  : queueSize=1000, threadCount=10
 2017-11-26 18:12:10,703 dxlbootstrap.app INFO     Attempting to connect to DXL
fabric ...
 2017-11-26 18:12:10,706 dxlclient.client INFO     Waiting for broker list...
 2017-11-26 18:12:10,805 dxlclient.client INFO     Trying to connect...
 2017-11-26 18:12:10,808 dxlclient.client INFO     Trying to connect to broker
{Unique id: {43161380-aea3-11e7-31b5-000c29cbc5d9}, Host name:
dxl.dxl.lab10.com,
 {Unique id: {43161380-aea3-11e7-31b5-000c29cbc5d9}, Host name:
dxl.dxl.lab10.com, IP address: 192.168.1.229, Port: 8883}...
 2017-11-26 18:12:10,845 dxlclient.client INFO     Connected to broker
{43161380- aea3-11e7-31b5-000c29cbc5d9}
 2017-11-26 18:12:10,868 dxlbootstrap.app INFO     Connected to DXL fabric.
 2017-11-26 18:12:10,869 dxleposervice.app INFO     Registering service ...
 2017-11-26 18:12:10,878 dxleposervice.app INFO     Service registration
succeeded.
 2017-11-26 18:12:10,878 dxleposervice.app INFO     On 'DXL connect' callback.
```

Step 12 Open up another terminal window, this will be required to run the python quarantine script

Step 13 Select **Operations->Adaptive Network Control->Policy List->Add**



List > quarantine_policy

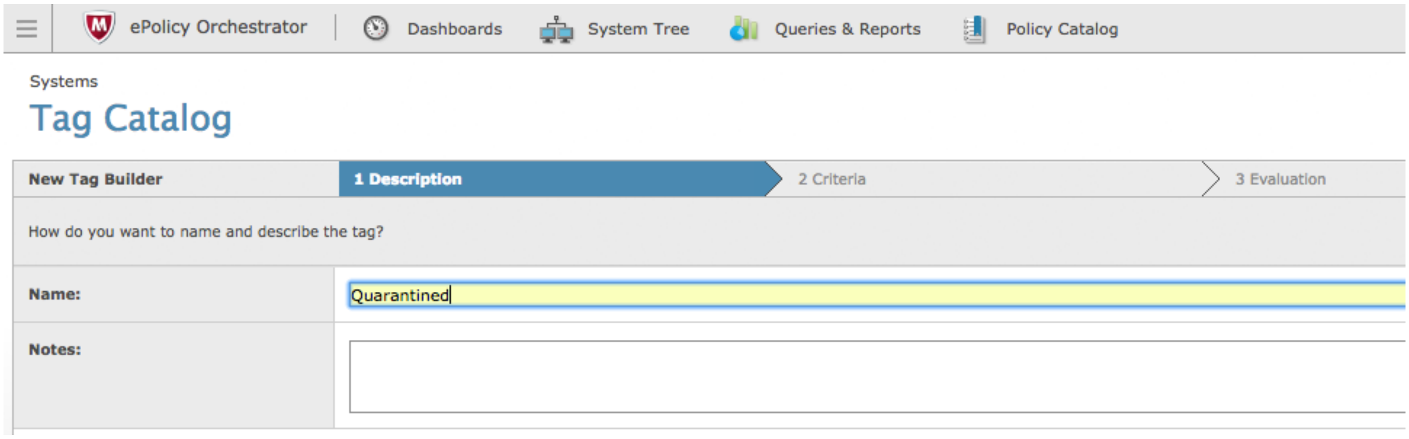
Input fields marked with an asterisk (*) are required.

name: quarantine_policy

Action *: QUARANTINE

Step 14 Select **Submit**

Step 15 Select **Menu->Systems->Tag Catalog->New Tag->Quarantined**



Systems

Tag Catalog

New Tag Builder — 1 Description — 2 Criteria — 3 Evaluation

How do you want to name and describe the tag?

Name: Quarantined

Notes:

Step 16 Select **Menu->Systems->Tag Catalog->New Tag->Quarantined**

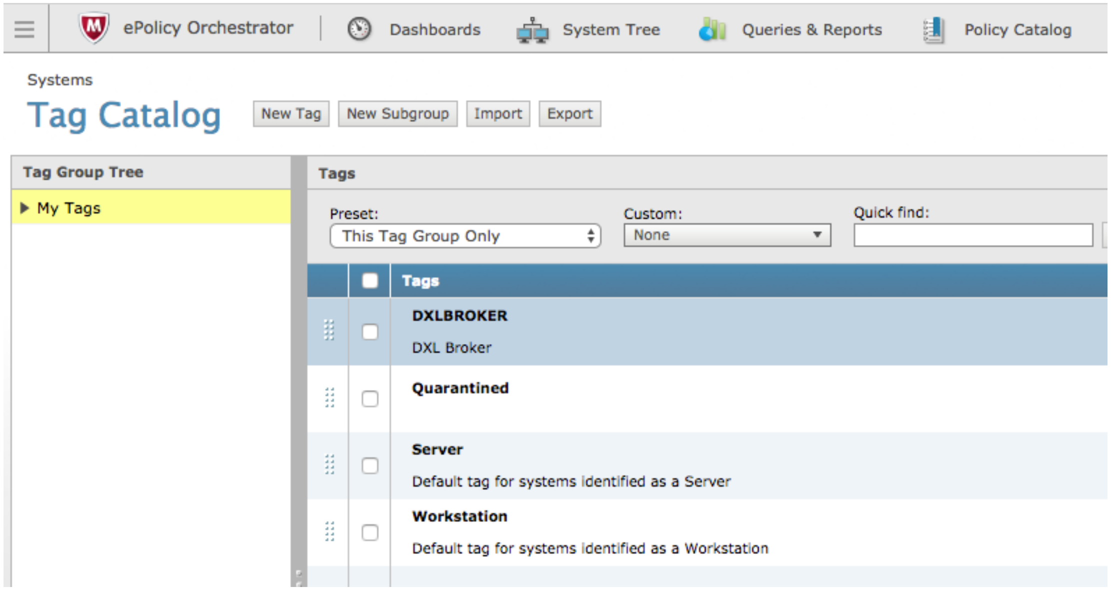
Step 17 Select **Next**

Step 18 Keep the defaults for **Criteria** and select **Next**

Step 19 Keep the defaults for **Evaluation** and select **Next**

Step 20 Keep the defaults for **Preview** and select **Save**

You should see:



Systems

Tag Catalog

Tag Group Tree: My Tags

Tags

Preset: This Tag Group Only

Custom: None

Quick find:

Tags
DXLBROKER DXL Broker
Quarantined
Server Default tag for systems identified as a Server
Workstation Default tag for systems identified as a Workstation

Step 21 On the second terminal window, Create folder dxl_clientquar1

Step 22 Change directory to dxl_clientquar1

Step 23 Install and extract the latest Cisco pxGrid DXL Python Client (https://github.com/opendxl/opendxl-pxgrid-client-python) in the **\dxl_clientquar1** folder

Step 24 Install Cisco pxGrid DXL client

```
C:\dxl_clientquar1>pip install dxlepoclient
 Requirement already satisfied: dxlepoclient in c:\python27\lib\site-packages
 Requirement already satisfied: dxlclient in c:\python27\lib\site-packages
(from dxlepoclient)
 Requirement already satisfied: asn1crypto in c:\python27\lib\site-packages
(from dxlclient->dxlepoclient)
 Requirement already satisfied: oscrypto in c:\python27\lib\site-packages (from
dxlclient->dxlepoclient)
Requirement already satisfied: configobj in c:\python27\lib\site-packages (from
 dxlclient->dxlepoclient)
Requirement already satisfied: requests in c:\python27\lib\site-packages (from
dxlclient->dxlepoclient)
 Requirement already satisfied: six in c:\python27\lib\site-packages (from
dxlclient->dxlepoclient)
 Requirement already satisfied: chardet<3.1.0,>=3.0.2 in c:\python27\lib\site-
packages (from requests->dxlclient->dxlepoclient)
 Requirement already satisfied: certifi>=2017.4.17 in c:\python27\lib\site-
packages (from requests->dxlclient->dxlepoclient)
 Requirement already satisfied: urllib3<1.23,>=1.21.1 in c:\python27\lib\site-
packages (from requests->dxlclient->dxlepoclient)
 Requirement already satisfied: idna<2.7,>=2.5 in c:\python27\lib\site-packages
(from requests->dxlclient->dxlepoclient)
```

Step 25 Change directories to the "sample" directory under the contents you just unzipped

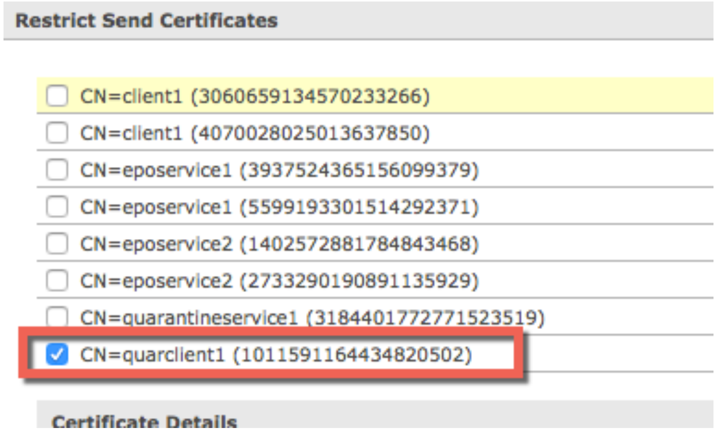
Step 26 Provision certificates for the Cisco pxGrid DXL Python Client to use

```
C:\dxl_clientquar1\dxlclient-python-sdk-4.0.0.416\sample>python -m dxlclient
provisionconfig . 192.168.1.15 quarclient1
 Enter server username:
 Enter server password:
 INFO: Saving csr file to .\client.csr
 INFO: Saving private key file to .\client.key
 INFO: Saving DXL config file to .\dxlclient.config
 INFO: Saving ca bundle file to .\ca-bundle.crt
 INFO: Saving client certificate file to .\client.crt
```

Note: The "quarclient1" text can be any name and will be used in the scripts later. The username and password will not be shown while typing; can use the –u username and –p password arguments to denote the admin username and password of the EPO Server.

Note: For more information on provisioning an OpenDXL Python Client see the documentation here: https://opendxl.github.io/opendxl-client-python/pydoc/basiccliprovisioning.html.

Step 27 Need to authorize the certificate created while provisioning the Cisco pxGrid DXL Python Client to send and receive pxGrid notifications in ePO
Select **Menu->Configuration->Server Settings-DXL Topic Authorization->Edit->DXL Cisco pxGrid Queries->Actions-> Restrict send certificates->select the certificate with a name of "quarclient1" or whatever name you used in Step 8**



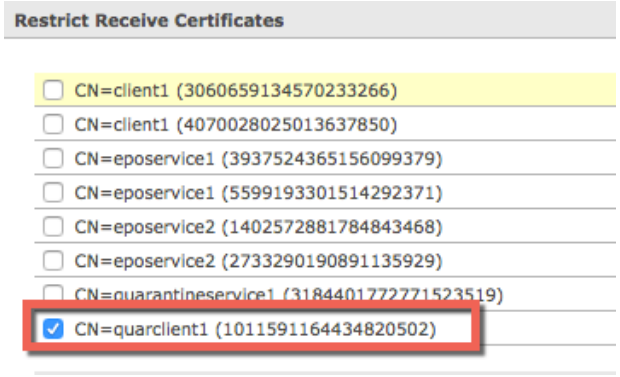
Restrict Send Certificates

□ CN=client1 (3060659134570233266)
□ CN=client1 (4070028025013637850)
□ CN=eposervice1 (3937524365156099379)
□ CN=eposervice1 (5599193301514292371)
□ CN=eposervice2 (1402572881784843468)
□ CN=eposervice2 (2733290190891135929)
□ CN=quarantineservice1 (3184401772771523519)
☑ CN=quarclient1 (1011591164434820502)

Certificate Details

Step 28 Select OK

Step 29 Select **Menu->Configuration->Server Settings->DXL Topic Authorization->Edit->DXL Cisco pxGrid Queries->Actions->Restrict Receive certificates->Select the certificate with name of "quarclient1" or whatever you named it in Step 8.**

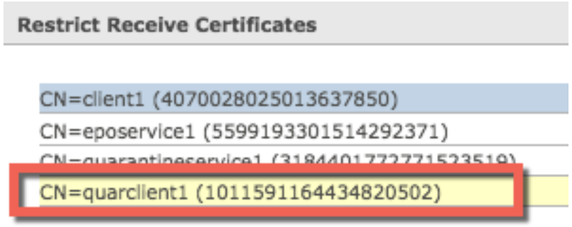


Restrict Receive Certificates

□ CN=client1 (3060659134570233266)
□ CN=client1 (4070028025013637850)
□ CN=eposervice1 (3937524365156099379)
□ CN=eposervice1 (5599193301514292371)
□ CN=eposervice2 (1402572881784843468)
□ CN=eposervice2 (2733290190891135929)
□ CN=quarantineservice1 (3184401772771523519)
☑ CN=quarclient1 (1011591164434820502)

Step 30 Select OK

Step 31 Select **Menu->Configuration->Server Settings->DXL Topic Authorization->Edit->DXL Cisco pxGrid Notifications->Actions->Receive Restrictions->Restrict Receive certificates->Select the certificate with name of "quarclient1" or whatever you named it in Step 8.**



Restrict Receive Certificates

CN=client1 (4070028025013637850)
CN=eposervice1 (5599193301514292371)
CN=quarantineservice1 (3184401772771523519)
CN=quarclient1 (1011591164434820502)

Step 32 Select OK

Step 33 Select **Save**

Step 34 In the "dxl_clientquar1\dxlclient-python-sdk-4.0.0.416\sample\basic" directory create a file called apply_tag_on_anc_notification.py.

Step 35 Edit apply_tag_on_anc_notification.py and add the following python code:
ANC_POLICY_NAME is the pre-defined ISE ANC policy (i.e. quarantine_policy)
EPO_TAG_NAME is the tag created in McAfee ePO (i.e. Quarantined)

Note: QUARANTINE_TAG is not the ISE Security Group Tag

```
 import os
 import sys
 import time

 from threading import Thread
 from dxlbootstrap.util import MessageUtils
 from dxlclient.client_config import DxlClientConfig
 from dxlclient.client import DxlClient
 from dxlclient._thread_pool import ThreadPool
 from dxlepoclient import EpoClient

 root_dir = os.path.dirname(os.path.abspath(__file__))
 sys.path.append(root_dir + "/../..")
 sys.path.append(root_dir + "/..")

 from dxlciscopxgridclient.client import CiscoPxGridClient
 from dxlciscopxgridclient.callbacks import AncApplyEndpointPolicyCallback

 # Import common logging and configuration
 from common import *

 # Configure local logger
 logger = logging.getLogger(__name__)

 # Create DXL configuration from file
 config = DxlClientConfig.create_dxl_config_from_file(CONFIG_FILE)

 # ISE ANC policy name to listen for ISE policy application
 ANC_POLICY_NAME = "quarantine_policy"
 # ePO tag name to apply to systems we receive notifications of the
ANC_POLICY_NAME being applied to
 EPO_TAG_NAME = "Quarantined"

 # The default size for the callback thread pool queue size
 CALLBACKS_QUEUE_SIZE = 10
 # The default number of threads for the callback thread pool
 CALLBACKS_THREAD_COUNT = 10


 # Tag system in ePO by MAC
 def tag_system_in_epo_by_mac(the_epo_client, mac_address):
     try:
         # Get system information from ePO for the input MAC address
         system_find_res = the_epo_client.run_command("system.find",
{"searchText": mac_address.replace(":", "")})

         # Convert response message in to a dictionary
         system_find_res_dict = MessageUtils.json_to_dict(system_find_res)

         if not system_find_res_dict:
             print("No system with MAC address \"" + mac_address + "\" found in
ePO.")
             return

         logger.debug("system_find_res_dict: " + str(system_find_res_dict))

         tag_system_in_epo_by_ip(the_epo_client,
system_find_res_dict[0]["EPOComputerProperties.IPAddress"])
     except Exception as ex:
         logger.exception("Error in tag_system_in_epo_by_mac")


 # Tag system in ePO by IP address
 def tag_system_in_epo_by_ip(the_epo_client, ip_address):
     try:
         # Call ePO remote command to apply a tag for the first system found
for the input MAC address
         apply_tag_res = the_epo_client.run_command("system.applyTag",
{"names": ip_address, "tagName": EPO_TAG_NAME})

         logger.debug("apply_tag_res: " + apply_tag_res)

         print("Response for applying \"" + EPO_TAG_NAME + "\" tag in ePO:")
         if apply_tag_res == "1":
             print("Success")
         else:
             print("Failed. Request to assign tag " + EPO_TAG_NAME +
                   " did not return a success value. See Orion.log on ePO
server for more information.")

     except Exception as ex:
         logger.exception("Error in tag_system_in_epo_by_ip")


 try:
     # Create thread pool
     callbacks_pool = ThreadPool(CALLBACKS_QUEUE_SIZE, CALLBACKS_THREAD_COUNT,
"CallbacksPool")

     # Create the client
     with DxlClient(config) as dxl_client:

         # Connect to the fabric
         dxl_client.connect()

         logger.info("Connected to DXL fabric.")

         epo_client = EpoClient(dxl_client)

         # Create client wrapper
         client = CiscoPxGridClient(dxl_client)


         class
MyAncApplyEndpointPolicyCallback(AncApplyEndpointPolicyCallback):
             def on_apply_endpoint_policy(self, apply_dict):
                 if apply_dict["policyName"] == ANC_POLICY_NAME:
                     print("Received notification of ANC policy \"" +
ANC_POLICY_NAME +
                           "\" being applied from pxGrid:\n" +
                           MessageUtils.dict_to_json(apply_dict,
pretty_print=True))

                     # Add to the thread pool to send synchronous request to
ePO to tag the system
                     if "macAddress" in apply_dict:
                         print("Attempting to apply tag \"" + EPO_TAG_NAME +
"\" for MAC address "
                               + apply_dict["macAddress"] + ".")
                         callbacks_pool.add_task(tag_system_in_epo_by_mac,
epo_client, apply_dict["macAddress"])
                     elif "ipAddress" in apply_dict:
                         print("Attempting to apply tag \"" + EPO_TAG_NAME +
"\" for IP address "
                               + apply_dict["ipAddress"] + ".")
                         callbacks_pool.add_task(tag_system_in_epo_by_ip,
epo_client, apply_dict["ipAddress"])

         # Attach callback for ANC Apply Endpoint Policy events

client.anc.add_apply_endpoint_policy_callback(MyAncApplyEndpointPolicyCallback(
))

         # Wait forever
         print("Waiting for ANC Apply endpoint policy events...")
         while True:
             time.sleep(60)

 finally:
     if callbacks_pool is not None:
         logger.info("Shutting down thread pool.")
         callbacks_pool.shutdown()
         logger.info("Thread pool shutdown.")
```

Step 36 Save apply_tag_on_anc_notification.py and then run it:

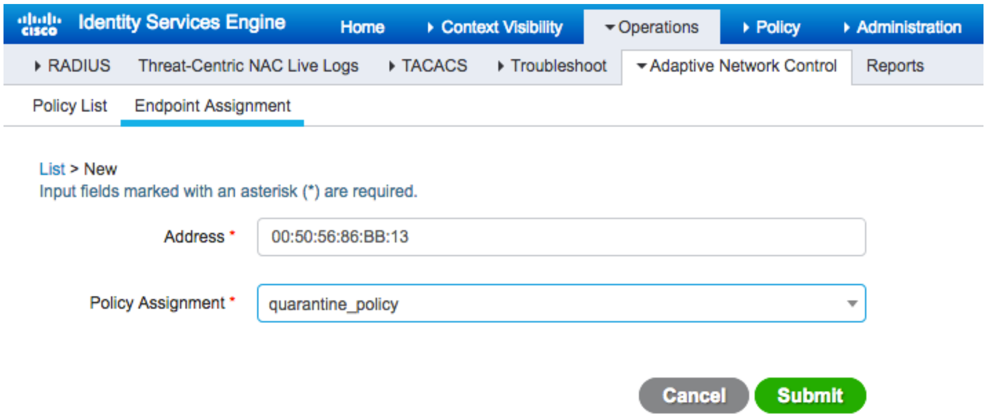
```
C:\dxl_clientquar1\dxlclient-python-sdk-4.0.0.416\sample\basic>dir
 Volume in drive C has no label.
 Volume Serial Number is A49A-C23E

 Directory of C:\dxl_clientquar1\dxlclient-python-sdk-4.0.0.416\sample\basic

11/26/2017  07:54 PM    <DIR>          .
11/26/2017  07:54 PM    <DIR>          ..
11/26/2017  07:53 PM             1,906 apply_tag_on_anc_notification.py
11/26/2017  07:31 PM             2,624 event_example.py
11/26/2017  07:31 PM             2,624 orig_event_example.py
               3 File(s)          7,154 bytes
               2 Dir(s)   6,035,963,904 bytes free

C:\dxl_clientquar1\dxlclient-python-sdk-4.0.0.416\sample\basic>python
apply_tag_on_anc_notification.py

Waiting for ANC Apply endpoint policy events...
```

Testing

Step 1 In ISE, select **Operations->Adaptive Network Control->Endpoint Assignment**

Step 2 Assign the endpoint MAC address to the quarantine_policy.

Note: IP Addresses can also be assigned



List > New

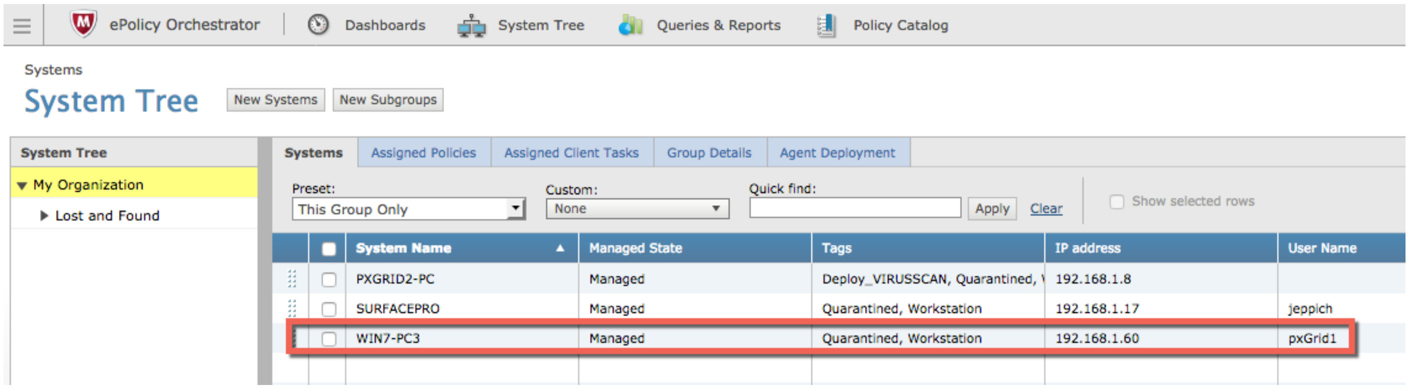
Input fields marked with an asterisk (*) are required.

Address * 00:50:56:86:BB:13

Policy Assignment * quarantine_policy

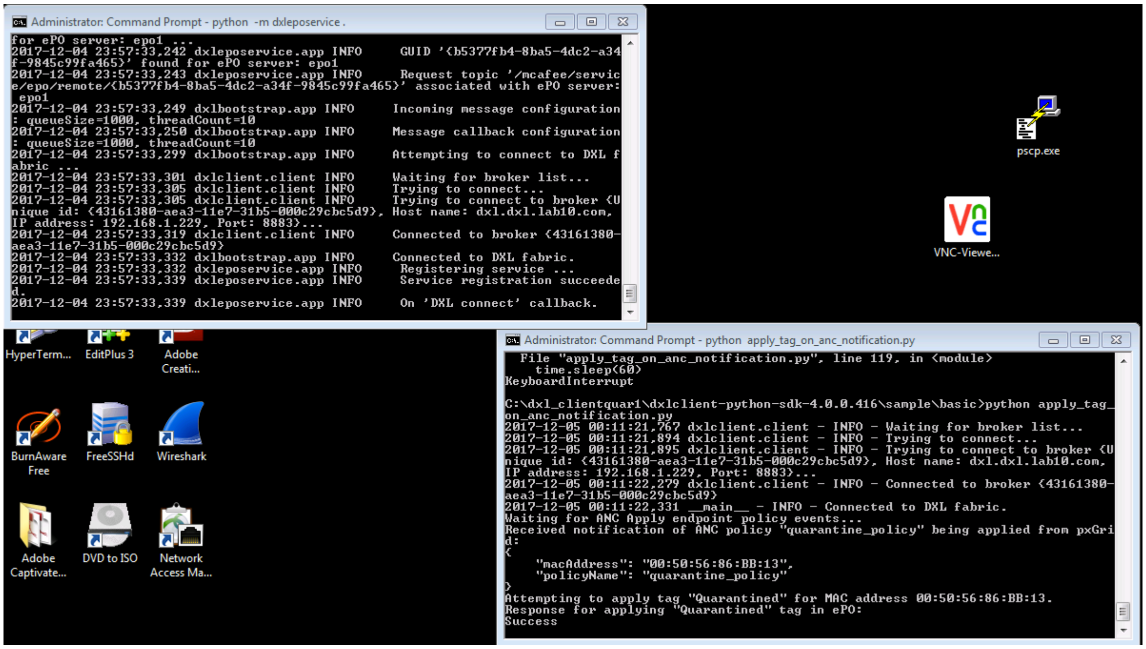
Step 3 Select **Submit**

Step 4 Select **System Tree**



System Name	Managed State	Tags	IP address	User Name
PXGRID2-PC	Managed	Deploy_VIRUSSCAN, Quarantined, \	192.168.1.8	
SURFACEPRO	Managed	Quarantined, Workstation	192.168.1.17	jeppich
WIN7-PC3	Managed	Quarantined, Workstation	192.168.1.60	pxGrid1

Step 5 Below we see the MAC address of the endpoint and the payload of the quarantine_policy



Administrator: Command Prompt - python -m dxleposervice .

```
for ePO server: epo1 ...
2017-12-04 23:57:33,242 dxleposervice.app INFO     GUID '{b5377fb4-8ba5-4dc2-a34
f-9845c99fa465}' found for ePO server: epo1
2017-12-04 23:57:33,243 dxleposervice.app INFO     Request topic '/mcafee/servic
e/epo/remote/{b5377fb4-8ba5-4dc2-a34f-9845c99fa465}' associated with ePO server:
 epo1
2017-12-04 23:57:33,249 dxlbootstrap.app INFO     Incoming message configuration
: queueSize=1000, threadCount=10
2017-12-04 23:57:33,250 dxlbootstrap.app INFO     Message callback configuration
: queueSize=1000, threadCount=10
2017-12-04 23:57:33,299 dxlbootstrap.app INFO     Attempting to connect to DXL f
abric ...
2017-12-04 23:57:33,301 dxlclient.client INFO     Waiting for broker list...
2017-12-04 23:57:33,305 dxlclient.client INFO     Trying to connect...
2017-12-04 23:57:33,305 dxlclient.client INFO     Trying to connect to broker {U
nique id: {43161380-aea3-11e7-31b5-000c29cbc5d9}, Host name: dxl.dxl.lab10.com,
IP address: 192.168.1.229, Port: 8883}...
2017-12-04 23:57:33,319 dxlclient.client INFO     Connected to broker {43161380-
aea3-11e7-31b5-000c29cbc5d9}
2017-12-04 23:57:33,332 dxlbootstrap.app INFO     Connected to DXL fabric.
2017-12-04 23:57:33,332 dxleposervice.app INFO     Registering service ...
2017-12-04 23:57:33,339 dxleposervice.app INFO     Service registration succeede
d.
2017-12-04 23:57:33,339 dxleposervice.app INFO     On 'DXL connect' callback.
```

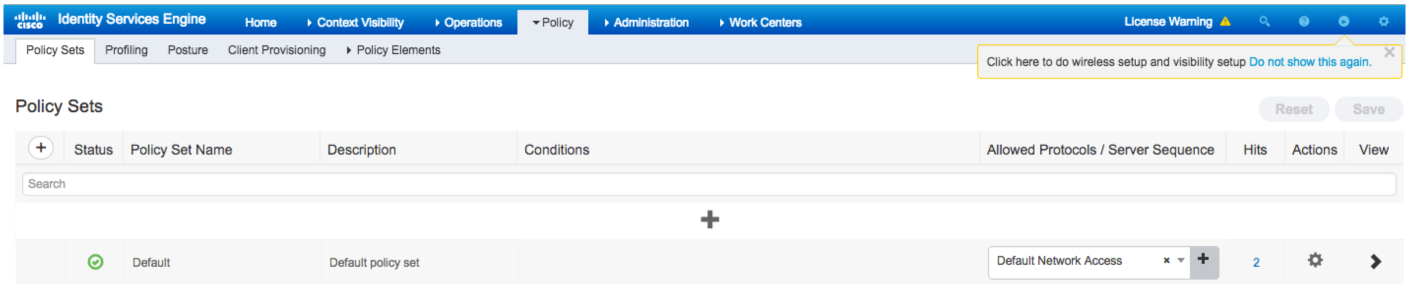
Administrator: Command Prompt - python apply_tag_on_anc_notification.py

```
  File "apply_tag_on_anc_notification.py", line 119, in <module>
    time.sleep(60)
KeyboardInterrupt

C:\dxl_clientquar1\dxlclient-python-sdk-4.0.0.416\sample\basic>python apply_tag_
on_anc_notification.py
2017-12-05 00:11:21,767 dxlclient.client - INFO - Waiting for broker list...
2017-12-05 00:11:21,894 dxlclient.client - INFO - Trying to connect...
2017-12-05 00:11:21,895 dxlclient.client - INFO - Trying to connect to broker {U
nique id: {43161380-aea3-11e7-31b5-000c29cbc5d9}, Host name: dxl.dxl.lab10.com,
IP address: 192.168.1.229, Port: 8883}...
2017-12-05 00:11:22,279 dxlclient.client - INFO - Connected to broker {43161380-
aea3-11e7-31b5-000c29cbc5d9}
2017-12-05 00:11:22,331 __main__ - INFO - Connected to DXL fabric.
Waiting for ANC Apply endpoint policy events...
Received notification of ANC policy "quarantine_policy" being applied from pxGri
d:
{
    "macAddress": "00:50:56:86:BB:13",
    "policyName": "quarantine_policy"
}
Attempting to apply tag "Quarantined" for MAC address 00:50:56:86:BB:13.
Response for applying "Quarantined" tag in ePO:
Success
```

Step 6 To se in ISE, need to add ANC "quarantined_policy" to ISE

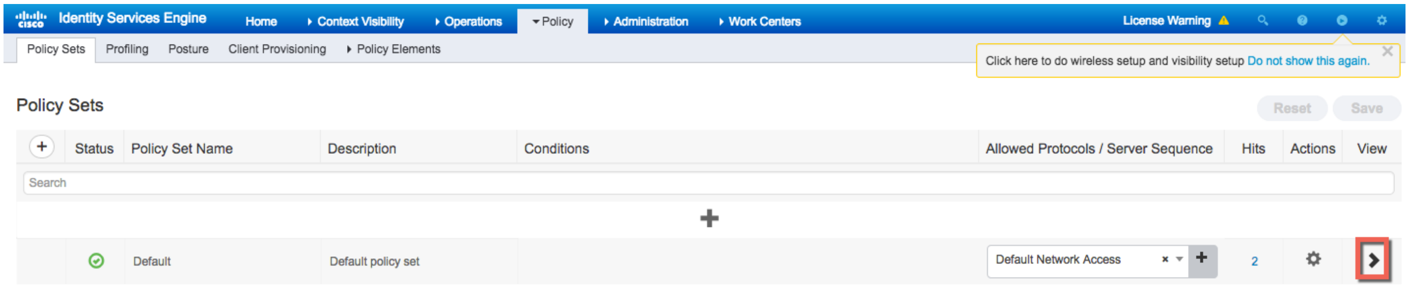
Step 7 Select **Policy->Policy Sets**

You should see:



+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	✓	Default	Default policy set		Default Network Access	2	⚙	>

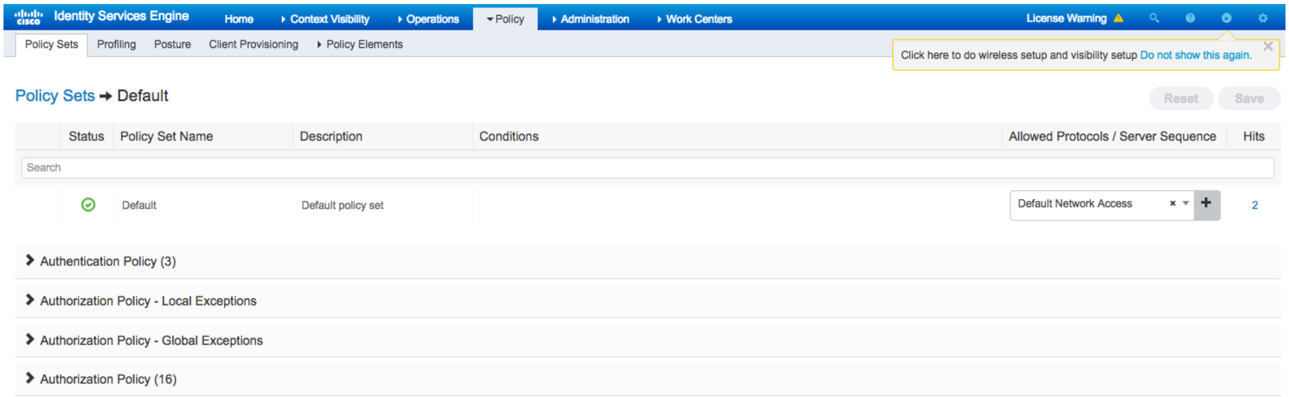
Step 8 Select " **>**" below



Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	✓	Default	Default policy set		Default Network Access	2	⚙	>

You should see:



Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	2

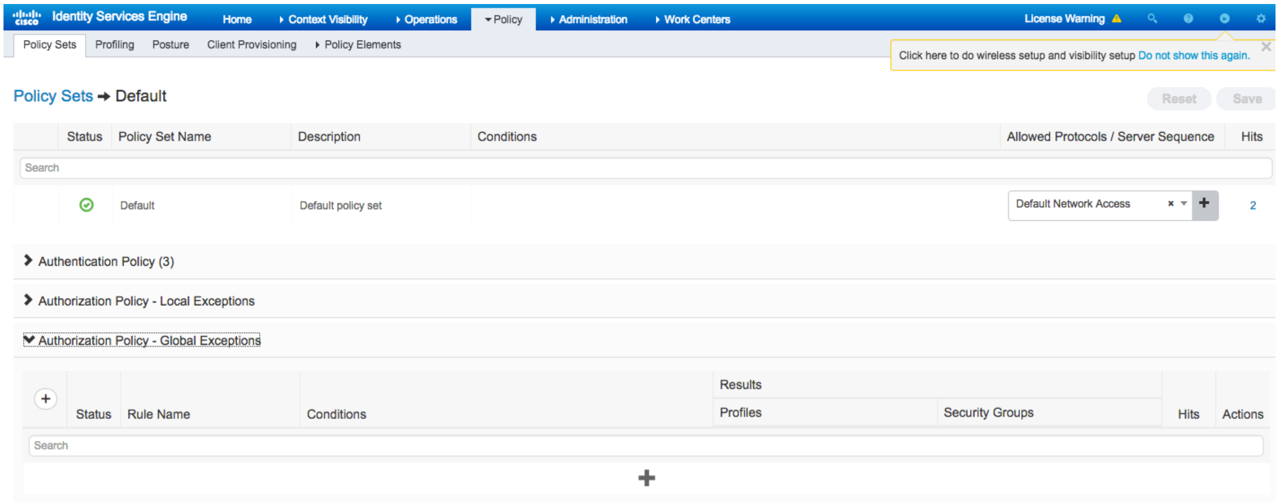
> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

> Authorization Policy (16)

Step 9 Select **Authorization Policy –> Global Exceptions**
You should see:



Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	2

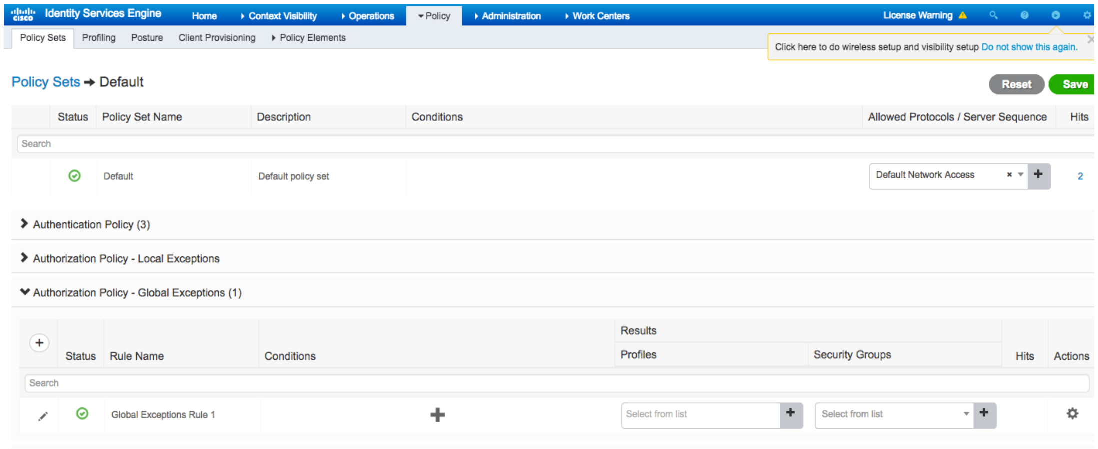
> Authentication Policy (3)

> Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

				Results			
+	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

Step 10 Select "+""
You should see:



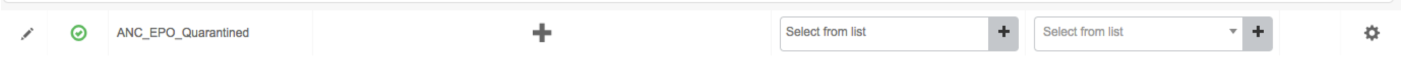
Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search					
✓	Default	Default policy set		Default Network Access	2

- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions (1)

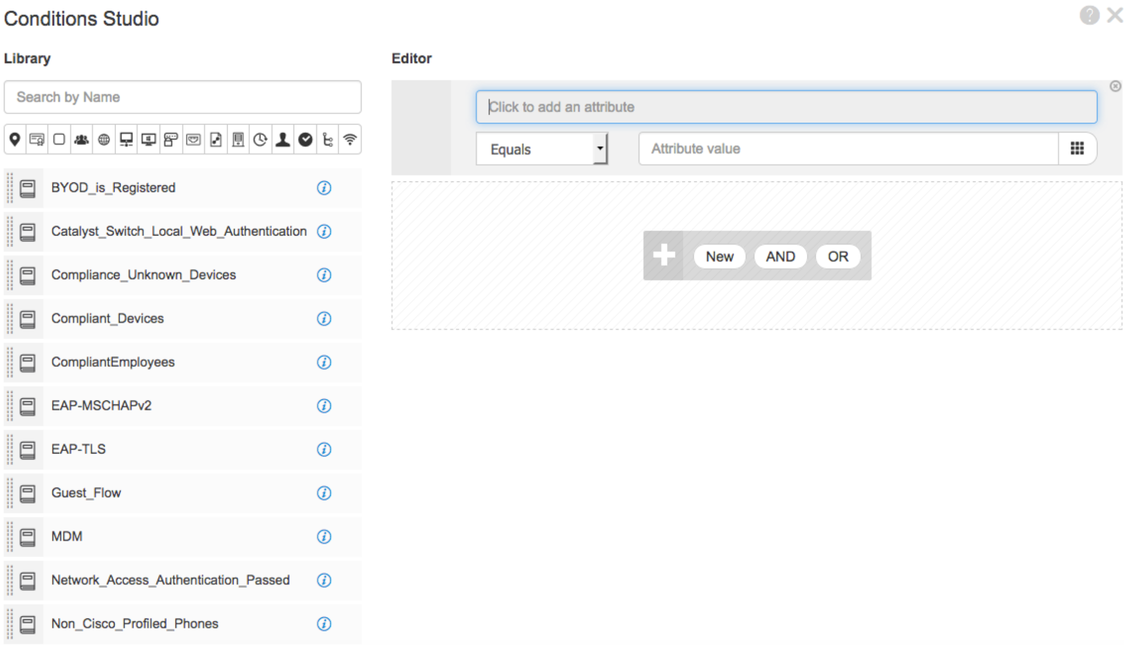
	Status	Rule Name	Conditions	Results Profiles	Results Security Groups	Hits	Actions
Search							
	✓	Global Exceptions Rule 1	+	Select from list	Select from list		

Step 11 Under “**Rule Name**” type **ANC_EPO Quarantined,** select “**+**”



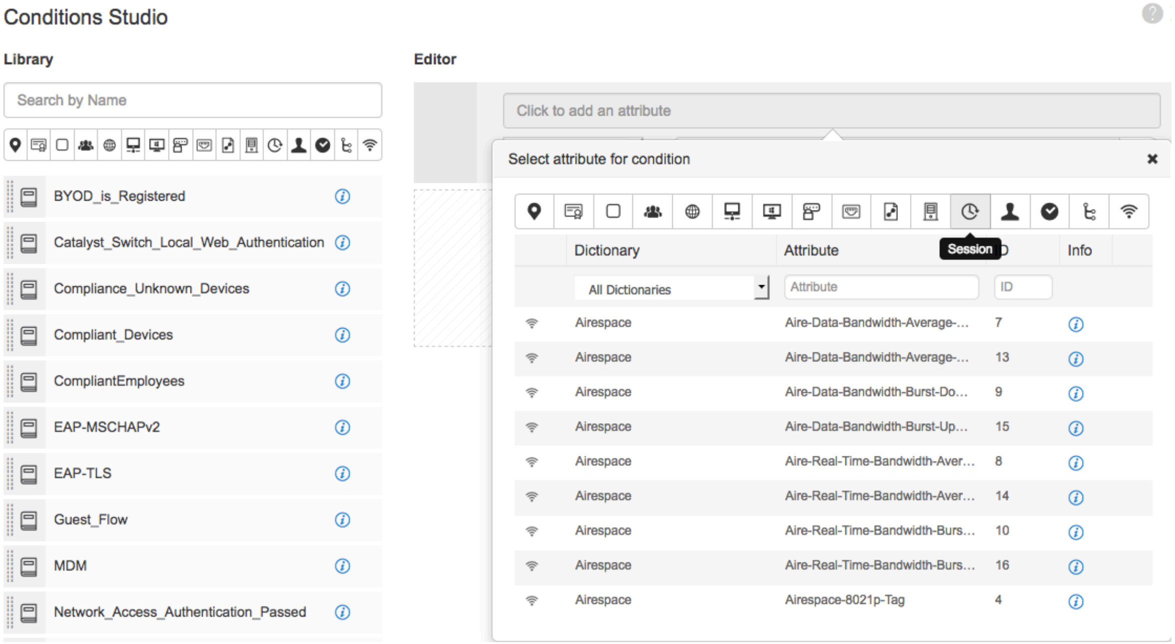
✓	ANC_EPO_Quarantined	+	Select from list	Select from list

Step 12 You should see:



- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- CompliantEmployees
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MDM
- Network_Access_Authentication_Passed
- Non_Cisco_Profiled_Phones

Step 13 Under Editor, “**Click to add an attribute**”, select “**Session**”



Conditions Studio

Library

Search by Name

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- CompliantEmployees
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MDM
- Network_Access_Authentication_Passed

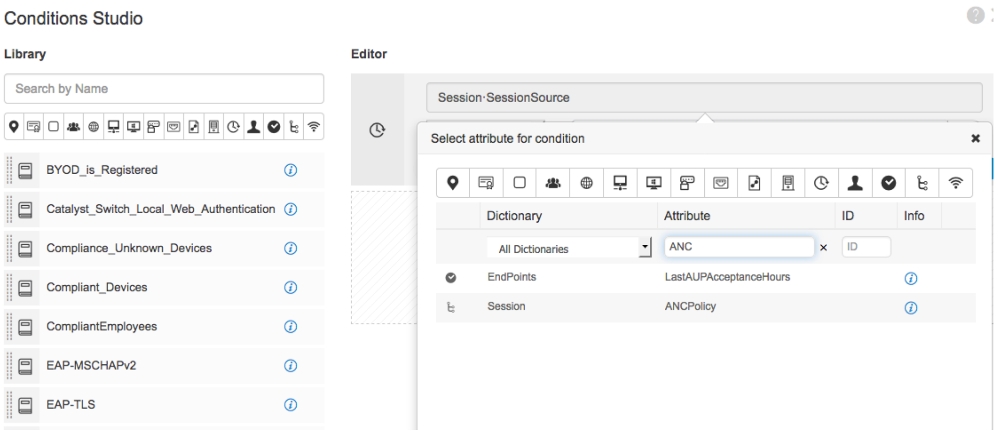
Editor

Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
Airespace	Aire-Data-Bandwidth-Average-...	7	ⓘ
Airespace	Aire-Data-Bandwidth-Average-...	13	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Do...	9	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Up...	15	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Aver...	8	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Aver...	14	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Burs...	10	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Burs...	16	ⓘ
Airespace	Airespace-8021p-Tag	4	ⓘ

Step 14 In the attribute field, type in "**ANC**"



Conditions Studio

Library

Search by Name

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- CompliantEmployees
- EAP-MSCHAPv2
- EAP-TLS

Editor

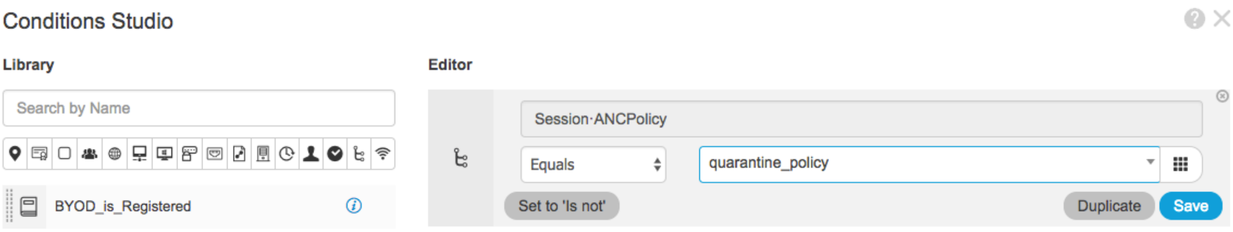
Session·SessionSource

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	ANC	ID	
EndPoints	LastAUPAcceptanceHours		ⓘ
Session	ANCPolicy		ⓘ

Step 15 Select "**ANCPolicy**"

Step 16 From the drop down select "**quarantine_policy**"



Conditions Studio

Library

Search by Name

- BYOD_is_Registered

Editor

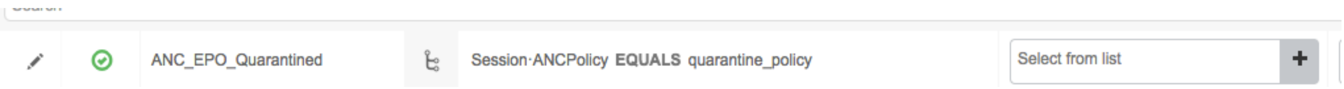
Session·ANCPolicy

Equals

quarantine_policy

Step 17 Select "**Use**"

You should see:



ANC_EPO_Quarantined | Session·ANCPolicy **EQUALS** quarantine_policy | Select from list

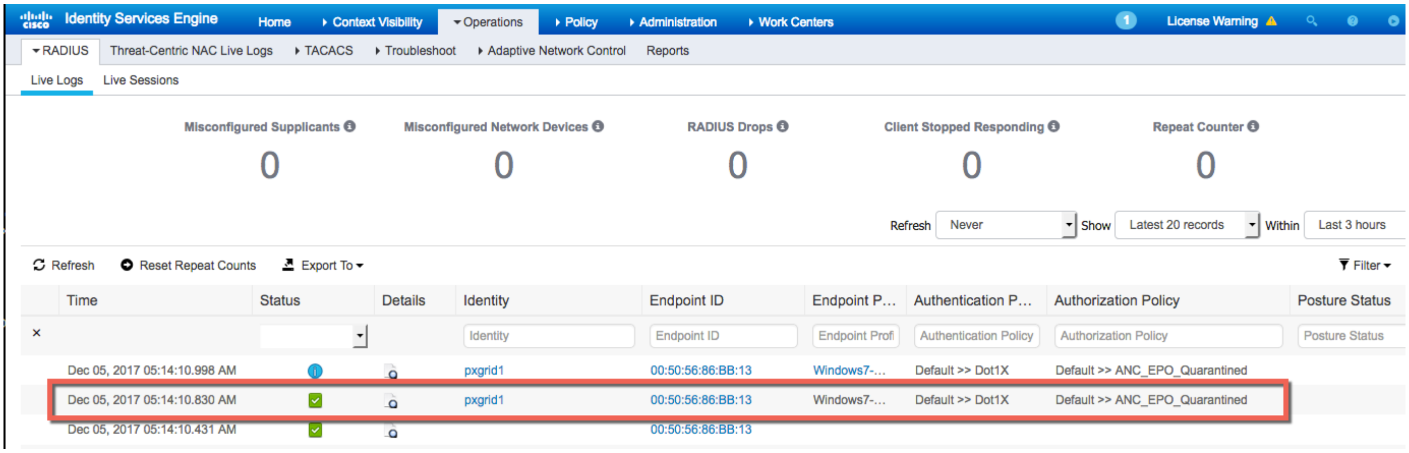
Step 18 Under **Profiles**, select **Permit Access**

Step 19 Under **Security Groups**, select **Quarantined Systems**

Step 20 Select **Save**

Step 21 Log out and log in should now see the endpoint has been quarantined in ISE

Note: You can also select Operations->RADIUS->Live Sessions->Action->Show COA Actions->Session Reauthentication for the selected user



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

Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

Time	Status	Details	Identity	Endpoint ID	Endpoint P...	Authentication P...	Authorization Policy	Posture Status
Dec 05, 2017 05:14:10.998 AM	i		pxgrid1	00:50:56:86:BB:13	Windows7-...	Default >> Dot1X	Default >> ANC_EPO_Quarantined	
Dec 05, 2017 05:14:10.830 AM	✓		pxgrid1	00:50:56:86:BB:13	Windows7-...	Default >> Dot1X	Default >> ANC_EPO_Quarantined	
Dec 05, 2017 05:14:10.431 AM	✓			00:50:56:86:BB:13				

ISE ePO Posture Check and Remediation (optional)

Posture

In this section, ISE posture will be configured. This includes obtaining the latest Opswat libraries, configuring posture conditions, remediation rules and posture requirements and the Posture Policy. This also includes uploading the AnyConnect modules and creating a Client Provisioning Policy for the Cisco AnyConnect client configuration files.

The example in this document, checks to ensure the McAfee Agent is running. If this service is not running, a remediation link will be provided to download the McAfee Agent. This link will be created and come from EPO and will be provided in an ISE remediation posture link to the end-user if non-compliant, if the service has stopped running or if it does not exist.

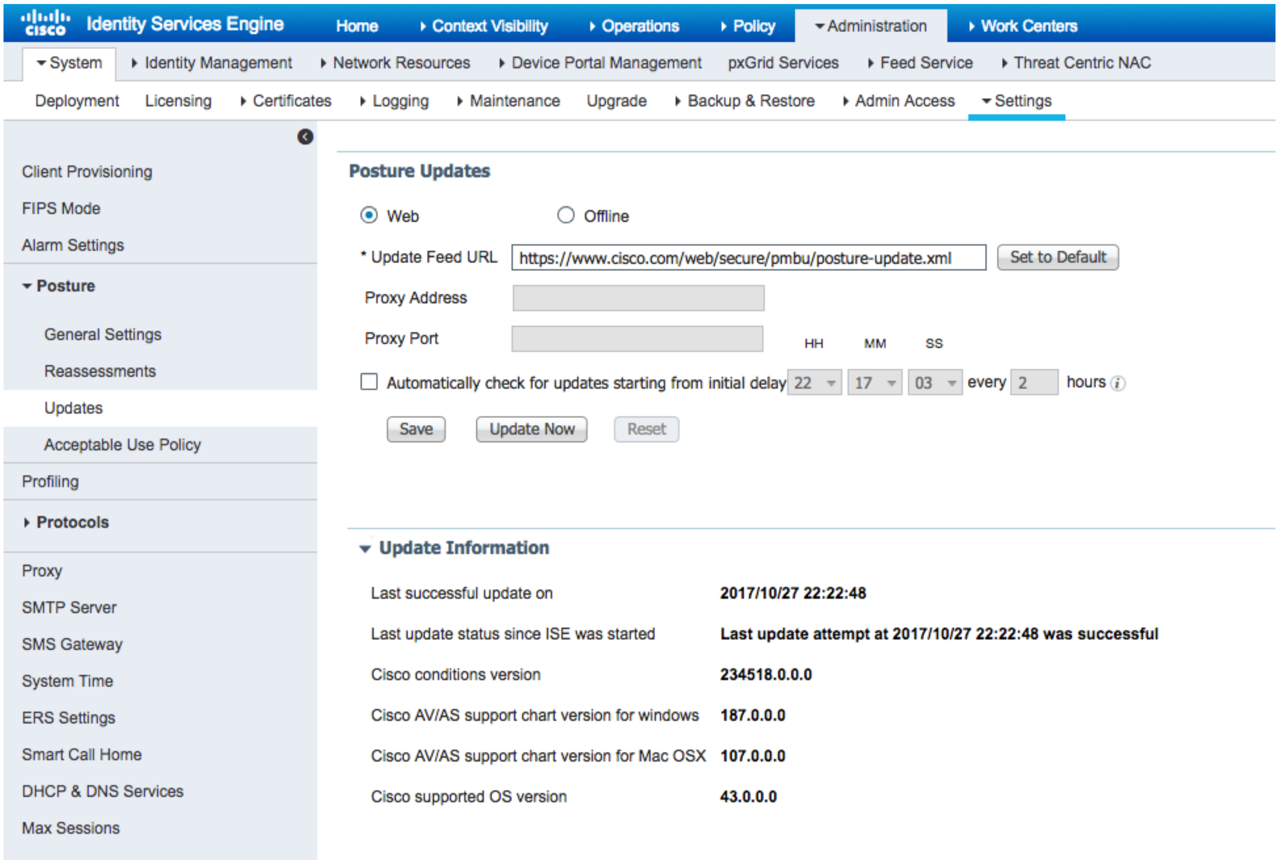
A service posture condition rule will be created to check to see if the McAfee Agent service is running. A remediation link will be created. The McAfee Agent link will be created in McAfee ePO and will be provided in the ISE remediation condition rule. A posture requirement rule will be created that ties this all together. For example, if the McAfee Agent Service is not running, the endpoint will be non-compliant and the McAfee ePO remediation link will be provided to the end-user. The end-user installs the downloaded agent executable from McAfee ePO, and will be re-scanned. Now the endpoint is in compliance, since the McAfee agent service is running.

The ISE Posture policy will contain the ISE posture agent and the posture compliance policy. The ISE Client Provisioning Policy will contain the Cisco AnyConnect Configuration files.

Configuring Posture Updates

Step 1 Select **Administration->System->Settings->Posture->Updates->Update Now**

Step 2 You should see:



Posture Updates

● Web ○ Offline

* Update Feed URL: https://www.cisco.com/web/secure/pmbu/posture-update.xml

Proxy Address:

Proxy Port:

□ Automatically check for updates starting from initial delay HH 22 MM 17 SS 03 every 2 hours

Update Information

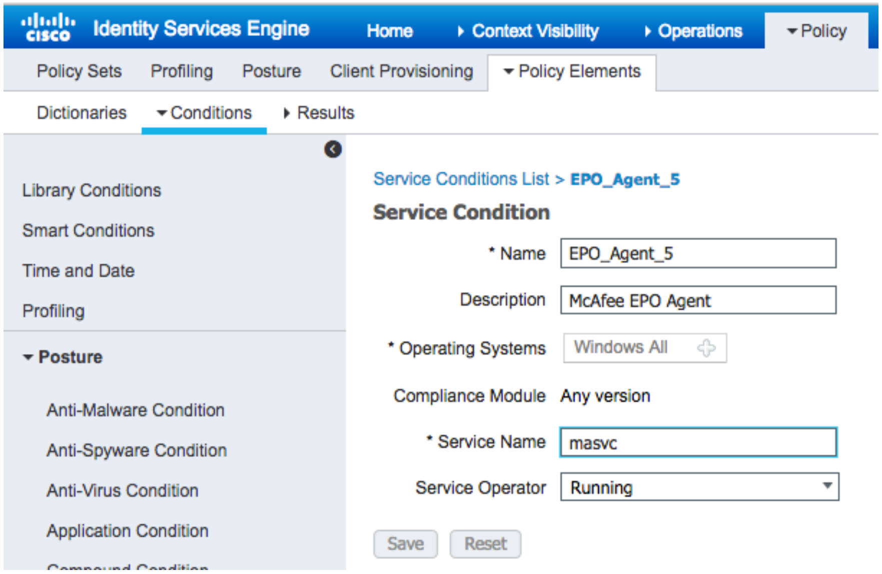
Last successful update on	2017/10/27 22:22:48
Last update status since ISE was started	Last update attempt at 2017/10/27 22:22:48 was successful
Cisco conditions version	234518.0.0.0
Cisco AV/AS support chart version for windows	187.0.0.0
Cisco AV/AS support chart version for Mac OSX	107.0.0.0
Cisco supported OS version	43.0.0.0

Creating McAfee Service Condition Check and McAfee ePO Remediation Action Link

Here we are defining the McAfee Agent Service as an ISE posture condition rule.

Step 1 Select **Policy->Policy Elements->Conditions->Posture->Service Condition->Add**

Step 2 **Enter the following:**



Service Conditions List > **EPO_Agent_5**

Service Condition

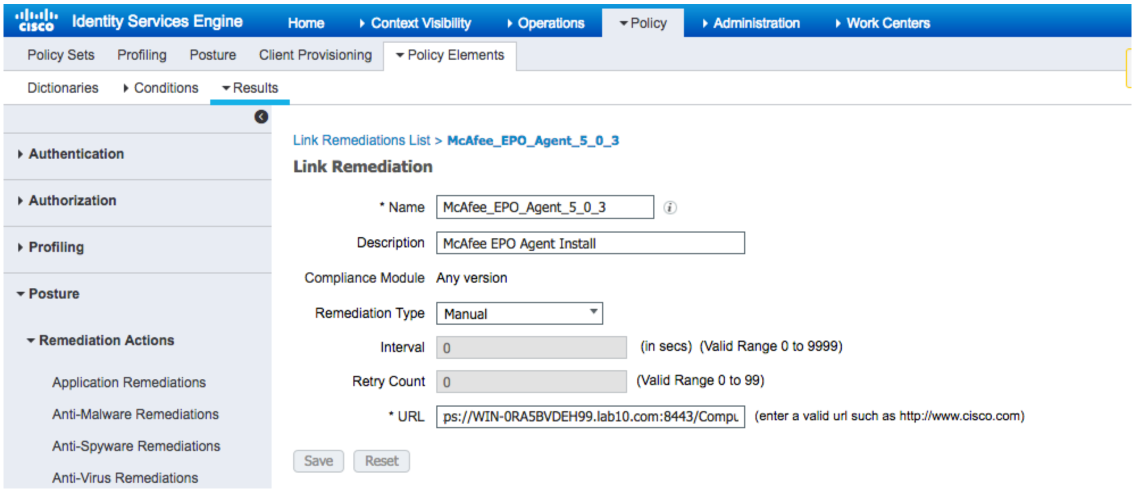
* Name	EPO_Agent_5
Description	McAfee EPO Agent
* Operating Systems	Windows All
Compliance Module	Any version
* Service Name	masvc
Service Operator	Running

Step 3 Select **Save**

Step 4 Select **Policy->Policy Elements->Results->Posture->Remediation Actions->Link Remediations->Add**

Step 5 **Enter the following**:

Note: The URL link represents the McAfee EPO agent download link: https://WIN-0RA5BVDEH99.lab10.com:8443/ComputerMgmt/agentPackage.get?token=1fda9abc84b832537e7a7d44447d57cef714b0e5



Link Remediations List > **McAfee_EPO_Agent_5_0_3**

Link Remediation

* Name: McAfee_EPO_Agent_5_0_3

Description: McAfee EPO Agent Install

Compliance Module: Any version

Remediation Type: Manual

Interval: 0 (in secs) (Valid Range 0 to 9999)

Retry Count: 0 (Valid Range 0 to 99)

* URL: ps://WIN-0RA5BVDEH99.lab10.com:8443/Compu (enter a valid url such as http://www.cisco.com)

Step 6 Select **Save**

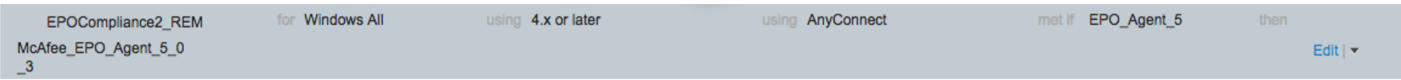
Creating Posture Requirement

The posture requirement is created that ties the posture condition rule and remediation link together. In the case, the McAfee EPO agent is not running, the end-user will launch the remediation link.

Step 1 Select **Policy->Policy Elements->Results->Posture->Requirements->Edit->Add New Requirements**

Step 2 Enter the following:
Rule Name: **EPOCompliance2_REM**
for: **Windows All**
using: **4.0.x or later**
using: **AnyConnect**
met if**: EPO_Agent_5**
then:
Actions: McAfee_Agent_5_0_3
Message shown to user: **Please be patient, the McAfee EPO agent is being installed on the endpoint**

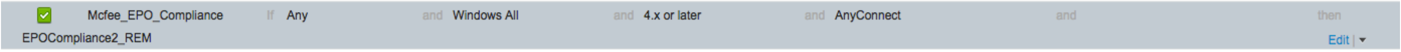
Step 3 Select **Save**



EPOCompliance2_REM for Windows All using 4.x or later using AnyConnect met if EPO_Agent_5 then McAfee_EPO_Agent_5_0_3

Creating Posture Policy

Step 1 Select **Policy->Posture->Posture Policy->Edit->Insert New Policy**
Step 2 Under **Rule Name**: type **McAfee_EPO_Compliance**
Step 3 Under **Identity Groups**: select **Any**
Step 4 Under **Operating System**: select **Windows 7 (all)**
Step 5 Under **Compliance Module**: select **4.x or later**
Step 6 Under **Posture Type**: select **AnyConnect**
Step 7 Under **Other**: leave the defaults for Optional
Step 8 Under **Requirements**: select **EPO_Compliance2_REM**
Step 9 Select **Done**
Step 10 Select **Save**


☑ Mcfee_EPO_Compliance If Any and Windows All and 4.x or later and AnyConnect and then EPOCompliance2_REM

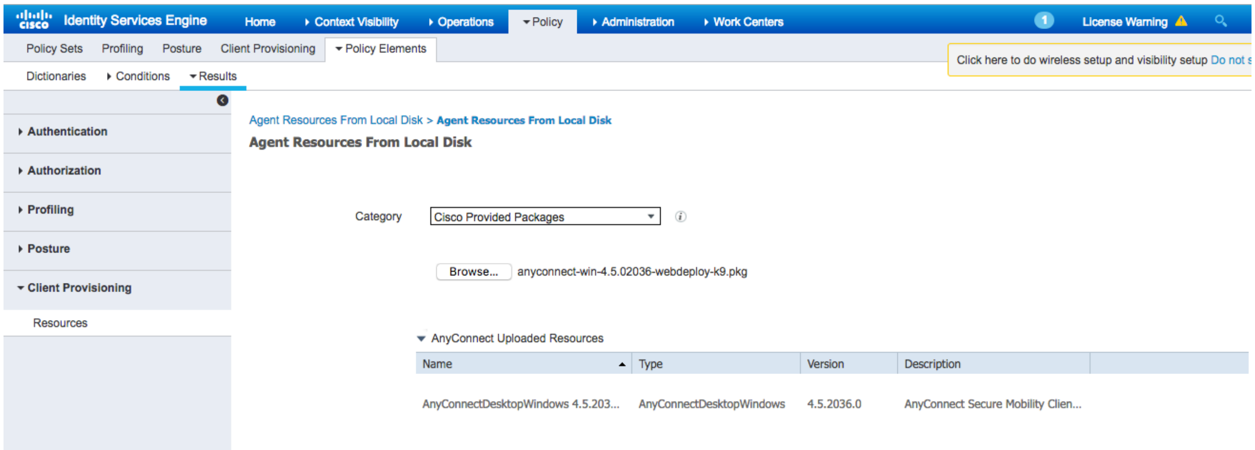
Client Provisioning

The Cisco AnyConnect client is required for ISE posture detection and remediation. The Cisco AnyConnect client also replaces the Windows supplicant for 802.1X authentication, and requires the Cisco Profile Editor for configuring the NAM network profile configuration file.

Upload AnyConnect Deployment Package

Step 1 Download Anyconnect Package from Cisco's website www.cisco.com/go/anyconnect ,"anyconnect-win-4.5.02036-webdeploy-k9.pkg"

Step 2 Select **Policy->Policy Elements->Results->Client Provisoning->Resources->Add->Add Agent from local disk->Category->Cisco provided package** and upload the anyconnect package



Agent Resources From Local Disk > **Agent Resources From Local Disk**

Agent Resources From Local Disk

Category: Cisco Provided Packages

anyconnect-win-4.5.02036-webdeploy-k9.pkg

AnyConnect Uploaded Resources

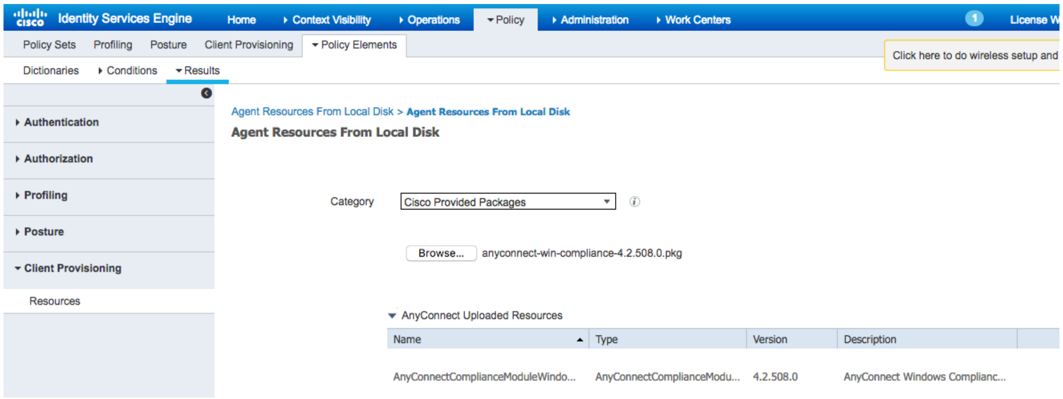
Name	Type	Version	Description
AnyConnectDesktopWindows 4.5.203...	AnyConnectDesktopWindows	4.5.2036.0	AnyConnect Secure Mobility Clien...

Step 3 Select **Submit** and conftrm the hash

Upload AnyConnect Compliance Package

Step 1 Upload the AnyConnectCompliance module anyconnect-win-compliance-4.2.508.0.pkg from Cisco AnyConnect Website: www.cisco.com/go/anyconnect

Step 2 Select **Policy->Policy Elements->Results->Client Provisioning->Resources->Add->Add Agent from local disk->Category->Cisco provided package** and upload the anyconnect package



Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Cisco Provided Packages

anyconnect-win-compliance-4.2.508.0.pkg

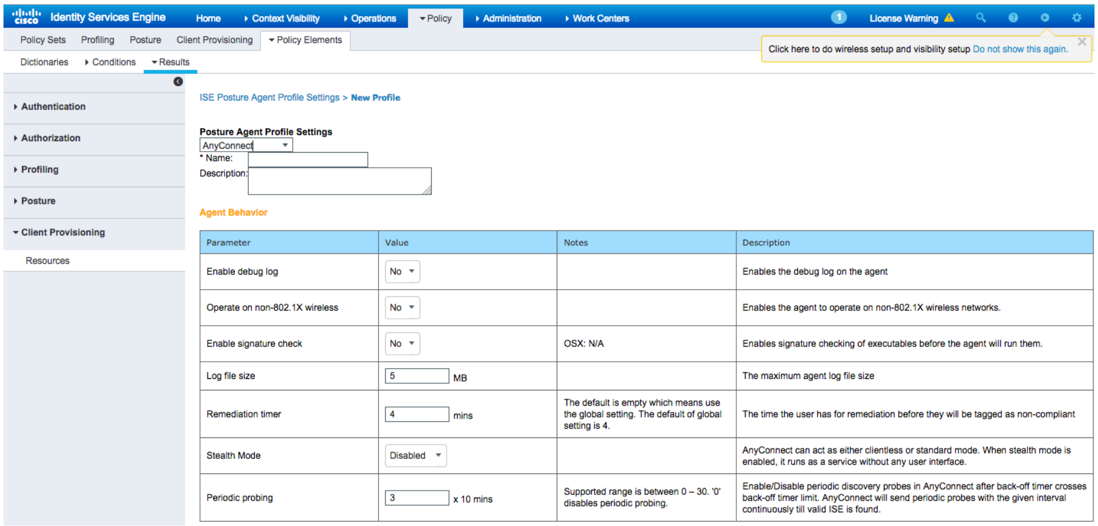
AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectComplianceModuleWindo...	AnyConnectComplianceModu...	4.2.508.0	AnyConnect Windows Complianc...

Step 3 Select **Submit** and confirm the hash.

Configure AnyConnect Posture Profile

Step 1 Select **Policy->Policy Elements->Results->Client Provisioning->Resources->Add-Add Agent from local disk->NAC agent or Anyconnect Posture Profile->Posture Agent Profile Settings->AnyConnect** You should see:



ISE Posture Agent Profile Settings > New Profile

Posture Agent Profile Settings

AnyConnect

* Name:

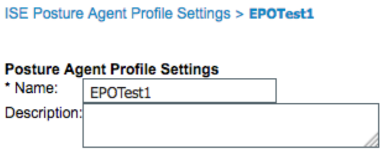
Description:

Agent Behavior

Parameter	Value	Notes	Description
Enable debug log	No		Enables the debug log on the agent
Operate on non-802.1X wireless	No		Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	OSX: N/A	Enables signature checking of executables before the agent will run them.
Log file size	5 MB		The maximum agent log file size
Remediation timer	4 mins	The default is empty which means use the global setting. The default of global setting is 4.	The time the user has for remediation before they will be tagged as non-compliant
Stealth Mode	Disabled		AnyConnect can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.
Periodic probing	3 x 10 mins	Supported range is between 0 – 30. '0' disables periodic probing.	Enable/Disable periodic discovery probes in AnyConnect after back-off timer crosses back-off timer limit. AnyConnect will send periodic probes with the given interval continuously till valid ISE is found.

Step 2 Under Name: type: **EPOTest1**

Note: EPOTest1 will be used in the Posture Policy



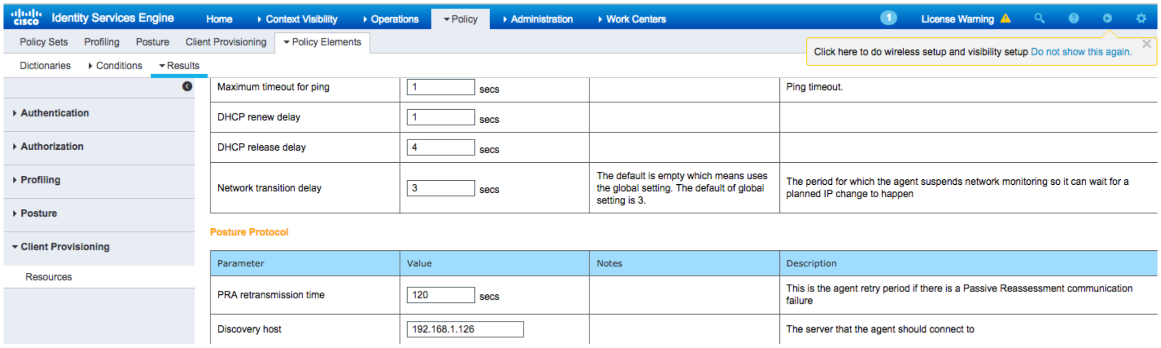
ISE Posture Agent Profile Settings > **EPOTest1**

Posture Agent Profile Settings

* Name: EPOTest1

Description:

Step 3 Under **Posture Protocol->Discovery Host**, type in the IP Address of the ISE PSN node. This will be the IP adress of the ISE node in a stand-alone ISE deployment.



Click here to do wireless setup and visibility setup Do not show this again.

Maximum timeout for ping	1 secs		Ping timeout.
DHCP renew delay	1 secs		
DHCP release delay	4 secs		
Network transition delay	3 secs	The default is empty which means uses the global setting. The default of global setting is 3.	The period for which the agent suspends network monitoring so it can wait for a planned IP change to happen

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host	192.168.1.126		The server that the agent should connect to

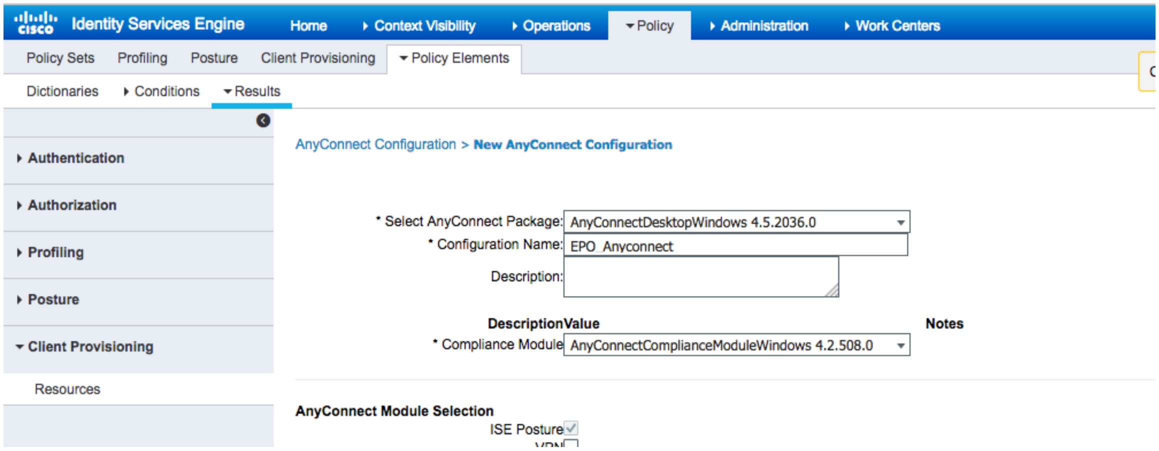
Step 4 Also add “*” under Server Name Rules

Step 5 Select **Submit**

Step 6 Select **Policy->Policy->Policy Elements->Results->Client Provisioning->Resources->Add->AnyConnect Configuration**, add the **Configuration Name**: **EPO_AnyConnect**

Step 7 Select the **Compliance Module**: **AnyConnectComplianceModuleWindows 4.2.508.0**

Step 8 Under **AnyConneect Module Selection**, enable **ISE Posture**



AnyConnect Configuration > **New AnyConnect Configuration**

* Select AnyConnect Package: AnyConnectDesktopWindows 4.5.2036.0

* Configuration Name: EPO_Anyconnect

Description:

DescriptionValue **Notes**

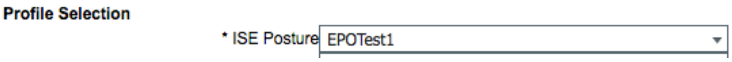
* Compliance Module AnyConnectComplianceModuleWindows 4.2.508.0

AnyConnect Module Selection

ISE Posture ☑

VPN ☐

Step 9 Under **Profile Selection->ISE Posture**, select **EPOTest1**



Profile Selection

* ISE Posture EPOTest1

Step 10 Select **Submit**

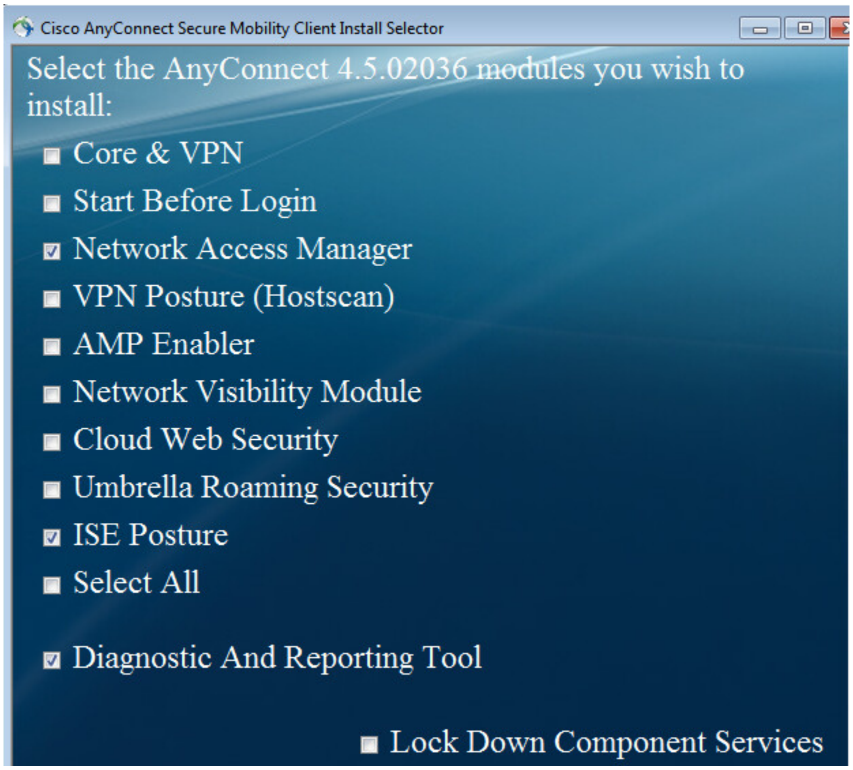
Installing Cisco AnyConnect Client

The Cisco AnyConnect client in this guides, will be configured for Network Access Manager (NAM), which is a replacement for the Windows supplicant.

Download the AnyConnect client *anyconnect-win-4.502036-predeploy-k9.zip* package from *www.cisco.com/go/anyconnect*

Step 1 Unzip and run **setup**

Step 2 Enable the following: Network Access Manager, ISE Posture and Diagnostic and Reporting Tool



Cisco AnyConnect Secure Mobility Client Install Selector

Select the AnyConnect 4.5.02036 modules you wish to install:

- □ Core & VPN
- □ Start Before Login
- ☑ Network Access Manager
- □ VPN Posture (Hostscan)
- □ AMP Enabler
- □ Network Visibility Module
- □ Cloud Web Security
- □ Umbrella Roaming Security
- ☑ ISE Posture
- □ Select All

- ☑ Diagnostic And Reporting Tool

□ Lock Down Component Services

Step 3 Select **Install Selected**

Installing Profile Editor

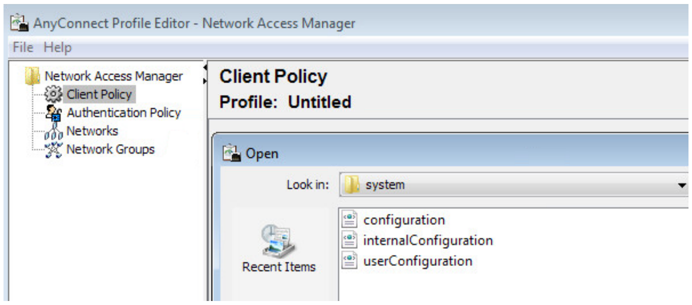
The NAM network configuration file machine and user authentication, PEAP/MSCHAPv2 will be created and used for IEEE 802.1X authentication. If not familiar with Profile Editor, please see *Configuring AnyConnect Profiler Editor* under **References**.

Step 1 Download Profile Editor: *tools-anyconnect-win-4.5.02036-profileeditor-k9.msi* from *www.cisco.com/go/anyconnect*

Step 2 Install Profile Editor, select a **Complete Install**

Note: You will need to install JRE 6 or higher

Step 3 In Profile Editor, select **File->Open->System->configuration.xml**



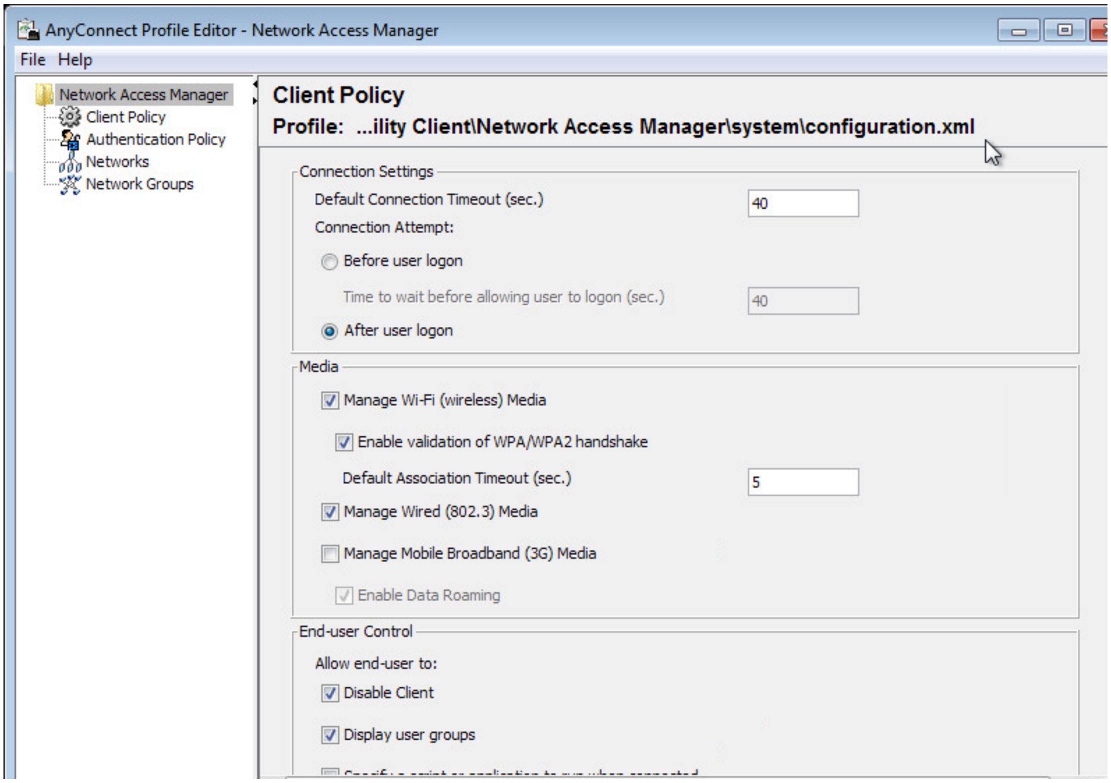
Client Policy

Profile: Untitled

Look in: system

configuration
internalConfiguration
userConfiguration

Step 4 Select **File Open->System->Configuration**



Client Policy

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Connection Settings

Default Connection Timeout (sec.) 40

Connection Attempt:

○ Before user logon

Time to wait before allowing user to logon (sec.) 40

● After user logon

Media

☑ Manage Wi-Fi (wireless) Media

☑ Enable validation of WPA/WPA2 handshake

Default Association Timeout (sec.) 5

☑ Manage Wired (802.3) Media

□ Manage Mobile Broadband (3G) Media

☑ Enable Data Roaming

End-user Control

Allow end-user to:

☑ Disable Client

☑ Display user groups

Step 5 Select **Networks->Add->Name:ISE23**

Step 6 Under **Configure your network media, select->Wired**

Step 7 Select **Next**

Step 8 Under **Security Level->**select **Authenticating network**

Step 9 Select **Next**

Step 10 Under **Network Type->**select **Machine and User**

Step 11 Select **Next**

Step 12 Under **Machine Auth->EAP Methods**, select **Peap**

Step 13 Under **EAP-Peap Settings**->Uncheck **Validate Server Identity**

Step 14 Select **Next**

Step 15 Under **Credentials**, leave the defaults

Step 16 Select **Next**

Step 17 Under **User Credentials->EAP Methods**, select **Peap**

Step 18 Under **EAP-Peap Settings->**Uncheck **Validate Server Identity**

Step 19 Select **Next**

Step 20 Under **Credentials**, leave the defaults

Step 21 Select **Next**

Step 22 Under **Certificates**, leave the defaults

Step 23 Select **Next**

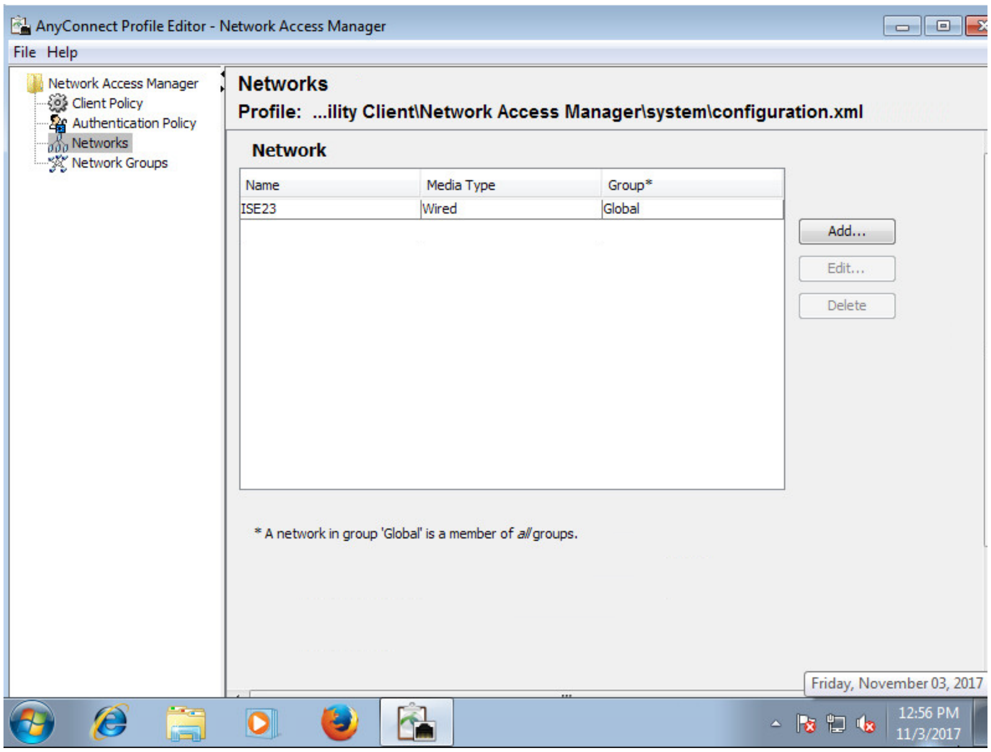
Step 24 Under **Credentials**, leave the defaults

Step 25 Select **Done**

Step 26 Edit the ISE23 Network and move into the Global Groups under Group Membership

Step 27 Select **Certificates** at the bottom-**>Done**

You should see:



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

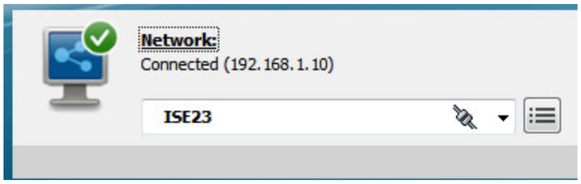
Network

Name	Media Type	Group*
ISE23	Wired	Global

* A network in group 'Global' is a member of *all* groups.

Step 28 Select **File->Save-as->configuration.xml->Save**

Step 29 **Right-click** on **AnyConnect Client->Network Repair**
Step 30 You should connect to ISE



Network:
Connected (192.168.1.10)

ISE23

Defining Authorization Policy

The authorization policy will be created that contains network access rules once the end-user authenticates. The authorization profile determines network access. For example, if the endpoint is non-compliant, the endpoint can be placed in a remediation VLAN, or assigned a TrustSec Security Group Tag.

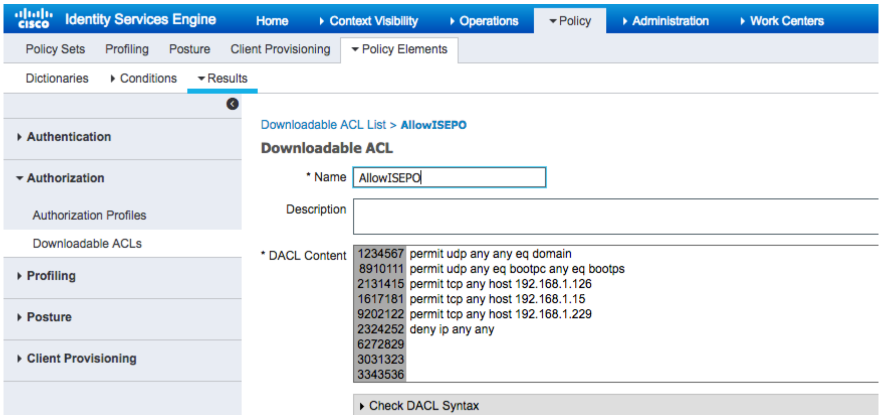
Authorization Profile

The DACL is used to provide redirection to ISE

Step 1 Select **Policy->Policy Elements->Results->Authorization->Download ACLs->add**
Step 2 For **Name**: type **AllowISEPO**
Step 3 For DACL Content: enter

```
permit udp any any eq domain
permit udp any any eq bootps
permit tcp any host 192.168.1.126     /* ISE */
permit tcp any host 192.168.1.15      /* McAfee ePO */
permit tcp any host 192.168.1.229     /* McAfee DXL Broker */
deny ip any any
```

Note: in a productional environment, you will want to include the ports for more secure access, Please see *Posture Services on the Cisco ISE Configuration Guide* under *References* for more information



Downloadable ACL List > **AllowISEPO**

Downloadable ACL

* Name: AllowISEPO

Description:

* DACL Content:

```
permit udp any any eq domain
permit udp any eq bootpc any eq bootps
permit tcp any host 192.168.1.126
permit tcp any host 192.168.1.15
permit tcp any host 192.168.1.229
deny ip any any
```

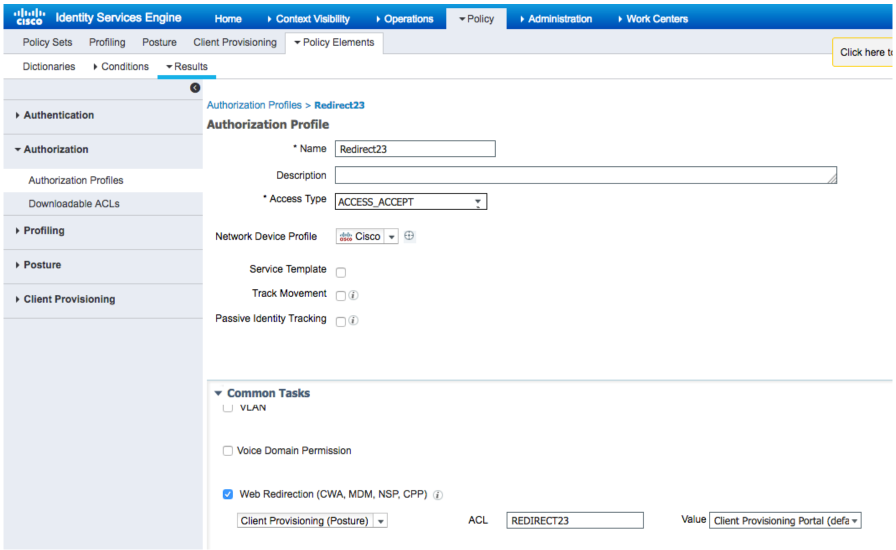
Step 4 Select **Save**

Step 5 Select **Policy->Policy Elements->Results->Authorization->Authorization Profiles-Add**

Step 6 Under **Name**: type **Redirect23**

Step 7 Under **Common Tasks**, **enable** Web Direction (CWA, MDM, NSP,CPP), select **Client Provisioning (Posture),** type in the **ACL**: **REDIRECT23**

Note: The *REDIRECT23 ACL* can be found in *Cisco Catalyst 3750x Settings* in *Appendices*



Authorization Profiles > **Redirect23**

Authorization Profile

* Name: Redirect23

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

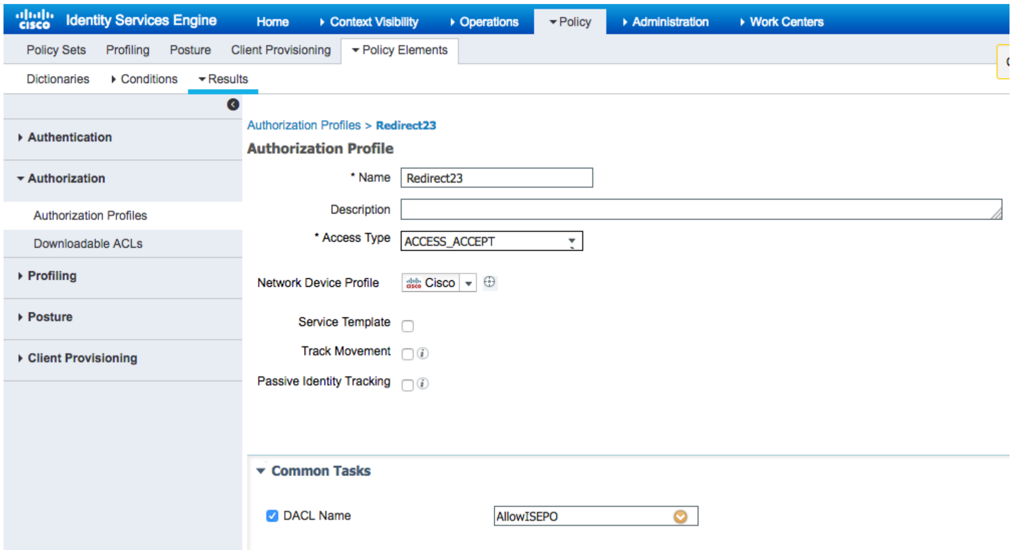
□ VLAN

□ Voice Domain Permission

☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: REDIRECT23 Value: Client Provisioning Portal (defa

Step 8 For **DACL Name**, select "**AllowISEEPO**"



Authorization Profiles > **Redirect23**

Authorization Profile

* Name: Redirect23

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

☑ DACL Name: AllowISEPO

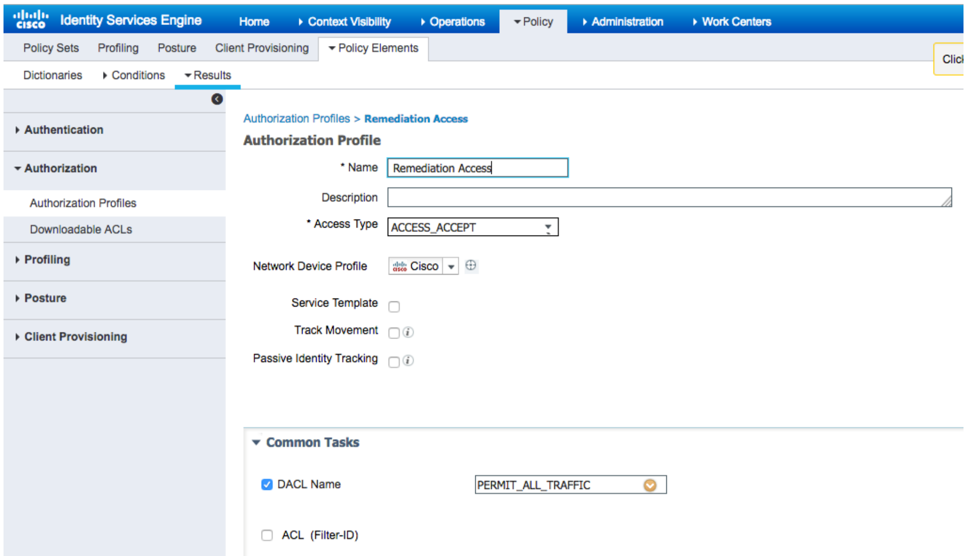
Step 9 Select **Save**

Step 10 Create Remediation Access Profile

Step 11 Select **Policy->Policy Elements->Results->Authorization->Authorization Profiles->Add**

Step 12 Under **Name**: type **Remediation Access**

Step 13 Under **DACL Name**: select **PERMIT ALL TRAFFIC**



Authorization Profiles > Remediation Access

Authorization Profile

* Name: Remediation Access

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

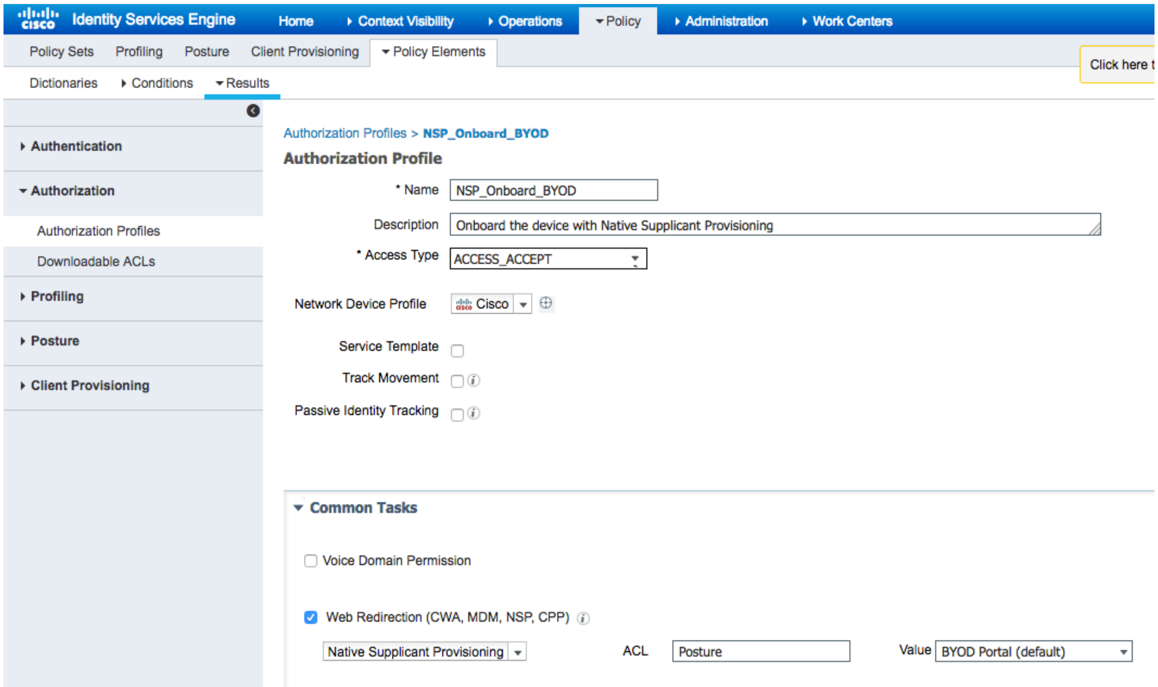
☑ DACL Name: PERMIT_ALL_TRAFFIC

□ ACL (Filter-ID)

Step 14 Select **Save**

Step 15 Create NSP Profiling Authorization Profile
Select **Policy->Policy Elements->Results->Authorization->Authorization Profiles->Add**
For **Name**: type **NSP_Onboard_BYOD**
Under **Common Tasks**, **enable Web Redirection (CWA, MDM, NSP, CPP),** select **Native Supplicant Provisioning**
For **ACL**: type **POSTURE**, *which represents the wireless ACL posture policy*

Note: The *POSTURE* ACL can be found under *Lab Configurations*



Authorization Profiles > NSP_Onboard_BYOD

Authorization Profile

* Name: NSP_Onboard_BYOD

Description: Onboard the device with Native Supplicant Provisioning

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

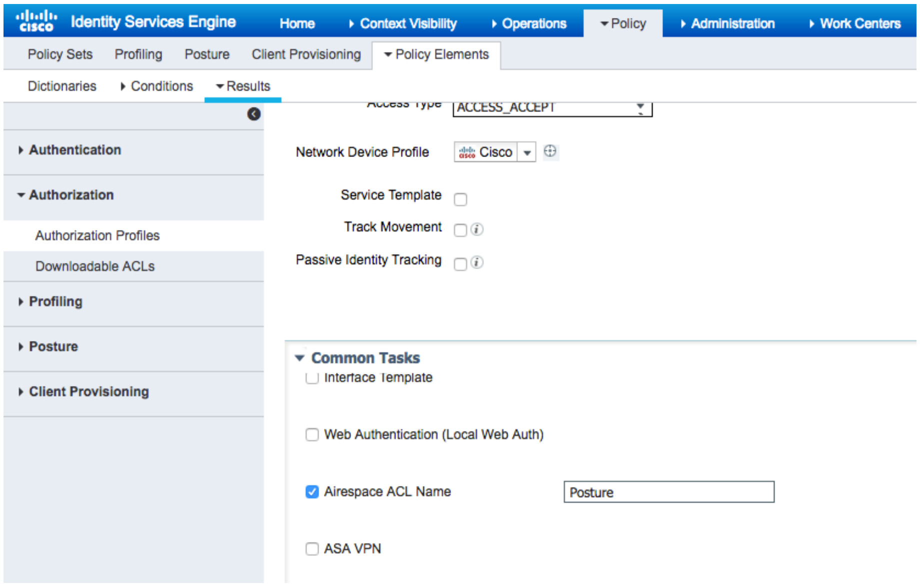
Common Tasks

□ Voice Domain Permission

☑ Web Redirection (CWA, MDM, NSP, CPP)

Native Supplicant Provisioning ACL: Posture Value: BYOD Portal (default)

Under **Airespace ACL Name**: type **Posture**



Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ Interface Template

□ Web Authentication (Local Web Auth)

☑ Airespace ACL Name Posture

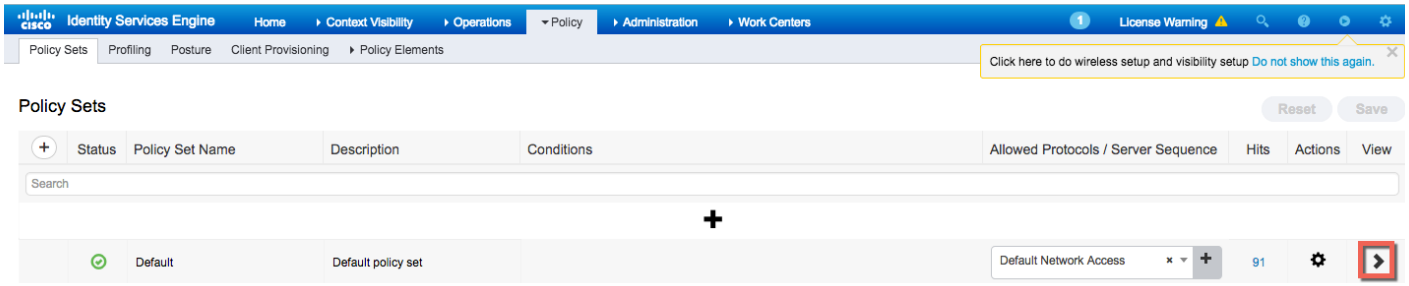
□ ASA VPN

Step 16 Select **Save**

Building Policy Sets

Policy sets are new in Cisco ISE 2.3 and above and represent the Authorization policy. If using Cisco ISE 2.0/2.1/2.2 please refer to *Managing Authorization Profiles* under *References*.

Step 1 Select ->**Policy->Policy Sets->”>”**

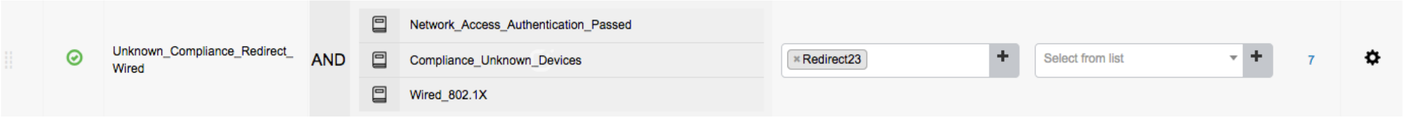


Click here to do wireless setup and visibility setup Do not show this again.

Policy Sets

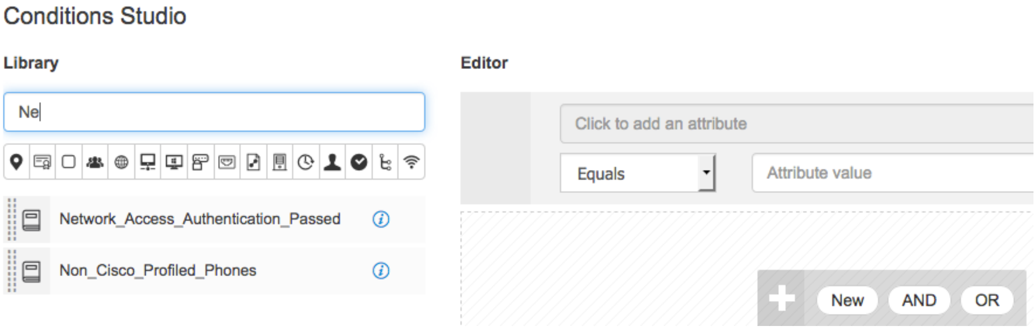
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Default	Default policy set		Default Network Access	91		>

Step 2 Select Authorization Policy
Step 3 Click on the **Gear** and **Insert new row above** and create the following rule for wireless redirection

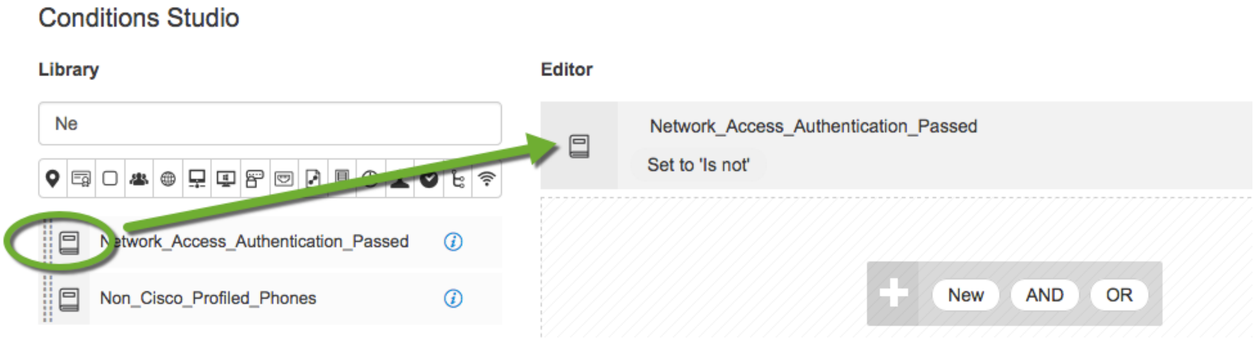


Status	Rule Name		Conditions	Profiles	Security Groups	Hits
✓	Unknown_Compliance_Redirect_Wired	AND	Network_Access_Authentication_Passed Compliance_Unknown_Devices Wired_802.1X	Redirect23	Select from list	7

Step 4 Type in “**Unknown Compliance_Redirect_Wired**” for the rule name
Step 5 Click on “**+**”
Step 6 Under **Conditions Studio->Library**->type in **Network_Authentication_Passed**


Conditions Studio
Library
Ne
Network_Access_Authentication_Passed
Non_Cisco_Profiled_Phones
Editor
Click to add an attribute
Equals
Attribute value
New
AND
OR

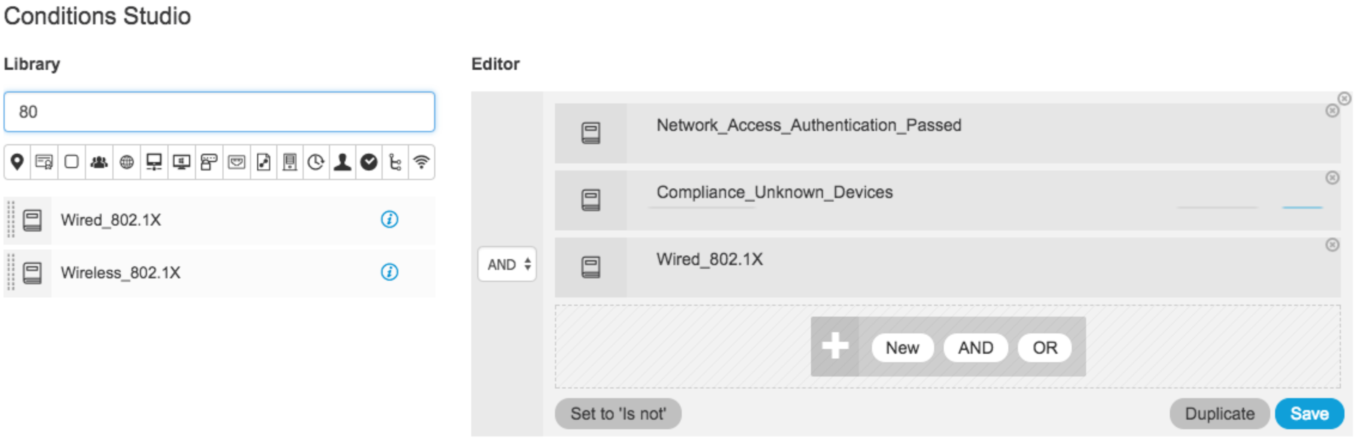
Step 7 Select **Network_Access_Passed** and drag into Editor


Conditions Studio
Library
Ne
Network_Access_Authentication_Passed
Non_Cisco_Profiled_Phones
Editor
Network_Access_Authentication_Passed
Set to 'Is not'
New
AND
OR

Step 8 Follow steps 6-8 for **Compliance_Unknown_Devices**

Step 9 Follow steps 6-8 for **Wired_802.1X**

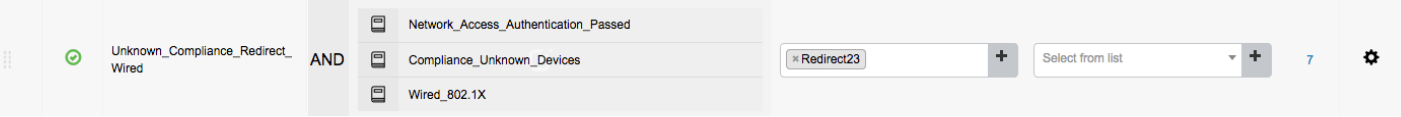
Step 10 You should see



Step 11 Select **Use**

Step 12 Under **Profiles** select **REDIRECT23**

Step 13 You should see



Unknown_Compliance_Redirect_Wired AND

Network_Access_Authentication_Passed

Compliance_Unknown_Devices

Wired_802.1X

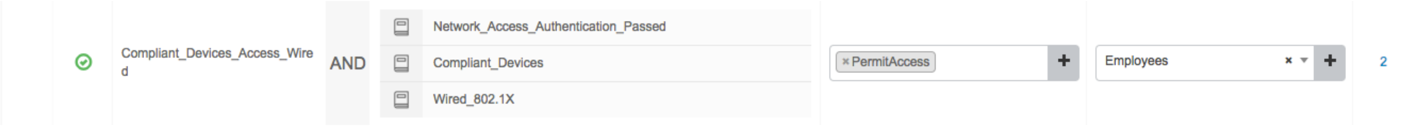
× Redirect23

Select from list

7

Step 14 Select **Save**

Step 15 Click on the **Gear** and **Insert new row above** and create the following rule for compliant access



Compliant_Devices_Access_Wired AND

Network_Access_Authentication_Passed

Compliant_Devices

Wired_802.1X

× PermitAccess

Employees

2

Step 16 Follow Steps 3-12 to create the rule for **Compliant_Devices_Access_Wired**

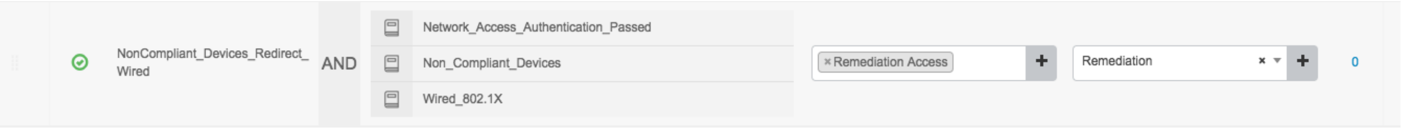
Step 17 Move the conditions: **Network_Access_Authentication_Passed, Compliant Devices, Wired_802.1X** into the Editor.

Step 18 Under **Profiles** select **Permit Access**

Step 19 Under **Security Groups**, select **Employees**

Step 20 Select **Save**

Step 21 Click on the **Gear** and **Insert new row above** and create the following rule for non-compliant remediation access



NonCompliant_Devices_Redirect_Wired AND

Network_Access_Authentication_Passed

Non_Compliant_Devices

Wired_802.1X

× Remediation Access

Remediation

0

Step 22 Follow Steps 3-12 to create the rule for **NonCompliant_Devices_Redirect_Wired**

Step 23 Move the conditions: **Network_Access_Authentication_Passed, Non_Compliant_Devices, Wired_802.1X** into the Editor.

Step 24 Under **Profiles** select **Remediation Access**

Step 25 Under **Security Groups**, select **Remediation**

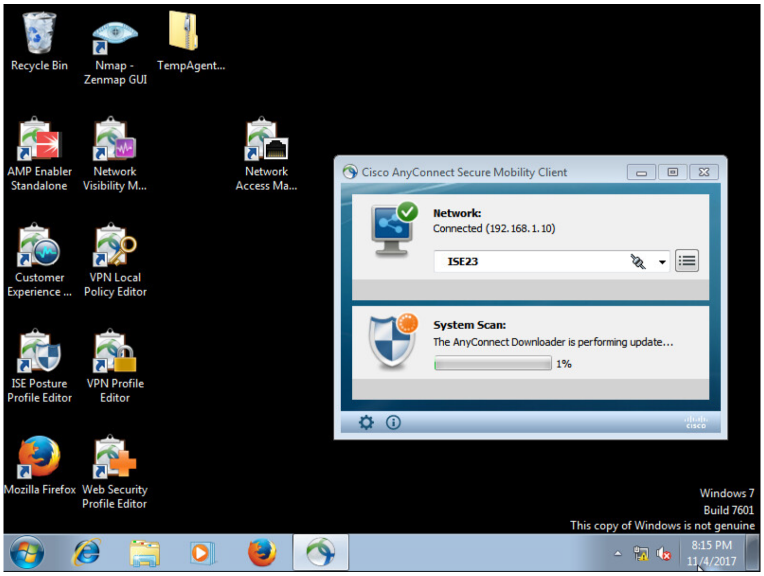
Step 26 Select **Save**

Testing

In this scenario, there is no McAfee agent on the endpoint; this is detected by the Cisco ISE posture policy. The remediation link will be provided to the end-user to download the McAfee agent from McAfee ePO. The endpoint will be deemed non-compliant, until the McAfee agent has been installed, and the endpoint has been re-scanned.

Step 1 The end-user logs in

Step 2 The endpoint is scanned for compliance



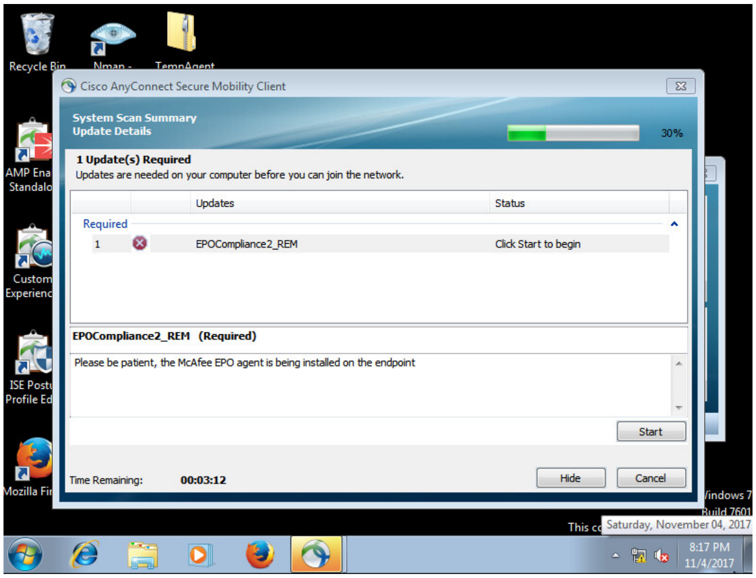
Cisco AnyConnect Secure Mobility Client

Network:
Connected (192.168.1.10)
ISE23

System Scan:
The AnyConnect Downloader is performing update...
1%

Step 3 The McAfee agent is not installed due to the absence of the McAfee Agent Service and the endpoint is deemed non-compliant

Step 4 The end-user clicks on **Start** to begin downloading the remediation link. This can be automated by a configuration in the remediation link rule.



Cisco AnyConnect Secure Mobility Client

System Scan Summary
Update Details
30%

1 Update(s) Required
Updates are needed on your computer before you can join the network.

		Updates	Status
Required			
1	☒	EPOCompliance2_REM	Click Start to begin

EPOCompliance2_REM (Required)

Please be patient, the McAfee EPO agent is being installed on the endpoint

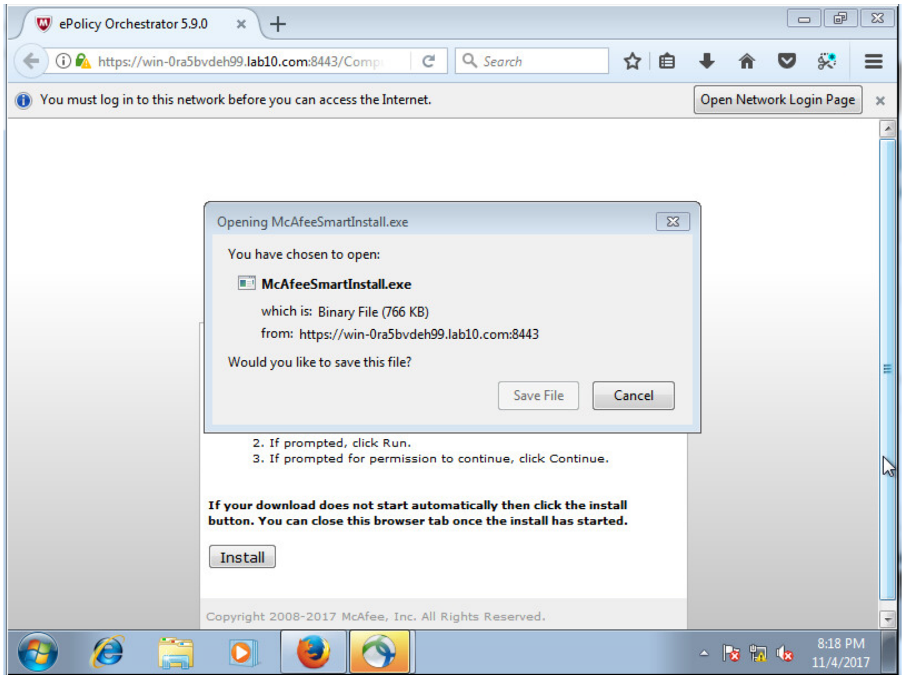
Start

Time Remaining: 00:03:12

Hide Cancel

Step 5 Select **Hide** on the AnyConnect UI

Step 6 The McAfee Agent link will be downloaded from McAfee ePO


ePolicy Orchestrator 5.9.0
https://win-0ra5bvdeh99.lab10.com:8443/Comp
Search
Open Network Login Page
Save File
Cancel
Install
8:18 PM
11/4/2017

You must log in to this network before you can access the Internet.

Opening McAfeeSmartInstall.exe

You have chosen to open:

McAfeeSmartInstall.exe

which is: Binary File (766 KB)

from: https://win-0ra5bvdeh99.lab10.com:8443

Would you like to save this file?

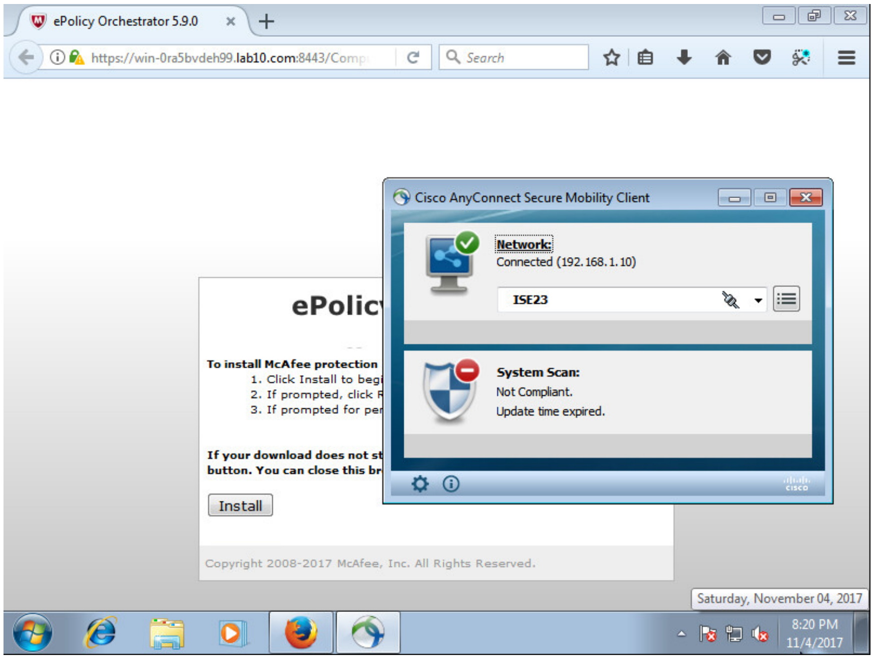
2. If prompted, click Run.
3. If prompted for permission to continue, click Continue.

If your download does not start automatically then click the install button. You can close this browser tab once the install has started.

Copyright 2008-2017 McAfee, Inc. All Rights Reserved.

Step 7 Save the file locally

Step 8 The endpoint will be deemed non-compliant


ePolicy Orchestrator 5.9.0
https://win-0ra5bvdeh99.lab10.com:8443/Comp
Search
Cisco AnyConnect Secure Mobility Client
ISE23
ePolic
Install
Saturday, November 04, 2017
8:20 PM
11/4/2017

Network:
Connected (192.168.1.10)

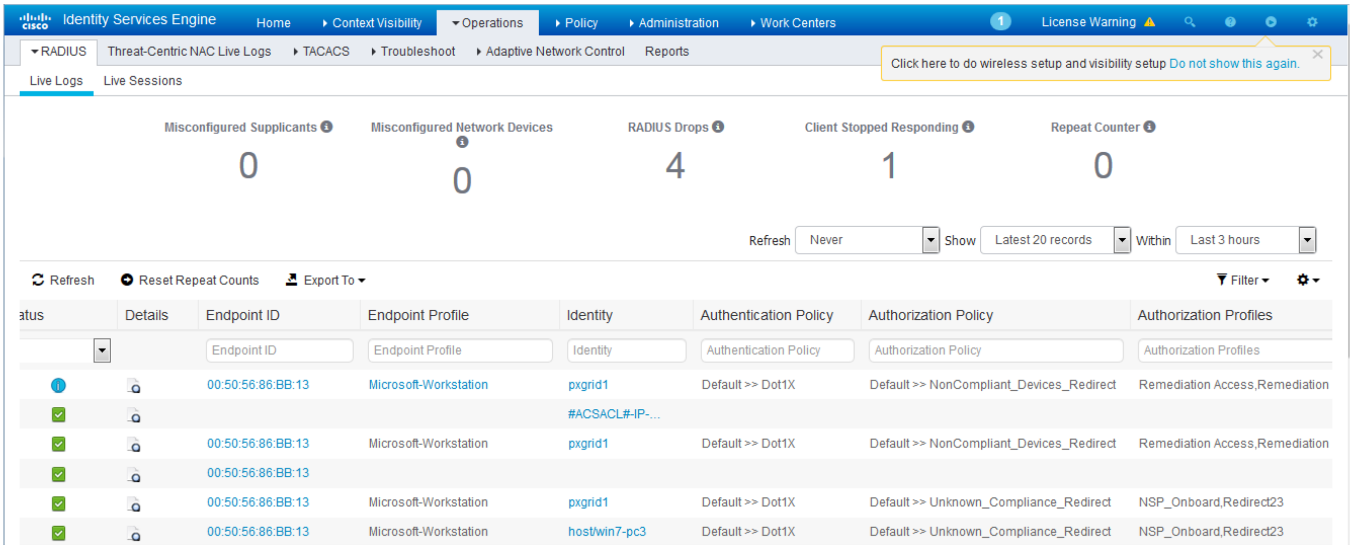
System Scan:
Not Compliant.
Update time expired.

To install McAfee protection
1. Click Install to begi
2. If prompted, click R
3. If prompted for per

If your download does not st
button. You can close this br

Copyright 2008-2017 McAfee, Inc. All Rights Reserved.

Step 9 The endpoint will be given limited network remediation access based on the remediation authorization rule.



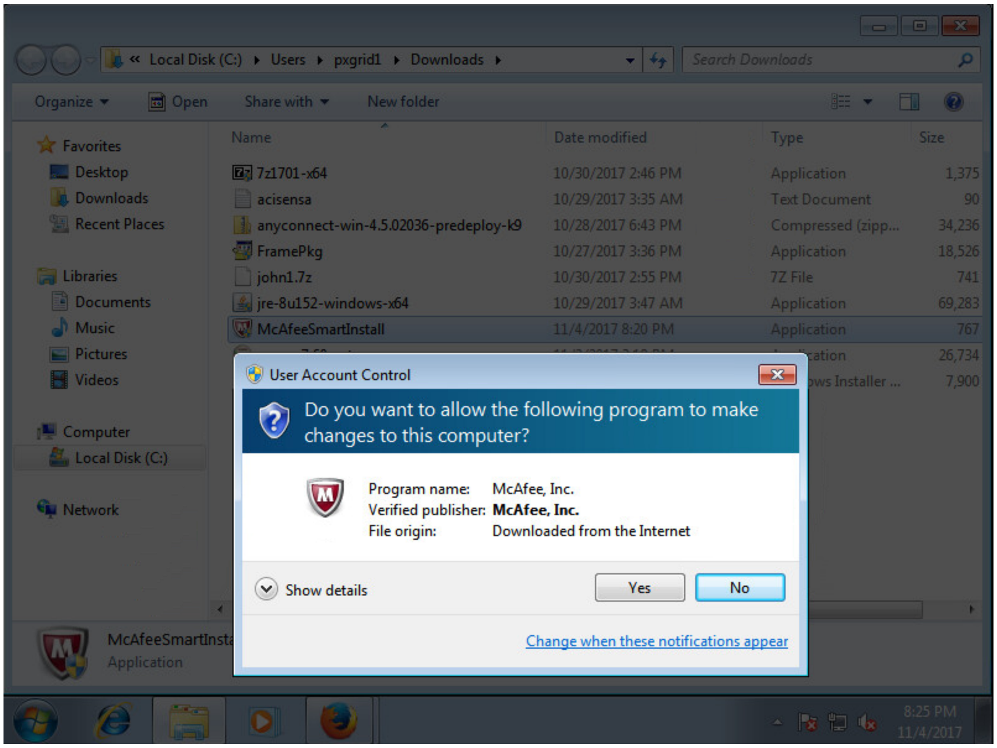
Click here to do wireless setup and visibility setup Do not show this again.

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	4	1	0

Refresh: Never · Show: Latest 20 records · Within: Last 3 hours

atus	Details	Endpoint ID	Endpoint Profile	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
ⓘ		00:50:56:86:BB:13	Microsoft-Workstation	pxgrid1	Default >> Dot1X	Default >> NonCompliant_Devices_Redirect	Remediation Access,Remediation
☑				#ACSACL#-IP-...			
☑		00:50:56:86:BB:13	Microsoft-Workstation	pxgrid1	Default >> Dot1X	Default >> NonCompliant_Devices_Redirect	Remediation Access,Remediation
☑		00:50:56:86:BB:13					
☑		00:50:56:86:BB:13	Microsoft-Workstation	pxgrid1	Default >> Dot1X	Default >> Unknown_Compliance_Redirect	NSP_Onboard,Redirect23
☑		00:50:56:86:BB:13	Microsoft-Workstation	host/win7-pc3	Default >> Dot1X	Default >> Unknown_Compliance_Redirect	NSP_Onboard,Redirect23

Step 10 The end-user runs the downloaded application



Name	Date modified	Type	Size
7z1701-x64	10/30/2017 2:46 PM	Application	1,375
acisensa	10/29/2017 3:35 AM	Text Document	90
anyconnect-win-4.5.02036-predeploy-k9	10/28/2017 6:43 PM	Compressed (zipp...	34,236
FramePkg	10/27/2017 3:36 PM	Application	18,526
john1.7z	10/30/2017 2:55 PM	7Z File	741
jre-8u152-windows-x64	10/29/2017 3:47 AM	Application	69,283
McAfeeSmartInstall	11/4/2017 8:20 PM	Application	767
		ation	26,734
		ws Installer ...	7,900

User Account Control

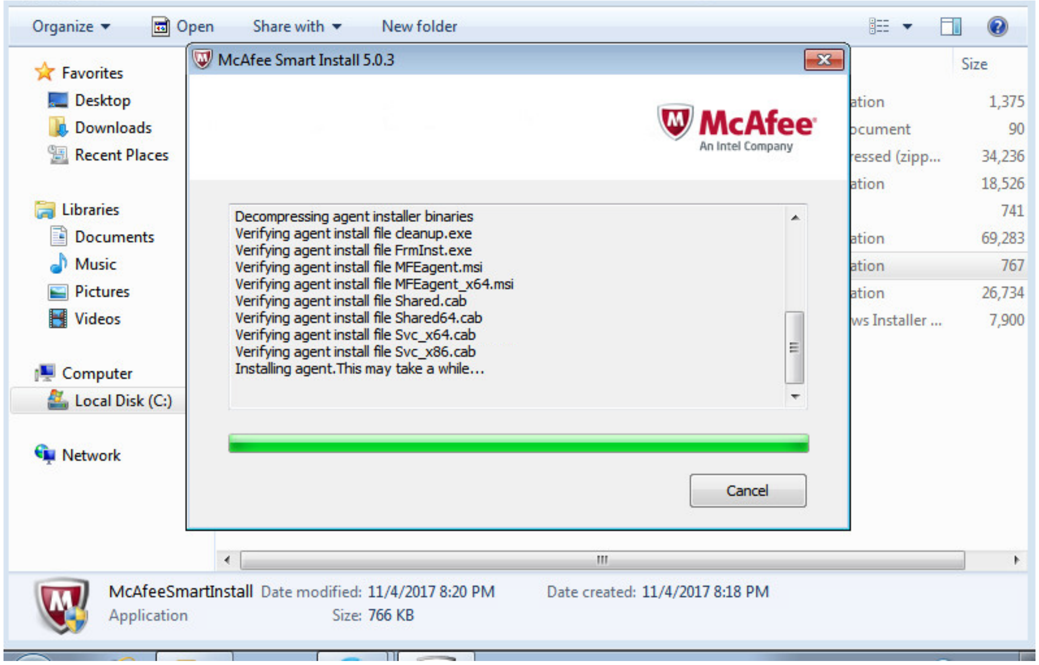
Do you want to allow the following program to make changes to this computer?

Program name: McAfee, Inc.
Verified publisher: **McAfee, Inc.**
File origin: Downloaded from the Internet

Show details Yes No

Change when these notifications appear

Step 11 This may take a little while to install the application

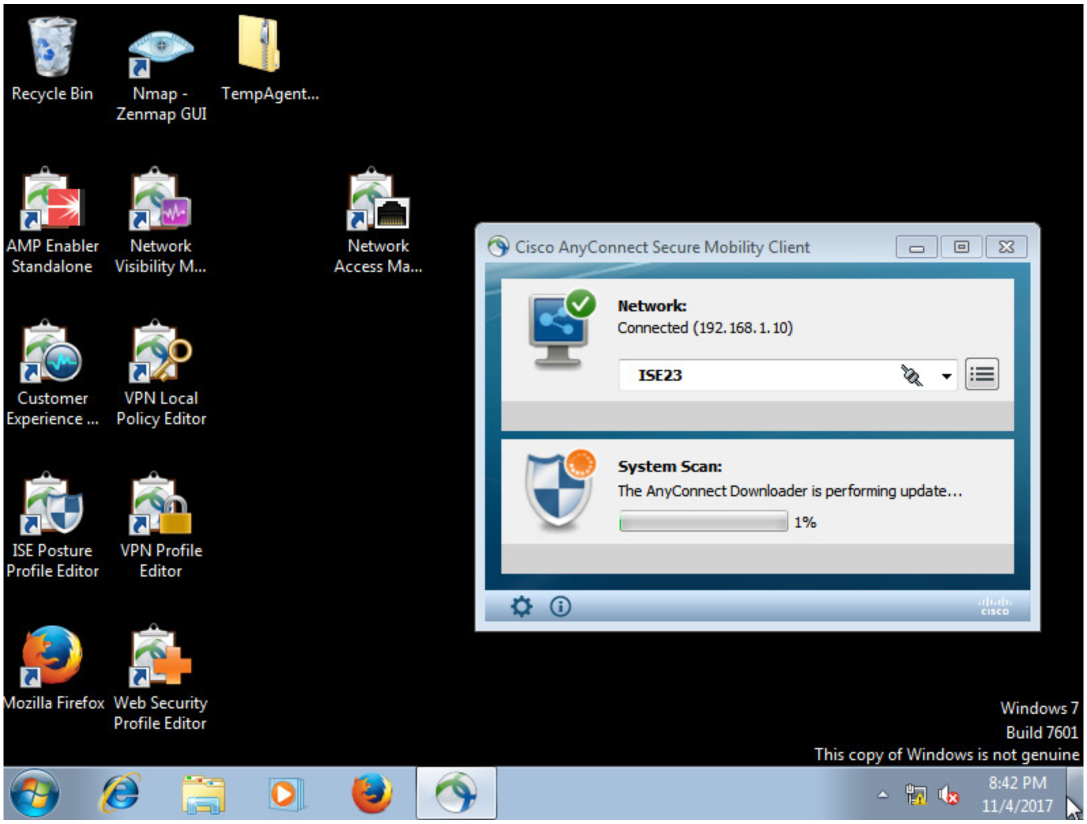


McAfee Smart Install 5.0.3

```
Decompressing agent installer binaries
Verifying agent install file cleanup.exe
Verifying agent install file FrmInst.exe
Verifying agent install file MFEagent.msi
Verifying agent install file MFEagent_x64.msi
Verifying agent install file Shared.cab
Verifying agent install file Shared64.cab
Verifying agent install file Svc_x64.cab
Verifying agent install file Svc_x86.cab
Installing agent.This may take a while...
```

McAfeeSmartInstall Date modified: 11/4/2017 8:20 PM Date created: 11/4/2017 8:18 PM
Application Size: 766 KB

Step 12 Once the user re-authenticates, the endpoint will be scanned again for compliance

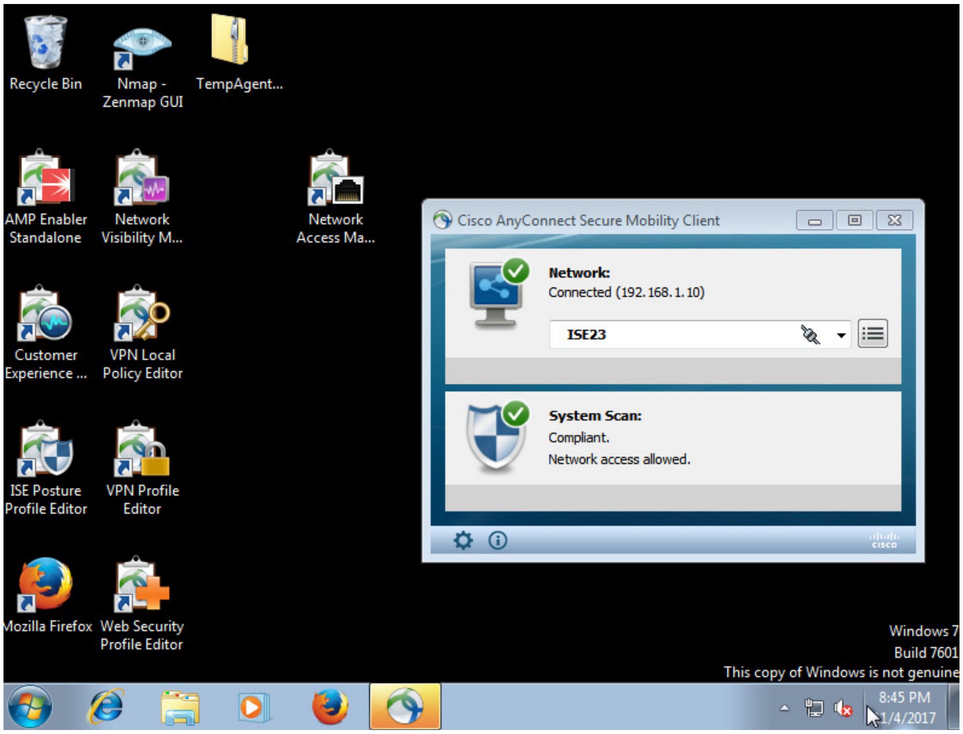


Cisco AnyConnect Secure Mobility Client

Network:
Connected (192.168.1.10)
ISE23

System Scan:
The AnyConnect Downloader is performing update...
1%

Step 13 The endpoint is now compliant



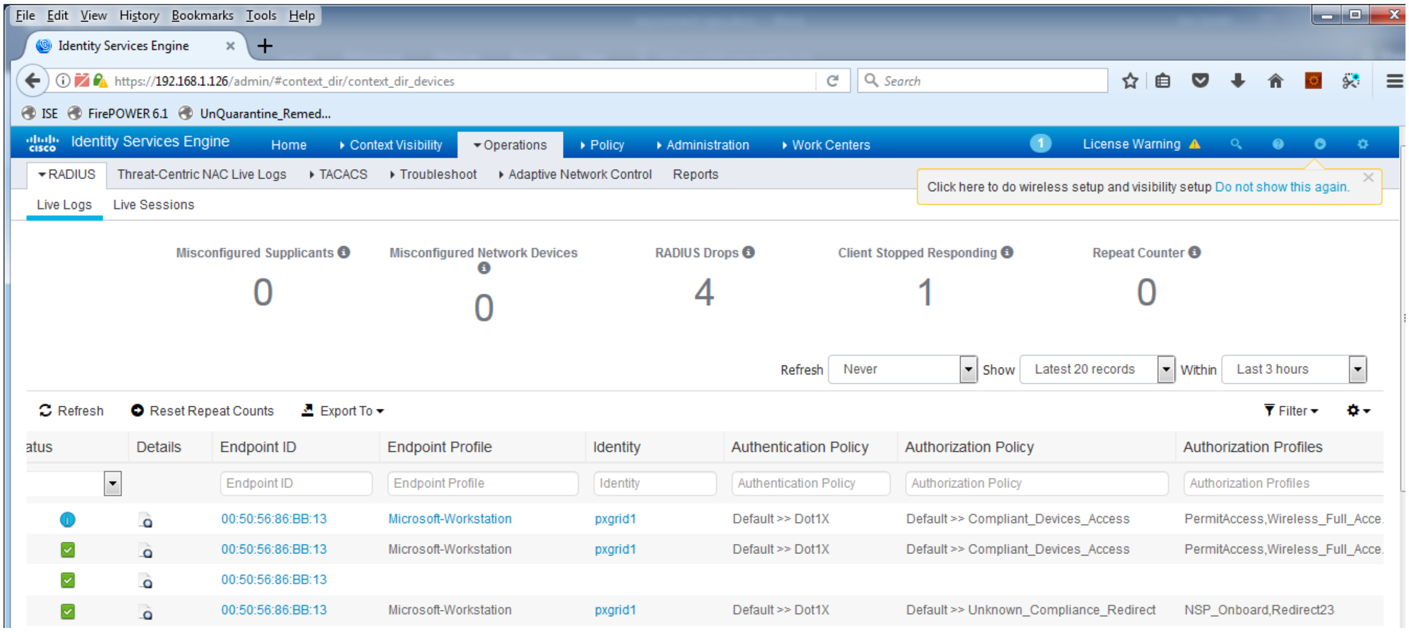
Cisco AnyConnect Secure Mobility Client

Network:
Connected (192.168.1.10)

ISE23

System Scan:
Compliant.
Network access allowed.

Step 14 You can see the compliant endpoint in ISE



Click here to do wireless setup and visibility setup Do not show this again.

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	4	1	0

Refresh: Never Show: Latest 20 records Within: Last 3 hours

Refresh Reset Repeat Counts Export To Filter

atus	Details	Endpoint ID	Endpoint Profile	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
●		00:50:56:86:BB:13	Microsoft-Workstation	pxgrid1	Default >> Dot1X	Default >> Compliant_Devices_Access	PermitAccess,Wireless_Full_Acce.
☑		00:50:56:86:BB:13	Microsoft-Workstation	pxgrid1	Default >> Dot1X	Default >> Compliant_Devices_Access	PermitAccess,Wireless_Full_Acce.
☑		00:50:56:86:BB:13					
☑		00:50:56:86:BB:13	Microsoft-Workstation	pxgrid1	Default >> Dot1X	Default >> Unknown_Compliance_Redirect	NSP_Onboard,Redirect23

On-Boarding Employee Laptop, installing McAfee Agent by McAfee ePO

In this section, we configure Cisco ISE for on-boarding and registering a device. In this document a Windows Surface Pro was used. This ensures that the device is corporately registered by the organization's BYOD policy and now the McAfee ePO admin can deploy the McAfee agent. Fore more information on BYOD, please see https://communities.cisco.com/docs/DOC-68160 - How To: ISE & BYOD: Onboarding, Registering and Provisioning in References. If using ISE 2.0 through 2.2, please see Managing Authorization Policies under references. References. ISE 2.3 and above use the GUI for Authorization Policies.

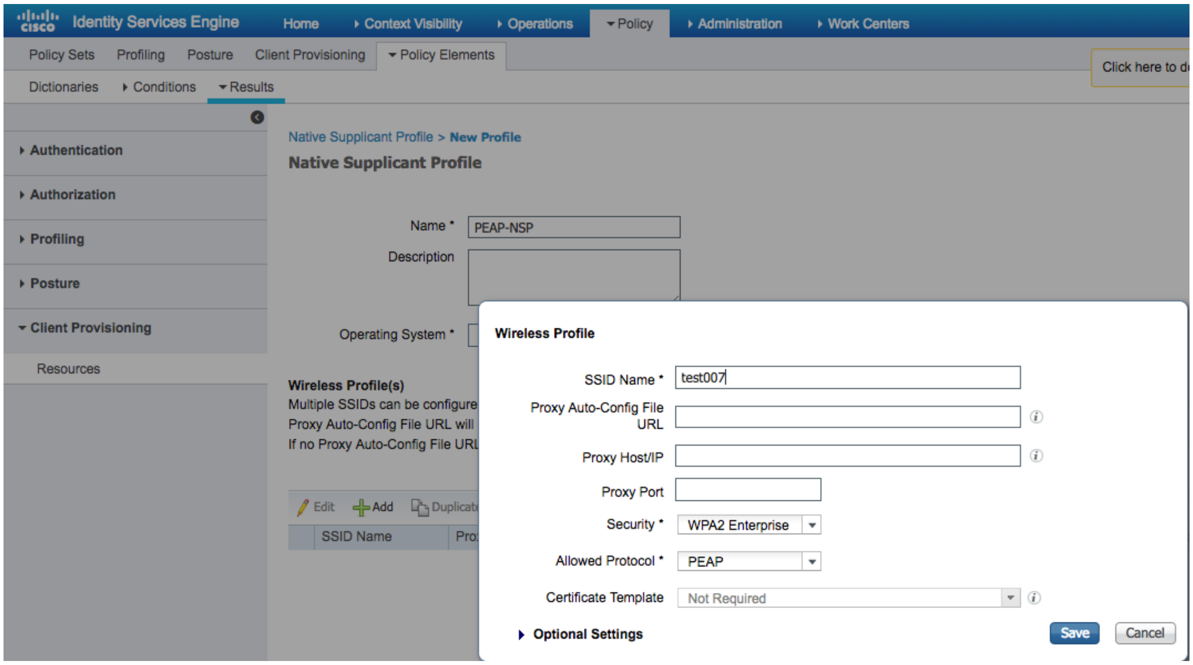
Creating NSP Profile

Step 1 Select **Policy-Policy Elements->Results->Client Provisioning->Resources->Add->Native Supplicant Profile**

Step 2 Under **Name**: type: **PEAP-NSP**

Step 3 Select **Add**

Step 4 Unser **SSID** Name: **type your SSID** , i.e. **test007**



Native Supplicant Profile > New Profile

Native Supplicant Profile

Name * PEAP-NSP

Description

Operating System *

Wireless Profile(s)
Multiple SSIDs can be configure
Proxy Auto-Config File URL will
If no Proxy Auto-Config File URL

Wireless Profile

SSID Name * test007

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

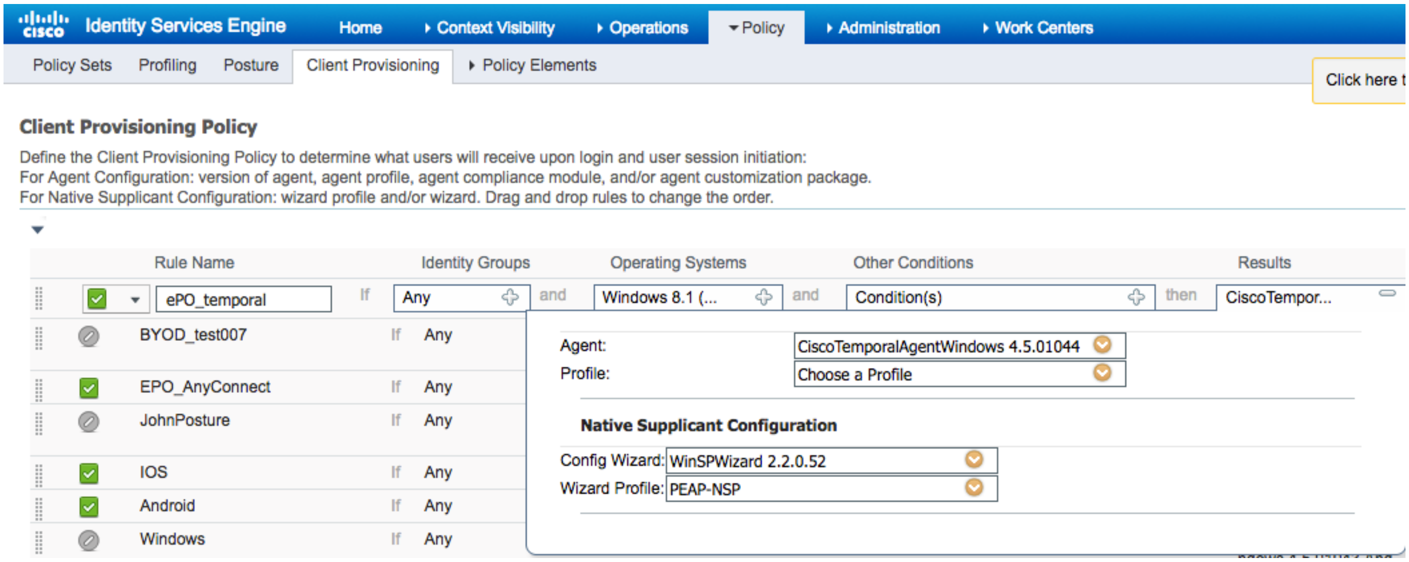
Allowed Protocol * PEAP

Certificate Template Not Required

Step 5 Select **Save**

Creating Client Provisioning Policy

Step 1 Select **Policy->Client Provisioning**
Step 2 Click on the **down arrow** next to Edit, and **Insert new policy above**
Step 3 Under **rule name**: type **ePO_temporal**
Step 4 Under **Operating Systems**: select **Windows 8.0, 8.1**
Step 5 Leave the defaults for Conditions
Step 6 Under **Results**, select the following



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

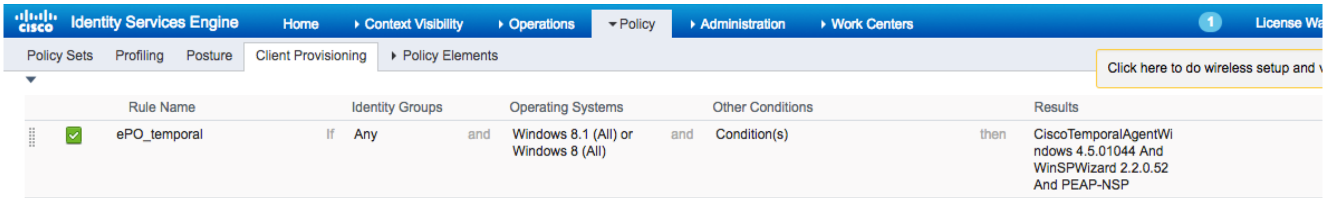
	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	ePO_temporal	If	Any	and	Windows 8.1 (...	and	Condition(s)	then	CiscoTempor...
⊘	BYOD_test007	If	Any						
☑	EPO_AnyConnect	If	Any						
⊘	JohnPosture	If	Any						
☑	IOS	If	Any						
☑	Android	If	Any						
⊘	Windows	If	Any						

Agent: CiscoTemporalAgentWindows 4.5.01044
Profile: Choose a Profile

Native Supplicant Configuration

Config Wizard: WinSPWizard 2.2.0.52
Wizard Profile: PEAP-NSP

Step 7 Select **Done**
Step 8 Select **Save**

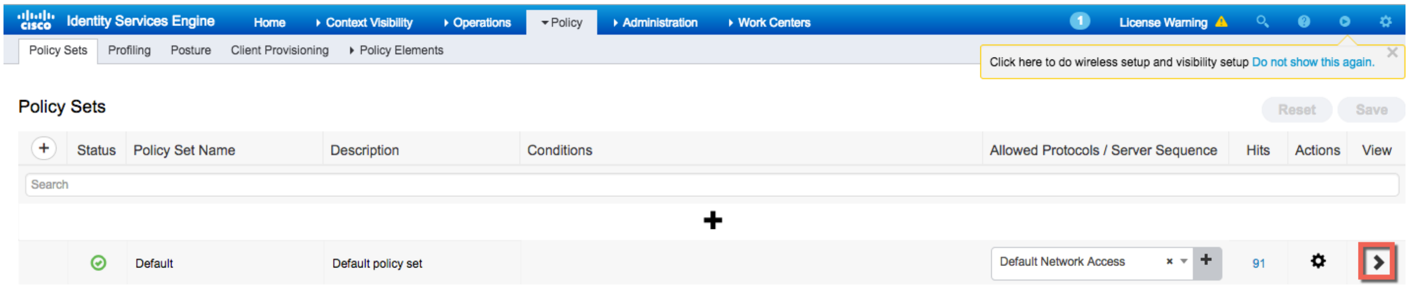


	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	ePO_temporal	If	Any	and	Windows 8.1 (All) or Windows 8 (All)	and	Condition(s)	then	CiscoTemporalAgentWindows 4.5.01044 And WinSPWizard 2.2.0.52 And PEAP-NSP

Creating Authorization Policy

Step 1 Select Policy-Policy Sets

Step 2 Select ->**Policy->Policy Sets->">"**



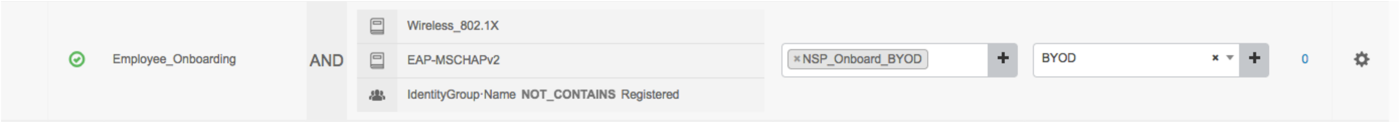
Click here to do wireless setup and visibility setup Do not show this again.

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Default	Default policy set		Default Network Access	91	⚙	>

Step 3 Select **Authorization Policy**

Step 4 Click on the **Gear** and **Insert new row above** and create the following rule for on-boarding



Status	Rule Name	Conditions		Results		Hits	Actions
✓	Employee_Onboarding	AND	Wireless_802.1X EAP-MSCHAPv2 IdentityGroup·Name NOT_CONTAINS Registered	NSP_Onboard_BYOD	BYOD	0	⚙

Step 5 Type in "**Employee Onboarding**" for the rule name

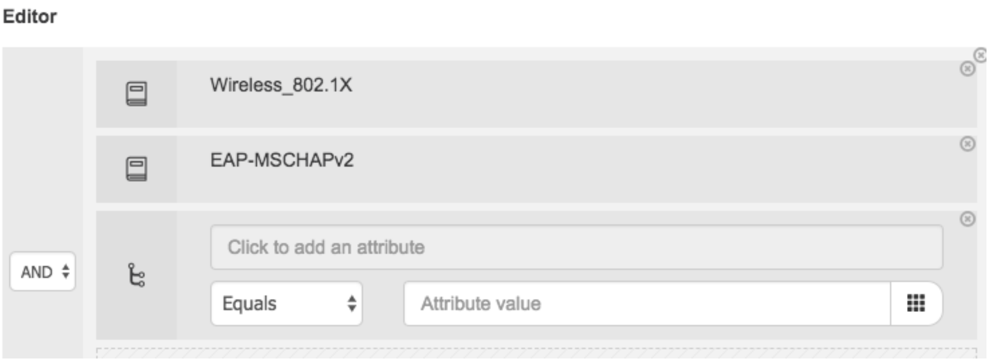
Step 6 Click on "**+**"

Step 7 Under **Conditions Studio->Library->**type in **Wireless_802.1X** and drag into Editor

Step 8 Under **Conditions Studio->Library**->type in **EAP-MSCHAPv2** and drag into Editor

Step 9 Under **Editor,** select **New**

You should see:



Editor

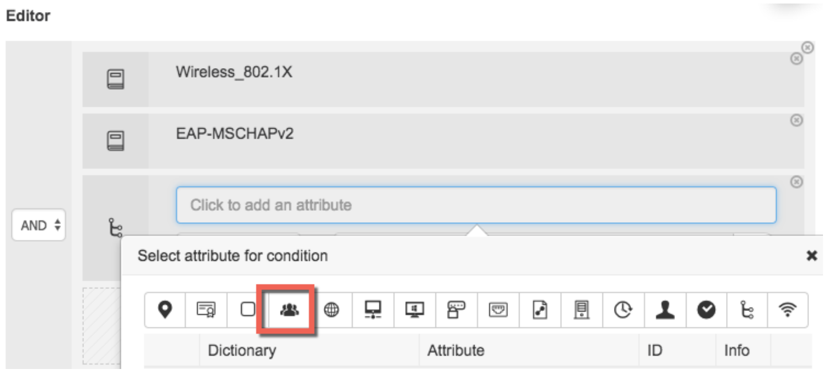
AND

Wireless_802.1X

EAP-MSCHAPv2

Step 10 Select **New**

Step 11 Click to add attribute, and click on **Identity Group**



Editor

AND

Wireless_802.1X

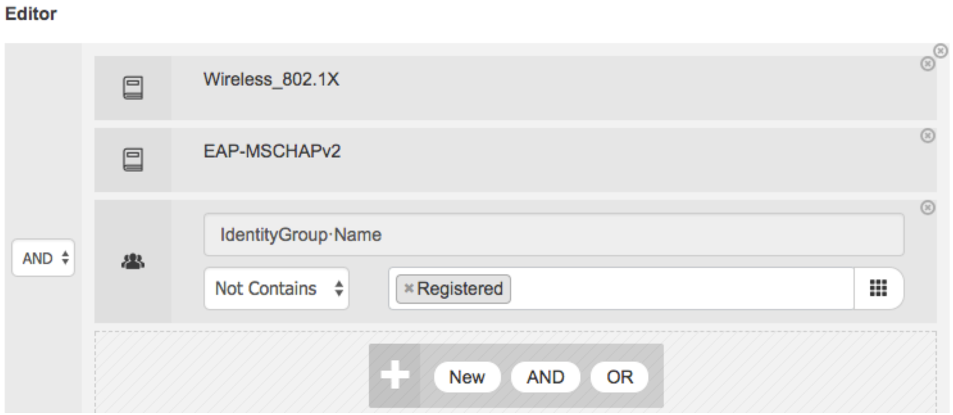
EAP-MSCHAPv2

Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID	Info

Step 12 Select **Identity->Group Name**, and type “**Registered**” to select from the dropdown. Also select **Not Contains** from the Drop-Down menu



Editor

AND

Wireless_802.1X

EAP-MSCHAPv2

IdentityGroup·Name

Not Contains

Registered

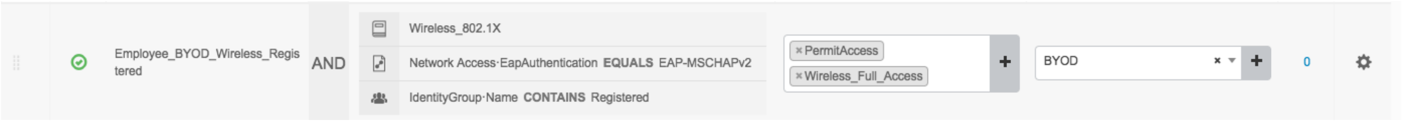
Step 13 Select **Use**

Step 14 Under **Profiles**, select **On-Board NSP**

Step 15 Under **Security Groups**, select **BYOD**

Step 16 Select **Save**

Step 17 Follow steps 4-12 to create the create the **Employee_BYOD_Wireless_Registered** Rule



Employee_BYOD_Wireless_Registered

AND

Wireless_802.1X

Network Access·EapAuthentication EQUALS EAP-MSCHAPv2

IdentityGroup·Name CONTAINS Registered

PermitAccess

Wireless_Full_Access

BYOD

0

Step 18 Select **Use**

Step 19 Under **Profiles**, select **Permit Access**, and **Wireless Full Access**

Step 20 Under **Security Groups**, select **BYOD**

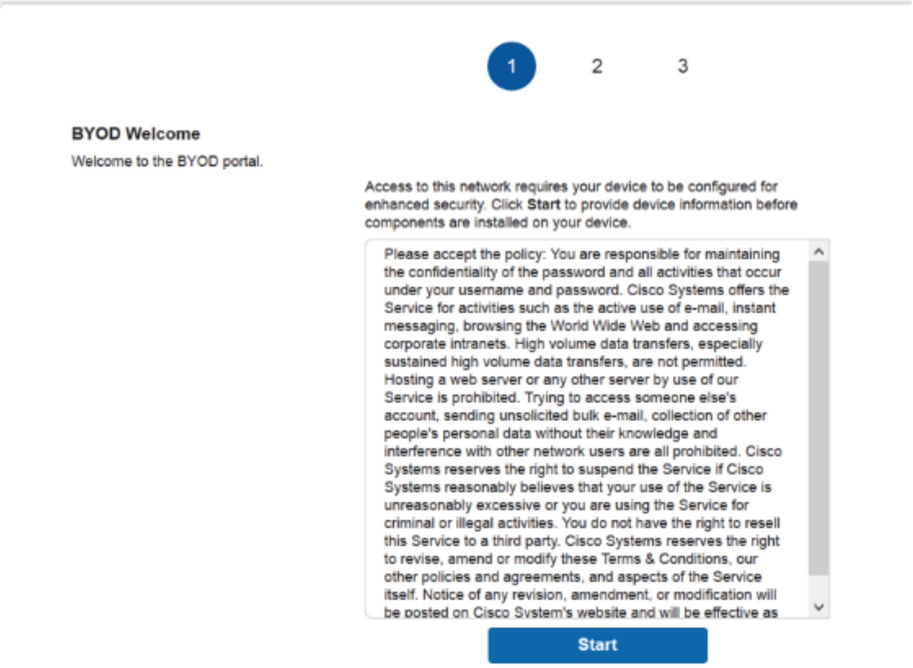
Step 21 Select **Save**

Testing

Step 1 Log in and connect to the appropriate SSID, in this case test007

Step 2 The end-user will be redirected to the BYOD portal page

Step 3 The end-user must agree to the AUP policy
Select **Start**



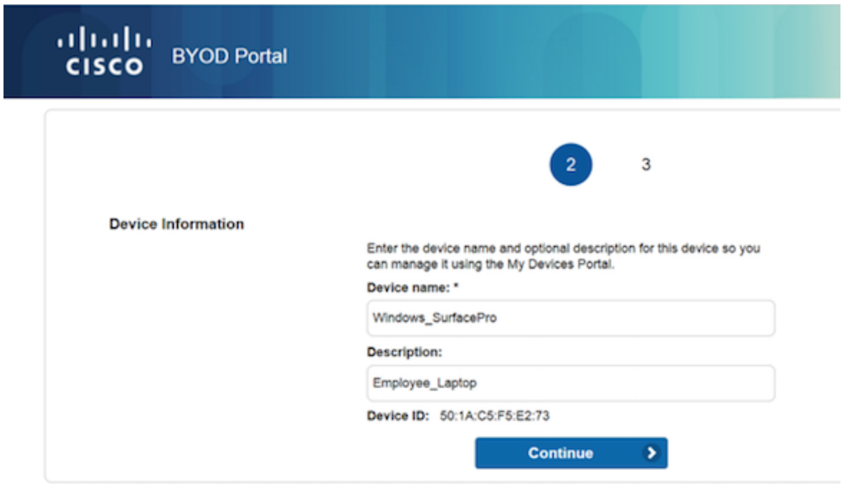
BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as

Step 4 Enter the device name information and select **Continue**



Device Information

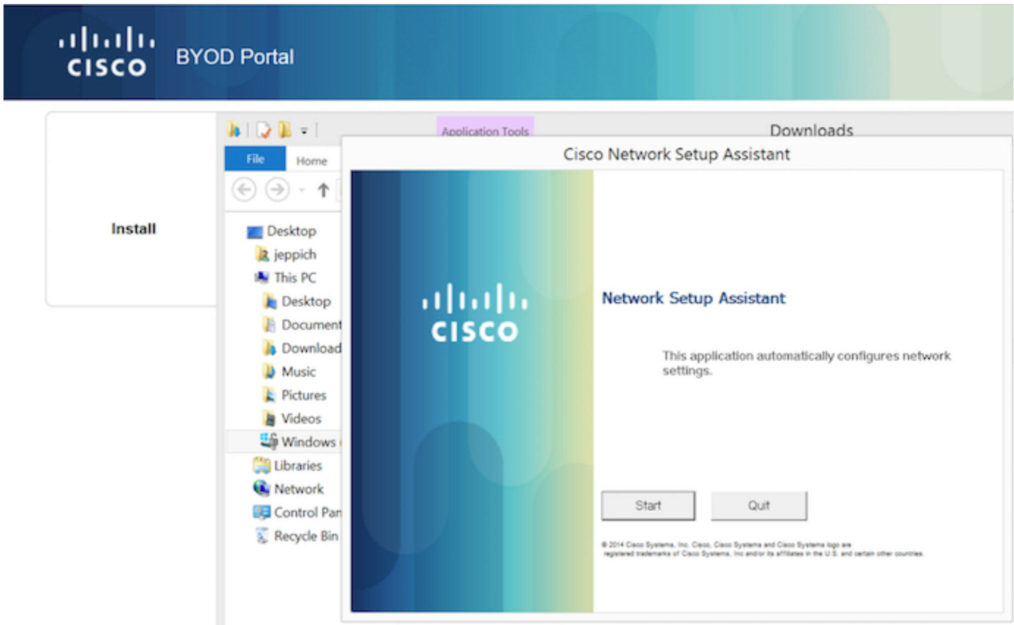
Enter the device name and optional description for this device so you can manage it using the My Devices Portal.

Device name: * Windows_SurfacePro

Description: Employee_Laptop

Device ID: 50:1A:C5:F5:E2:73

Step 5 The endpoint will be provisioned, select **Start**



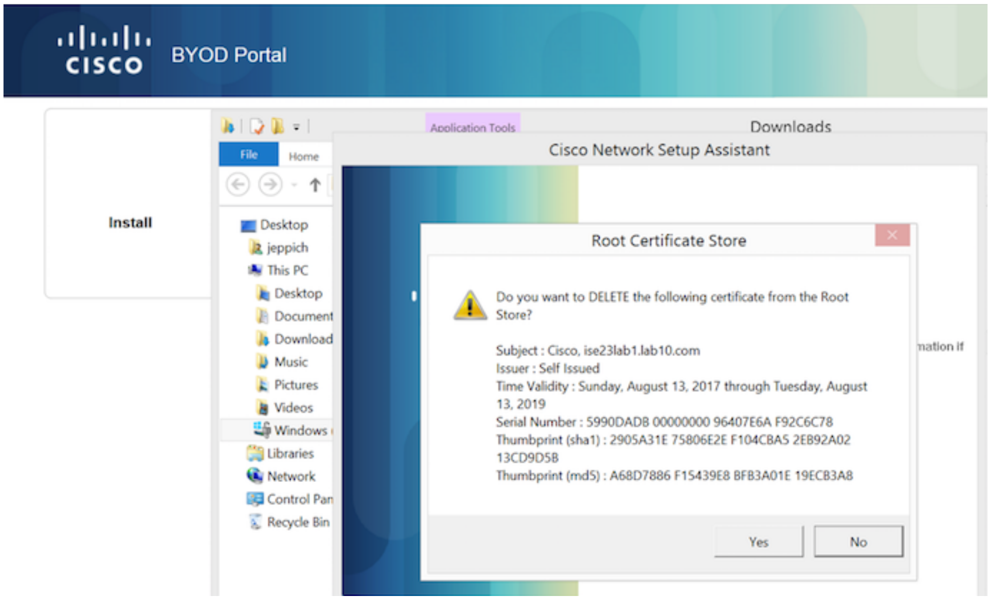
Cisco Network Setup Assistant

Network Setup Assistant

This application automatically configures network settings.

© 2014 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

Step 6 If prompted, select **YES**, delete the certificate from the root store

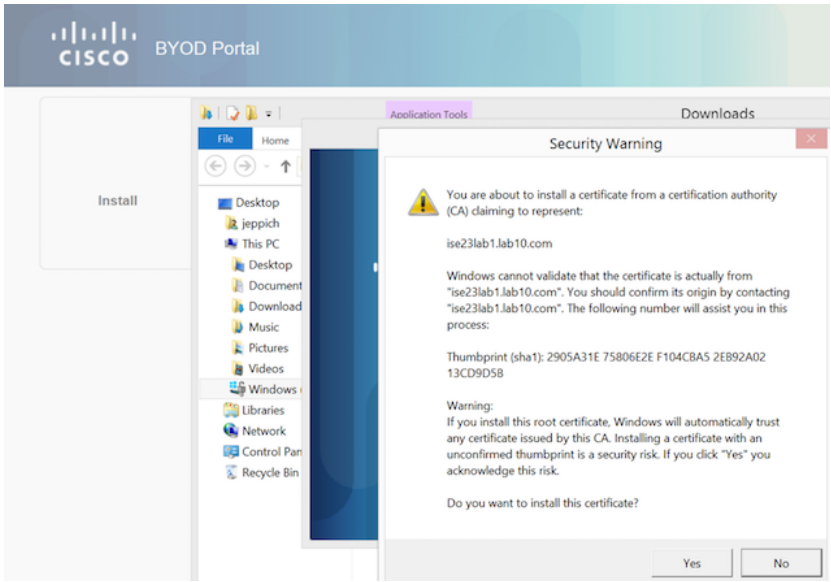


Root Certificate Store

Do you want to DELETE the following certificate from the Root Store?

Subject : Cisco, ise23lab1.lab10.com
Issuer : Self Issued
Time Validity : Sunday, August 13, 2017 through Tuesday, August 13, 2019
Serial Number : 5990DADB 00000000 96407E6A F92C6C78
Thumbprint (sha1) : 2905A31E 75806E2E F104CBA5 2EB92A02 13CD9D5B
Thumbprint (md5) : A68D7886 F15439E8 BFB3A01E 19ECB3A8

Step 7 Select **YES** to install the ISE internal CA certificate



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

ise23lab1.lab10.com

Windows cannot validate that the certificate is actually from "ise23lab1.lab10.com". You should confirm its origin by contacting "ise23lab1.lab10.com". The following number will assist you in this process:

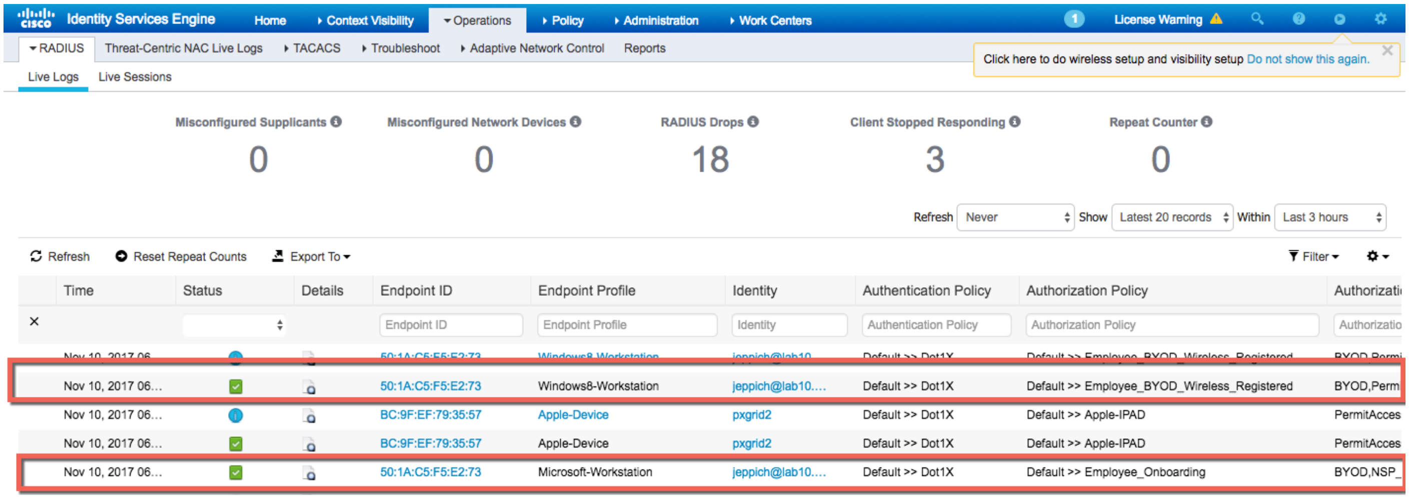
Thumbprint (sha1): 2905A31E 75806E2E F104CBA5 2EB92A02 13CD9D5B

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Step 8 You should now have Internet access, and the McAfee ePO admin can then issue a link to download the McAfee agent manually.

Step 9 To verify the endpoint is registered, select **Operations, RADIUS, Live Logs**, you should see the registered user.



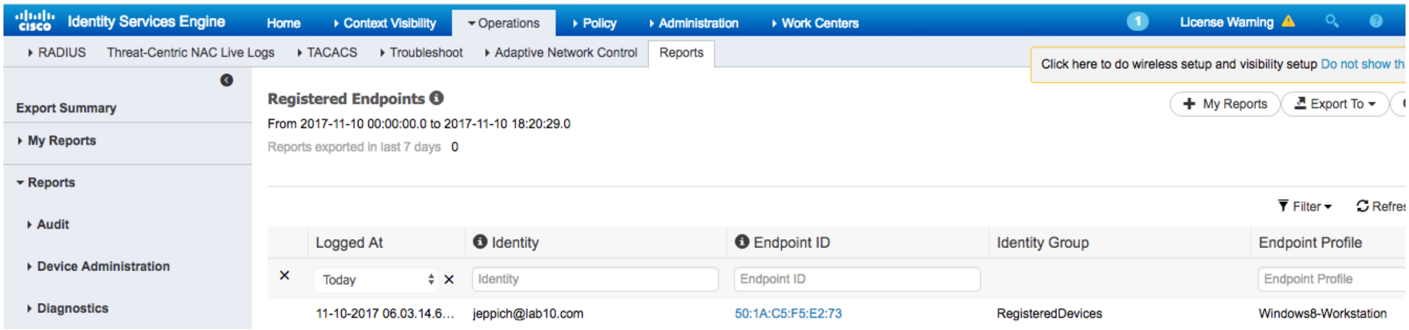
Click here to do wireless setup and visibility setup Do not show this again.

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	18	3	0

Refresh Never Show Latest 20 records Within Last 3 hours

Time	Status	Details	Endpoint ID	Endpoint Profile	Identity	Authentication Policy	Authorization Policy	Authorizati
Nov 10, 2017 06	●		50:1A:C5:F5:E2:73	Windows8-Workstation	jeppich@lab10	Default >> Dot1X	Default >> Employee_BYOD_Wireless_Registered	BYOD,Permi
Nov 10, 2017 06...	✓		50:1A:C5:F5:E2:73	Windows8-Workstation	jeppich@lab10....	Default >> Dot1X	Default >> Employee_BYOD_Wireless_Registered	BYOD,Perm
Nov 10, 2017 06...	●		BC:9F:EF:79:35:57	Apple-Device	pxgrid2	Default >> Dot1X	Default >> Apple-IPAD	PermitAcces
Nov 10, 2017 06...	✓		BC:9F:EF:79:35:57	Apple-Device	pxgrid2	Default >> Dot1X	Default >> Apple-IPAD	PermitAcces
Nov 10, 2017 06...	✓		50:1A:C5:F5:E2:73	Microsoft-Workstation	jeppich@lab10....	Default >> Dot1X	Default >> Employee_Onboarding	BYOD,NSP_

Step 10 To view the registered user in ISE, select **Operations->Reports->Registered Endpoints**



Click here to do wireless setup and visibility setup Do not show th

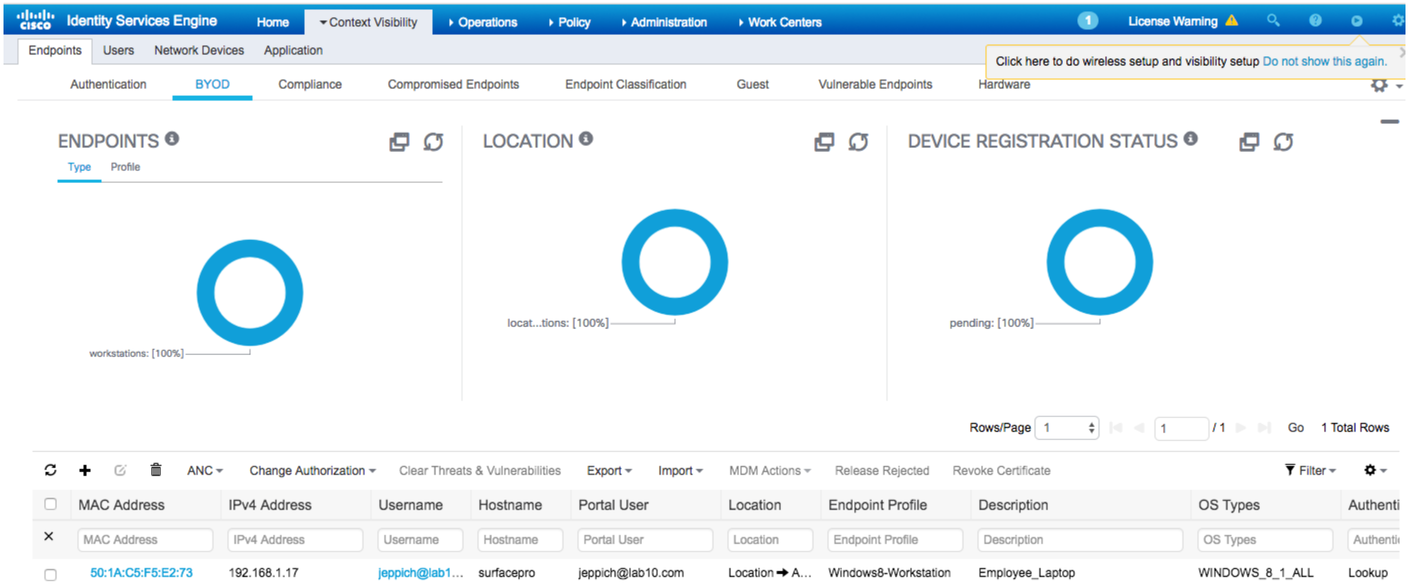
Registered Endpoints

From 2017-11-10 00:00:00.0 to 2017-11-10 18:20:29.0

Reports exported in last 7 days 0

Logged At	Identity	Endpoint ID	Identity Group	Endpoint Profile
Today	Identity	Endpoint ID		Endpoint Profile
11-10-2017 06.03.14.6...	jeppich@lab10.com	50:1A:C5:F5:E2:73	RegisteredDevices	Windows8-Workstation

Step 11 To view to in the ISE BYOD screen, select **Context Visibility->Endpoints->BYOD**



Click here to do wireless setup and visibility setup Do not show this again.

Rows/Page 1 | 1 /1 Go 1 Total Rows

	MAC Address	IPv4 Address	Username	Hostname	Portal User	Location	Endpoint Profile	Description	OS Types	Authenti
✕	MAC Address	IPv4 Address	Username	Hostname	Portal User	Location	Endpoint Profile	Description	OS Types	Authenti
□	50:1A:C5:F5:E2:73	192.168.1.17	jeppich@lab1...	surfacepro	jeppich@lab10.com	Location ➔ A...	Windows8-Workstation	Employee_Laptop	WINDOWS_8_1_ALL	Lookup

Troubleshooting

Checking Certificates on McAfee DXL Broker

If you encounter connection issues between the ISE pxGrid node and the McAfee DXL broker, verify that the certificates are correct.

```
-bash-4.1# tail /var/McAfee/dxlbroker/logs/ipe.log

 INFO {2017-10-26 18:20:23,625} [pool-1-thread-1]
(MemoryBasedMessageProcessor.java:54) - pxgrid.pxgridFabric_ipe-memoryprocessor
(type:ipe-memoryprocessor) : Memory based processor created, queueSize=5000,
threadCount=100
 WARN {2017-10-26 18:20:23,626} [pool-1-thread-1]
(CiscoPxGridFabricConnector.java:129) - pxgrid.pxgridFabric (type:ipe-
ciscopxgridconnector) : Ignoring request to add binding for unsupported name:
pxgrid:error:/dxl/response
 WARN {2017-10-26 18:20:23,626} [pool-1-thread-1]
(CiscoPxGridFabricConnector.java:129) - pxgrid.pxgridFabric (type:ipe-
ciscopxgridconnector) : Ignoring request to add binding for unsupported name:
pxgrid:response:/dxl/response
 INFO {2017-10-26 18:20:23,626} [Thread-10] (PxGridClient.java:239) -
pxgrid.pxgridFabric (type:ipe-ciscopxgridconnector) : pxGrid connect thread
started.
 INFO {2017-10-26 18:20:23,631} [Thread-10] (PxGridClient.java:307) -
pxgrid.pxgridFabric (type:ipe-ciscopxgridconnector) : Connecting to PxGrid...:
 INFO {2017-10-26 18:20:23,632} [Thread-10] (Configuration.java:311) -
Connecting to host 192.168.1.126
 INFO {2017-10-26 18:20:24,360} [Thread-10] (Configuration.java:316) -
Connected OK to host 192.168.1.126
 INFO {2017-10-26 18:20:24,361} [Thread-10] (Configuration.java:341) - Client
Login to host 192.168.1.126
 INFO {2017-10-26 18:20:36,376} [Thread-10] (Configuration.java:343) - Client
Login OK to host 192.168.1.126
 INFO {2017-10-26 18:20:41,758} [Thread-10] (PxGridClient.java:314) -
pxgrid.pxgridFabric (type:ipe-ciscopxgridconnector) : Successfully connected to
PxGrid.
-bash-4.1#
```

Restarting McAfee DXL Broker Service

If you need to restart the McAfee DXL broker service, type the following:

```
service dxlbroker restart
```

Appendices

This section contains the lab configurations for the Cisco Catalyst 3750x switch and Cisco WLC 2504 used in this document.

Catalyst 3750-x Switch

This contains the bootstrapping details for 802.1X, posture, and redirection details.

Note: Change the IP address of 192.168.1.101 to reflect the IP address of your ISE node. Also the radius server key will be used for the "shared secret" in ISE when defining the network device. In this example, the "shared secret" is "password" and port 15 is configured for IEE 802.1x configuration.

For more information on the switch commands a configuration, please see: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/howto_10_universal_switch_config.pdf

```
aaa new model
!
!
ip http server
ip http secure server
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start stop group radius
!
aaa server radius dynamic-author
client 192.168.1.101 server key password
!
ip dhcp snooping
ip device tracking
!
dot1x system-auth-control
!
interface GigabitEthernet1/0/15
switchport mode access
authentication event fail retry 0 action next-method
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication fallback mab
mab
dot1x pae authenticator
spanning-tree portfast
!
ip access-list extended REDIRECT23
permit tcp any any eq www
```

```
deny   ip any host 192.168.1.15
deny   ip any host 192.168.1.229
deny   udp any any eq domain
deny   ip any any
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-acces-req

radius-server attribute 25 access-requst include
radius-server host 192.168.1.101
radius-server key password
radius-server vsa send accounting
radius-server vsa send authentication
```

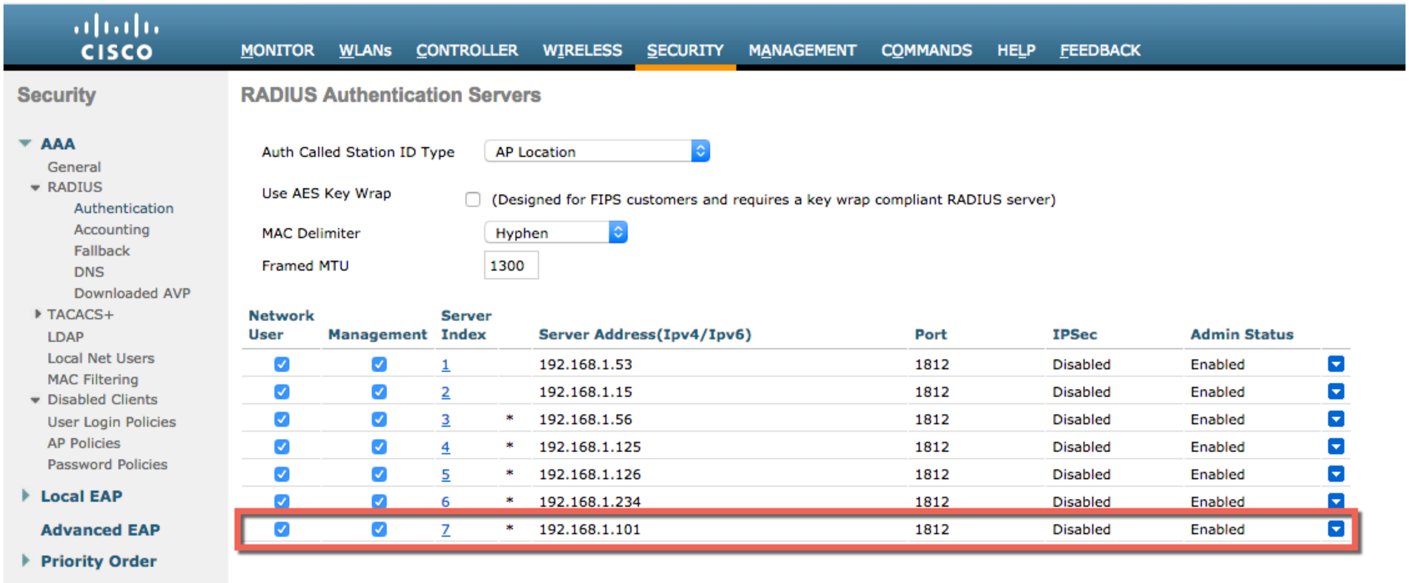
Catalyst 3750-x switch redirection ACL Details

```
ip access-list extended REDIRECT23
deny   ip any host 192.168.1.126    /* Cisco ISE Server */
permit tcp any any eq www
deny   ip any host 192.168.1.15     /* McAfee EPO Server */
deny   ip any host 192.168.1.229    /* McAfee DXL Broker */
deny   udp any any eq domain
deny   ip any any
```

WLC policies

.Please see http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/howto_11_universal_wlc_config.pdf as reference

Configuring Cisco Identity Services Engine (ISE) as Authentication Server



RADIUS Authentication Servers

Auth Called Station ID Type: AP Location

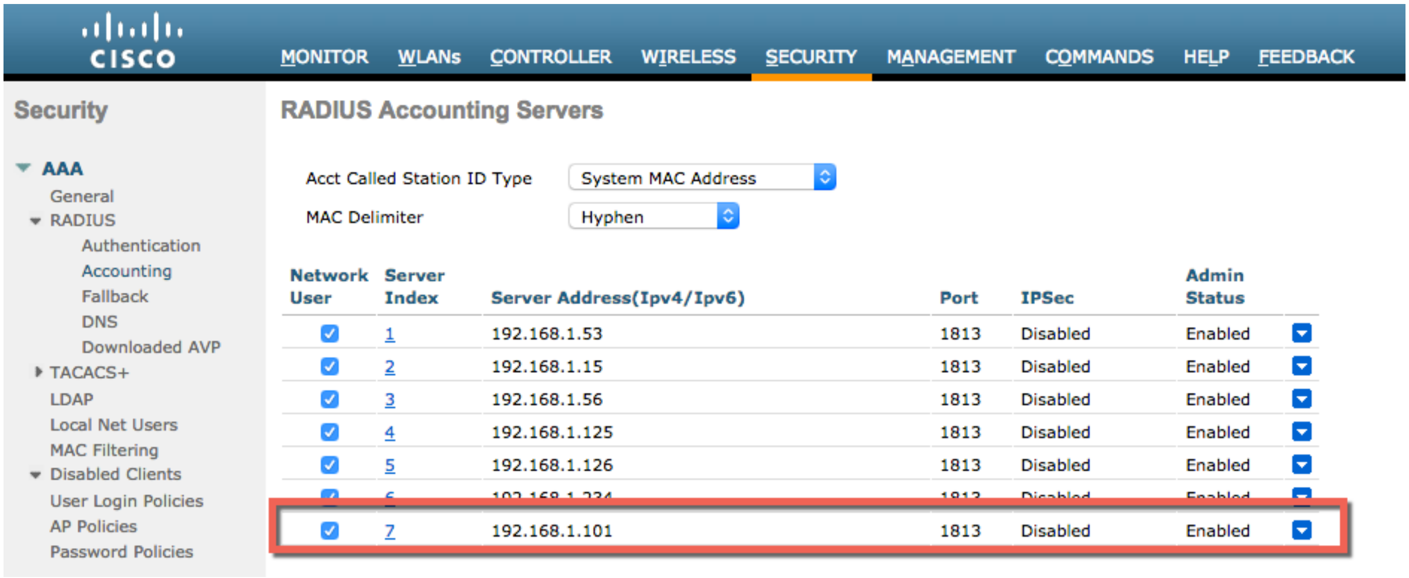
Use AES Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Framed MTU: 1300

Network User	Management	Server Index		Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	☑	1		192.168.1.53	1812	Disabled	Enabled
☑	☑	2		192.168.1.15	1812	Disabled	Enabled
☑	☑	3	*	192.168.1.56	1812	Disabled	Enabled
☑	☑	4	*	192.168.1.125	1812	Disabled	Enabled
☑	☑	5	*	192.168.1.126	1812	Disabled	Enabled
☑	☑	6	*	192.168.1.234	1812	Disabled	Enabled
☑	☑	7	*	192.168.1.101	1812	Disabled	Enabled

Configuring Cisco Identity Services Engine (ISE) as Accounting Server



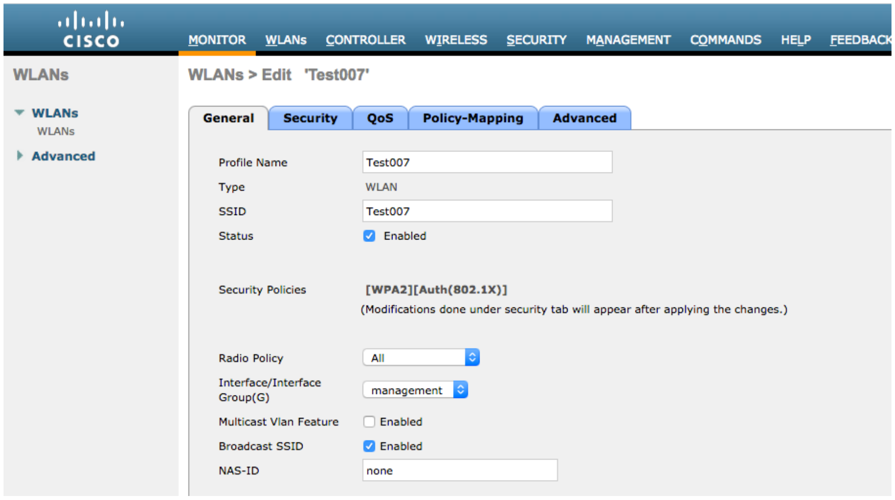
RADIUS Accounting Servers

Acct Called Station ID Type: System MAC Address

MAC Delimiter: Hyphen

Network User	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	1	192.168.1.53	1813	Disabled	Enabled
☑	2	192.168.1.15	1813	Disabled	Enabled
☑	3	192.168.1.56	1813	Disabled	Enabled
☑	4	192.168.1.125	1813	Disabled	Enabled
☑	5	192.168.1.126	1813	Disabled	Enabled
☑	6	192.168.1.234	1813	Disabled	Enabled
☑	7	192.168.1.101	1813	Disabled	Enabled

Configuring Test007 SSID for IEEE 802.1X



WLANs > Edit 'Test007'

Profile Name: Test007

Type: WLAN

SSID: Test007

Status: ☑ Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

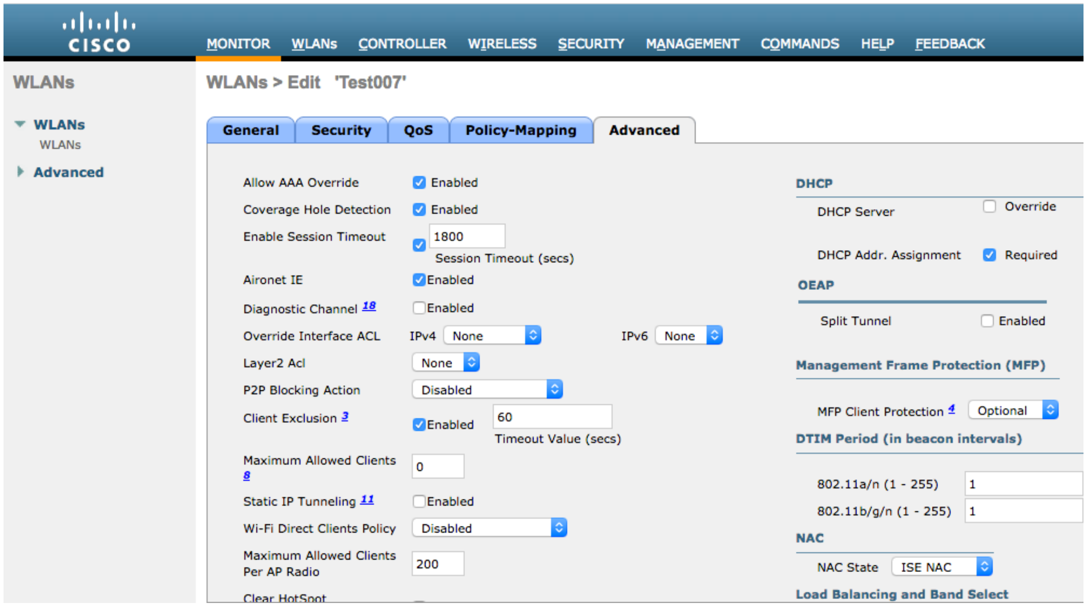
Interface/Interface Group(G): management

Multicast Vlan Feature: □ Enabled

Broadcast SSID: ☑ Enabled

NAS-ID: none

Configuring wireless operation for posture, NAC state set for ISE NAC



WLANs > Edit 'Test007'

Allow AAA Override: ☑ Enabled

Coverage Hole Detection: ☑ Enabled

Enable Session Timeout: ☑ 1800 Session Timeout (secs)

Aironet IE: ☑ Enabled

Diagnostic Channel [18]: □ Enabled

Override Interface ACL: IPv4 None IPv6 None

Layer2 Acl: None

P2P Blocking Action: Disabled

Client Exclusion [3]: ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients [8]: 0

Static IP Tunneling [11]: □ Enabled

Wi-Fi Direct Clients Policy: Disabled

Maximum Allowed Clients Per AP Radio: 200

Clear HotSpot

DHCP

DHCP Server: □ Override

DHCP Addr. Assignment: ☑ Required

OEAP

Split Tunnel: □ Enabled

Management Frame Protection (MFP)

MFP Client Protection [4]: Optional

DTIM Period (in beacon intervals)

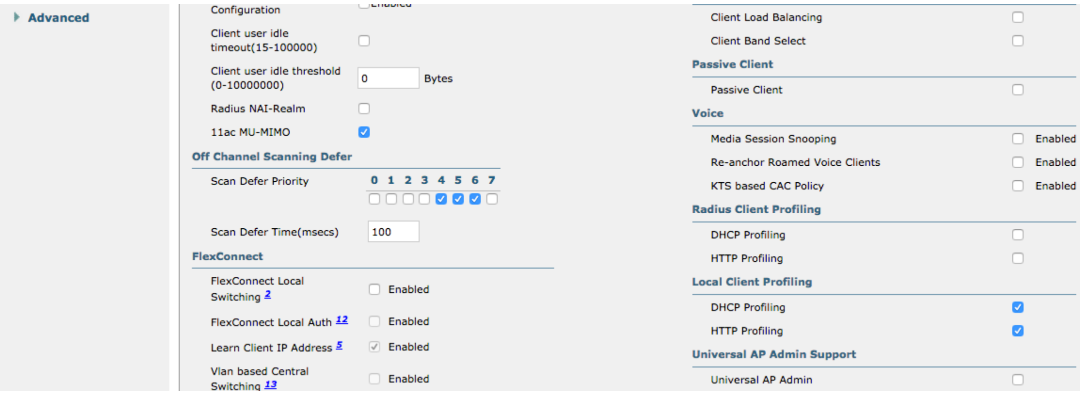
802.11a/n (1 - 255): 1

802.11b/g/n (1 - 255): 1

NAC

NAC State: ISE NAC

Load Balancing and Band Select



Configuration

Client user idle timeout(15-100000): □

Client user idle threshold (0-10000000): 0 Bytes

Radius NAI-Realm: □

11ac MU-MIMO: ☑

Off Channel Scanning Defer

Scan Defer Priority: 0 □ 1 □ 2 □ 3 □ 4 ☑ 5 ☑ 6 ☑ 7 □

Scan Defer Time(msecs): 100

FlexConnect

FlexConnect Local Switching [2]: □ Enabled

FlexConnect Local Auth [12]: □ Enabled

Learn Client IP Address [5]: ☑ Enabled

Vlan based Central Switching [13]: □ Enabled

Client Load Balancing: □

Client Band Select: □

Passive Client

Passive Client: □

Voice

Media Session Snooping: □ Enabled

Re-anchor Roamed Voice Clients: □ Enabled

KTS based CAC Policy: □ Enabled

Radius Client Profiling

DHCP Profiling: □

HTTP Profiling: □

Local Client Profiling

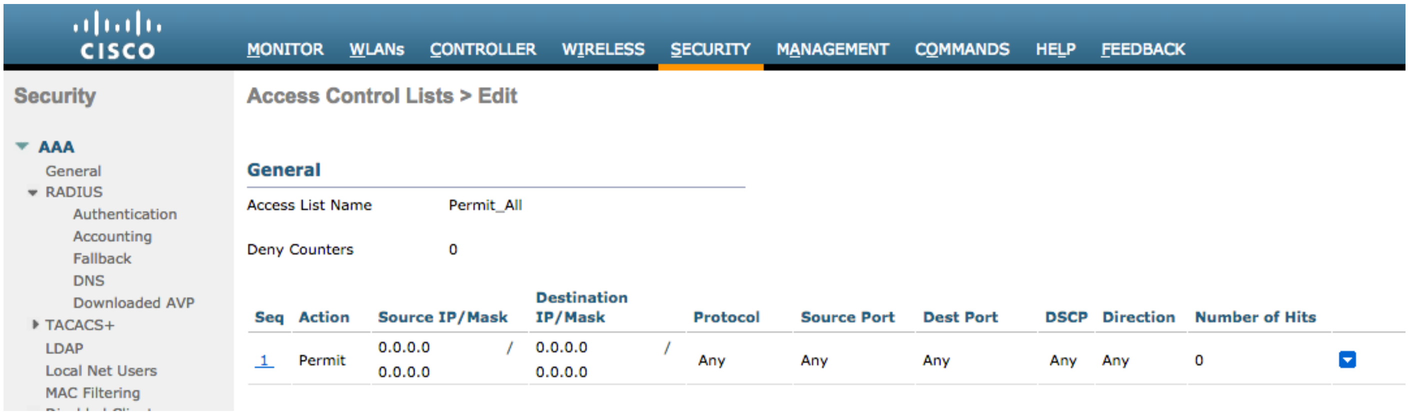
DHCP Profiling: ☑

HTTP Profiling: ☑

Universal AP Admin Support

Universal AP Admin: □

Wireless Permit All ACL



Access Control Lists > Edit

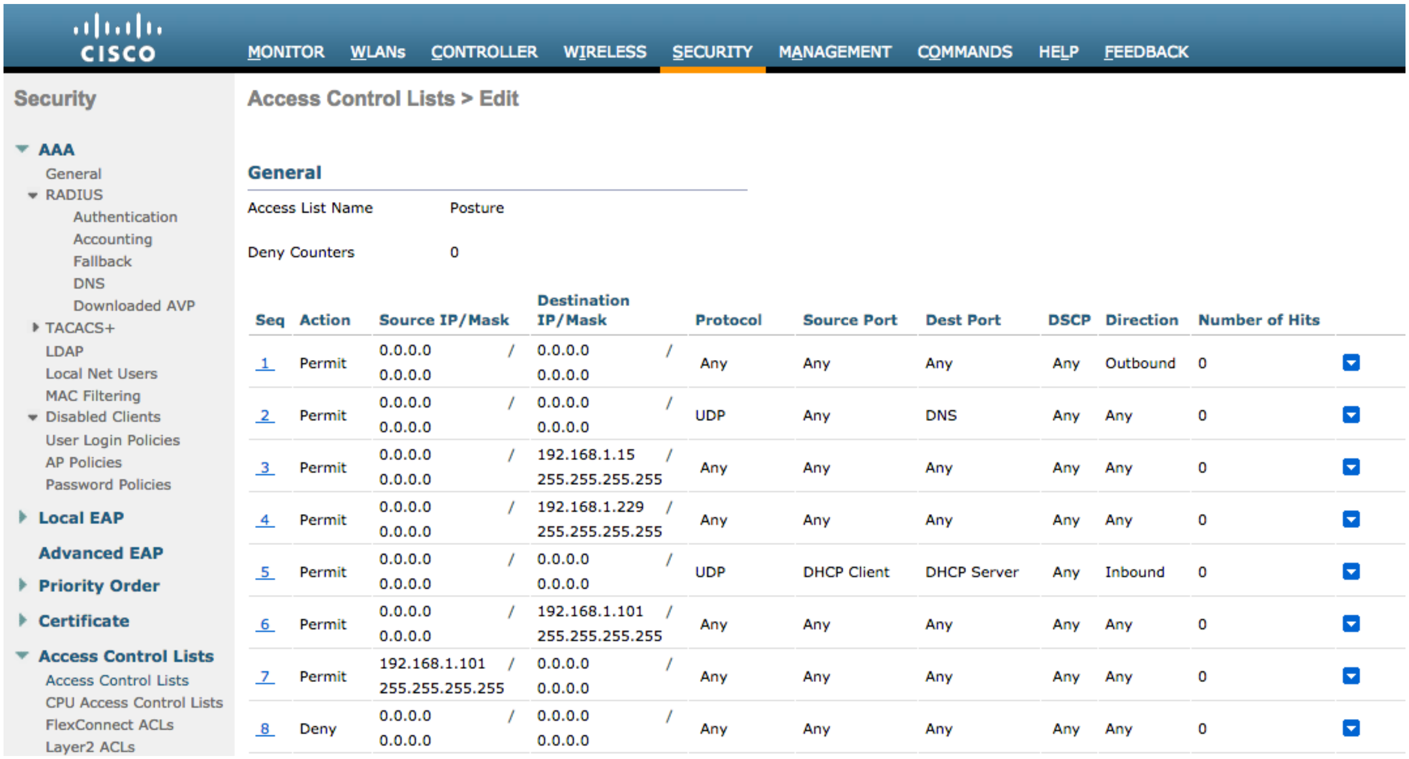
General

Access List Name Permit_All

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

Posture ACL also used for Client Provisioning



Access Control Lists > Edit

General

Access List Name Posture

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	192.168.1.15 / 255.255.255.255	Any	Any	Any	Any	Any	0
4	Permit	0.0.0.0 / 0.0.0.0	192.168.1.229 / 255.255.255.255	Any	Any	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DHCP Client	DHCP Server	Any	Inbound	0
6	Permit	0.0.0.0 / 0.0.0.0	192.168.1.101 / 255.255.255.255	Any	Any	Any	Any	Any	0
7	Permit	192.168.1.101 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
8	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

References

https://communities.cisco.com/docs/DOC-68284 How to Configure pxGrid in ISE Production Environments

https://communities.cisco.com/docs/DOC-71927 Using ISE 2.1 Internal Certificate Authority (CA) to Deploy Certificates to Cisco pxGrid clients *(not using external CA Server)*

https://communities.cisco.com/docs/DOC-71928 Using ISE 2.2 Internal Certificate Authority (CA) to Deploy Certificates to Cisco pxGrid clients *(not using external CA Server)*

https://communities.cisco.com/docs/DOC-71926 - Deploying Certificates with Cisco pxGrid- Using an external Certificate Authority (CA) with updates to Cisco ISE 2.0/2.1/2.2

https://communities.cisco.com/docs/DOC-71925- Deploying Certificates with pxGrid- Using Self-Signed Certificates Updates to Cisco ISE 2.0/2.1/2.2

https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_authz_polprfls.pdf - Managing Authorization Profiles for ISE 2.1/ISE 2.2

https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_010011.html - Managing Authorization Profiles in for ISE 2.0

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116143-config-cise-posture-00.html - Posture Services on the Cisco ISE Configuration Guide

https://communities.cisco.com/docs/DOC-68160 - How To: ISE & BYOD: Onboarding, Registering and Provisioning

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/configure-nam.html - Cisco AnyConnect Profile Editor

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect45/administration/guide/b_AnyConnect_Administrator_Guide_4-5/deploy-anyconnect.html - Cisco AnyConnect Client

https://kc.mcafee.com/corporate/index?page=content&id=KB89737 - How to Use Data Exchange Layer with Cisco Platform Exchange Grid