

L12

Profiling Service in ISE

Lab Overview

This lab examines the use of the profiler service within ISE. We will investigate the available probes including a newer probe available in IOS version 15.x on the switch platforms.

Estimated Completion Time

75 minutes

Lab Procedures

1. Prepare for this lab
2. Get Your Probe On!
3. Examine the current endpoints and configure probes
4. Spoofing Endpoints

Get Your Probe On!

Currently in ISE 1.1.2 there are 9 probes that can be enabled (NETFLOW, DHCP, DHCP SPAN, HTTP, RADIUS, NMAP, DNS, SNMPQUERY, SNMPTRAP). Some of these are more passive than others, in that network access devices (NADs) will send data that is to be profiled to ISE. Other probes use more aggressive techniques for discovering endpoints, such as NMAP. In this section, we will be configuring the L3-Switch and Wireless-Switch to report to ISE using DHCP, RADIUS, and SNMP polls and traps options.

1. Configure the SNMP PROBE commands on the L3-Switch to allow ISE to poll and receive traps from the switch:
 - 1.1. Launch **SecureCRT** from the desktop of the **Admin-PC** and double-click the **L3-Switch** entry if the console is not already connected.
 - 1.2. Verify the current switch configuration:

```
SISE-L3-SW#sh run | incl radius
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
ip radius source-interface Vlan6
radius-server host 10.10.2.50 auth-port 1645 acct-port 1646
radius-server host 10.10.2.60 auth-port 1645 acct-port 1646
radius-server key sharedsecret
radius-server vsa send accounting
radius-server vsa send authentication
```

2. Configure SNMPv3 on the switch:
 - 2.1. Create a standard ACL, only allowing the management subnet to the switch using SNMP:

Note If you don't want to enter the following configuration mode commands by hand for SNMPv3, you can open Windows Explorer on the Admin-PC and enter **ftp://1.1.1.10/ISE**. Then drag the **Lab 12 – L3-Sw Config.txt** file to the desktop of the Admin-PC. Open the file and copy the contents of the file into global configuration mode on the L3-Switch. It's probably best to use SecureCRT on the desktop of the Admin-PC for this copy/paste process.

```
SISE-L3-SW#conf t
SISE-L3-SW(config)#ip access-list standard MANAGEMENT_DEVICES
SISE-L3-SW(config-ext-nacl)#permit 10.10.2.0 0.0.0.255
SISE-L3-SW(config-ext-nacl)#exit
```

Lab 12: Profiling Service in ISE

- 2.2. The following command creates an SNMP group and assigns the same read-only view as the older SNMP v2. Note that not specifying specific views defaults to this view. Also notice that the ACL created in the last command is assigned:

```
SISE-L3-SW(config)#snmp-server group ISE-GROUP v3 priv read V3Read notify TRAP_VIEW
access MANAGEMENT_DEVICES
SISE-L3-SW(config)#snmp-server view V3Read iso included
SISE-L3-SW(config)#snmp-server view TRAP_VIEW iso included
```

- 2.3. Next, create the user account that will be used for communications between ISE and the switch (polling or traps) and assign that user to the group just created:

```
SISE-L3-SW(config)# snmp-server user ISEBOX ISE-GROUP v3 auth sha ISE_AUTH priv aes
128 ISE_ENCRYPT
4d20h: Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...
```

- 2.4. Configure the trap destination (ISE) and the user used to secure the connection:

```
SISE-L3-SW(config)#snmp-server host 10.10.2.50 version 3 priv ISEBOX
SISE-L3-SW(config)#snmp-server host 10.10.2.60 version 3 priv ISEBOX
SISE-L3-SW(config)#snmp-server enable traps snmp linkdown linkup
SISE-L3-SW(config)#snmp-server enable traps mac-notification change move
```

- 2.5. Enable mac-notifications on the f0/3 interface. For production, please see the note below:

```
SISE-L3-SW(config)#interface range f0/2 - 3
SISE-L3-SW(config-if)#snmp trap mac-notification change added
SISE-L3-SW(config-if)#end
```

Note	In production, we typically disable the mac notification and linkup notification features. The reason being that the SNMP processes could become overwhelmed with processing the data. Also, since we will use other probe detection mechanisms, there would be an overlap.
-------------	---

- 2.6. Confirm the that SNMP v3 group is setup correctly on the switch:

```
SISE-L3-SW#sh snmp group
groupname: ISE-GROUP                      security model:v3 priv
readview : V3Read                        writeview: <no writeview specified>
notifyview: TRAP_VIEW
row status: active      access-list: MANAGEMENT_DEVICES
```

- 2.7. Confirm that the SNMP v3 user is setup correctly:

```
SISE-L3-SW#show snmp user

User name: ISEBOX
Engine ID: 800000090300001A6CE39E03
storage-type: nonvolatile      active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ISE-GROUP
```

3. Configure the DHCP Helper in the L3-Switch to forward DHCP data to the PSN:

```
SISE-L3-SW(config)#int range vlan 6-7
SISE-L3-SW(config-if)#ip helper-address 10.10.2.50
SISE-L3-SW(config-if)#ip helper-address 10.10.2.60
SISE-L3-SW(config-if)#exit
SISE-L3-SW(config)# logging monitor
```

Note	Cisco ISE profiling service will re-profile endpoints based only on new requests of DHCP INIT-REBOOT, and DHCP SELECTING message types. Though other DHCP message types are processed such as RENEWING, and REBINDING, they are not used for profiling endpoints.
-------------	---

4. Test DHCP:

4.1. Issue the debug dhcp command:

```
SISE-L3-SW#term mon
SISE-L3-SW#debug ip dhcp server packet
DHCP server packet debugging is on.
```

4.2. Now, go to a command prompt on the **Consultant-PC** and issue a dhcp release/renew:

```
c:\>ipconfig -release
```

Windows IP Configuration

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix  . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
```

```
c:\>ipconfig -renew
```

Windows IP Configuration

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix  . : gkl.local
IP Address. . . . . : 10.10.10.14
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.1
```

Lab 12: Profiling Service in ISE

- 4.3. You should see the debug output and the highlighted line below indicating the message was successfully sent to ISE:







```
SISE-L3-SW#
4d22h: DHCPD: Reload workspace interface Vlan7 tableid 0.
4d22h: DHCPD: tableid for 10.10.10.1 on Vlan7 is 0
4d22h: DHCPD: client's VPN is .
4d22h: DHCPD: using received relay info.
4d22h: DHCPD: Sending notification of DISCOVER:
4d22h:   DHCPD: htype 1 chaddr 000c.2924.1572
4d22h:   DHCPD: interface = Vlan7
4d22h:   DHCPD: class id 4d53465420352e30
4d22h:   DHCPD: out_vlan_id 0
4d22h: DHCPD: Looking up binding using address 10.10.10.1
4d22h: DHCPD: setting giaddr to 10.10.10.1.
4d22h: DHCPD: BOOTREQUEST from 0100.0c29.2415.72 forwarded to 10.10.1.25.
4d22h: DHCPD: BOOTREQUEST from 0100.0c29.2415.72 forwarded to 10.10.2.50.
4d22h: DHCPD: BOOTREQUEST from 0100.0c29.2415.72 forwarded to 10.10.2.60.
4d22h: DHCPD: Reload workspace interface Vlan5 tableid 0.
<Text Ommitted>
```

Examine the Endpoints and Configure Probes in ISE

Now that we have three probes enabled on the switch (SNMP polling, SNMP traps and the DHCP probe), we'll examine the current endpoints and then enable the probes within ISE.

5. Examine the current endpoints:
- 5.1. In the web console of ISE, navigate to **Administration > Identity Management > Identities**. Then, select **Endpoints** in the menu tree.
 - 5.2. You should only see a single host listed which is the IP-Phone from the last lab. Leave this host in the database for now.

Endpoints

Selected 0 Total 1				
 Edit	 Add	 Delete	 Import	» Show All
Endpoint Profile	MAC Address	Static Assignment		
<input type="checkbox"/> Unknown	00:0C:29:94:96:64	true		

- 5.3. Click the **Unknown** link to bring up the endpoints details. Note the EndpointSource attribute indicating that the endpoint was created through the My Device Portal page.

* MAC Address **00:0C:29:94:96:64**

* Policy Assignment **VMWare-Device**

Static Assignment ☒

* Identity Group Assignment **Blacklist**

Static Group Assignment ☒

Attribute List

Description	IP-Phone
DeviceRegistrationStatus	registered
EndPointPolicy	Unknown
EndPointSource	REST
IdentityGroup	Blacklist
IdentityStoreName	GKL_AD

6. Next, configure the probes in ISE. Remember, there are 9 probes. The only ones we care about currently are the SNMP and DHCP related probes (non SPAN).
 - 6.1. In the web console of ISE, navigate to **Administration > System > Deployment**.
 - 6.2. Select **ISE-Primary** and click **Edit**.

Deployment Nodes

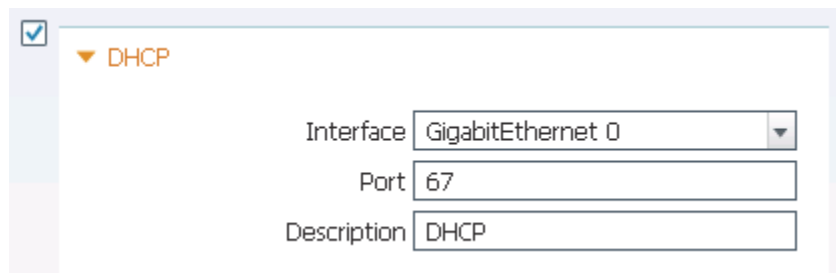
Selected 1 | Total 2

Hostname	Node Type	Personas	Role(s)
<input checked="" type="checkbox"/> ISE-Primary	ISE	Administration, Monitoring, Policy Service	PRI(A), PRI(M)
<input type="checkbox"/> ISE-Secondary	ISE	Administration, Monitoring, Policy Service	SEC(A), SEC(M)

Lab 12: Profiling Service in ISE

6.3. Click the **Profiling Configuration** tab.

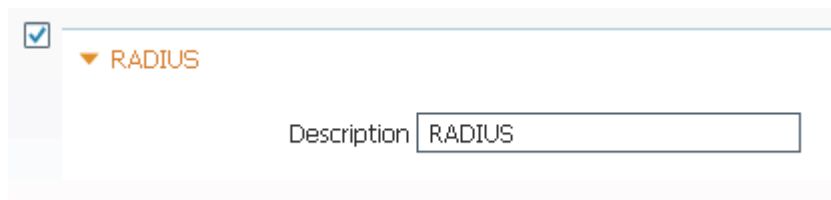
6.3.1. Enable the **DHCP** Probe (not DHCP SPAN). Since we have the helper address configured, ISE will recognize these packets and process the requests, not the responses from the DHCP server.



A screenshot of the DHCP probe configuration interface. On the left, there is a checkbox that is checked, followed by a dropdown menu showing 'DHCP'. To the right of this, there are three input fields: 'Interface' with a dropdown menu showing 'GigabitEthernet 0', 'Port' with a text box containing '67', and 'Description' with a text box containing 'DHCP'.

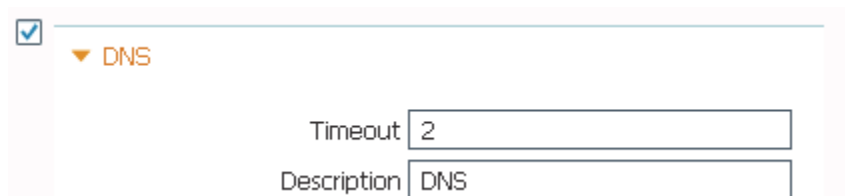
Note Although we only have a single interface on the VM, adding more interfaces allows you to divide up various traffic flows to different interfaces. This is especially important since you really don't want to manage ISE through the same interface where a high number of probe packets are received for contention reasons. As an example, ISE could have a dedicated interface connected to a switch port that would be spanning DHCP traffic to it.

6.3.2. Enable the **RADIUS** Probe. This obviously listens for RADIUS accounting packets and filters out only interesting data for probe processing. This probe is relied on more heavily nowadays with the newer features in IOS 15.0 code, as you'll see later.



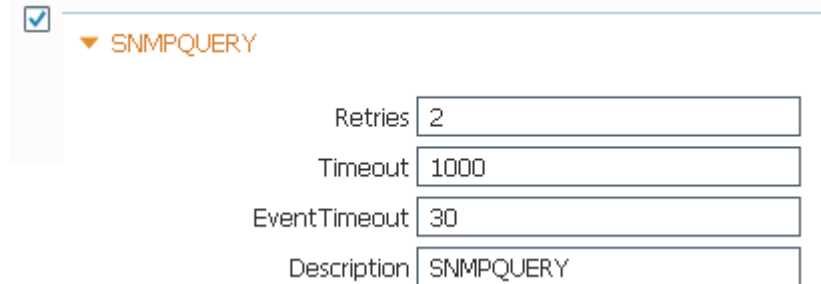
A screenshot of the RADIUS probe configuration interface. On the left, there is a checkbox that is checked, followed by a dropdown menu showing 'RADIUS'. To the right of this, there is one input field: 'Description' with a text box containing 'RADIUS'.

6.3.3. Enable the **DNS** Probe. This probe requires that one of the other probes be enabled. It's more of an enhancement to other probes and provides a reverse DNS lookup for IP addresses already discovered through such probes as the DHCP one.



A screenshot of the DNS probe configuration interface. On the left, there is a checkbox that is checked, followed by a dropdown menu showing 'DNS'. To the right of this, there are two input fields: 'Timeout' with a text box containing '2', and 'Description' with a text box containing 'DNS'.

- 6.3.4. Enable the **SNMPQUERY** Probe. This probe monitors hosts on switchports and uses CDP/LLDP for device discovery as well as mac table discovery, ARP table mappings and a large, very large list of other attributes. Leave the settings at their defaults. Note that the NAD needs to also be configured. This step was done earlier in the lab.



☒ **SNMPQUERY**

Retries

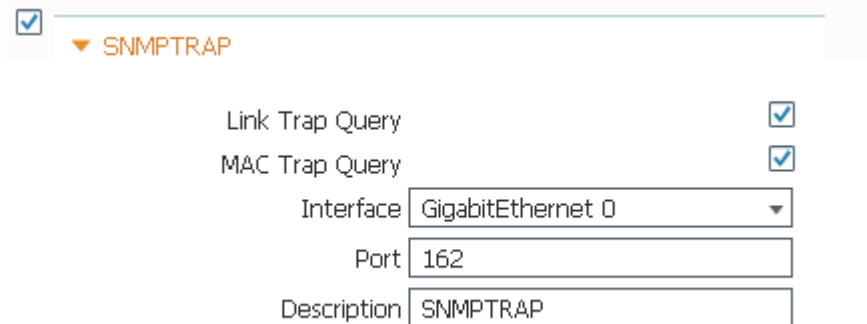
Timeout

EventTimeout

Description

Note The community strings are configured under the device configuration, not here.

- 6.3.5. Enable the **SNMPTRAP** Probe. This allows ISE to profile based upon traps sent from the switch, including MAC-Notifications, that is, when new MACs are learned or when they are moved and linkup/linkdown notifications.



☒ **SNMPTRAP**

Link Trap Query ☒

MAC Trap Query ☒

Interface

Port

Description

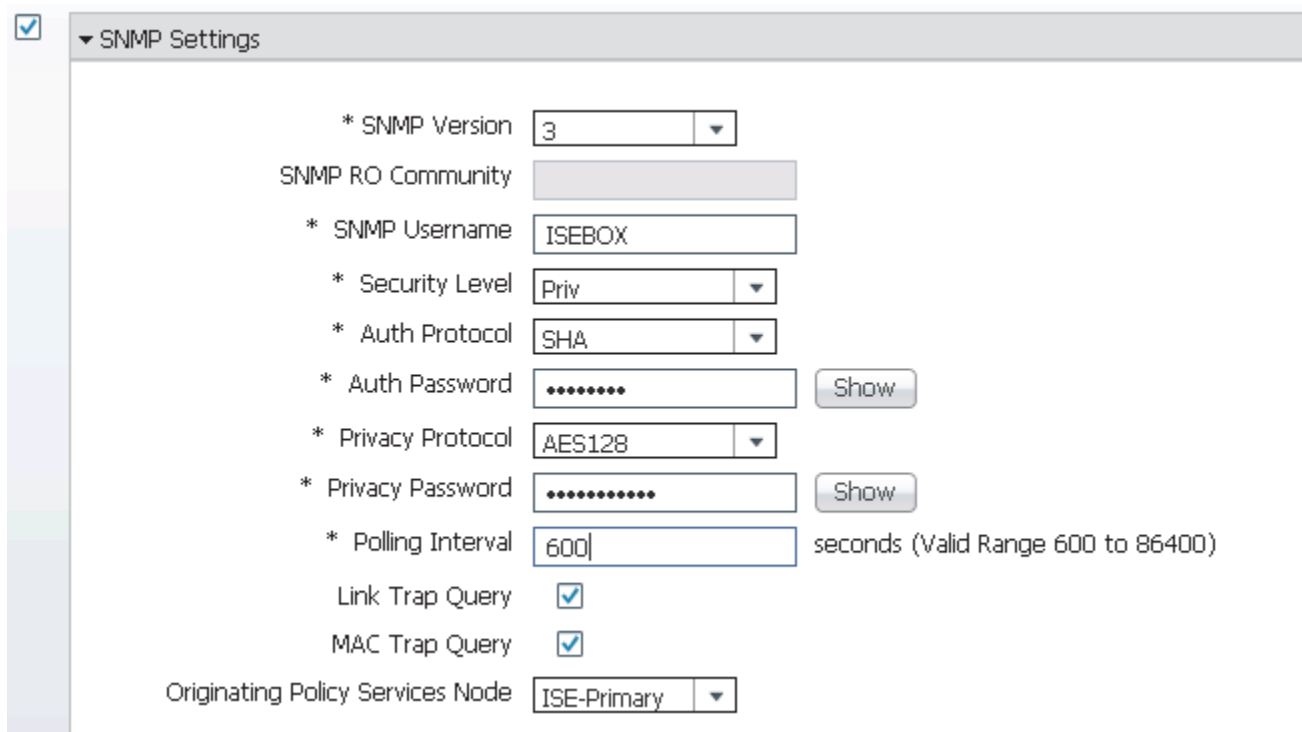
- 6.3.6. Click **Save**.

7. Next, navigate to the AAA client configuration in ISE and configure the SNMP settings that will be used to poll and process traps:
- 7.1. Navigate to **Administration > Network Resources > Network Devices** and click the **L3-Switch**.
 - 7.2. The only IP address that should be associated with the L3-Switch is the 10.10.2.1 address.

Lab 12: Profiling Service in ISE

- 7.3. Scroll down and **Check** SNMP Settings and enter the following in the fields provided:

SNMP Version: **3**
SNMP Username: **ISEBOX**
Security Level: **Priv**
Auth Protocol: **SHA**
Auth Password: **ISE_AUTH**
Privacy Protocol: **AES128**
Privacy Password: **ISE_ENCRYPT**
Polling Interval: **600**
Originating Policy Service Node: **ISE-Primary**



▼ SNMP Settings

* SNMP Version

SNMP RO Community

* SNMP Username

* Security Level

* Auth Protocol

* Auth Password

* Privacy Protocol

* Privacy Password

* Polling Interval seconds (Valid Range 600 to 86400)






Link Trap Query ☒

MAC Trap Query ☒

Originating Policy Services Node

- 7.3.1. Click **Save**.

8. ISE will contact the switch using SNMP and discover quite a few endpoints. This can take up to a 600 second interval. Examine the endpoints and their profile policies:
 - 8.1. Navigate back to **Administration > Identity Management > Identities > Endpoints**.
 - 8.2. You will see a large number of endpoints discovered, for more devices than what appear on your topology diagram. The devices may appear immediately or may appear after 10 minutes (600 seconds) due to the polling interval. Click the first of the endpoints labeled as a **Cisco Device**.

 Edit	 Add	 Delete ▼	 Import ▼	»	Show	All ▼	
<input type="checkbox"/>	Endpoint Profile ▲	MAC Address	Static Assignment				
<input type="checkbox"/>	Cisco-Device	00:1A:6C:E3:9E:41	false				
<input type="checkbox"/>	Cisco-Device	00:1A:6C:E3:9E:46	false				
<input type="checkbox"/>	Cisco-Device	00:1A:6C:E3:9E:43	false				
<input type="checkbox"/>	Cisco-Device	00:C2:82:E1:7D:A7	false				
<input type="checkbox"/>	Cisco-Device	00:1A:6C:E3:9E:42	false				
<input type="checkbox"/>	Cisco-Device	00:1A:6C:E3:9E:45	false				

- 8.3. In the details of the endpoint, you will see the Policy Assigned listed as *Cisco Device*. Also examine the attribute list. You will see the IP address of the NAD where the endpoint was discovered and the IP of the endpoint itself which is the giveaway. It turns out that the IP listed is a VLAN interface on the L3-Switch.

Attribute List	
DeviceRegistrationStatus	notRegistered
EndPointPolicy	Cisco-Device
EndPointProfilerServer	ISE-Primary
EndPointSource	SNMPQuery Probe
IdentityGroup	Profiled
MACAddress	00:19:2F:8F:2E:0F
MatchedPolicy	Cisco-Device
NADAddress	10.10.2.1
OUI	Cisco Systems
PolicyVersion	9
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	161
Total Certainty Factor	10
ip	10.10.0.1

- 8.4. Click Endpoints in the menu list in order to view all of the endpoints again. In the list, you will see the endpoint we added in an earlier lab associated with the **VMWare-Device** endpoint profile (MAC address 00:0C:29:94:96:64). Select the endpoint and click **Delete > Delete Selected**. Confirm the deletion.

NMAP Probe

Next, we'll examine the Network Scan (NMAP) probe. Before enabling the scanning feature, we'll need to allow return traffic from the scan to come back to ISE. What does this mean? It means that the dACLs pushed to switch interfaces for endpoints sessions are non-stateful and needs some adjustments.

- 8.5. In ISE, navigate to **Policy > Policy Elements > Results**. In the menu list, select **Authorization > Downloadable ACLs**. Edit the **CWA-Temp-ACL** dACL. Insert the following lines into the first entries in the list, then click **Save**:

```
permit tcp any host 10.10.2.50 established
permit tcp any host 10.10.2.60 established
permit udp any eq 161 host 10.10.2.50
permit udp any eq 161 host 10.10.2.60
```

8.6. Flap the fa0/3 interface to download the latest ACL to the switch:

```
SISE-L3-SW# conf t
SISE-L3-SW(config)# int f0/3
SISE-L3-SW(config-if)# shut
SISE-L3-SW(config-if)# no shut
SISE-L3-SW(config-if)# end
```

9. Next, examine the Network Scan (NMAP) Probe in ISE:

9.1. Navigate to **Administration > System > Deployment**.

9.2. Select **ISE-Primary** and click **Edit**.

9.3. Click the **Profiling Configuration** tab.

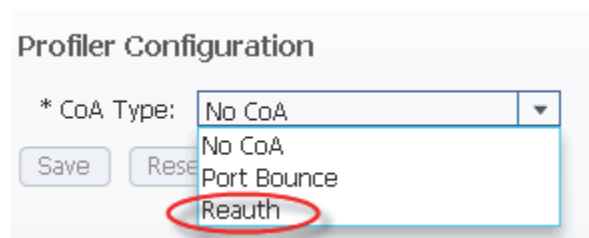
9.4. Enable the Network Scan (NMAP) probe and click **Save**. The Manual Scan feature is not very useful. The intent of NMAP is to associate an endpoint with a profiling profile and that in-turn causes the scan to take place.

10. Navigate to **Administration > Identity Management > Identities > Endpoints**. Locate the **00:0C:29:24:15:72** endpoint and note its association to the VMWARE profile. This is very generic and doesn't buy us a whole lot. Let's get a little more intrusive and kick off an NMAP scan when a VMWare device is detected to see if we can retrieve a little more info on the endpoint:

10.1. Let's presume that NMAP **does** find something about the VMWare device that makes ISE adjust its profile. In that case, we really want the re-profiling to cause a CoA change, meaning that we want the authentication/authorization policies to be re-examined for the endpoint. Investigate the current CoA settings for Profiler. Navigate to **Administration > System > Settings** and click **Profiling** in the menu list.

Note The reason this is not configured by default is because some organizations just use profiling to collect and run inventory reports of the endpoints attached to the system and not so much concerned with re-authorization of the endpoint.

10.2. Change the CoA type to **Reauth** and click **Save**.



Lab 12: Profiling Service in ISE

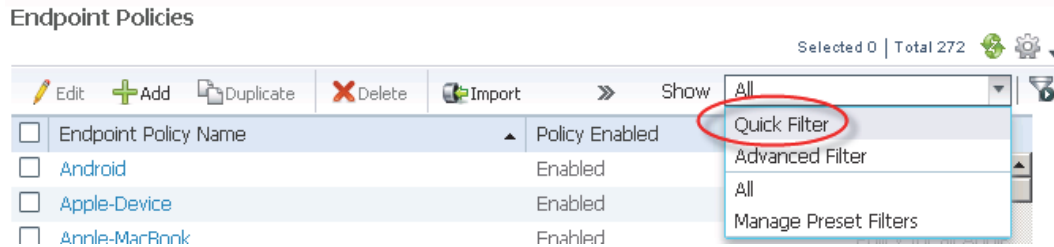
Note This setting change will affect any newly profiled devices.

11. Next, investigate profiling elements that will be used to determine what to do when a re-profile occurs:
 - 11.1. Navigate to **Policy > Policy Elements > Results > Profiling > Exception Actions**. You will see 3 exceptions listed. Click the **Add** button. These policies are referenced from within Profiling policies and can create exceptions to the global setting we just modified in the last step. **We will not create an exception** at this time; we just wanted to point out the location of the configuration. Click **Cancel**.
12. Next, modify the VMWare profiling policy to take an additional action of an NMAP scan for all VMWare endpoints. The following chart indicates the ports that are scanned during the process:

NMAP probe: ports scanned by default

TCP Ports		UDP Ports	
Ports	Service	Ports	Service
21/tcp	ftp	53/udp	domain
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3306/tcp	mysql	631/udp	ipp
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

- 12.1. Navigate to **Policy > Profiling > Profiling Policies**. In the Show drop-down list, select **Quick Filter**.



- 12.2. In the Endpoint Policy Name field, enter **VM** and hit enter. Only one entry in the list should appear. **Click** the entry name.

Note The filter fields are case-sensitive.

<input type="checkbox"/>	Endpoint Policy Name	Policy Enabled	Description
	VM		
<input type="checkbox"/>	VMWare-Device	Enabled	Policy for VMWare D

- 12.3. In the Network Scan (NMAP) Action drop down list, select **CommonPortsAndOS-scan**.

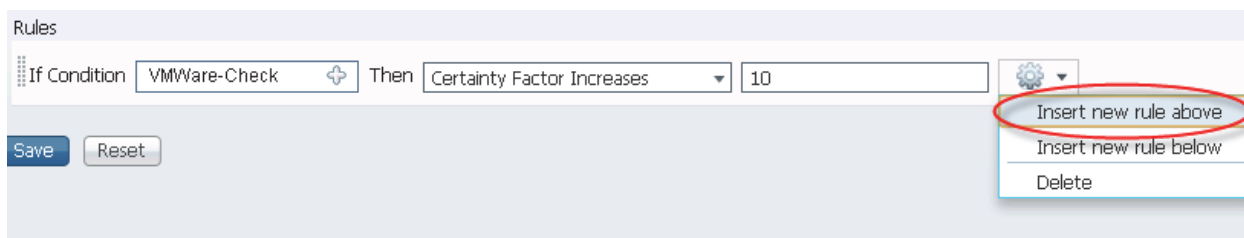
Profiler Policy List > VMWare-Device

Profiler Policy

* Name	VMWare-Device	Description	Policy for VMWare Device
Policy Enabled	<input checked="" type="checkbox"/>		
* Minimum Certainty Factor	10	(Valid Range 1 to 65535)	
* Exception Action	NONE		
* Network Scan (NMAP) Action	CommonPortsAndOS-scan		
	<input type="radio"/> Create Matching Identity Group <input checked="" type="radio"/> Use Hierarchy		
* Parent Policy	NONE		

Lab 12: Profiling Service in ISE

- 12.4. Next, a rule must be created which kicks off the NMAP scan action we just created. In the Rules section at the bottom of the form, click the configuration button and select **Insert new rule above**.



- 12.5. In the Condition name field, click on **Select Existing Condition from Library** and select **VMWare-check**. In the *Then* field, select **Take Network Scan Action**.



- 12.6. Click **Save**.

- 12.7. Go to the **L3-Switch** and shutdown the port f0/3.

```
SISE-L3-SW(config)#int f0/3
SISE-L3-SW(config-if)#shut
```

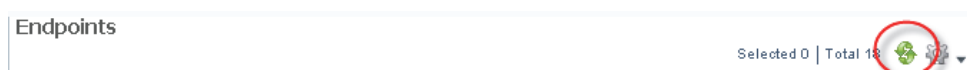
- 12.8. Go back to the web console of ISE and delete the Consultant-PC endpoint from the local endpoint store. Navigate to **Administration > Identity Management > Identities > Endpoints**. Locate and select the entry with the **00:0C:29:24:15:72** MAC address.

- 12.9. **Delete** the endpoint and **confirm** the deletion.

- 12.10. Now go back to the switch and bring up the interface.

```
SISE-L3-SW(config-if)#no shut
```

- 12.11. Go back to ISE and click the refresh link in the endpoints section. You should see the endpoint reappear. Wait about 3 or 4 minutes for the NMAP scan to complete.



- 12.12. **Edit** the endpoint and examine the attributes. You should see new attributes appear relating to the open ports on the endpoint. As of this point, all NMAP has completed is successfully scanning an endpoint and finding open ports. In order to use these scan results, one would need to create a custom profile that references these ports. Please note that the results may differ. Close the endpoint details.

Endpoint

* MAC Address **00:0C:29:24:15:72**

* Policy Assignment **VMWare-Device**

Static Assignment ☐

* Identity Group Assignment **Profiled**

Static Group Assignment ☐

Attribute List

1026-tcp	LSA-or-nterm
123-udp	ntp
135-tcp	msrpc
135-udp	msrpc
137-udp	netbios-ns
138-udp	netbios-dgm
139-tcp	netbios-ssn
139-udp	netbios-ssn
1434-udp	ms-sql-m
161-udp	snmp
1900-udp	upnp
25-tcp	smtp

Endpoint Profiling Using an Device Sensor

Included in IOS 15.0(1) software release is a newly added feature specifically designed with ISE in mind. The feature removes the previous requirements of configuring the switch for DHCP, CDP and LLDP collection. The new command gathers the endpoint data and transfers the data to ISE as RADIUS accounting packets.

13. Configure ISE with the Wireless-Sw as a NAD:
- 13.1. In ISE, navigate to **Administration > Network Resources > Network Devices**. Select the **L3-Switch** and click the **Duplicate** button.

Lab 12: Profiling Service in ISE

13.2. In the fields provided, enter the following:

Name: **Wireless-Sw**

IP Address: **10.10.2.33**

Model Name: **Cisco_3560**

Software Version: **15.0(1)M1**

13.3. Remove any other IP addresses associated with the switch.

13.4. Leave the rest of the settings at their defaults and click **Submit**.

14. Configure the IOS sensor in the **Wireless-Sw**:

14.1. Either open another session in SecureCRT to the **Wireless-Sw** or open a console connection from the hotspot diagram.

14.2. On the Admin-PC, use Windows Explorer and navigate to **ftp://1.1.1.10/SISE** and open the **Lab 12 - Wireless-Sw-Config** file.

14.3. Copy the entire contents of the file into the SecureCRT session to the Wireless-Sw in global configuration mode.

14.4. Next issue the following commands to enable the forwarding of information to ISE on the Wireless-Sw:

```
SISE-Wireless-SW#conf t
SISE-Wireless-SW(config)#device-sensor accounting
SISE-Wireless-SW(config)#device-sensor notify all-changes
SISE-Wireless-SW(config)#aaa accounting update periodic 1
SISE-Wireless-SW(config)#end
SISE-Wireless-SW# wr m
```

14.5. Verify that the switch is caching information related to CDP data. This may take a few minutes to populate the table:

```
SISE-Wireless-SW#show device-sensor cache all
Device: 001a.6ce3.9e1a on port FastEthernet0/1
-----
Proto Type:Name                               Len Value
cdp      2:address-type                        17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A
0A 02
                                01
cdp      6:platform-type                      23 00 06 00 17 63 69 73 63 6F 20 57 53 2D 43
33 35
                                36 30 2D 32 34 54 53
cdp      1:device-name                        27 00 01 00 1B 49 53 45 2D 41 54 50 2D 4C 33
2D 53
                                57 2E 67 6B 6C 2E 6C 6F 63 61 6C

Device: 0007.7df5.60e9 on port FastEthernet0/8
-----
Proto Type:Name                               Len Value
cdp      16:power-type                        6 00 10 00 06 3A 98
cdp      2:address-type                      17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A
0A 02
```

```

                                0A
cdp      6:platform-type      30 00 06 00 1E 63 69 73 63 6F 20 41 49 52 2D
4C 41

                                50 31 31 34 31 4E 2D 41 2D 4B 39 20 20 20
cdp      1:device-name        20 00 01 00 14 41 50 30 30 30 37 2E 37 64 66
35 2E

                                36 30 65 39

```

Device: d0c2.82e1.7da7 on port FastEthernet0/8

```

-----
Proto Type:Name              Len Value
cdp      6:platform-type      17 00 06 00 11 41 49 52 2D 43 54 32 35 30 34
2D 4B

                                39
cdp      2:address-type        17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A
0A 02

                                50
cdp      1:device-name         7 00 01 00 07 57 4C 43

```

Note Currently, the only device plugged into the wireless switch is the AP on port Fa0/8 with a static IP address which is why DHCP info isn't seen in the output. Also, since we are using a virtual WLC, the controller will appear off fa0/1 on the L3-Sw.

14.6. Determine the MAC address of the AP attached to the f0/8 port:

```

SISE-Wireless-SW# show mac address-table | incl 0/8
1      0007.7df5.60e9      DYNAMIC      Fa0/8
75     0007.7df5.60e9      DYNAMIC      Fa0/8

```

Note The MAC address of your AP might differ from the one shown above.

14.7. Now, go back to the endpoints section in ISE and refresh the endpoints list. You should see the **Cisco-Access-Point** endpoint in the list (this may take around 5 minutes, you can continue with the lab while this working in the background). The point is this; you could have used the traditional probe methods that we did earlier in the lab but you had no real control of what data was sent to ISE. With these newer commands you can control the data that is collected and forwarded to ISE for DHCP, CDP and LLDP.

Spoofing Endpoints

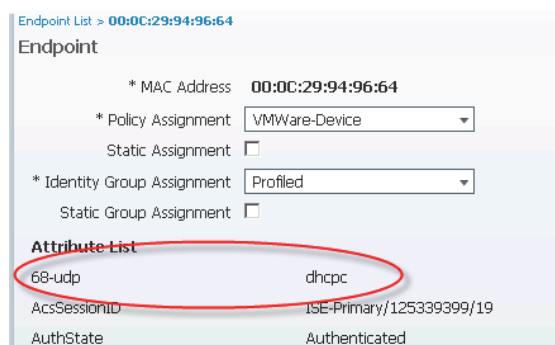
One of the biggest issues that we are trying to remedy is the issue of spoofing. If an attacker portrayed attributes that are similar to what the profiling function believes is a different device, the attacker may gain escalated privileges onto the network. In this section of the lab, we will adjust the profiler policies to weed out these attacks.

15. Now, let's see how the DHCP probe works. Go to the **IP Phone's** console. There should be a command prompt already open. Issue the **dhclient** command. You should see a dhcp request message on the console.

```
root@bt:~# dhclient
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/00:0c:29:94:96:64
Sending on   LPF/eth0/00:0c:29:94:96:64
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8
DHCPOFFER of 10.10.10.11 from 10.10.10.1
DHCPREQUEST of 10.10.10.11 on eth0 to 255.255.255.255 port 67
DHCPACK of 10.10.10.11 from 10.10.10.1
bound to 10.10.10.11 -- renewal in 423107342 seconds.
root@bt:~#
```

- 15.1. Now, go back to the Endpoint database in ISE and click the **00:0C:29:94:96:64** MAC address. You should now see the probe that was used to discover the endpoint is DHCP. After a while (you can refresh the page after a few minutes) you will see the results of the port scan as seen below:



Note In order for the NMAP action to function, some other probe needs to determine the endpoints' IP address which is what the DHCP probe accomplished.

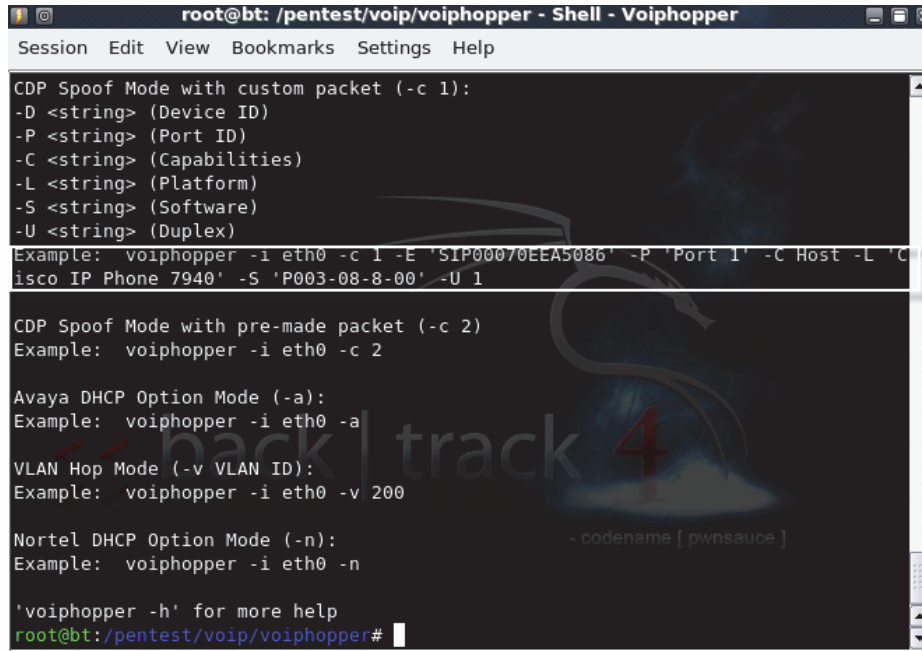
16. Thinking about things with ISE: it really all boils down to endpoint containment with authorization policies. If a host is granted access in an authorization policy, they are on the network or at least to the Internet in some fashion. Think about the policy we currently have for the IP Phone. If any host can meet the requirements of the policy that profiles the endpoint, it too will be thought of as an IP Phone and have some type of access to the network. Examine the existing Profiling policies:
 - 16.1. Navigate to **Policy > Profiling**.
 - 16.2. Click the **Show** drop down box and select **Quick Filter**.
 - 16.3. In the Endpoint Policy Name field, enter **Cisco-IP-Phone** and press **Enter**. Click the **first entry**, the parent policy, to bring up details.
 - 16.4. Scan through the Rules list: you'll see that there are 8 rules for identifying a Cisco IP Phone. An attacker would need to exhibit these same conditions (at least to meet the required certainty factor) in order to fool the system and be considered a Cisco IP Phone. Well, it turns out we'll attempt just that.
 - 16.5. Go to the console of the **IP-Phone**. There will already be a console window open. Run the **voiphopper** command which will be used to spoof an endpoint, making the system believe that it is really a 7940 phone. Issue the following commands on the IP-Phone:

```
cd /pentest/voip/voiphopper
```

```
./voiphopper
```

Lab 12: Profiling Service in ISE

- 16.6. The voiphopper command that was executed will reveal the available commands and syntax for the command. Locate the example within the text and copy the entire line and then paste it back into the console and press **enter**. The line we are copying is circled in the following image.



```
root@bt: /pentest/voip/voiphopper - Shell - Voiphopper
Session Edit View Bookmarks Settings Help

CDP Spoof Mode with custom packet (-c 1):
-D <string> (Device ID)
-P <string> (Port ID)
-C <string> (Capabilities)
-L <string> (Platform)
-S <string> (Software)
-U <string> (Duplex)
Example: voiphopper -i eth0 -c 1 -E 'SIP00070EEA5086' -P 'Port 1' -C Host -L 'Cisco IP Phone 7940' -S 'P003-08-8-00' -U 1

CDP Spoof Mode with pre-made packet (-c 2)
Example: voiphopper -i eth0 -c 2

Avaya DHCP Option Mode (-a):
Example: voiphopper -i eth0 -a

VLAN Hop Mode (-v VLAN ID):
Example: voiphopper -i eth0 -v 200

Nortel DHCP Option Mode (-n):
Example: voiphopper -i eth0 -n

'voiphopper -h' for more help
root@bt:/pentest/voip/voiphopper#
```

```
root@bt:/pentest/voip/voiphopper# ./voiphopper -i eth0 -c 1 -E 'SEP00070EEA5086' -P 'Port 1' -C Host -L 'Cisco IP Phone 7940' -S 'P003-08-8-00' -U 1
```

```
VoIP Hopper 1.00 Running in CDP Spoof mode
eth0 Current MAC: 00:07:0e:ea:50:86
ERROR: Can't change MAC: interface up or not permission: Device or resource busy
Sending 1st CDP Spoofed packet on eth0 with CDP packet data:
Device ID: SEP00070EEA5086; Port ID: Port 1; Software: P003-08-8-00
Platform: Cisco IP Phone 7940; Capabilities: Host; Duplex: 1
Made CDP packet of 121 bytes - Sent CDP packet of 121 bytes
Captured IEEE 802.3, CDP Packet of 461 bytes
Discovered VoIP VLAN: 60
Sending 2nd CDP Spoofed packet on eth0 with CDP packet data:
Device ID: SEP00070EEA5086; Port ID: Port 1; Software: P003-08-8-00
Platform: Cisco IP Phone 7940; Capabilities: Host; Duplex: 1
Made CDP packet of 121 bytes - Sent CDP packet of 121 bytes
Error trying to add VLAN 60 to Interface eth0: File exists
Added VLAN 60 to Interface eth0
Current MAC: 00:07:0e:ea:50:86\
```

Note	If the output seen in the lab guide did not appear on your console, execute the next two steps then repeat the command.
-------------	---

- 16.7. Go back to ISE and navigate to **Administration > Identity Management > Identities > Endpoints**. You should see the 7940 phone that was discovered (the discovery process may take up to 10 minutes based on the SNMP polling time). Unfortunately what that means to us now is that because our authorization policies are in place for IP Phones have certain access rights to the network, so will this attacker. **Keep checking the IP-Phones' console. The voiphopper command may have stopped so just up-arrow and re-execute the script.**

Endpoints

Selected 0 | Total 19

Edit	Add	Delete	Import	Show	All
Endpoint Profile	MAC Address	Static Assignment			
<input type="checkbox"/> Cisco-Access-Point	00:07:7D:F5:60:E9	false			
<input type="checkbox"/> Cisco-Device	D0:C2:82:E1:7D:A0	false			
<input type="checkbox"/> Cisco-Device	00:1A:6C:E3:9E:1A	false			
<input type="checkbox"/> Cisco-Device	C0:C1:C0:69:5A:D2	false			
<input type="checkbox"/> Cisco-Device	D0:C2:82:E1:7D:A7	false			
<input type="checkbox"/> Cisco-Device	00:19:2F:8F:2E:0F	false			
<input type="checkbox"/> Cisco-IP-Phone-7940	00:07:0E:EA:50:86	false			
<input type="checkbox"/> Cisco-Switch	00:1A:6C:E3:9E:42	false			

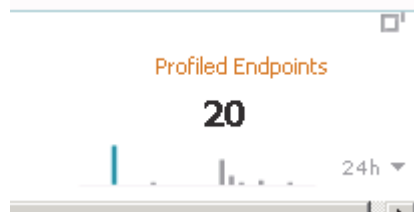
- 16.8. We won't go into it further but in order to thwart such an attack would require use-case scenarios where one could create NMAP scans once a device is profiled into the Cisco-IP-Phone Endpoint Profiles and then based on the ports that were discovered open, create a rule that matches those ports and immediately associates the endpoint with a different profile. That's what the exception policies would do for you in the endpoint profile configuration.

How would an attacker get around that? Block the NMAP scan. There's a lot of thought that goes into planning these strategies which ends up being cat/mouse type games.

Verifying the Profiled Endpoints

Examine the dashboard in ISE and the current endpoint count.

17. In ISE, click the **Home** tab.
18. Note the current Endpoint count on the top right of the screen.

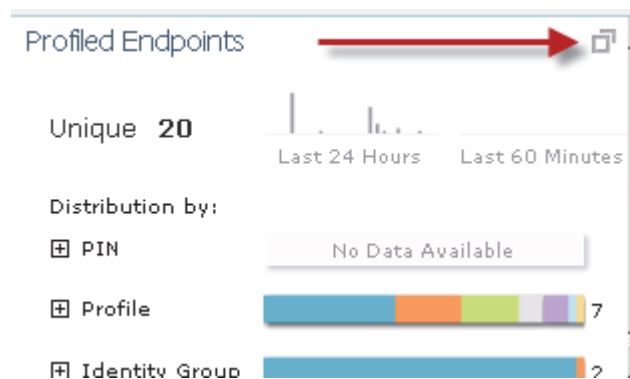


Note The endpoint count in your pod will differ depending upon the probes.

- 18.1. Note that you can mouse-over any of the spark lines in the graph to view statistics based on time.



19. In the center of the page is a Profiled Endpoints graph. Expand the graph by clicking on the overlaying boxes on the top right of the graph box.



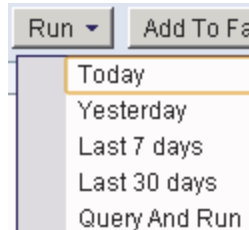
20. Expand the Profile section and examine the various endpoints types discovered.



21. Next review the endpoint reports by navigating to **Operations > Reports > Catalog > Endpoint**.

- 21.1. Click the **Endpoint Profiler Summary**.

Note If you select the report and then click the Run drop-down, you can define a wider time range than 24 hours or specify criteria using the Query and Run.



Lab 12: Profiling Service in ISE

Launch Interactive Viewer

Endpoint > Endpoint Profiler Summary

Showing Page 1 of 1 | First Prev Next Last | Goto Page:

Time Range : February 05,2013 ([Today](#) | [Yesterday](#) | [Last 7 Days](#) | [Last 30 Days](#))

Generated on February 6, 2013 2:13:13 AM UTC

Logged At	Details	Mac Address	Host	Policy	Source	Action Name
Feb 5, 2013 4:37 PM	Raw Log	00:1A:6C:E3:9E:43		Cisco-Switch		
Feb 5, 2013 4:38 PM	Raw Log	00:1A:6C:E3:9E:46		Cisco-Router		
Feb 5, 2013 4:38 PM	Raw Log	00:1A:6C:E3:9E:44		Cisco-Switch		
Feb 5, 2013 9:39 AM	Raw Log	00:08:30:D7:E3:A1		Cisco-Device		
Feb 5, 2013 11:57 PM	Raw Log	00:07:0E:EA:50:86		Cisco-IP-Phone-7940		

- 21.2. Click any of the Raw Log messages to review its content. Scroll through the list of details and also examine the summary at the bottom of the page.

Endpoint > Endpoint Profiler Summary > Endpoint Profiler Detail

Showing Page 1 of 1 | First Prev Next Last | Goto Page:

Total Certainty Factor=50
 operating-system=Cisco 2950
 2960
 3550
 3560
 or 3750 switch (IOS 12.1 - 12.2)
 MatchedPolicyID=194cdf70-ad9b-11e1-ace9-000c29545f40
 NmapScanCount=1
 NmapSubnetScanID=0
 PortalUser=

Profiler Summary		Day
Logged At :	Feb 5, 2013 4:37 PM	Feb 5, 2013 4:37 PM
Server :	ISE-Primary	Feb 5, 2013 5:38 AM
Event :	Profiler EndPoint profiling event occurred	
Endpoint MAC Address :	00:1A:6C:E3:9E:43	
Endpoint Policy :	Cisco-Switch	
Certainty Metric :	50	
Endpoint Matched Policy :	Cisco-Switch	
Identity Group :	Profiled	

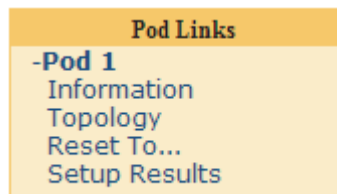
22. Now that you've examined some endpoint details, let's see how these endpoints are affecting the current license count.
- 22.1. Navigate to **Administration > System > Licensing**. Note that your current license count of active devices is extremely low, much lower than the number of endpoint profiled. This is a great example of how the profiling service only consumes licenses for endpoints that are referenced in authorization policies. In other words, it's not the act of profiling that requires the license, it's the use of the profiled endpoint in an authz policy that consumes it.

Base (Active / Allowed)	Advanced (Active / Allowed)
3/20	3/20

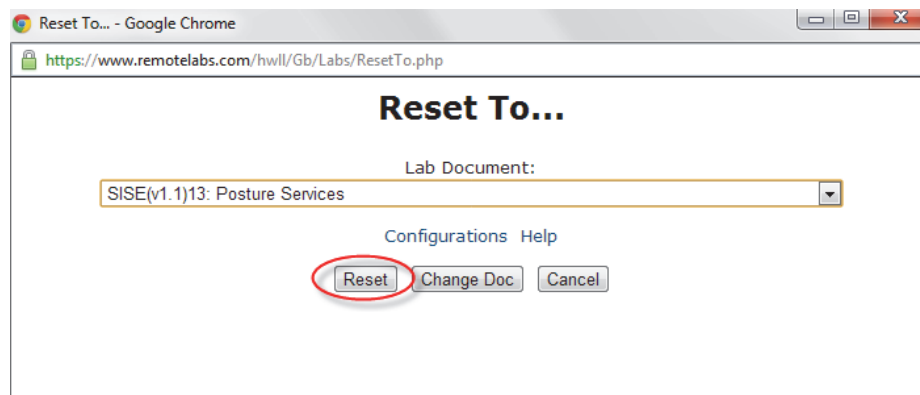
Preparing for the Next Lab

The following lab requires a mandatory reset. Follow the instructions below to reset your pod to Lab 13.

23. Close the RDP session.
24. Navigate your browser to **<https://www.remotelabs.com>** and log in.
25. Locate the Pod Links section on the left side of the screen.



26. Click **Reset To...**
27. In the Lab Document drop-down, select **Lab 13** and then click reset. Wait approximately 15 minutes before accessing the ISE web GUI for the next lab.



Lab Complete

Please let your instructor know that your Pod has completed the lab.