|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Profiling |
| An Aston training document explaining how to configure Profiling Services for Cisco ISE |

Contents

[Contents 2](#_Toc465505)

[Introduction 3](#_Toc465506)

[Lab Diagram 4](#_Toc465507)

[Configure Windows host 5](#_Toc465508)

[Configure ISE Probes 5](#_Toc465509)

[ISE Probes 6](#_Toc465510)

[Configure Access Switch 8](#_Toc465511)

[Base Switch Config 8](#_Toc465512)

[Profiling Devices 15](#_Toc465513)

[Profiling Polices 19](#_Toc465514)

[Logical Profiles 27](#_Toc465515)

[Conclusion 30](#_Toc465516)

Introduction

Cisco ISE Profiling Service provides a dynamic classification of endpoints connected to the network. It does this by using MAC addresses OUI (Organizationally Unique Identifier) as an identifier as well as ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process then matches the collected attributes to either a prebuilt or user-defined condition. These profiles include a range of device types, including mobile clients (iPads, Android tablets, and so on), desktop operating systems (Windows, Mac OS X, Linux, and others), and nonuser systems such as printers, phones and cameras.

Once endpoints are classified, they can be authorized to the network and given access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method.

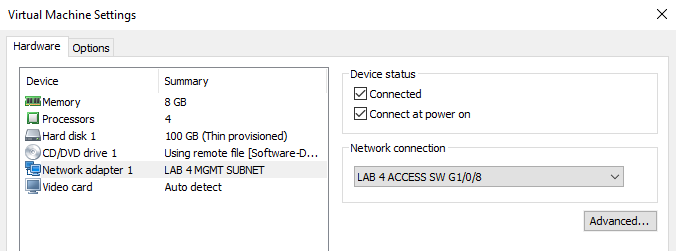
Now that you have a little information on what profiling is let’s start to configure the ISE Profiling service and the NADs to send the endpoint attributes to lay the ground work for the upcoming labs.

## Lab Diagram



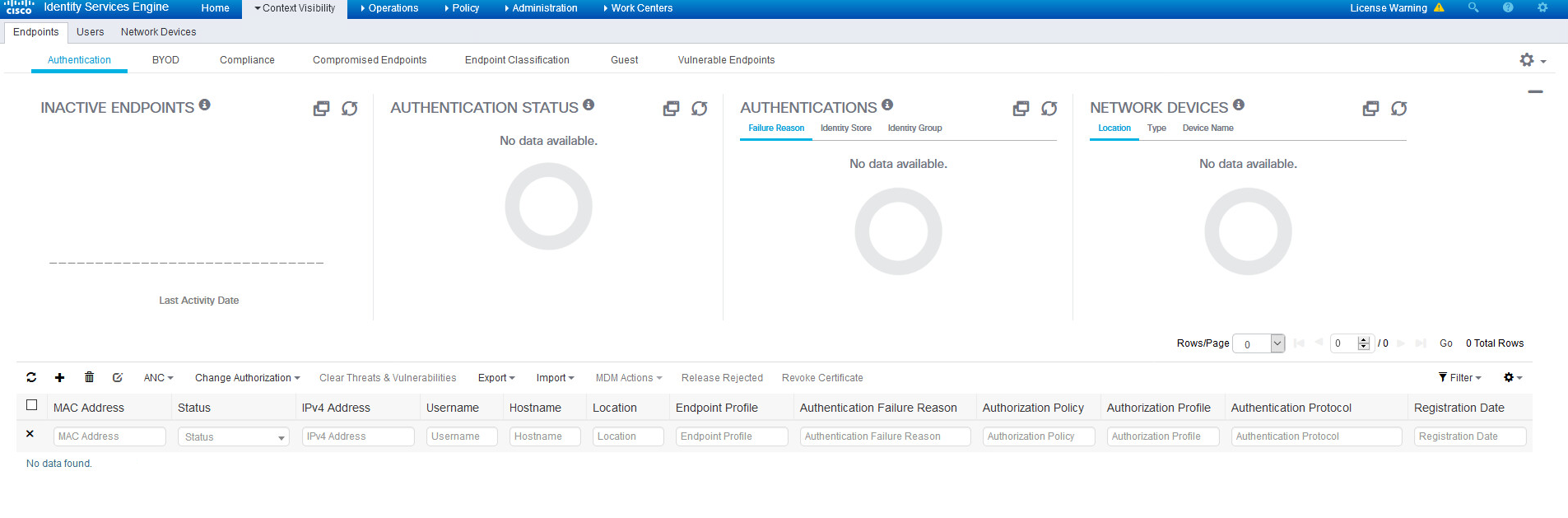
Configure Windows host

Before we get started make sure you have moved **LAB (x) PC-1** from **LAB (x) MGMT SUBNET** network to **LAB (x) Access-SW G1/0/8**.



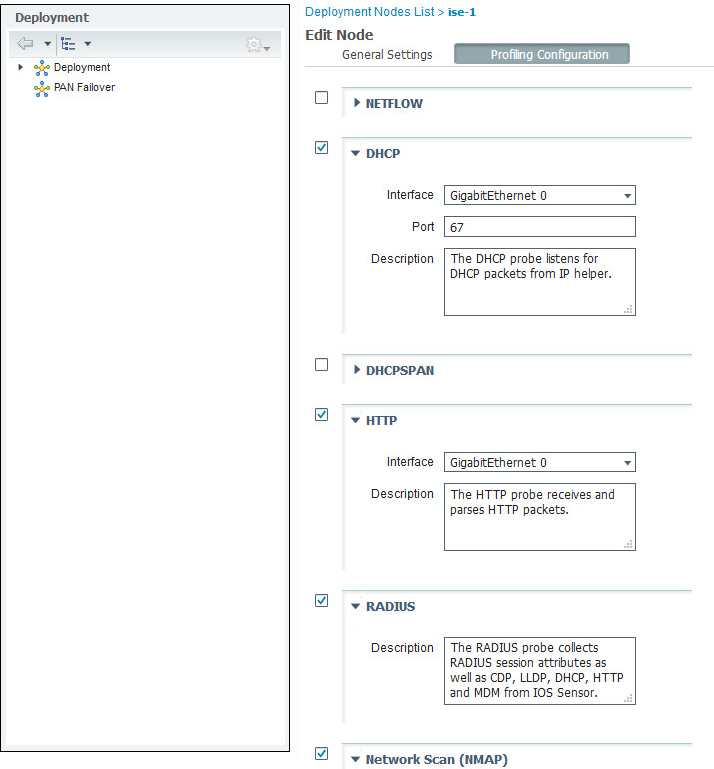
Configure ISE Probes

First off, I wanted to point out a page in ISE that we will reference throughout this lab. Navigate to **Context Visibility > Endpoints**. Here is where you’ll find all the information about Endpoints connected to the network. As you can see I currently don’t have any endpoints showing up yet.



ISE Probes

There are two main components in ISE for the profiling service - Probes and Profiling Policy. We’ll start with configuring the Probes. Probes are configured on a per PSN basis which means if you have a use case for it you can have PSNs with different profiling probes configured across the deployment. Navigate to **Administration > System > Deployment**, if you get a popup message click **OK** then click on the node itself then the **Profiling Configuration** tab.



 As you can see you can configure one or any of the following probes:

* Netflow Probe
* DHCP Probe
* DHCP SPAN Probe
* HTTP Probe
* RADIUS Probe
* DNS Probe
* SNMP Query Probe
* SNMP Trap Probe
* Active Directory Probe (New in ISE 2.1)

For our lab, we will configure the following probes tick the checkbox for each probe below and click **Save**.

* **DHCP** - This looks at the DHCP packets by forwarding DHCP requests to ISE with the IP Helper command
* **HTTP** - Checks the identity information that the browser sends that typically identifies the browser, application type, operating system, software vendor, and software revision.
* **RADIUS** - This collects attributes such as NAS-IP-Address, NAS-Port, Calling-Station-ID, Acct-Session-ID, Framed-IP-Address, Acct-Session-Time, and Acct-Terminate-Cause. I would say this is one of the more important probes to make sure is enabled
* **DNS** - This probe allows the profiler to lookup an endpoint and get the FQDN of that endpoint
* **SNMP Query** - This allows querying to your Network Access Devices (NADs) for configurations such as link up and new MAC notifications, and CDP
* **SNMP Trap** - This allows the PSN to receive information from specific NADs that support MAC notification, linkup, and linkdown. For SNMP Trap to be fully functional, you must enable SNMP Query as well. This is important for receiving information when ports go up and down and endpoints are connected and disconnected in your network
* **Active Directory Probe** (ISE 2.1 and later) - Since Active Directory details OS information for AD-joined computers including version and service pack levels. The AD probe retrieves this information directly using the AD Runtime connector to provide a highly reliable source of client OS information. It can also help you distinguish between corporate and non-corporate assets

Configure Access Switch

Base Switch Config

Now that we have the probes that we will be using enabled in ISE and we already added our Access switch to our network devices in ISE. We are ready to configure the switch with our AAA configuration. **SSH** to the **Access-SW** (172.16.101.2) and login with **admin/cisco**.

I’m going to walk through the commands first with a brief explanation of what they do. Make sure you take some time and get familiar with what these commands are doing. I’ll follow that with the full configuration that you can copy from.

The first one you should already know. We are adding ip helper-address pointing at our ISE PSN to the default gateway for our subnets to forward DHCP requests for the DHCP probe.

interface Vlan11

ip helper-address 172.16.100.50

!

interface Vlan20

ip helper-address 172.16.100.50

!

interface Vlan35

ip helper-address 172.16.100.50

!

interface Vlan40

ip helper-address 172.16.100.50

!

interface Vlan55

ip helper-address 172.16.100.50

Next, we are going to configure our AAA commands. We’ll configure ISE as the RADIUS server on the switch for network access. Configure the switch to send certain RADIUS attributes to ISE. Then our SNMP settings so that ISE can collect information on our endpoints.

**aaa new-model** – This enables aaa new-model

!Configures ISE as the RADIUS server

**radius server ISE**

**address ipv4 172.16.100.50 auth-port 1812 acct-port 1813** – configures the Switch to send on RADIUS ports 1812 and 1813. Most older switches use the legacy ports 1645 and 1645 by default

**key cisco123** - This is the shared key that we configured on ISE when we added this NAD

**radius-server dead-criteria tries 3** - determines when a RADIUS server is considered unavailable. The switch tries 3 times

**radius-server deadtime 30** - Sets the number of minutes during which a RADIUS server is not sent requests if mark dead.

**aaa group server radius ISE-GROUP**

**server name ISE** - We configure this a few lines back. If you we had multiple ISE nodes, we'd add them all to this RADIUS group

**aaa authentication login console local** – Let’s keep console login local

**aaa authentication login vty local** - Keep VTY login local

**aaa authentication enable default enable**

**aaa authorization exec default local** - Keeping EXEC mode local

**aaa authentication dot1x default group ISE-GROUP** - Specifying to use our RADIUS group for dot1x authentication

**aaa authorization exec vty local** - Keeping EXEC VTY authorization local

**aaa authorization network default group ISE-GROUP** - Specifying our RADIUS group for network authorization

**aaa authorization auth-proxy default group ISE-GROUP** - Required for VLAN/ACL CoA

**aaa accounting dot1x default start-stop group ISE-GROUP** - Specifying our RADIUS group for dot1x accounting

**aaa accounting auth-proxy default start-stop group ISE-GROUP** - Enables accounting for dynamic ACLs and VLANs that get downloaded

**aaa session-id common**

**aaa accounting update periodic 5** - Updates the accounting information every 5 minutes

**aaa server radius dynamic-author** - This enables ISE to act as an AAA server when interacting with the client

**client 172.16.100.50 server-key cisco123**

**server-key cisco123** - You may not need to do this with your version of IOS

**radius-server vsa send accounting** - Tells the switch to send accounting vendor-specific attributes

**radius-server vsa send authentication** - Tells the switch to send authentication vendor-specific attributes

**radius-server attribute 6 on-for-login-auth** - Used to identify the Service-Type this RADIUS request is used for

**radius-server attribute 6 support-multiple** - Supports multiple Service-Type values for each RADIUS profile

**radius-server attribute 8 include-in-access-req** - This is to send the IP address of a user to the RADIUS server in the access request.

**radius-server attribute 25 access-request include** - This is to include the class attribute in the access request which specifies the authorization action

**radius-server attribute 31 mac format ietf upper-case** - This is to specify the MAC address format in the Calling Station ID

**radius-server attribute 31 send nas-port-detail** - This includes all NAS port details in the Calling Station ID

**ip radius source-interface lo0 –** Sets loopback 0 as the source for all radius communication

**dot1x system-auth-control** - Globally enables 802.1x port-based authentication

!This is the SNMP configuration

**access-list 10 permit 172.16.100.0 0.0.0.255**

**access-list 10 deny any log**

**mac address-table notification change**

**mac address-table notification mac-move**

**mac address-table notification change interval 0**

**authentication mac-move permit** - Enables MAC move on a switch between any authentication-enabled ports (MAB, 802.1X or Web-Auth)

**snmp-server enable traps mac-notification change move threshold**

**snmp-server enable traps mac-notification change**

**snmp-server enable traps snmp linkdown linkup**

**snmp-server host 172.16.100.50 version 2c iselab-ro mac-notification**

**snmp-server community iselab-ro ro 10**

**snmp-server trap-source lo0**

**snmp-server source-interface inform lo0**

**lldp run**

**logging origin-id ip** - This specifies that the IP address of the sending interface will be used as the message origin identifier

**logging source lo0**

**logging host 172.16.100.50 transport udp port 20514**

**logging monitor informational**

**no ip dhcp snooping information option** - Disables the switch from adding Option 82 into the packet before forwarding it to ISE. If this option is enabled, it will send the giaddr field with a zero value to ISE.

**ip dhcp snooping**

**ip dhcp snooping vlan 11,20,35,40,55**

**epm logging** – Enables standard logging functions on a switch to support possible troubleshooting/recording for ISE functions

**ip device tracking** - This allows the switch to maintain an IP device tracking table. You must enable this feature to use web-based authentication

**ip device tracking probe auto-source override** - This configures the switch to send an non-RFC compliant ARP Probe. The IP source will not be 0.0.0.0 but it will be the SVI in the VLAN where the host resides. If it's a Windows machine, it'll no longer see the probe as defined by RFC 5227 and therefore will not flag a potential duplicate IP

**device-sensor accounting** - This command enables the addition of sensor protocol data to accounting records

**device-sensor notify all-changes** - Enables client notifications and accounting events for all TLV changes where either a new TLV is received or a previously received TLV is received with a new value in the context of a given sessions.

Here is the whole config:

!

logging monitor informational

!

aaa new-model

!

!

aaa group server radius ISE-GROUP

server name ISE

!

aaa authentication login VTY local

aaa authentication login CONSOLE local

aaa authentication enable default enable

aaa authentication dot1x default group ISE-GROUP

aaa authorization exec default local

aaa authorization exec VTY local

aaa authorization network default group ISE-GROUP

aaa authorization auth-proxy default group ISE-GROUP

aaa accounting update periodic 5

aaa accounting auth-proxy default start-stop group ISE-GROUP

aaa accounting dot1x default start-stop group ISE-GROUP

!

!

!

!

!

aaa server radius dynamic-author

client 172.16.100.50 server-key cisco123

server-key cisco123

!

aaa session-id common

device-sensor accounting

device-sensor notify all-changes

!

!

!

ip dhcp snooping vlan 11,20,35,40,55,90

no ip dhcp snooping information option

ip dhcp snooping

!

!

device-tracking tracking auto-source override

authentication mac-move permit

epm logging

!

dot1x system-auth-control

!

lldp run

!

!

interface Vlan11

ip helper-address 172.16.100.50

!

interface Vlan20

ip helper-address 172.16.100.50

!

interface Vlan35

ip helper-address 172.16.100.50

!

interface Vlan40

ip helper-address 172.16.100.50

!

interface Vlan55

ip helper-address 172.16.100.50

!

interface Vlan90

ip helper-address 172.16.100.50

!

!

!

ip radius source-interface Loopback0

logging origin-id ip

logging source-interface Loopback0

logging host 172.16.100.50 transport udp port 20514

logging monitor informational

access-list 10 permit 172.16.100.0 0.0.0.255

access-list 10 deny any log

!

snmp-server community iselab-ro RO 10

snmp-server trap-source Loopback0

snmp-server source-interface informs Loopback0

snmp-server enable traps snmp linkdown linkup

snmp-server enable traps mac-notification change move threshold

snmp-server host 172.16.100.50 version 2c iselab-ro mac-notification

!

radius-server vsa send accounting

radius-server vsa send authentication

radius-server attribute 6 on-for-login-auth

radius-server attribute 6 support-multiple

radius-server attribute 8 include-in-access-req

radius-server attribute 25 access-request include

radius-server attribute 31 mac format ietf upper-case

radius-server attribute 31 send nas-port-detail

radius-server dead-criteria tries 3

radius-server deadtime 30

!

radius server ISE

address ipv4 172.16.100.50 auth-port 1812 acct-port 1813

key cisco123

!

!

!

!

line con 0

login authentication CONSOLE

line aux 0

line vty 0 4

login authentication VTY

line vty 5 15

login authentication VTY

!

mac address-table notification change interval 0

mac address-table notification change

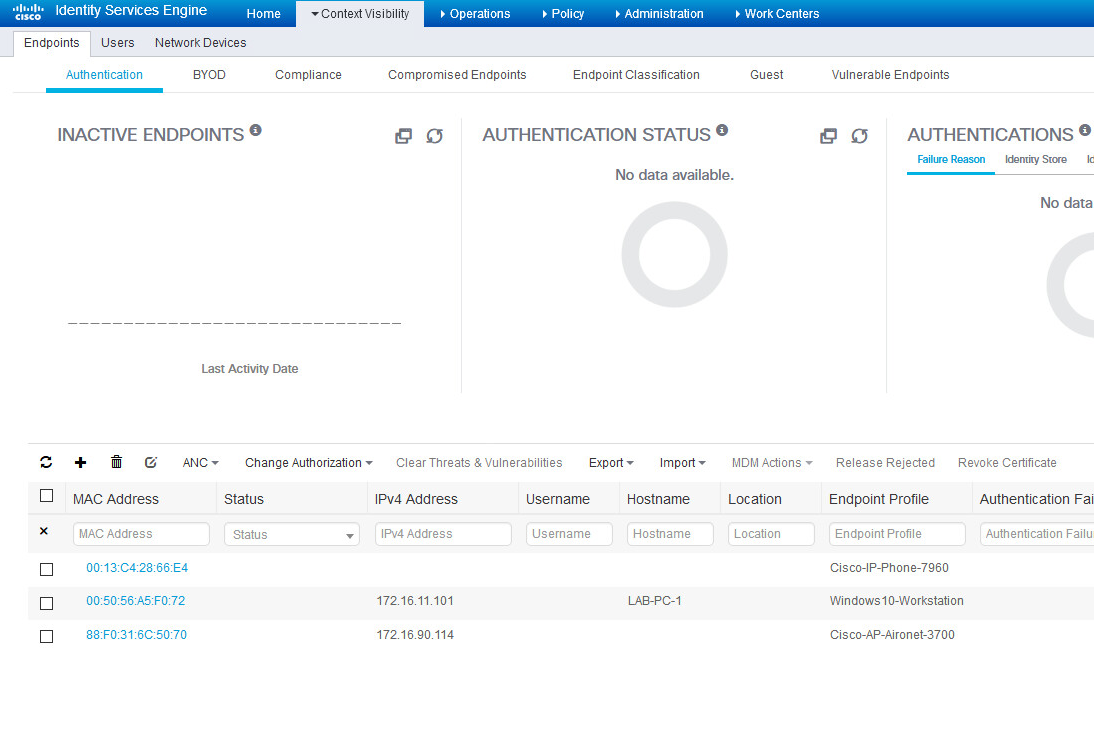
mac address-table notification mac-move

!

end

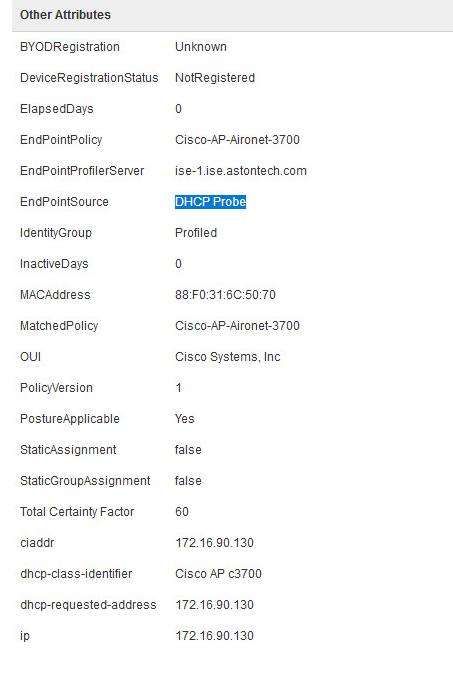
Profiling Devices

Now if we go back to ISE we should see at least the 3 devices that we have connected to the switch have been profiled. Navigate to **Context Visibility > Endpoints**. You should see a screen similar:

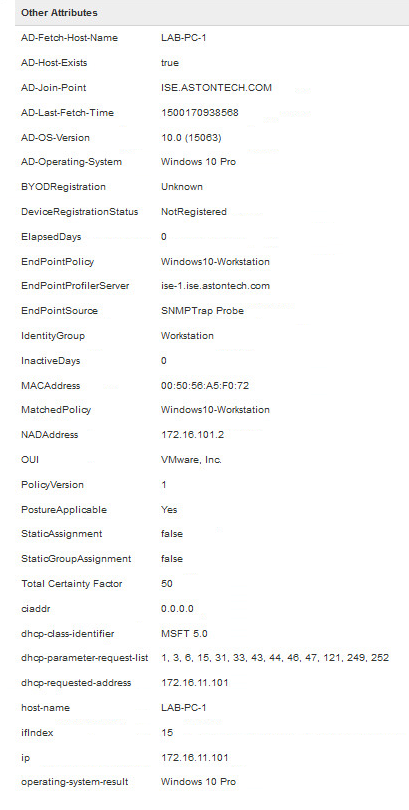


If your Windows 10 VM is showing up as a VMware device. That more than likely means the Active Directory probe hasn’t kicked off yet. ISE needs to see the host name attribute for the AD probe to work. **Shutdown** the port the Windows VM is connected to (G1/0/8). Then clear the DHCP bindings on the switch – **clear ip dhcp binding \*, reboot the PC,** then **no shut** the port. Give it a minute or so and refresh the endpoint page. It should now be showing up as a Windows 10 workstation.

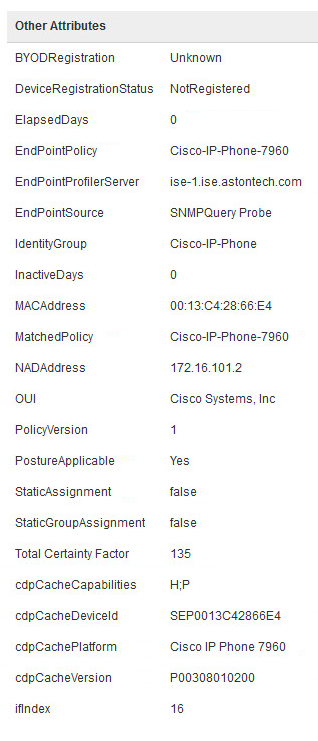
Let’s look at how these devices were profiled. Click on the the Cisco-AP-Aironet-3700 **MAC Address**, then on **Attributes**. Scroll down to the bottom of the page.



You can see here that we learned what this device was from the DHCP probe and that it also matched a policy. Which we’ll talk about a little later. Let’s go back and look at the Windows 10 host.

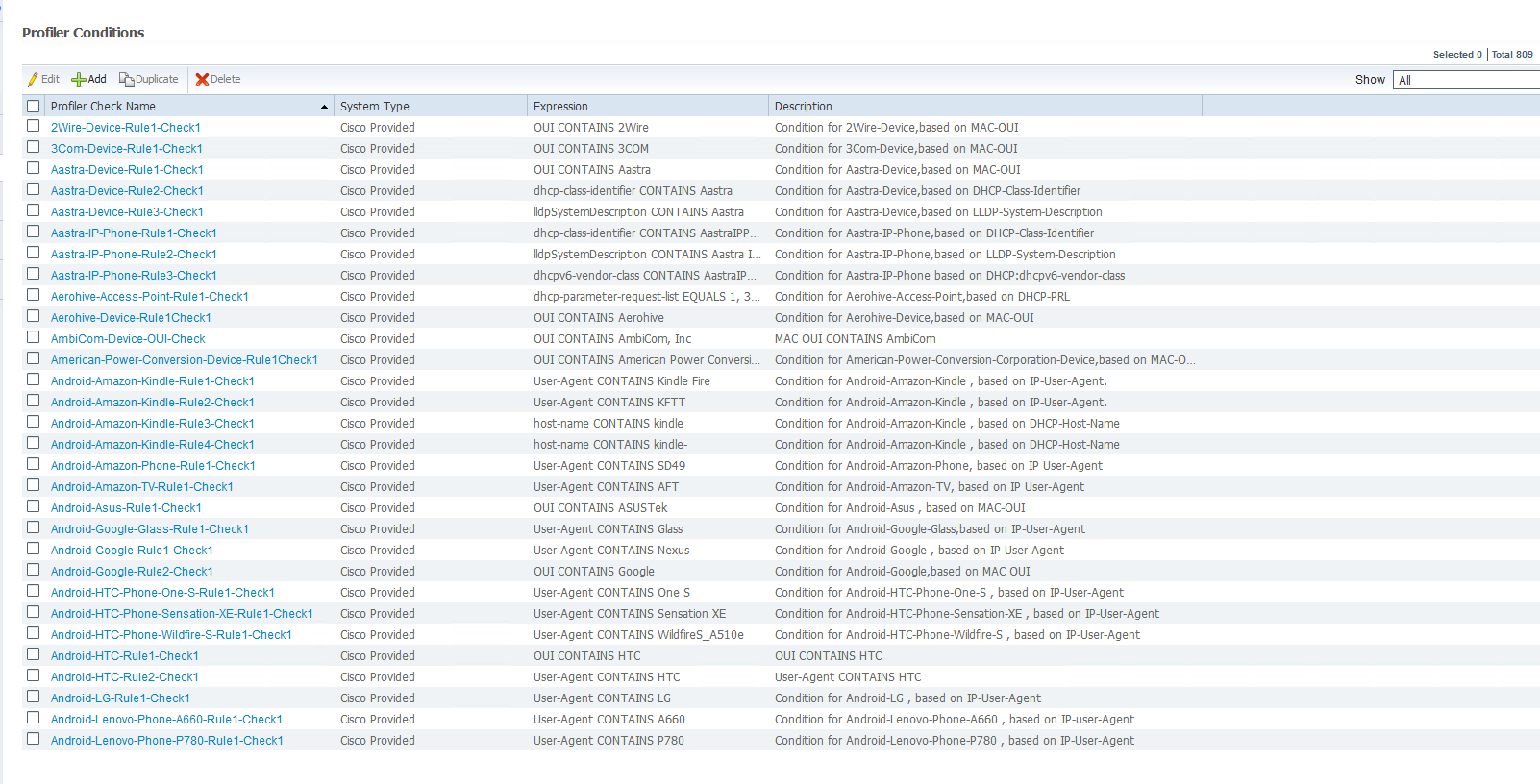


You can see that we have bit more information on this host than we did for the AP. ISE collected information from three different probes. We have AD, DHCP and the probe that provided the most information and was used to profile the device was the SNMP Trap probe. If we look at the phone you’ll see that ISE used SNMP query probe which returned CDP information from the switch to learn that it’s a 7960 IP phone.

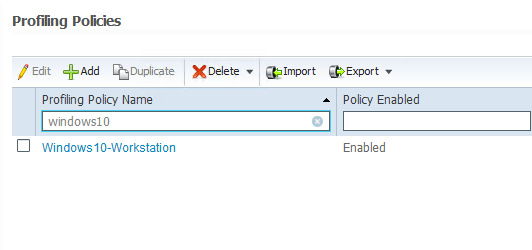


Profiling Polices

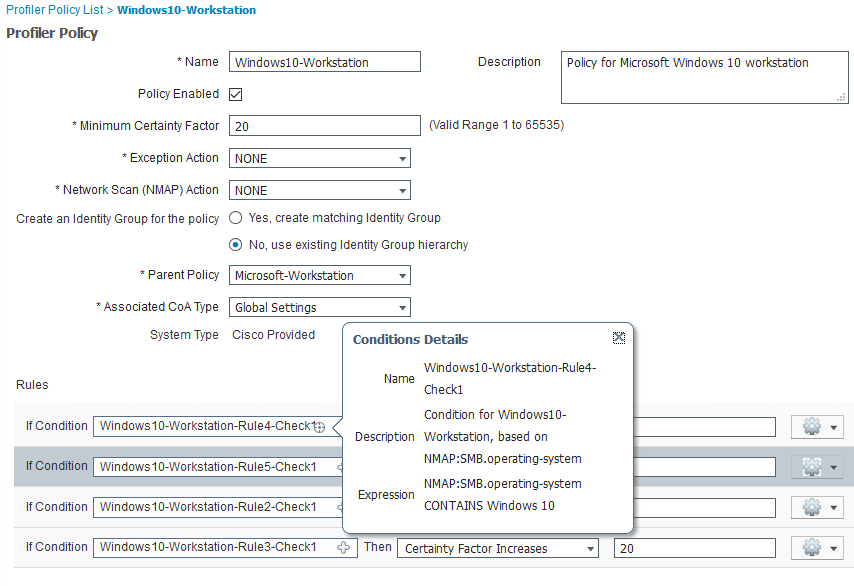
I’ve mentioned Profiling polices previously in this lab now let’s talk about what they are. At a high level, Profiling polices are what ISE uses to determine what type of endpoint a device is. Used in combination with the probes which we have configured and seen in action. ISE receives or retrieves attributes on a per endpoint basis which it correlates to a library of conditions which are then reference in a policy. Navigate to **Policy > Conditions > Profiling**. There are currently over 800 predefined conditions that come with ISE which Cisco adds/updates periodically through the profiler feed service that we enabled in the previous lab. You can also create your own custom Conditions as well if needed.



Now let’s look at the policies that tie those conditions together. Navigate to **Policy > Profiling > Profiling Polices**. As you can see currently we have over 500 predefined polices already in ISE. Again, this is something that will get updated periodically as Cisco publishes new devices. Let’s look at what the conditions are that used to profile our Windows 10 VM. Click the filter button on the right side and in the Profiling policy name type windows10.



Click **Windows10-Workstation** and let’s look at what the checks are. If you hover over the crosshairs at the end of the rule check the details will popup.

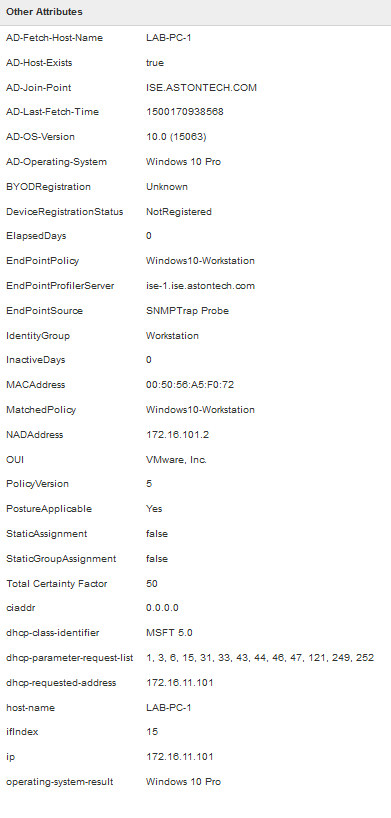


Here we can see there are 4 rule checks for this policy. If one is matched it increase the Certainty Factor by 20 which is currently set for a Minimum Certainty Factor 20. That’s enough for ISE to declare this device is a Windows 10 machine if one is matched. Certainty Factor is just what it sounds like, the likelihood of the endpoint being whatever the policy is. In this case Windows 10. It’s possible for an endpoint to match conditions from different policies. However, the policy it matches with the highest Certainty Factor will be the policy that gets assigned.

These profiling polices are editable if you wanted to modify the Minimum Certainty Factor or how much the Certainty Factor increase if a condition is met for example, you can. As well as take an exception action or do an NMAP scan of the endpoint to gather more information. For now, we’ll just leave the defaults.

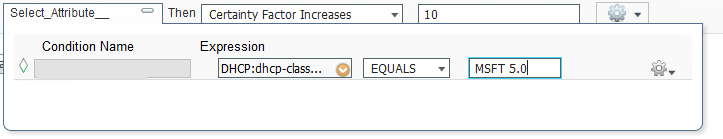
So, with that said what if we have a device that isn’t getting profiled correctly? Unfortunately, in our lab we don’t really have a good example since everything is but let’s say the Windows 10 machine wasn’t being profiled the way we wanted. At Aston, our Windows machines go up to 11.

First thing we’ll need to do is check the attributes that ISE is learning for our Windows 10 host so we can create a new policy based on that information. Navigate back to **Context Visibility > Endpoints.** Click on our **Windows 10** host then **Attributes.**

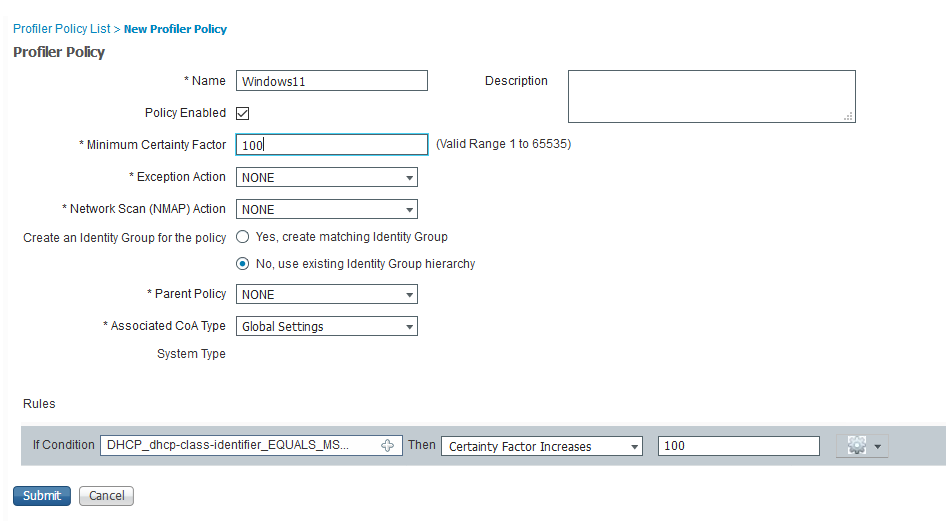


Here we can see what our current options are and we can also ascertain that the new policy will need to have a higher certainty factor than 50. In this case let’s use the dhcp-class-identifier attribute. Navigate to **Policy > Profiling > Profiling Polices** and click **Add.** Give it these settings:

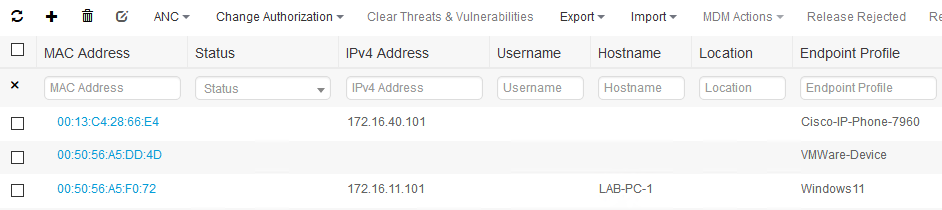
* Name – Windows11
* Minimum Certainty Factor – 100
* Click No for the Create an Identity Group
* Click on the Plus sign for the Conditions
  + Create New Condition
  + Select Attribute – DHCP then dhcp-class-identifier
  + In the dropdown select EQUALs
  + In the last box type – MSFT 5.0



* Certainty Factor Increases – 100
* Submit

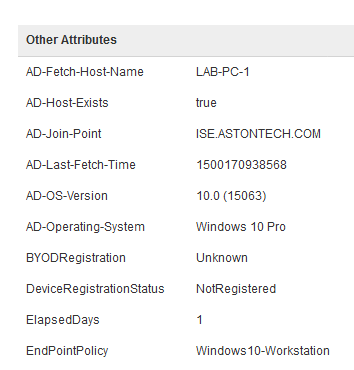


If we go back to **Context Visibility > Endpoints** almost immediately we should now see that our Windows 10 host is now showing up as Windows11. Any changes to the Profiling Policies will force ISE to re-evaluate all its endpoints.

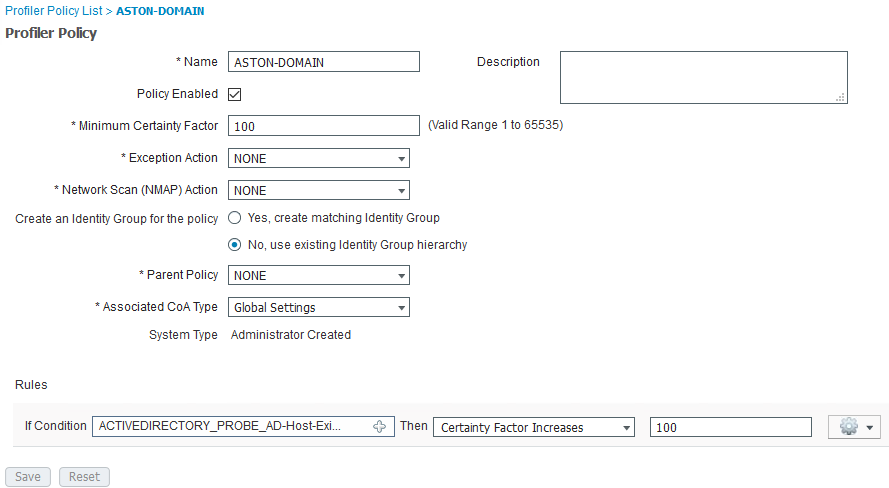


|  |  |
| --- | --- |
| Now that we’ve seen an example of how we can influence the endpoint profile let’s go ahead and delete the Windows11 policy that we just created. |  |

What if we simply wanted all the devices that are joined to the domain to be profiled to a single policy? What could we use to do that? If we look at the attributes that ISE has complied on the Windows 10 host we have attributes from the AD probe.



As we can see here we have an AD-Host-Exists attribute. If we create a policy with the condition **AD-Host-Exists** attribute **equals** **true** that should be exactly what we are looking for. Create a new Profiling Policy as shown below and **Submit**:



Now if we go back and look at our endpoints we see the Windows host showing up with the Profile (ASTON-DOMAIN) that we want.

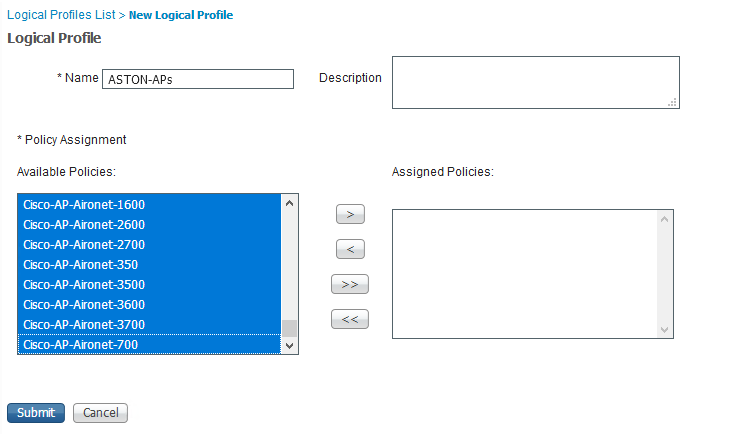


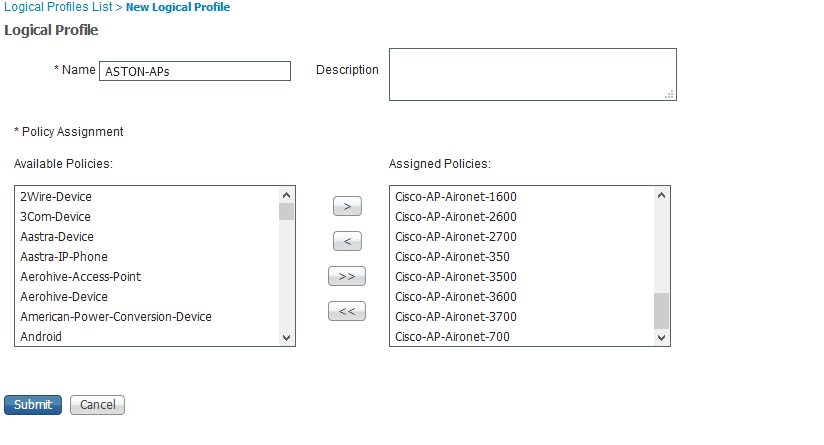
Logical Profiles

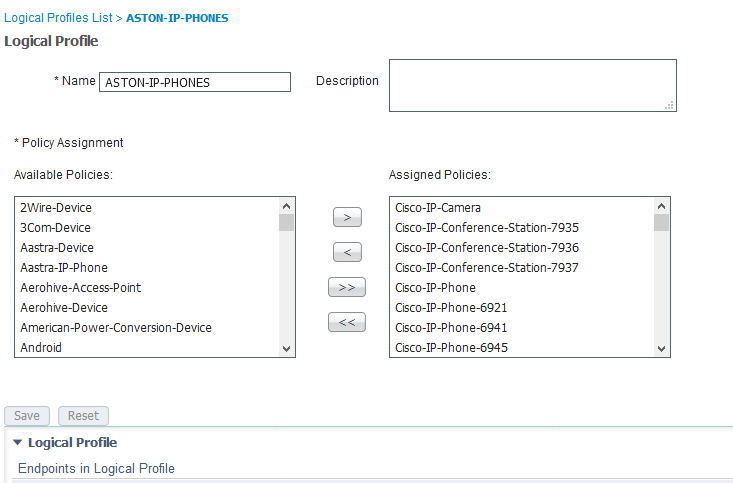
ISE is now profiling our devices that we have in our lab the way we want it to. Say we want to use this profiling information in our Authorization policies to grant/restrict access to our devices (AP, Phone and devices in AD). We can do that with something called a Logical Profile. Logical Profiles are just “Logical” Profiles that contain “actual” Profiling policies that can be reference in our Authorization policies. If that makes sense. You’ll find with ISE it seems that all you are doing is creating policy to be referenced in another policy that gets referenced in another policy and so on but digress.

Navigate to **Policy > Profiling > Logical Profiles** and let’s create profiles for the devices that we’ll use in upcoming labs. Click **Add**.

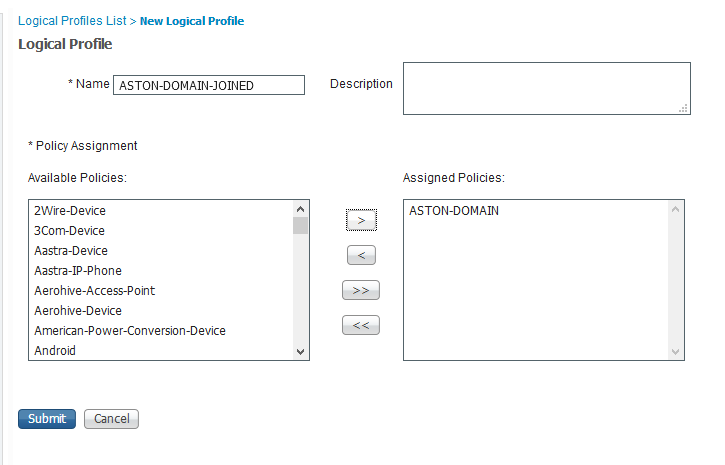
Let’s create a logical profile for our APs. Give a name like **Aston-APs** we could just add the model we have in the lab (Aironet3700) but what if we were to add a new model of AP? We would have to go back into ISE and add it here before it could access the network. That may be desirable in the environment you’re working in but for this lab let’s just add them all. Highlight all the Cisco Aironet APs in the Available Polices.



Click the **>** button to move them over to **Assigned Policies** and click **Submit**. Even though there is a default IP-Phone Profile, do the same for our Cisco IP phone and name it **ASTON-IP-PHONES**.



Create the last one for our domain joined hosts as shown below:



Conclusion

In this lab, we have:

* Enabled the Probes in ISE
* Configured our Access Switch with the radius server (ISE) along with radius attributes to send to ISE and finally SNMP
* Looked at how our lab devices got profiled and made some modifications to influence their profile
* Created Logical Profiles to group our lab devices to reference in our authorization polices

I also wanted to point out that we could correctly profile our lab devices without configuring any dot1x on any of the switchports on the switch. It’s common misconception that dot1x needs to be configured for profiling services to work as you can tell that’s not the case.

In the next lab we are going to build on the groundwork we have laid here and use profiling to grant/restrict network access to our lab devices via wired MAB.