|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Mac Authentication Bypass (MAB) |
| An Aston training document explaining how to configure MAC Authentication Bypass |

Contents

[Contents 2](#_Toc492462819)

[Introduction 3](#_Toc492462820)

[Lab Diagram 4](#_Toc492462821)

[Policy Creation 5](#_Toc492462822)

[Work Centers 5](#_Toc492462823)

[Allowed Protocols 5](#_Toc492462824)

[Downloadable ACLs 7](#_Toc492462825)

[Authorization Profiles 8](#_Toc492462826)

[Configure Policy Set 12](#_Toc492462827)

[Configure Switchports 15](#_Toc492462828)

[Verify Policies 16](#_Toc492462829)

[Whitelisting 19](#_Toc492462830)

[Policy Creation 19](#_Toc492462831)

[Conclusion 25](#_Toc492462832)

Introduction

In the previous lab, we looked at profiling and built some profiling policies that we are going to take advantage of. In this lab, we are going to build some policies to allow devices on the network using MAC Authentication Bypass which we will refer to as MAB going forward.

With the publication of dot1x back in the year 2000 they needed a way to authenticate endpoints in a dot1x configured network that couldn’t speak EAPoL, like printers, cameras, phones and other various network attached devices. Although a lot of newer devices like phones and printers do support it now. They decided to incorporate MAB which **bypasses** the dot1x authentication by using the devices MAC address as the username and password for credentials.

MAB which often gets lumped in with dot1x authentication but dot1x is a standard, MAB is not. Like I mentioned before MAB uses MAC addresses for username and password that gets forwarded from the NAD. The endpoint is completely unaware that any authentication is happening at all. Because of this MAB provides little security compared to dot1x, a MAC address is easily spoofed.

There are ways to provide a little more security by building policies with the use of profiling to prove the device is what it should be or restricting access for devices that authenticate with MAB to services that they really need. Point being, best security practice would be to use dot1x when able.

Lab Diagram

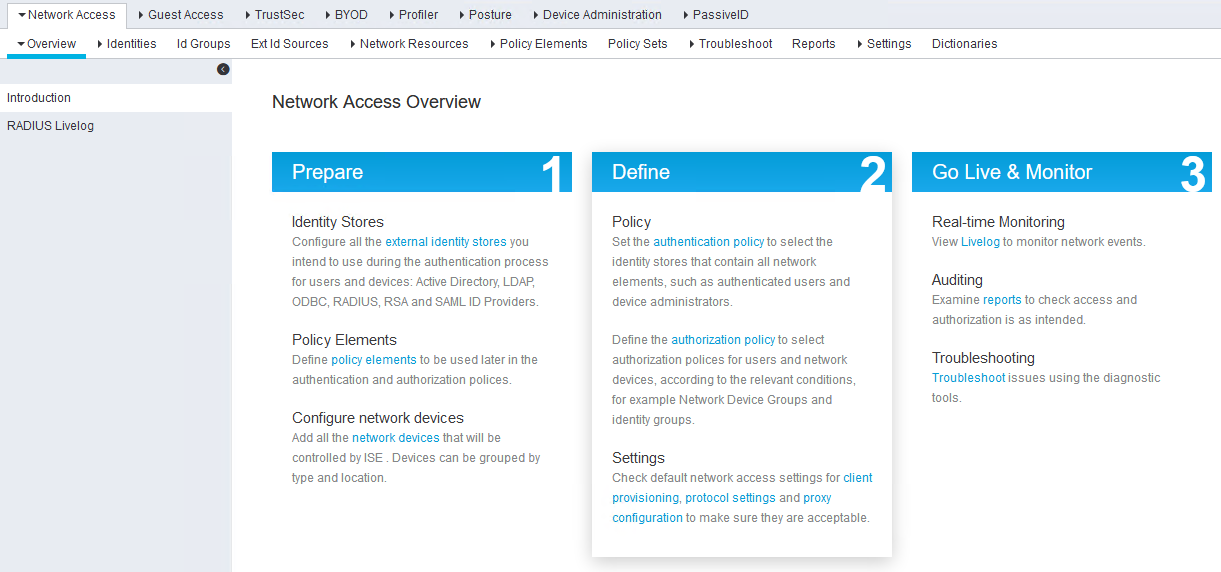


Policy Creation

Work Centers

Starting in ISE 2.0 there is a new feature in the web UI called Work Centers. Cisco came up with the idea to make it easier to configure features by using a single pane that takes you through the work flow step by step. Previously you had to jump around the GUI like we have been doing. I’ve never used this feature before but I think it’s going to makes things a little easier let’s see how it goes.

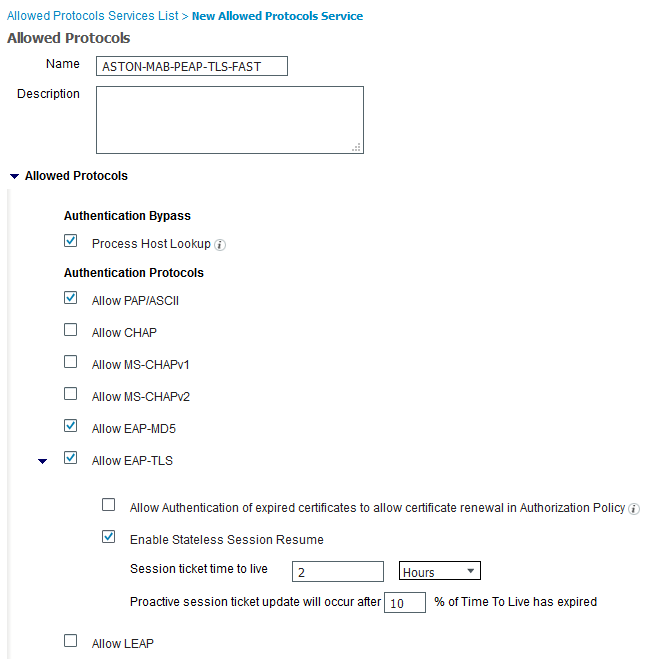
Open your browser and navigate to ISE and log in. Go to **Work Center > Network Access > Overview**.

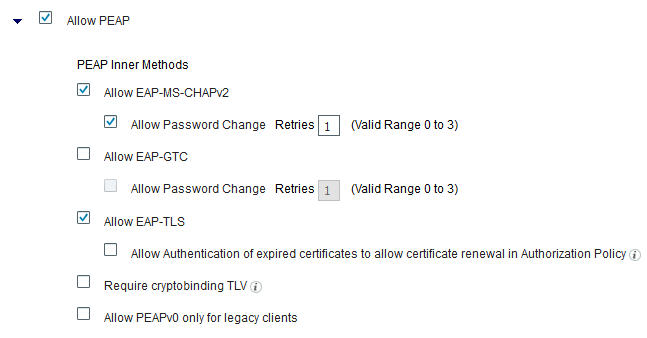


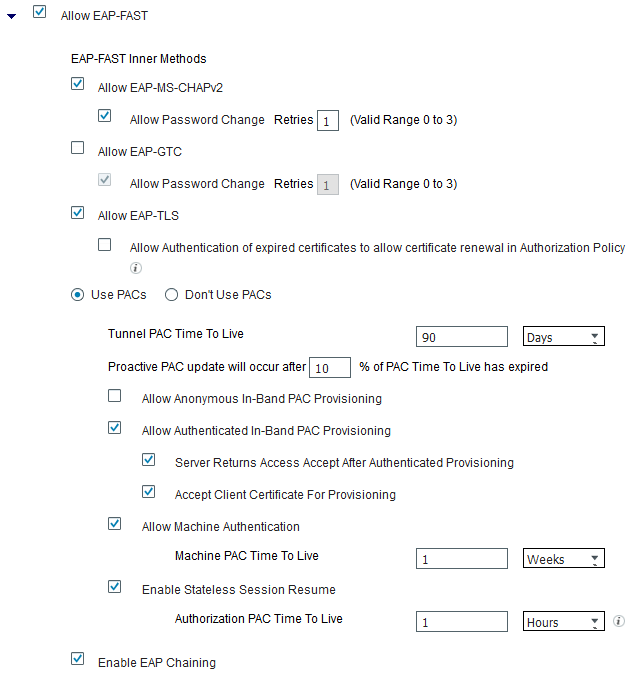
You see they provide a high-level step by step and the bottom row of the tabs at the top is the progression of configuration.

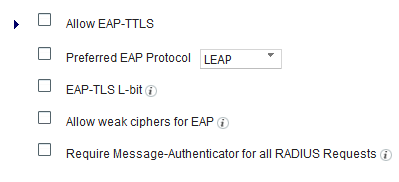
Allowed Protocols

We’ve already taken care of the first few tabs, skip to **Policy Elements > Results > Allowed Protocols**. We are going to create a new one that only allows MAB. Click **Add**, give it a name and configure the following. Then hit **Submit**.



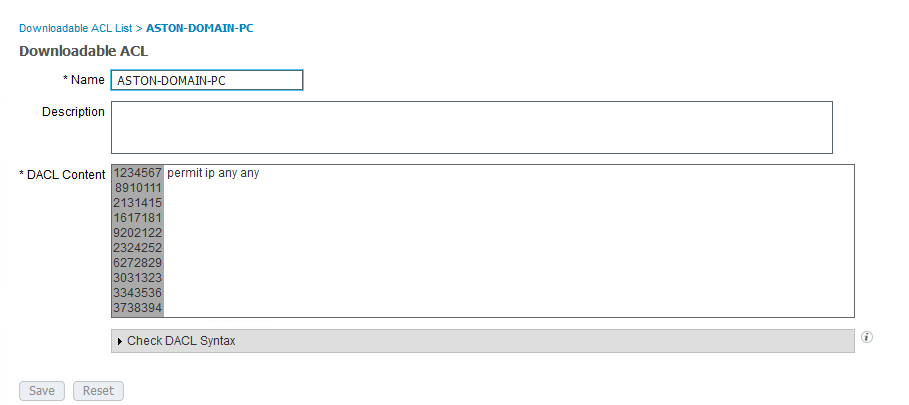


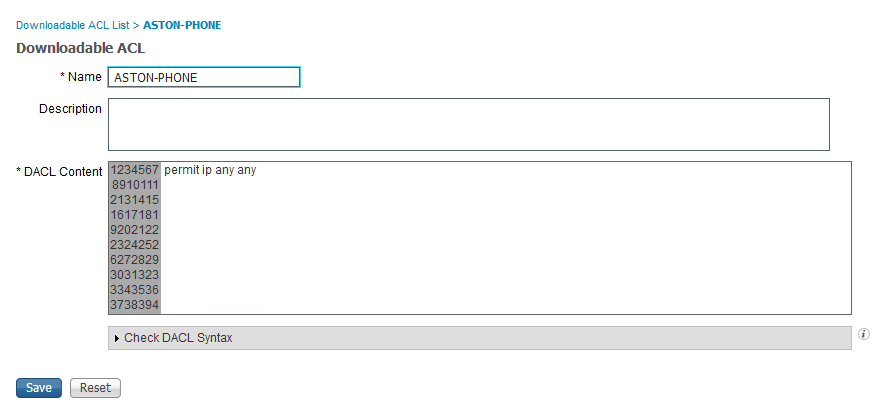


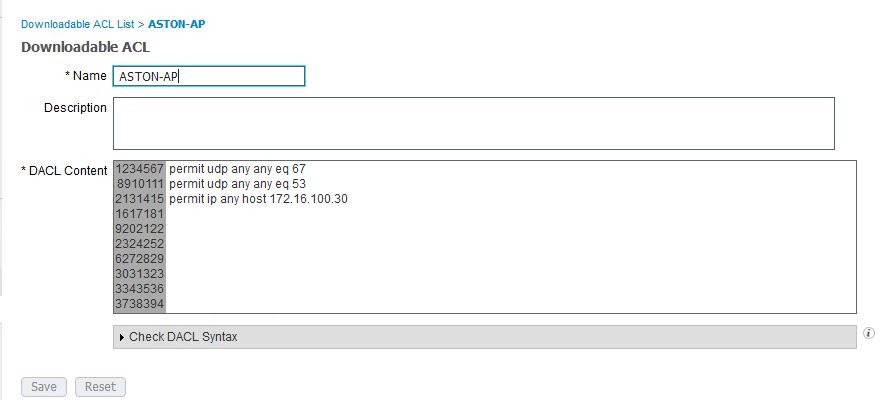


Downloadable ACLs

Next, we need to create some results for our device types. We are going to use probably the most common method which is to send a downloadable access control lists (dACL) to the NAD to change authorization. Let’s keep these simple for now. Click on **Downloadable ACLs** and **Add** the following dACLs be sure to use the check **DACL Syntax button** before you **Submit**:

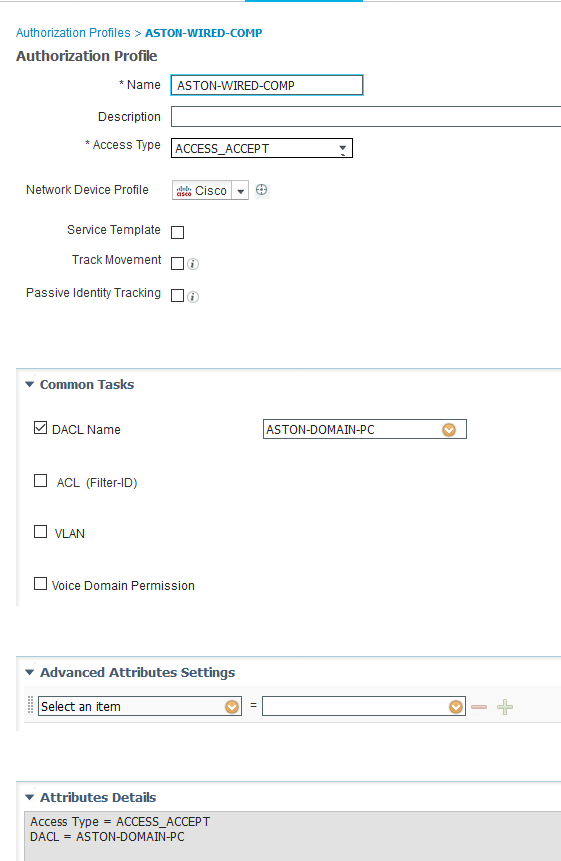


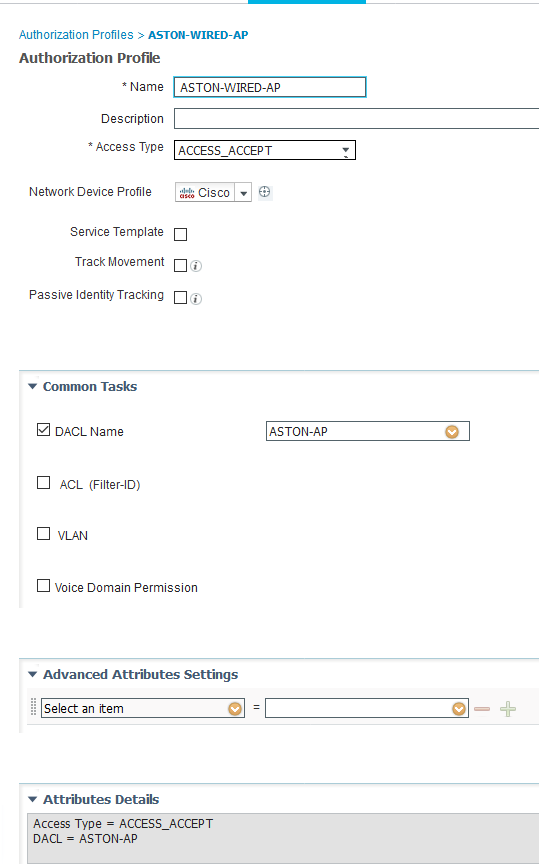


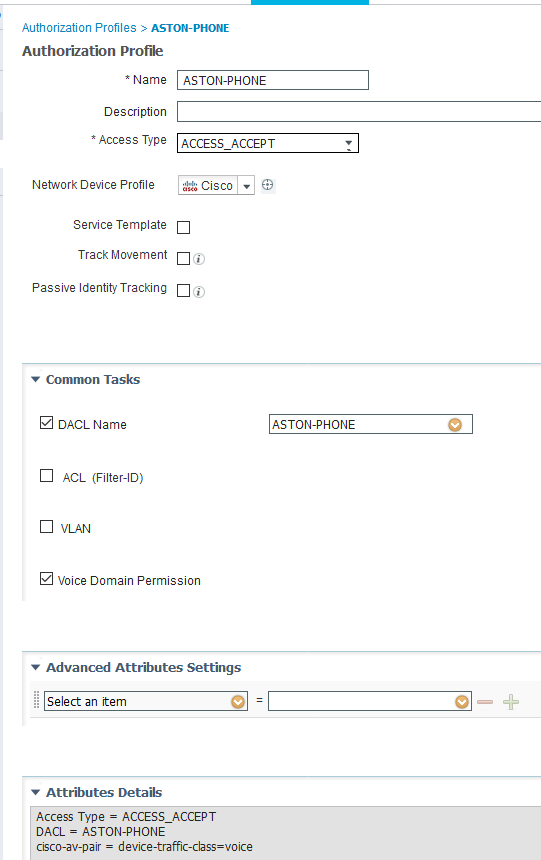


Authorization Profiles

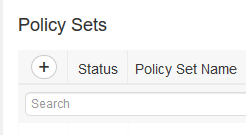
Next, we’ll create an Authorization Profile for each device type. This is where we’ll define what RADIUS attributes we will send to the NAD when we match the conditions in the policy we are going to create. We are going to send the downloadable ACL that we just created for each profile. For the phone, we also need to send a Voice Domain Permission attribute to allow the phone on the voice VLAN. Go to **Authorization Profiles** and **Add** the following Profiles:







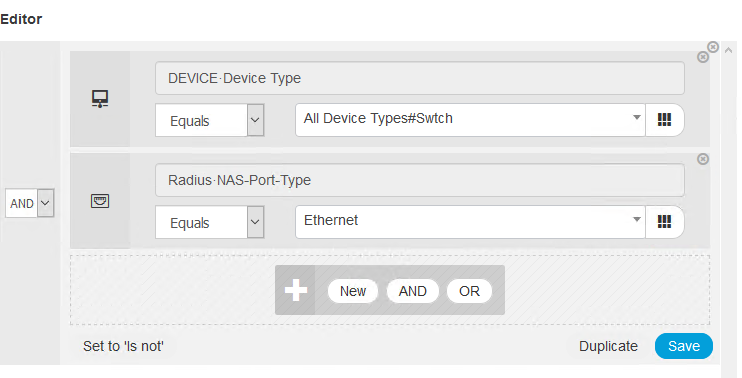
Configure Policy Set

Now we’re ready to start to create the authC (authentication) and authZ (authorization) policies. Navigate to **Policy Sets**. We are going to add a new Policy Set. Click the **+** button. 

We are going to give the policy set a name and define what type of traffic is going to ran against this policy set. In ACS, they used to call these Service Selection Rules. Name the policy set **WIRED** then click the **+** button. For **Conditions** hit the **Click** **to add an attribute**.



Then add the following **Conditions**:



Then hit **Use**.

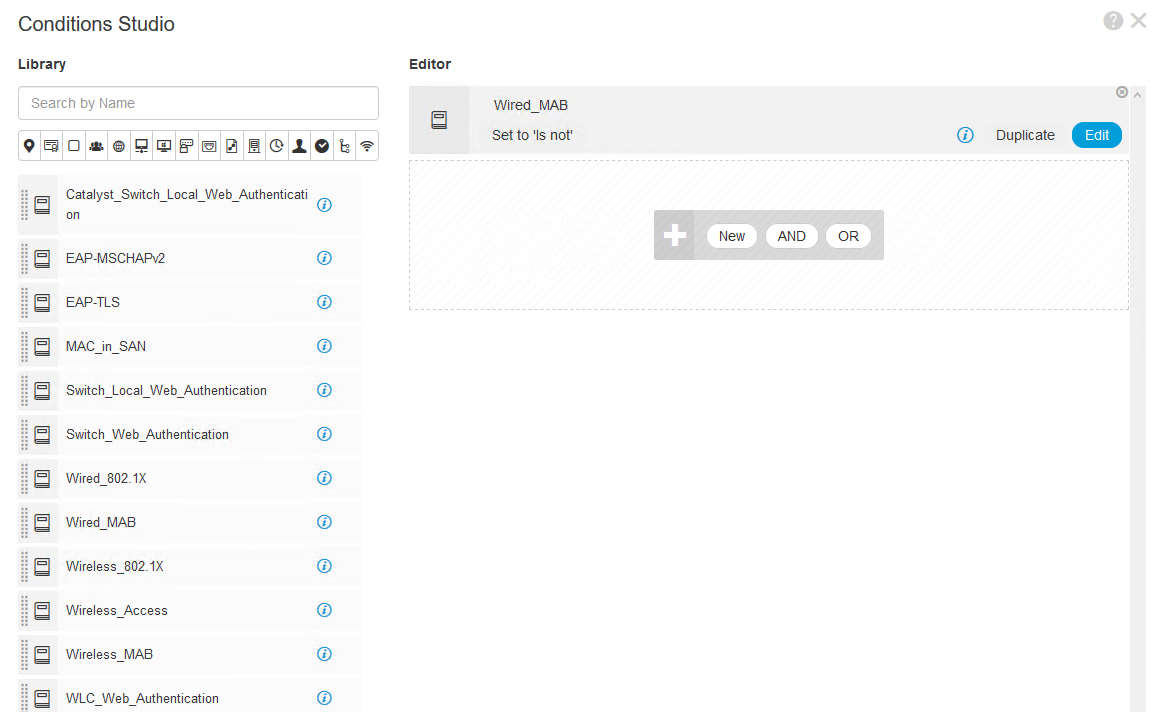
Change the Allowed Protocols to ASTON-**MAB-PEAP-TLS-FAST**. Then hit **Save**.



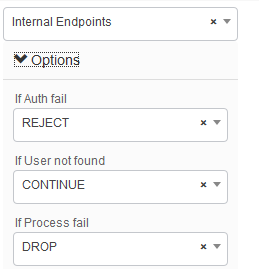
Click the **View** Icon on the right side to start creating policy.



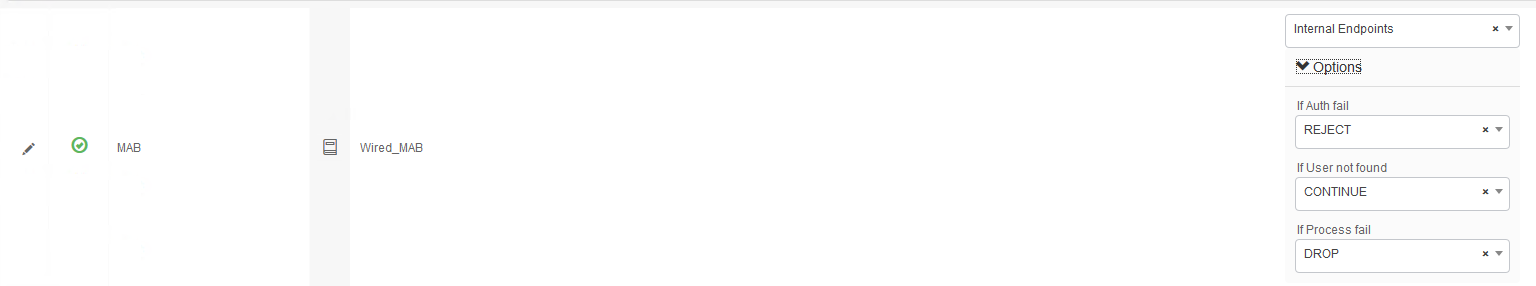
Under **Authentication Policy** add a new rule, give it a name of **MAB**. This time for Conditions we are going to take advantage of predefined condition. Hit the **+** symbol under conditions then drag over **Wired\_MAB**. Then hit **Use.**



For the **Identity Source**, we need to change that to **Internal Endpoints** and change the option of **If user not found** to Continue.



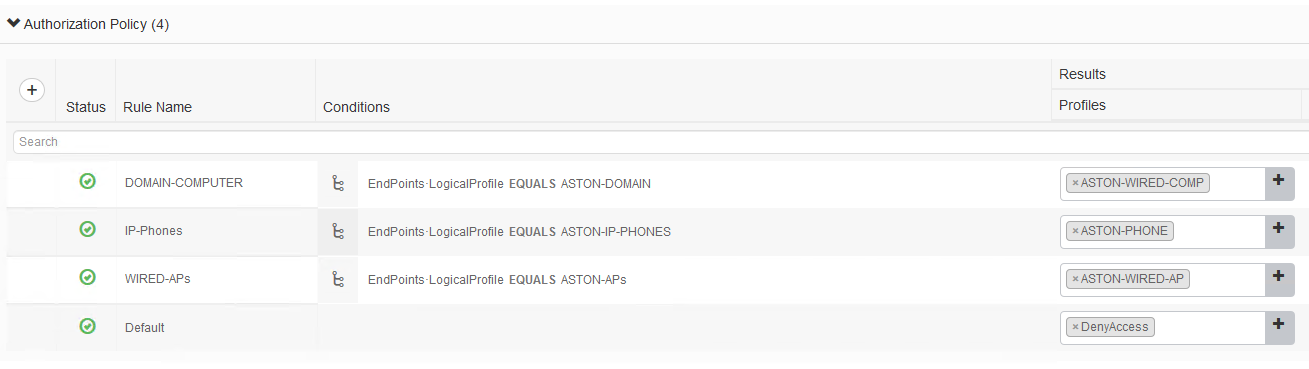
When done, it should look similar to the following:



Authorization policies will be pretty much the same process so I’m not going to walk you through the whole process step by step. Click the arrow and Insert New Rule above. Don’t forget to **Save**.

* Name: Domain Computer
* Conditions: Create New Condition
* Attribute: **Endpoints > LogicalProfile**
* Equals
* **ASTON-DOMAIN-JOINED**
* Permissions: **Standard >** **ASTON-WIRED-COMP**

Do the same process for our other devices (AP, Phone). When finished, it should look similar to the following:



Configure Switchports

Now it’s time to test these policies but first we need to configure the switchports for dot1x/MAB. Log in to ISE-Access-SW and apply the following commands:

terminal monitor

!

conf t

!

ip access-list extended ACL-DEFAULT

permit udp any eq bootpc any eq bootps

permit udp any any eq domain

permit icmp any any

permit udp any any eq tftp

deny ip any any

!

interface range GigabitEthernet 1/0/7 - 12

ip access-group ACL-DEFAULT in

authentication event fail action next-method

authentication event server dead action reinitialize vlan 55

authentication event server dead action authorize voice

authentication host-mode multi-domain

authentication open

authentication order dot1x mab

authentication priority dot1x mab

authentication port-control auto

authentication periodic

authentication timer reauthenticate server

authentication timer inactivity server

authentication violation restrict

mab

snmp trap mac-notification change added

snmp trap mac-notification change removed

dot1x pae authenticator

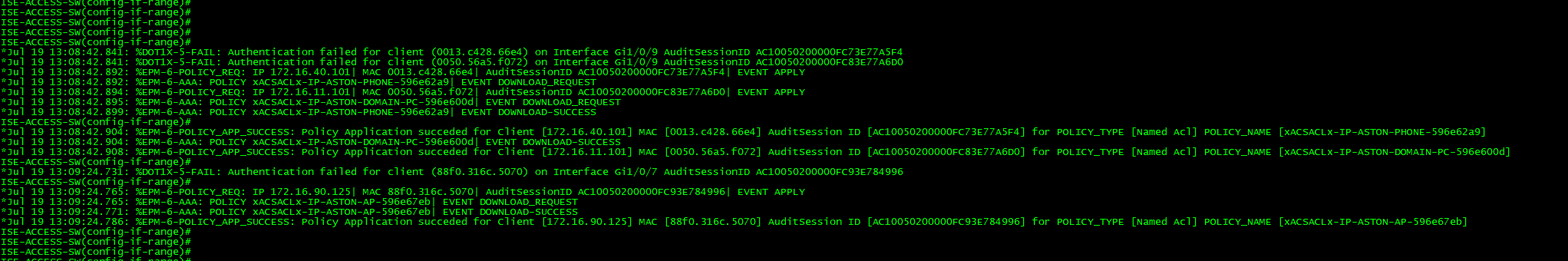
dot1x timeout tx-period 10

spanning-tree portfast

spanning-tree bpduguard enable

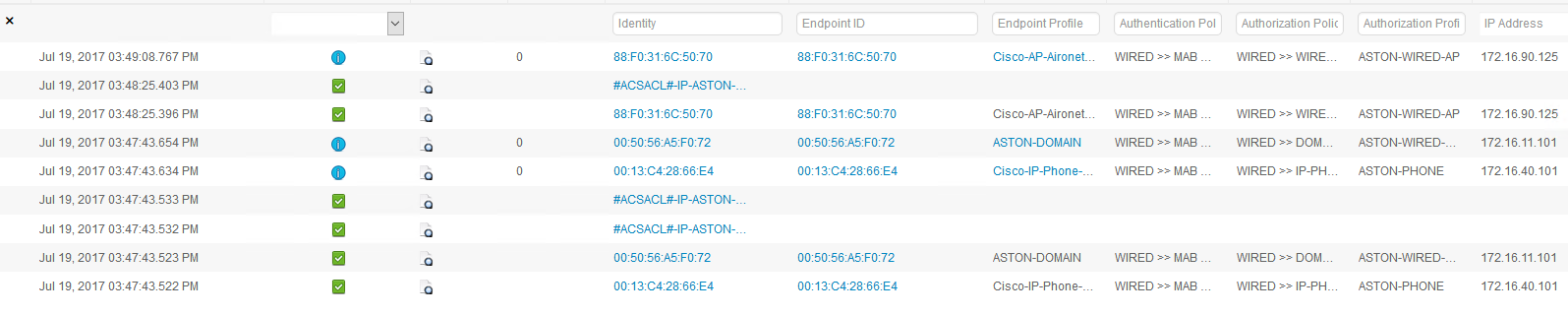
end

You should start to see dot1x failures and some success messages starting to appear in the terminal window.

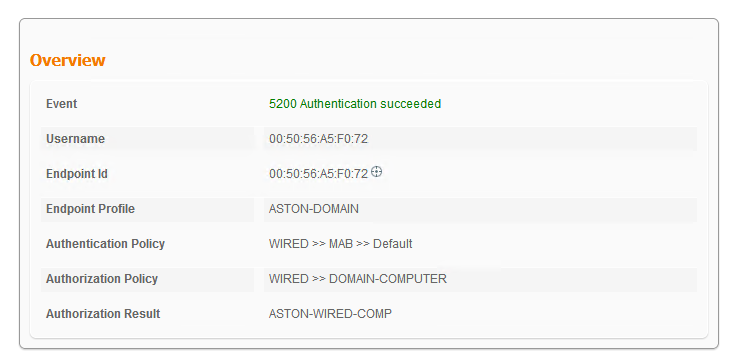


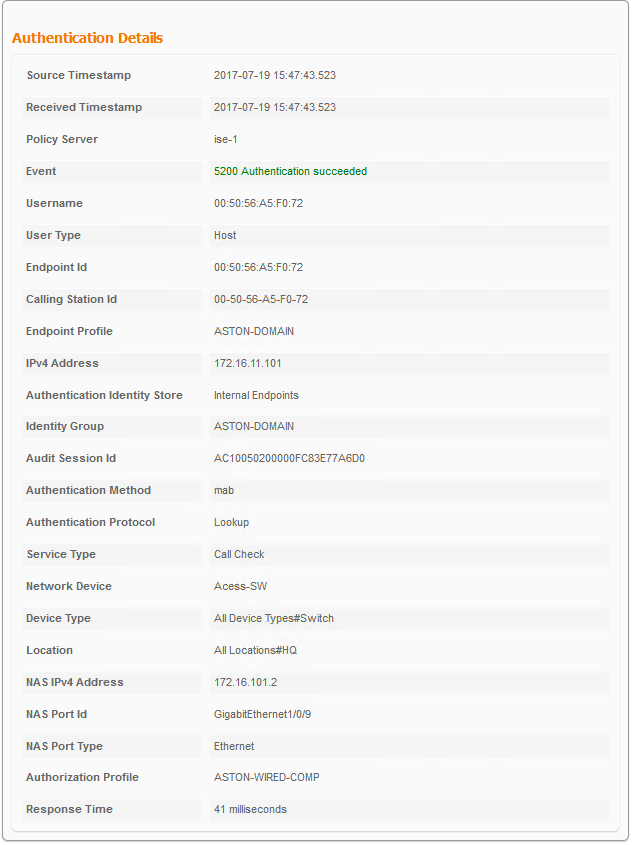
Verify Policies

Let’s check the logs in ISE. Navigate to **Operations > RADIUS > Live Logs**. This is the place to start when you are troubleshooting issues with ISE.

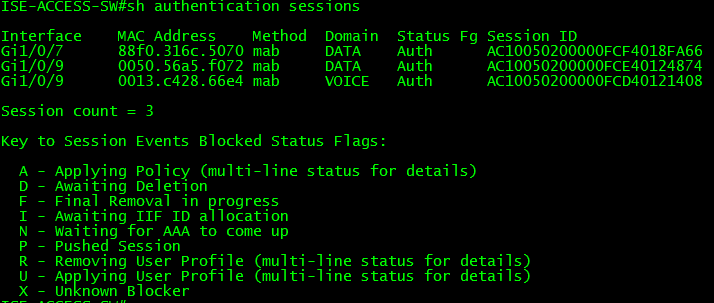


Click the  icon to dive into the details. Here we can see what policies we matched, Authentication details, RADIUS attributes, results and each step that was taken in the process.

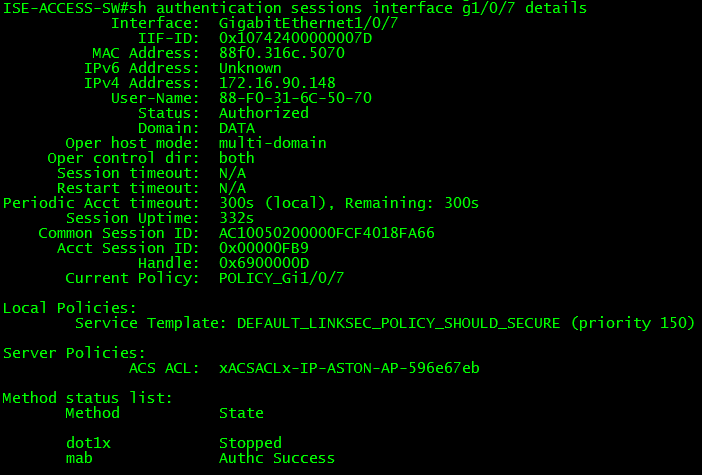




On the switch, there are some show commands that we can run. If you do a **show authentication sessions**. You can see the basics – Method used, MAC address Domain etc.



If you want to see more detail, we can add the interface you want to look at and the keyword details and get a bit more information. Run a **show authentication sessions interface g1/0/7 details**.

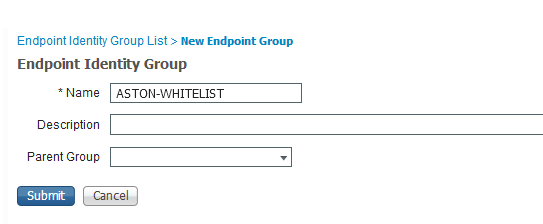


This provides quite a bit of information. We can see MAC/IP address, host mode, uptime, ACL applied method and more.

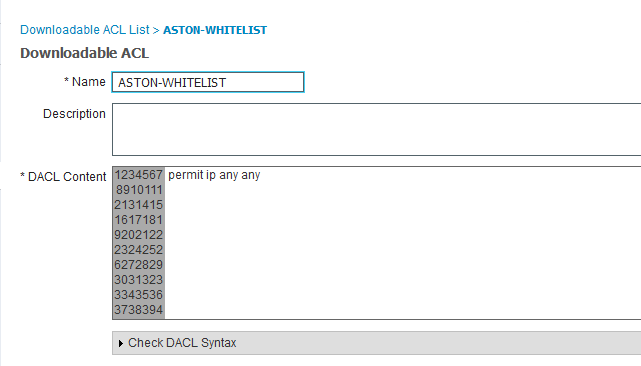
Whitelisting

What if you have a device that doesn’t send enough attributes to be reliably profiled or if you just want a quick way to allow a device on the network? We can statically assign endpoints to device profile or identity group. Let’s see how that works.

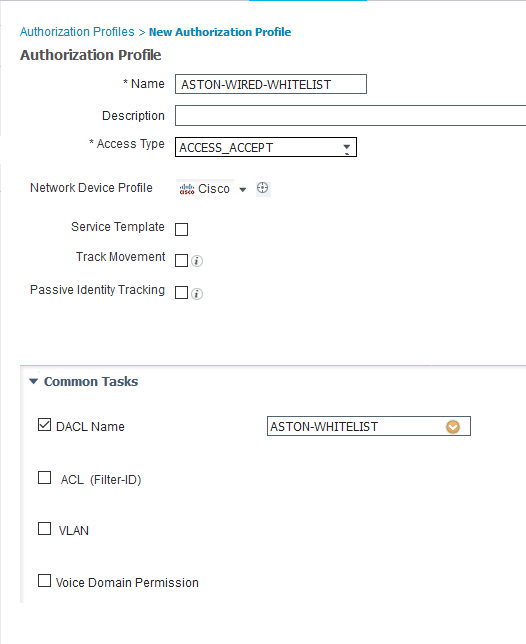
Policy Creation

In the Network Access Work Center go to **Network Access >** **Id Groups > Endpoint Identity Groups**. Click **Add** and give it a name of **ASTON-WHITELIST** and **Submit**.

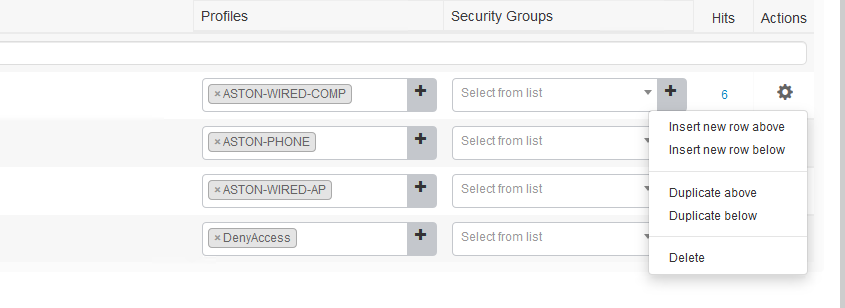
Create a dACL go to **Policy Elements > Results > Downloadable ACLs** and configure the following and **Save**:



Now create a new Authorization Profile:



Now back to our WIRED policy set to create an authz policy. We are going to want this to be at the top so go to your first policy and click on the **Gear** and hit **Insert New Rule Above**.



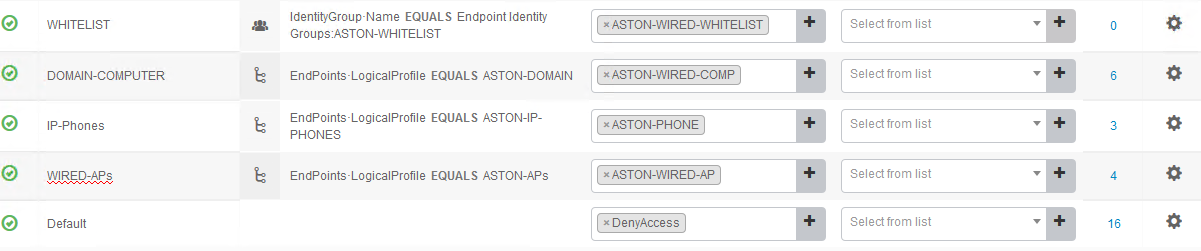
Name it **WHITELIST** then for **Conditions**: **Endpoint Identity Group > ASTON-WHITELIST**.



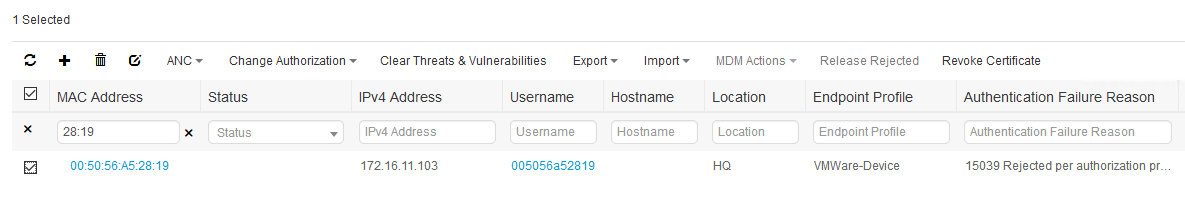
For Permissions, we’ll give it the new Profile we just created – **ASTON-WIRED-WHITELIST** then **Save**.



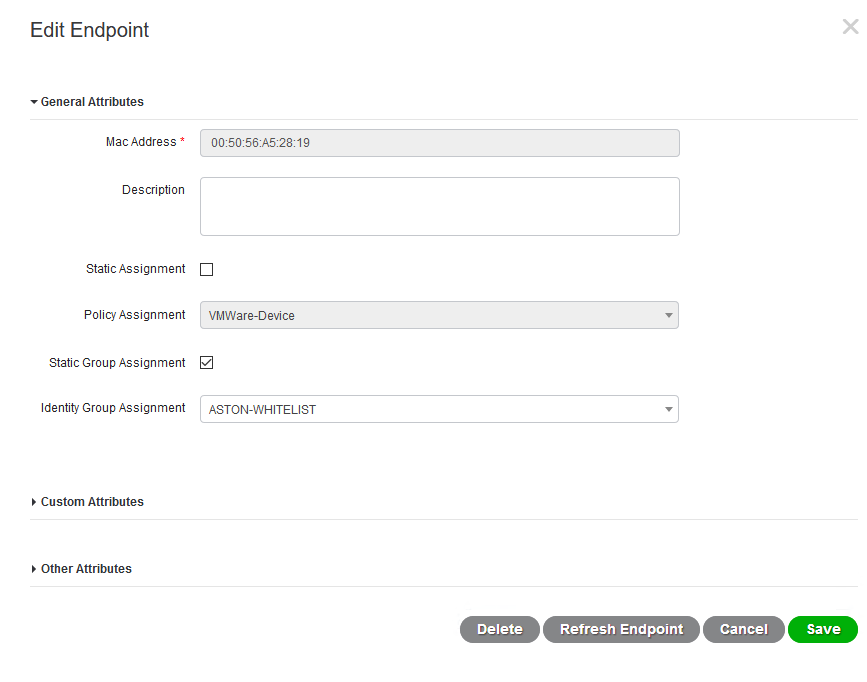
Your Policies should now look similar to this:



Log into ESXi and console into **LAB(x) PC-3**. Change the Network adapter to **LAB (x) ACESS SW G1/0/11**. Get the last 4 digits of the MAC address of your host in my case it’s 28:19. In ISE navigate to **Context Visibility > Endpoints** and filter on the last 4 of your MAC address. Click the checkbox next the MAC and **Edit** 

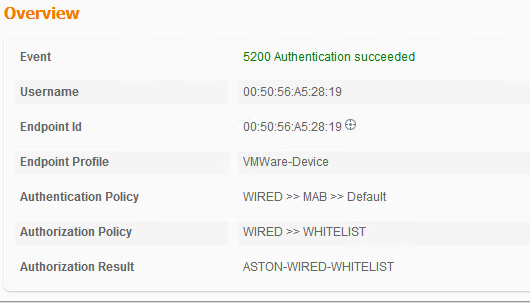


We want to assign this endpoint to a group. Tick the **Static Group Assignment** checkbox and in the dropdown, apply our whitelist group and **Save.**

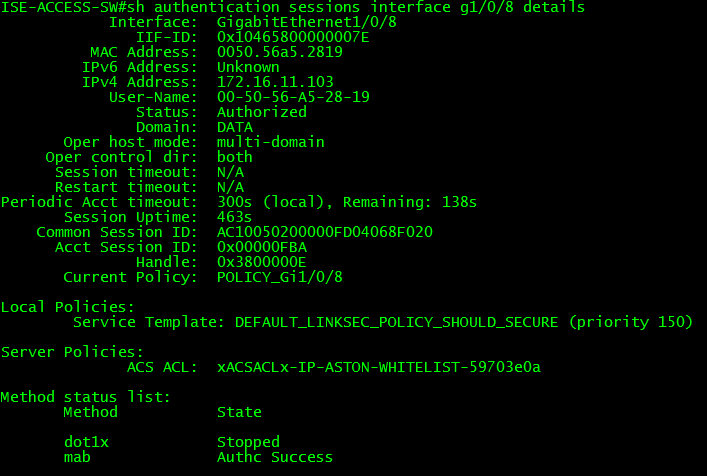


Now if we look at the live logs we can see that we previously failed authorization but once we changed the assignment we are now passing and hitting correct Authorization Policy.





And if we look at the switch we can see that MAB has success and we have downloaded the correct ACL:



Conclusion

In this lab, we have:

* Introduced Work Centers
* Configured Allowed Protocols
* Configured dACLS and applied them to Authorization Profiles
* Built our Policy Set for Wired MAB with examples using profiling and whitelisting

In the next lab, we will start configuring our endpoints and ISE for Dot1x. We’ll configure a few common EAP methods and we’ll use a both the native and AnyConnect supplicant.