|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) IEEE 802.1x Wireless |
| An Aston training document explaining how to configure 802.1x with Cisco ISE |

Contents

[Contents 2](#_Toc492499208)

[Introduction 3](#_Toc492499209)

[Lab Diagram 4](#_Toc492499210)

[WLC Configuration 5](#_Toc492499211)

[Pre-Configured Settings 5](#_Toc492499212)

[Define Airespace ACLs 8](#_Toc492499213)

[ISE Configuration 12](#_Toc492499214)

[Authorization Profiles 12](#_Toc492499215)

[Wireless Policy Set 14](#_Toc492499216)

[Windows Host Configuration (Native Supplicant) 17](#_Toc492499217)

[PEAP-MSCHAPv2 17](#_Toc492499218)

[PEAP-EAP-TLS 22](#_Toc492499219)

[Windows Host Configuration (AnyConnect Supplicant) 24](#_Toc492499220)

[EAP-FASTv2 24](#_Toc492499221)

[Conclusion 32](#_Toc492499222)

Introduction

People have been doing wireless dot1x since the beginning of time or at least since around the early 2000s. Most enterprise companies have been doing wireless dot1x with ACS or some other RADIUS server for some time so when they decide to upgrade to the next generation and deploy ISE. Wireless dot1x is typically the first use case that will get deployed.

You’ll see that the configuration is very similar to what we did in the wired dot1x lab. We’ll have to make a few tweaks here and there but not much. Because of that this lab is going to be a bit shorter than the previous labs have been. Let’s get started.

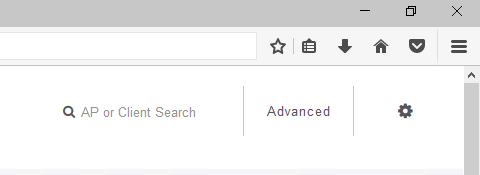
Lab Diagram



WLC Configuration

Pre-Configured Settings

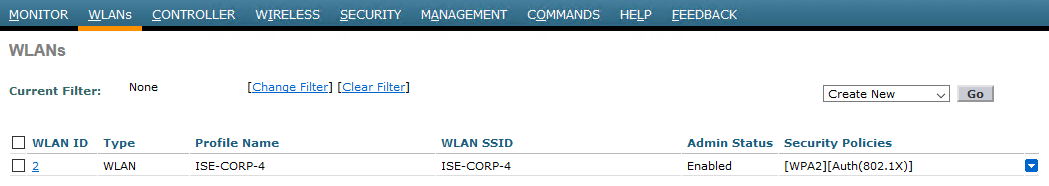
From your jumphost log in to the WLC by opening a browser and going to <https://wlc.lab.astontech.com>. Log in with **admin/qwe123$!**. Once logged in, hit the Advanced tab in the upper right corner.



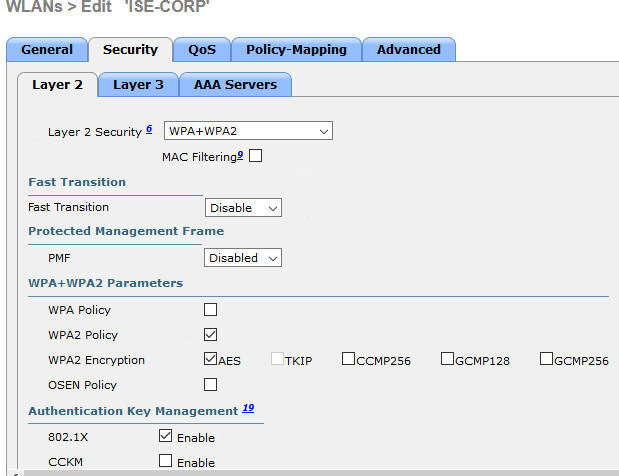
The Lab WLC should already have a base configuration and the AP should have been joined, if not contact your mentor for assistance.

Let’s walk through what we have configured pertaining to ISE so far:

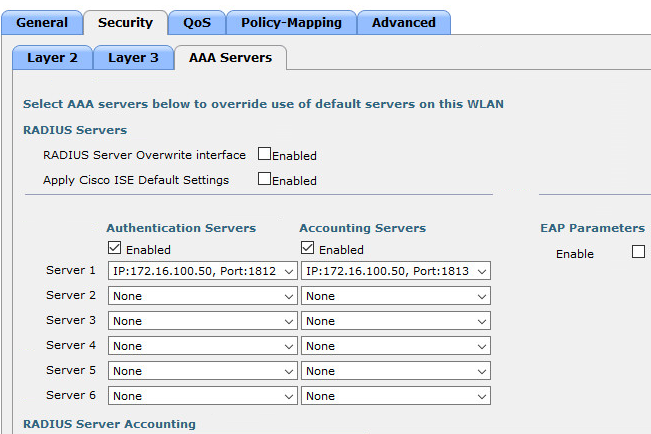
We have one SSID configured called ISE-CORP-(x).



WPA2 with 802.1x authC.



Applied ISE as our RADIUS server.

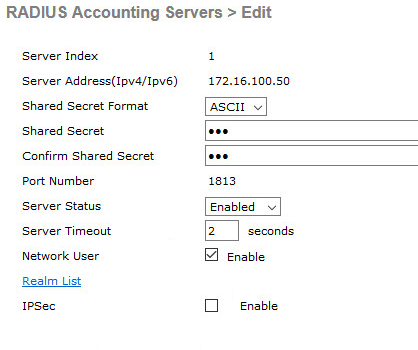
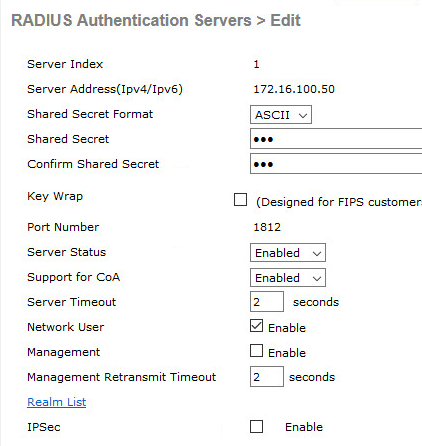


In the **Advanced** tab we have checked: **Allow AAA Override**, **DHCP Addr. Assignment Required**, changed **NAC State** to **ISE NAC**, and checked the boxes in **RADIUS Client Profiling** for **DHCP** and **HTTP**.

In the **Security** tab we have configured ISE for Authentication and Accounting.



And finally, in the **Management** tab we have SNMP configured.



Define Airespace ACLs

Unlike Cisco IOS, Cisco AireOS doesn’t support downloadable ACLS (dACLs). Instead the ACLs are configured locally on the WLC and the name is sent from ISE and applied to the user authZ.Go to **Security > Access Control Lists > Access Control Lists**. I have already created two ACLs.



Click on the DOMAIN-PC to see the rules that have been created.

Your Access List should look like this:



Hit the button and click on the **PERMIT-ALL ACL**. Here we just have a permit everything on this one.



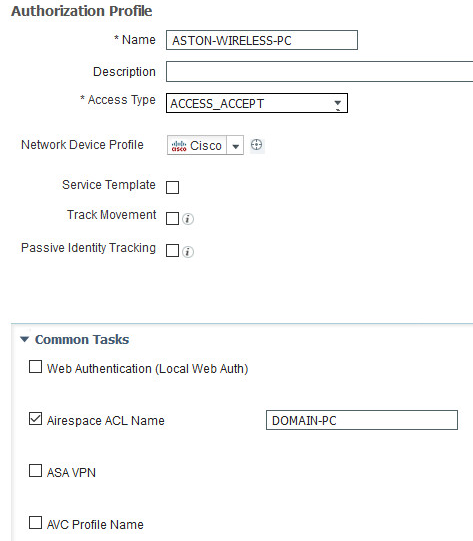
ISE Configuration

Authorization Profiles

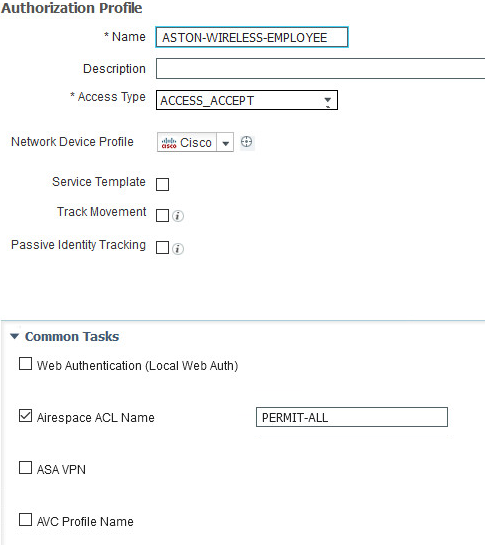
As I mentioned previously we can reuse most of what we have already configured in our wired dot1x lab for wireless. However, since our WLC doesn’t support dACLs like we used in the wired lab we’ll need to create some new Authorization Profiles.

For this lab, we are only going to allow an employee with a corporate owned device on the wireless. Let’s create one for our domain computer and for employee. Log into ISE and go to **Work Centers > Network Access > Policy Elements > Results > Authorization Profiles** and click **Add**.

Give it a name of **ASTON-WIRELESS-PC** then we need to send the Airespace ACL Name. In the **Common Tasks** scroll down to **Airespace ACL Name** check the box. Add the name of the ACL exactly as it is on the WLC in our case it’s **DOMAIN-PC**. Then Click **Submit**.



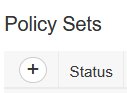
Now add one for the employee.



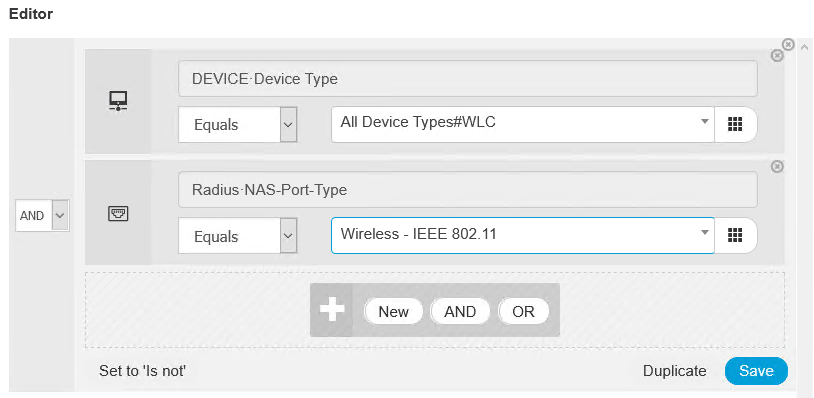
Wireless Policy Set

Now we are ready to start building our Policy. Since this is a completely different use case than wired we are going to create a separate Policy Set for wireless.

Head over to **Policy Sets** and click the **+** sign and **Create Above.**

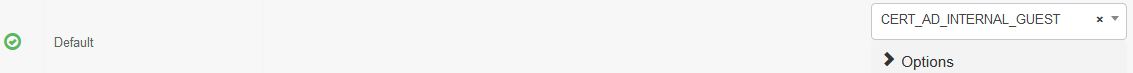


We are going to name this Policy Set **WIRELESS** and set the Conditions to **DEVICE Type EQUALS WLC** and **RADIUS NAS-Port-Type EQUALS Wireless – IEEE 802.11**. Set **Allowed Protocols** to **ASTON-PEAP-TLS-FAST**. Then hit **Save**.

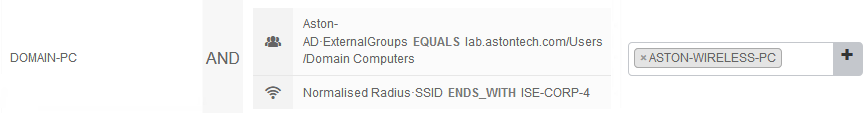


This means that any request that ISE receives that matches these conditions will get processed against these policies.

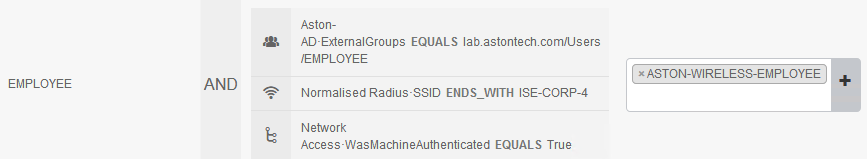
For the Authentication Policy let’s just edit the **Default**. For **Identity Source** use **CERT\_AD\_INTERNAL\_GUEST** and hit **Save**.



Now for authorization we need to create one for our domain PC and one for employee. Insert a **New Rule Above**. Name it **DOMAIN-PC**, for the conditions we are going to add **AD:ExternalGroups EQUALS Domain Computers**. The second condition we are going to add is going to match only if the user is trying to connect from our corporate SSID (ISE-CORP). Add **Normalised Radius:SSID ENDS WITH ISE-CORP-(x)**. Then we are going to give it the authorization profile we created for the domain PC earlier - **ASTON-WIRELESS-PC**.

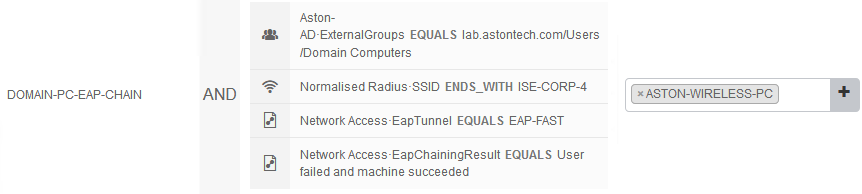


For our Employee policy let’s duplicate the policy we just created and edit it. Click the **Gear Icon** and select **Duplicate Below**. Change our AD group to Employee and add another attribute for MAR. **Network Access: WasMachineAuthenticated EQUALS True** then **Save**.

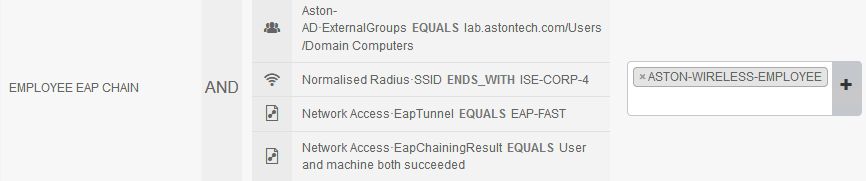


Since we going to test with EAP Chaining and we are here now let’s configure more specific policies for EAP Chaining.

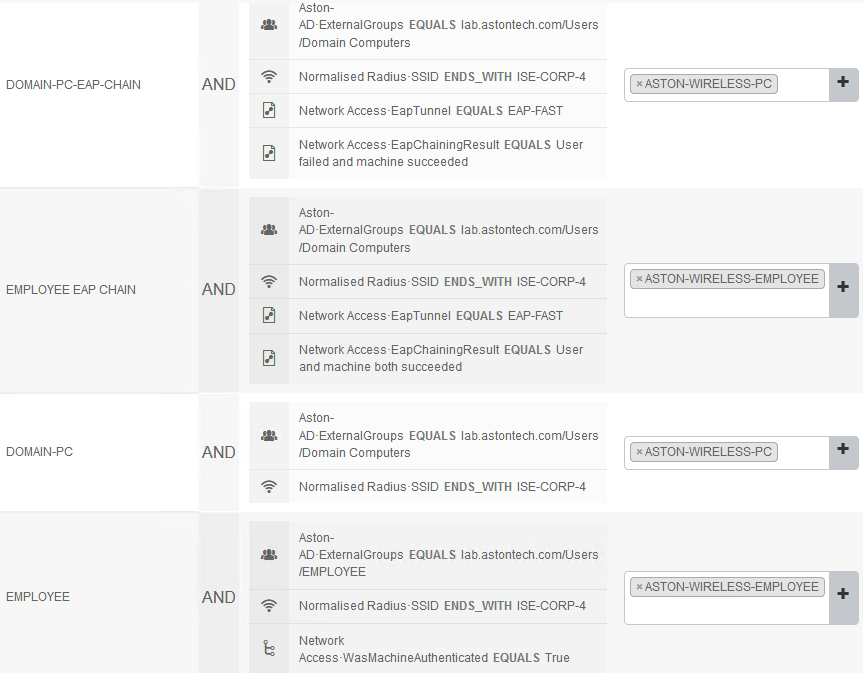
On the **DOMAIN-PC** policy click the **Gear Icon** then select **Duplicate Above**. Rename it and add **Network Access:EAPTunnel EQUALS EAP-FAST** then add **Network Access:EapChainingResult EQUALS User failed and machine succeeded**.



Duplicate the EMPLOYEE policy. Rename it and remove the last condition we have there for MAR then add **Network Access:EAPTunnel EQUALS EAP-FAST** and **Network Access:EapChainingResult EQUALS User and machine both succeeded**.



Now we need to move our EAP Chaining policies above our MAR policies. Your Policy Set should look like this:

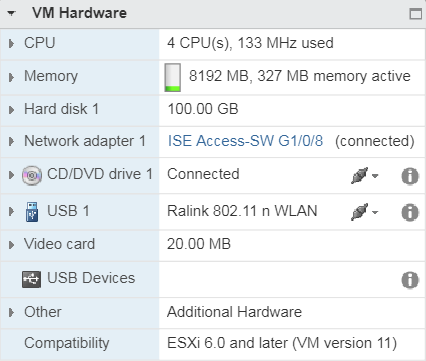


Remember to **Save**. Now we’re set to start configuring the hosts and start testing.

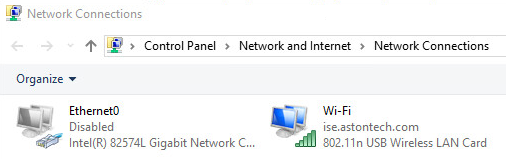
Windows Host Configuration (Native Supplicant)

PEAP-MSCHAPv2

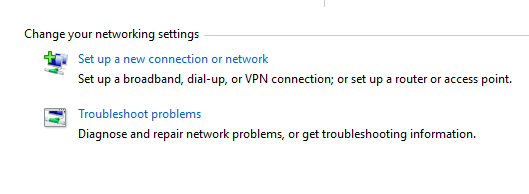
Console in to LAB-PC-1. Make sure you have the wireless USB adaptor attached to the host.



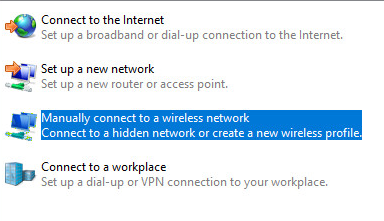
Go to your **Network Connections** and Disable your **Ethernet0** adaptor.



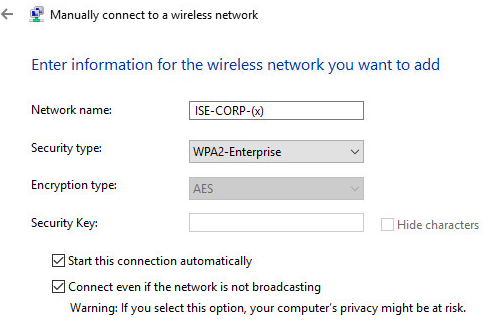
Go to **Control Panel > Network and Internet > Network and Sharing Center** and Click on **Set up a new connection or network**.



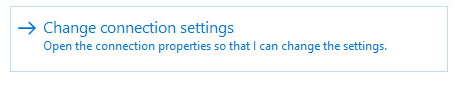
Select **Manually connect to wireless network** then **Next**.



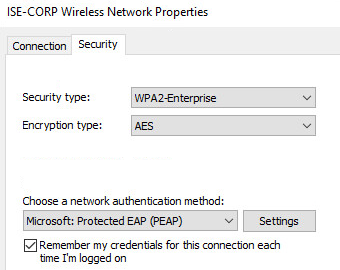
Add the following and click **Next**:



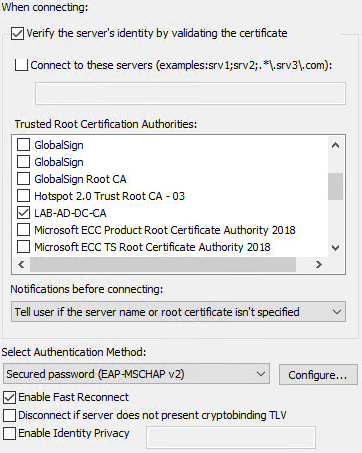
Select **Change connection settings**.



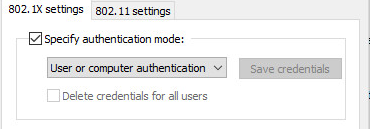
Click on the **Security** tab then **Settings**.



Click your **Root CA cert** in the **Trusted Root Certification Authorities** then **OK**.



Click **Advanced settings**. Make sure **User or Computer authentication** is selected. Then hit **OK**.



Hit **OK** again to finish out the configuration. Sign out of the host so we can kick off the machine authentication.

Let’s check ISE for the results. On ISE go to **Operations > RADIUS > Live Logs**. You should see that the machine authentication has passed.



Now let’s look at the details. Click the **Magnifying Glass**. Here we can see we are hitting the correct Policy Set, authZ policy and authZ result.



If we scroll down and look at the Authentication Details, we can see we are authC via dot1x and the protocol is PEAP-MSCHAPv2.



And if we scroll down to Results we see that we are sending the correct Airespace ACL.



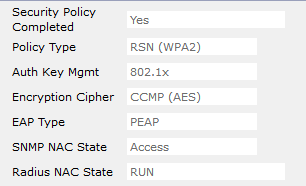
Now let’s look at the WLC. Log into the WLC and go to Monitor > Clients. We can see we have one client here. Click on the client MAC address for more details.



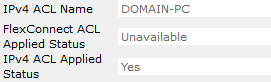
Here we can see the username is the host machine.



If you scroll down to the Security Information we can see we are doing WPA2, dot1x and PEAP.



A little further down we can see the ACL that was applied.



Now let’s log back into LAB-PC-1. Look at the ISE Live Logs you should see that the user has now passed authentication.



Now let’s look at the details. Click the **Magnifying Glass**. Here we can see we are hitting the correct Policy Set, authZ policy and authZ result.



if we scroll down to Results we see that we are sending the correct Airespace ACL.



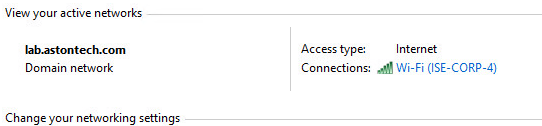
Let’s check the WLC and make sure everything matches up. We can see the username has changed and the PERMIT-ALL ACL was applied.



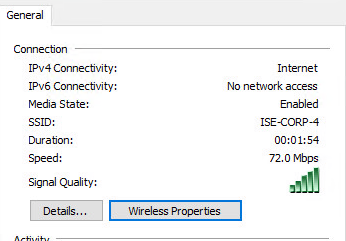


PEAP-EAP-TLS

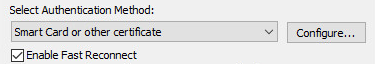
Let’s make a few changes on the host and test out PEAP-EAP-TLS. On LAB-PC-1 go to **Control Panel > Network and Internet > Network and Sharing Center**. Click on **Wi-Fi (ISE-CORP-(x))**.



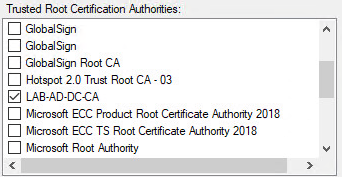
Click on **Wireless Properties**.



Click on the **Security** tab then **Settings**. Change **Select Authentication Method** to **Smart Card or other certificate**. Then hit **Configure**.



Tick the checkbox for our Root CA. Then click **OK** until you’re out of the configuration.



If you check the Live Logs in ISE you should see you have already passed authentication but let’s log out and see the machine auth for good measure. After you log out you should see that the Identity has changed a little as ISE is pulling it from the certificate now and the authentication protocol is now PEAP-EAP-TLS but the results should be the same.

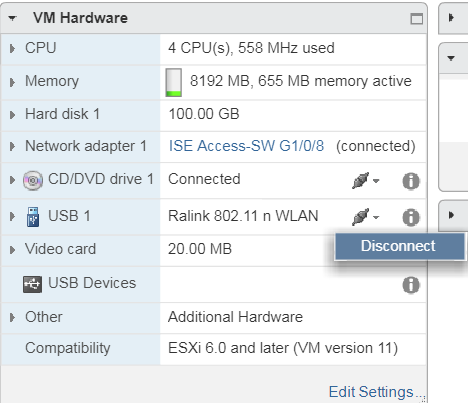
Now we have EAP-TLS working as an inner method for PEAP. What about just EAP-TLS? See if you can get EAP-TLS working.

Windows Host Configuration (AnyConnect Supplicant)

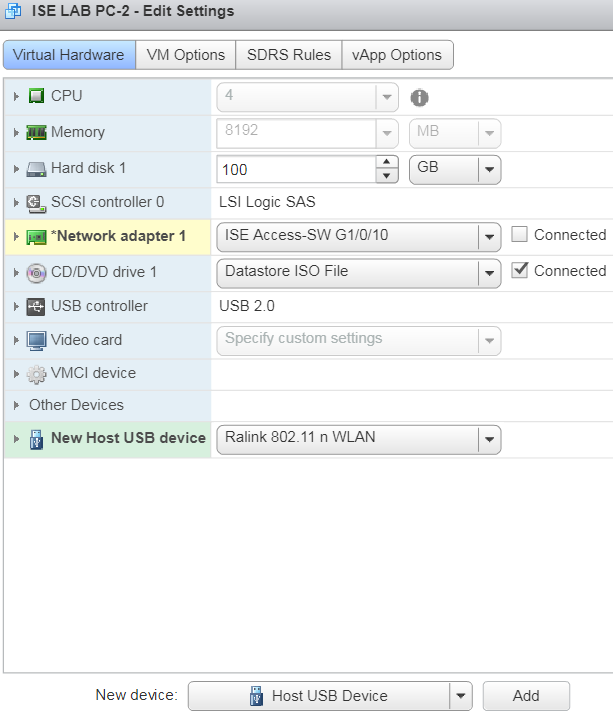
EAP-FASTv2

Now let’s configure EAP Chaining with EAP-FASTv2 and use EAP-TLS as the inner method on LAB-PC-2.

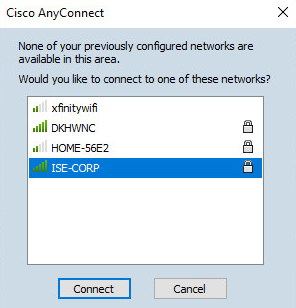
First, on LAB-PC-1 reenable your Ethernet0 adaptor. Then in ESXi disconnect the wireless USB adaptor.



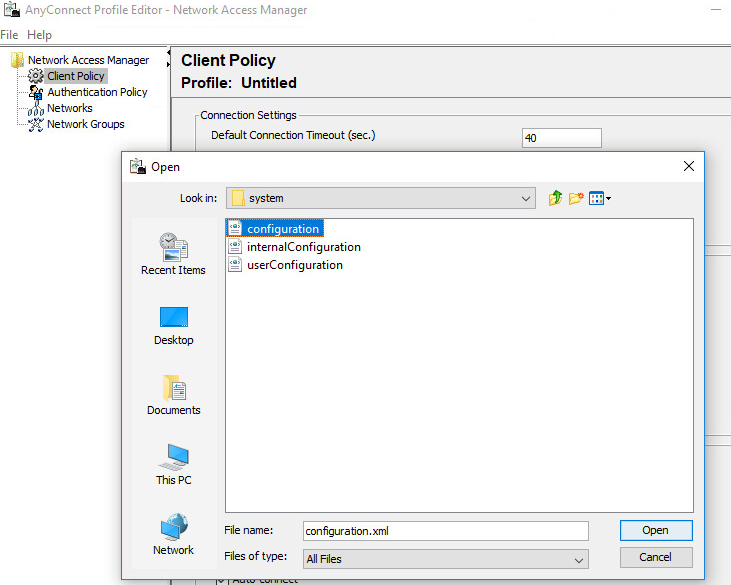
In ESXi disconnect the Ethernet adaptor on LAB-PC-2 and add the wireless USB adaptor.



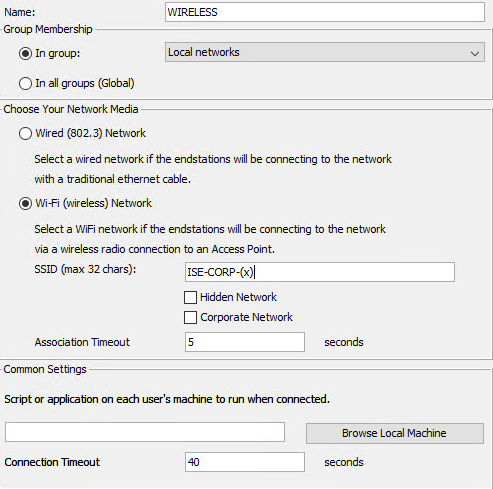
Console into LAB-PC-2. You may see this screen below. If so, click **Cancel** we are going to configure our network through the NAM Profile Editor.



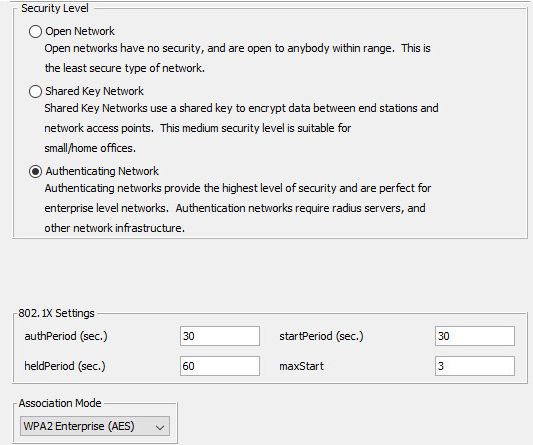
Open the AnyConnect NAM Profile Editor. Go to **File > Open** then select the configuration file and **Open**.



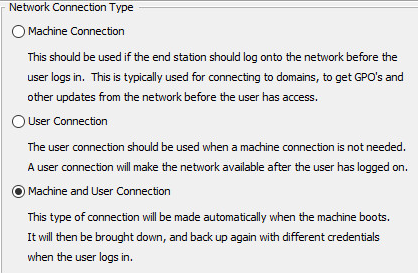
Go to **Networks** and click **Add**. Configure the following: Then click **Next**.



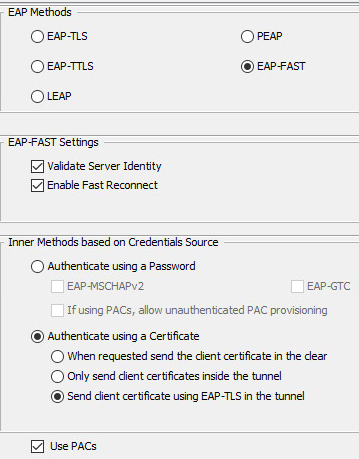
Select **Authenticating Network** and then for Association Mode select **WPA2 Enterprise**. Then Click **Next**.



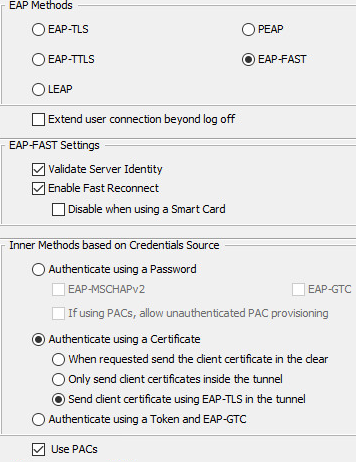
Set the **Connection Type** to Machine and User Connection. Then Click **Next**.



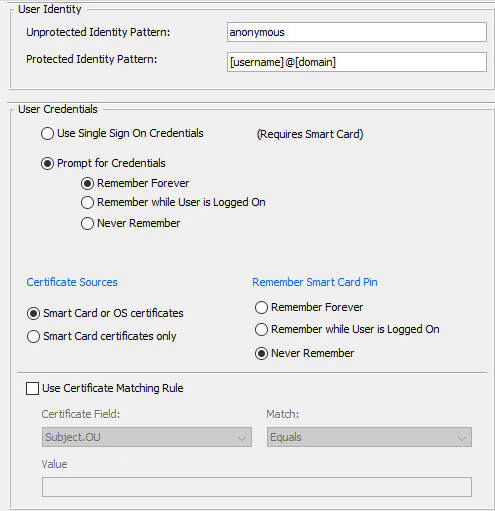
Select **EAP-FAST** as the **EAP Method** and for the **Inner Methods** select **Authenticate using a Certificate**. Then click **Next**.



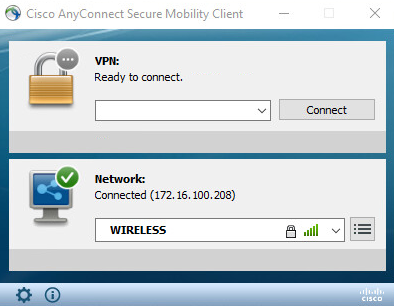
Click **Next** until you get to the **User Auth** **Page**. For **EAP Methods** select **EAP-FAST** and the **Inner Method** to **Authenticate using a Certificate**. Then click **Next**.



Click **Next** on the **Certificates page**. Then, on the **Credentials page** for **User Credentials** select **Prompt for Credentials** and **Remember Forever**. Then hit **Done**. Go to **File** and hit **Save**.



Same as before right click on the AnyConnect icon in the system tray and hit **Network Repair**. Now you should be connected to the wireless.



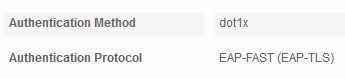
And we can see in ISE we have passed.



Now let’s check ISE and the WLC for details. If we look at ISE we can see that we are matching the correct policy.



Our Authentication Protocol is EAP-FAST-EAP-TLS.



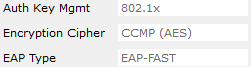
Radius Flow Type is Wireless and UseCase is EAP Chaining.



And we are sending an Airespace ACL Name of PERMIT-ALL.



On the WLC we can see we are doing dot1x with EAP-FAST.



And we can confirm we are applying the PERMIT-ALL ACL.



Now test out some other EAP methods with the AnyConnect supplicant. Like EAP-FAST-MSCHAPv2, PEAP-MSCHAPv2, PEAP-EAP-TLS and EAP-TLS.

Conclusion

In this lab, we have:

* Reviewed the WLC configuration
* Configured ACLs locally on the WLC
* Configured Authorization Profiles for our wireless policies
* Configured a new Policy Set for our wireless use case
* Configured Authentication and Authorization policies utilizing MAR on ISE
* Configured Authentication and Authorization policies for EAP Chaining on ISE
* Configured Windows Native Supplicant and tested various EAP methods:
  + PEAP-MSCHAPv2
  + PEAP-EAP-TLS
* Configured AnyConnect supplicant for EAP-FASTv2 and EAP Chaining and tested

In the next lab, we are going to start to look at the BYOD (Bring your own device) use case.