|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Wired BYOD |
| An Aston training document explaining how to deploy wired BYOD |

Contents

[Contents 2](#_Toc37015635)

[Introduction 3](#_Toc37015636)

[Lab Diagram 4](#_Toc37015637)

[ISE BYOD Configuration 5](#_Toc37015638)

[BYOD Prerequisite Configuration 5](#_Toc37015639)

[My Devices Portal Configuration 8](#_Toc37015640)

[Guest Portal Configuration 12](#_Toc37015641)

[BYOD Policy Creation 13](#_Toc37015642)

[Testing Wired BYOD 16](#_Toc37015643)

[Conclusion 26](#_Toc37015644)

Introduction

In this lab, will take our first shot at BYOD (Bring Your Own Device). When you think of BYOD the first thing that usually comes to mind is wireless but we are going to start off with wired devices. We’ll configure the WLC, ISE and the Access Switch to permit one of our Windows 10 hosts for wired BYOD. In all our BYOD labs, we are going to use EAP-TLS to authenticate our BYOD users. While we could use our internal CA for this but ISE has a built-in CA that’s great for this use case, so we’re going to use that instead. Let’s get started.

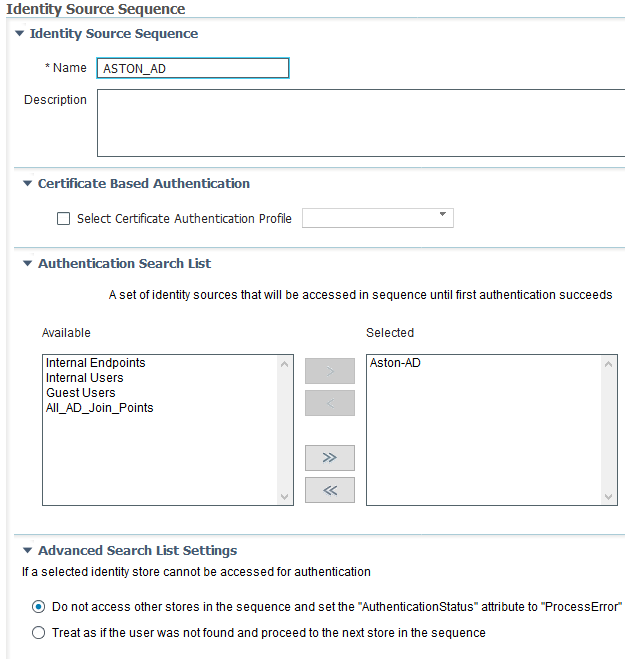
Lab Diagram



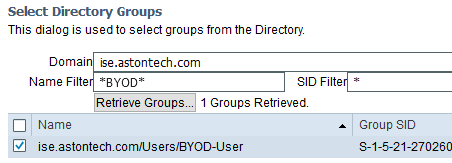
ISE BYOD Configuration

BYOD Prerequisite Configuration

Log into ISE and go to **Work Centers > BYOD > Identities > Identity Source Sequences**. Since we are only going to be using AD as an identity source we are going to create one with just AD in it. Click **Add**, Name it **ASTON\_AD**, add **ASTON-AD** to the Search List and **Submit**.

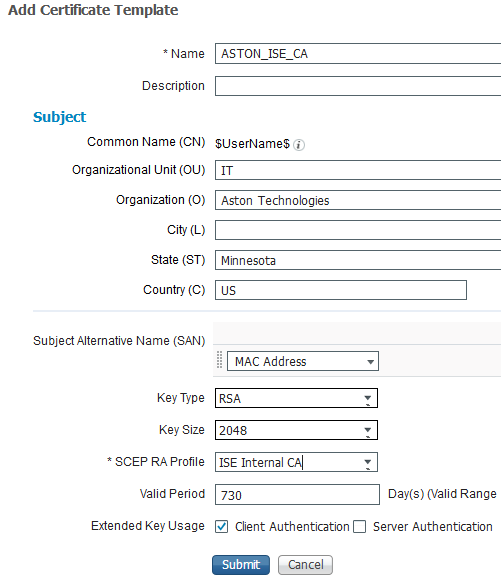


We’re only going to allow certain employees bring in devices from home to use on our network. Go to **EXT ID Sources > Active Directory > Aston-AD > Groups** and add our **BYOD-Users** group if you haven’t already.

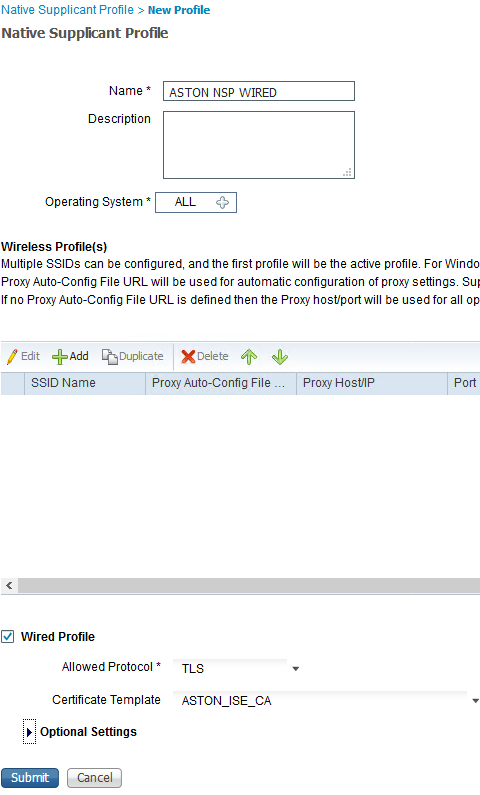


Click **OK** then **Save**.

Navigate to **Portals & Components > Certificates > Certificate Templates**. We could just use the one provided by default but we’ll create one. Click **Add** and provide the following configuration then **Submit**:



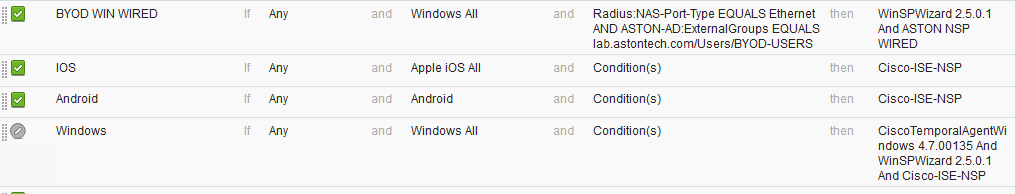
Next navigate back to **Client Provisioning > Resources**. Here we are going to create a new Native Supplicant Profile (NSP). This tells the endpoint what the connection parameters are. In our case, we are going to use certificates (TLS). Click **Add** then **Native Supplicant Profile** and configure the following:



Navigate to **Client Provisioning Policy**. This is where we define by Operating System who gets which profile and configuration wizard if necessary. Click on the down arrow on the **Windows rule** and **Duplicate Above**. Name it **BYOD WIN WIRED**. We want to match on the conditions of **Aston-AD:ExternalGroups EQUALS BYOD-User** AND **Radius:NAS-Port-Type EQUALS Ethernet**. Then for results **Config Wizard:WinSPWizard 2.2.0.52** and **Wizard Profile:ASTON NSP WIRED**.

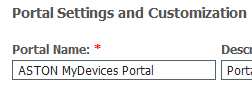


Then **Disable** the **Windows policy** and move our new **BYOD WIN WIRED** policy to the top and hit **Save**.

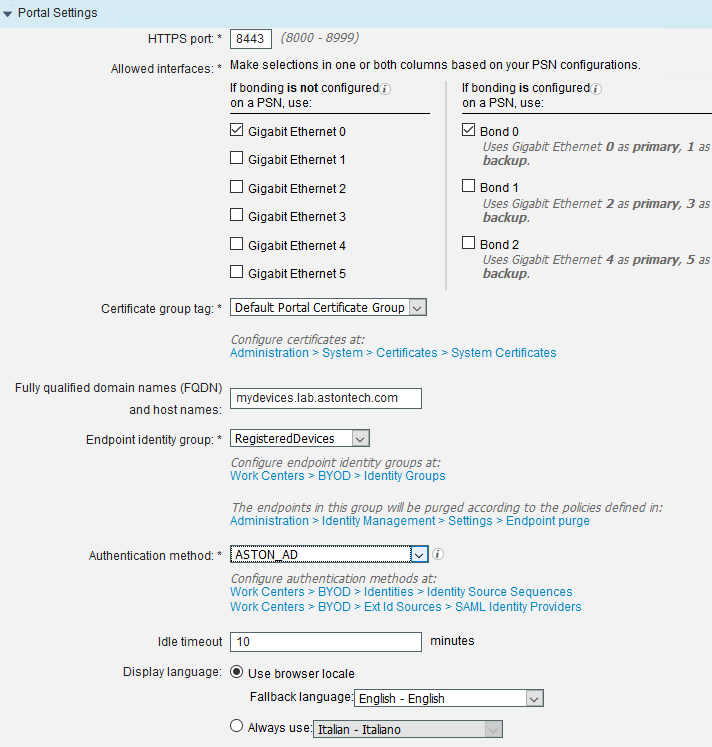


My Devices Portal Configuration

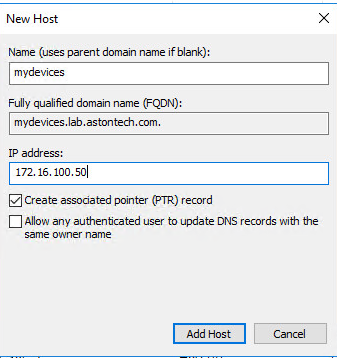
Navigate to **Portals & Components > My Devices Portals**. This is where users can manage their BYOD devices. If one of their devices were to get lost or stolen, then can go to this page and report it as such. We are going to add a new one, click **Create**. Name it **ASTON My Devices Portal**.



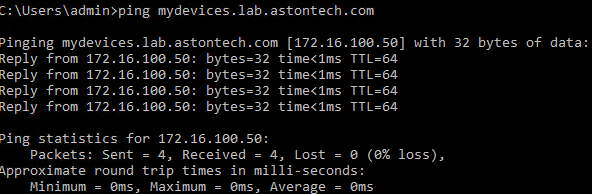
Expand **Portal Settings** and configure the following:



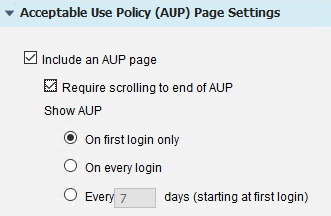
For the FQDN we need to make that resolvable. Open the console to your AD server and add MyDevices as an A record pointing to your ISE PSN.



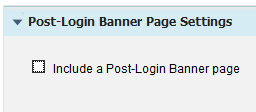
On your Jump box make sure **mydevices.lab.astontech.com** is resolvable to our ISE PSN.



Expand **Acceptable Use Policy (AUP) Page Settings**. Let’s force the user to scroll to the end of the AUP.



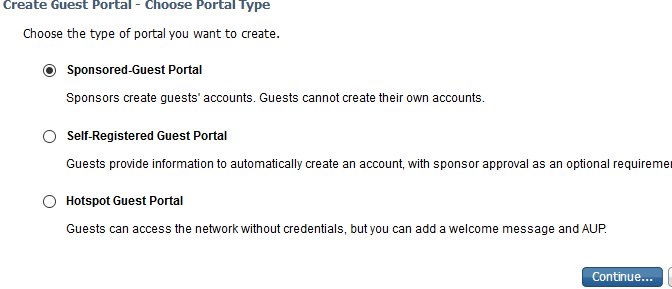
Let’s also remove the Post-Login Banner. Uncheck the box to include a Post-Login Banner Page.



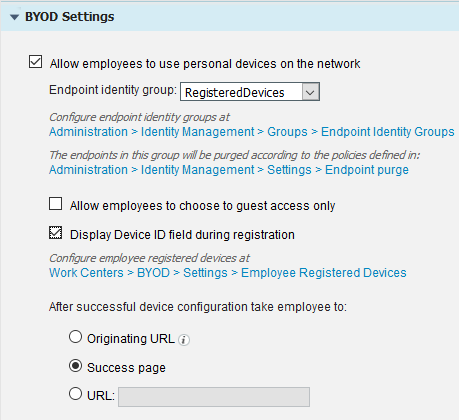
The rest we can leave default. Scroll back to the top and click **Save**.

Guest Portal Configuration

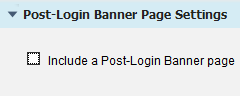
You wouldn’t expect the users would have their devices configured for dot1x so we need a way for users to authenticate and then onboard their devices. We are going to use a sponsored Guest Portal for this since that will provide a user login that we need. Navigate to **Work Centers > Guest Access > Portals & Components > Guest Portals**. Hit **Create** and Select **Sponsored-Guest Portal** and **Continue**.



Let’s name it **ASTON CWA**. CWA stands for Central Web Authentication. Skip down to and expand **BYOD Settings**. We want to check **Allow employees to use personal devices on the network** and **Display Device ID field during registration**.



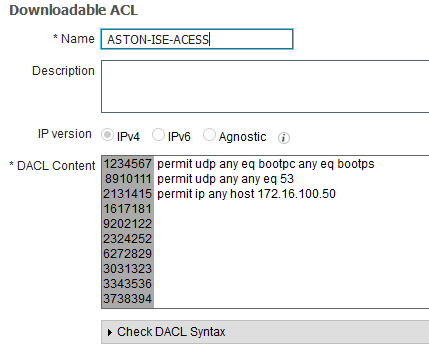
Let’s also remove the **Post-Login Banner**.



Scroll to the top and **Save**.

BYOD Policy Creation

Navigate back to the **Work Centers > BYOD > Policy Elements > Results > Downloadable ACLs**. This process is going to be two rounds of authentication for the endpoint first being MAB and second EAP-TLS. Once we pass MAB we need to send an authorization to the switch and not allow more access than needed. At this point all the endpoint needs to talk to is ISE. Create a new dACL and provide access only for DHCP, DNS and ISE.



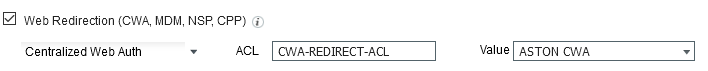
Now we need an Authorization Profile that will reference our new dACL and force the CWA. Go to **Authorization Profiles** and **Add**. Name it **ASTON-WIRED-CWA**.



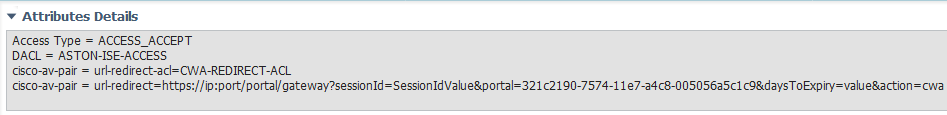
Check the DACL Name checkbox and give it the value of ASTON-ISE-ACCESS.



Scroll down in the **Common Tasks** box and check the **Web Redirection (CWA, MDM, NSP, CPP) box**. Here we will define the type of redirect, the redirect ACL on the switch (which we are about to add) and the redirect URL. Configure as shown below:



If you look at the bottom in the Attributes Details you can see that we are sending the dACL, redirect ACL and the redirect URL.



Now we need to log into ISE-ACCESS-SW and apply the CWA-REDIRECT-ACL.

ip access-list extended CWA-REDIRECT-ACL

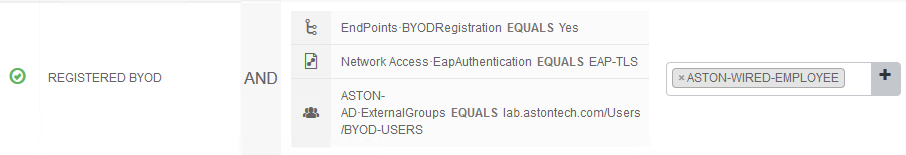
deny ip any host 172.16.100.50

permit tcp any any eq www

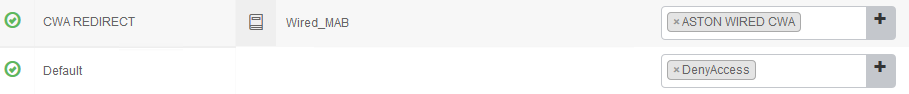
permit tcp any any eq 443

The logic on the redirect ACL is the opposite of what you would think for a typical ACL. Anything that we permit will get redirected and the deny statements will not.

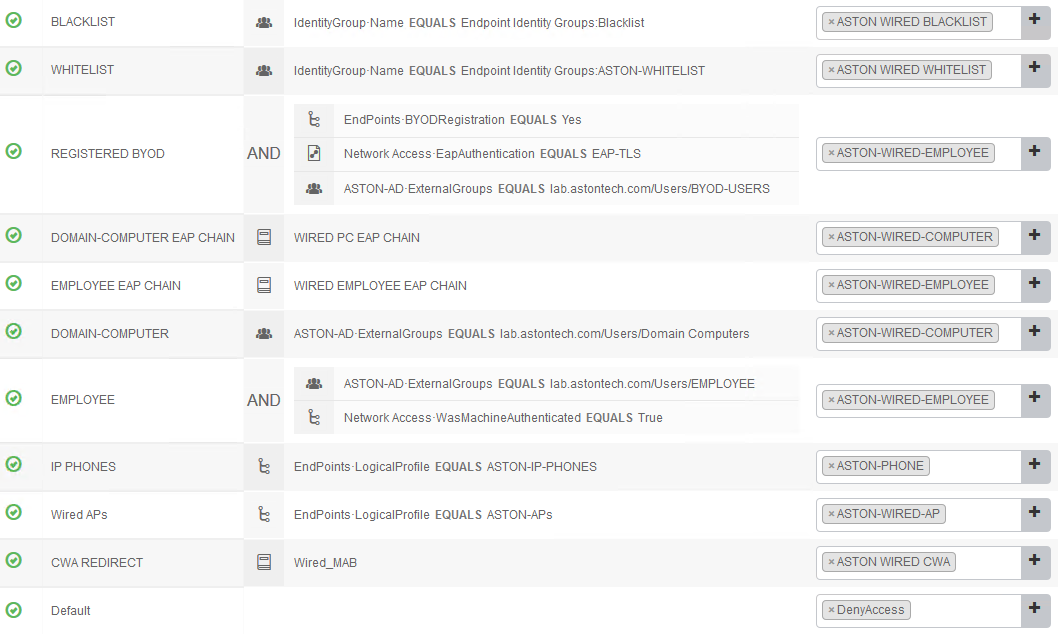
Now we want to create a rule for **REGISTERED-BYOD**. **Insert New Rule Above** DOMAIN-COMPUTER-EAP-CHAIN. Conditions are **Aston-AD:ExternalGroups Equals ise.astontech.com/Users/BYOD-User** AND **Network Access:EapAuthentication Equals EAP-TLS** AND **EndPoints:BYODRegistration Equals Yes** then **ASTON-WIRED-EMPLOYEE**.



The last one for our CWA redirect is going to go above the Default rule. **Insert Rule Above** the Default rule and name it **CWA-REDIRECT**. Conditions are if **Wired\_MAB** then **ASTON-WIRED-CWA**. Then **Save**.

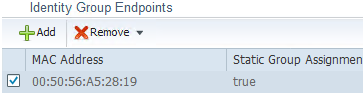


Your **WIRED** Policy Set should look something like this:

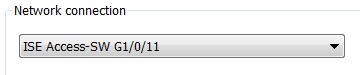


Testing Wired BYOD

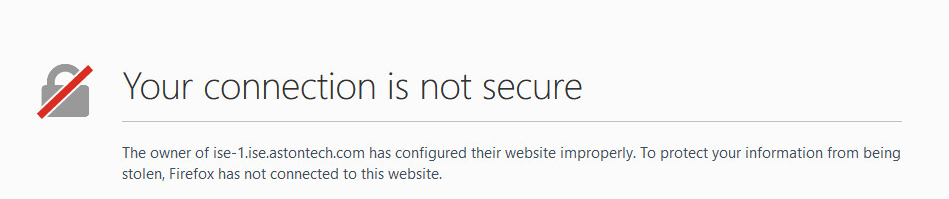
Back in the MAB lab we added LAB-PC-3 to our Whitelist if you didn’t remove it from the Endpoint Id group then we need to do so now. In ISE navigate to **Administration > Identity Management > Groups > Endpoint Identity Groups > ASTON-WHITELIST**. If it’s there tick the checkbox and hit **Remove Selected**.



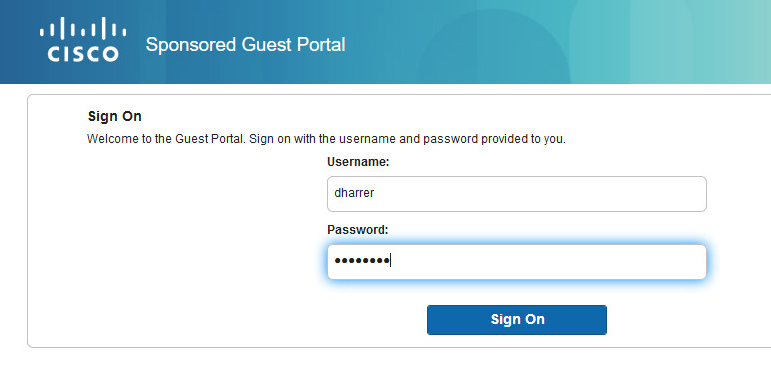
On the Access-SW shutdown port G1/0/11 and turn on terminal monitor to view the authentication log messages. Then Console into LAB-PC-3. Change the Network Adaptor to ISE Access-SW G1/0/11.



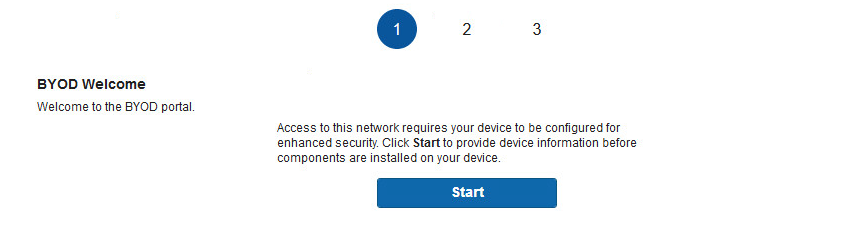
Then no shut the port on the switch. A browser window should open automatically and you will most likely be prompted with a certificate error since we don’t trust the CA yet. Continue and add the exception.



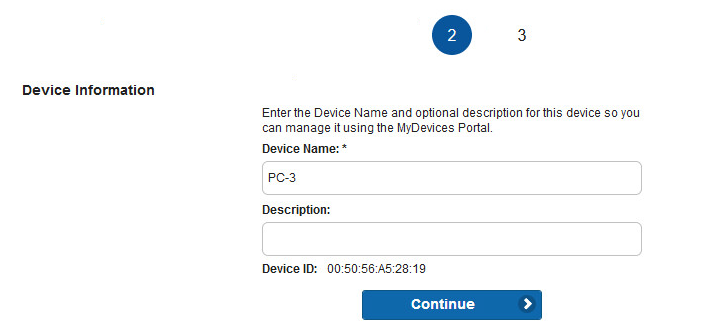
Now we need to step through the onboarding process. Login with your AD credentials.

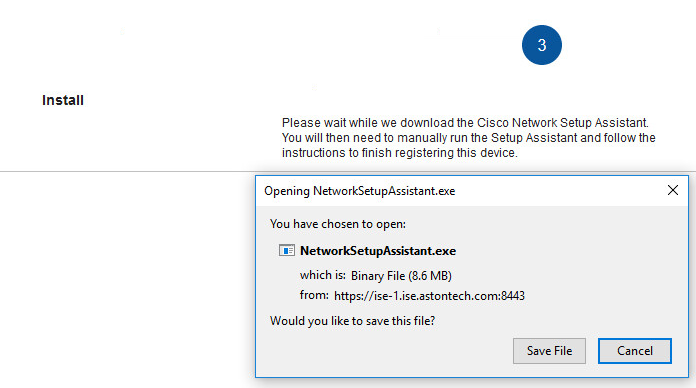


Click **Start**.



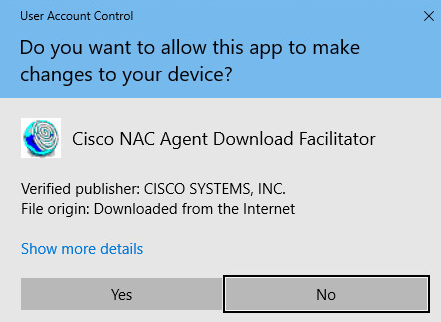
Give the device a name and if you want to include a description add it here. Then Click **Continue**.



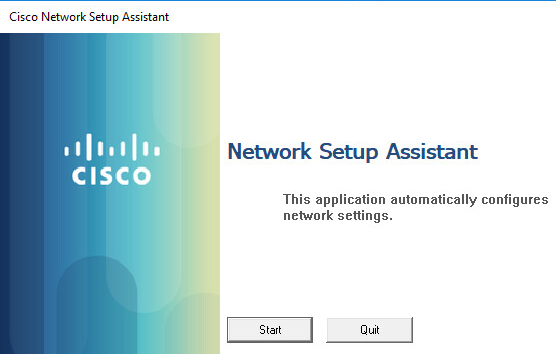
Click **Save** on the Network Setup Assistant prompt.

Run the executable once it’s downloaded.

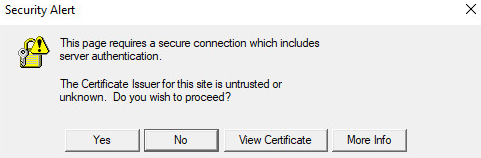
Click **Yes**.



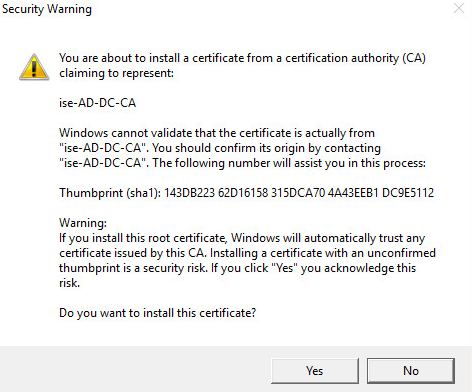
**Start** the Network Setup Assistant.



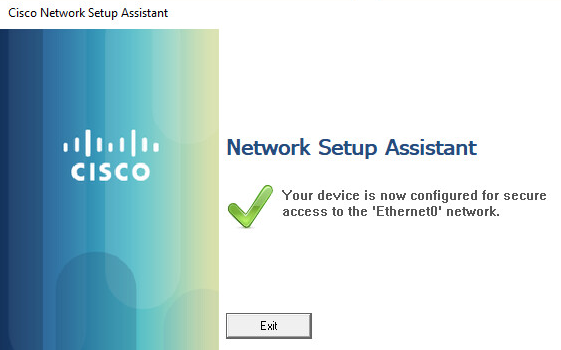
Select **Yes** on the Security Alert prompt.



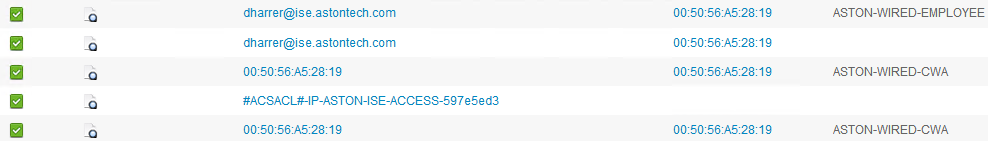
This is going to install our Root Certificate. Click **Yes**.



That’s it. You should have now successfully authenticated to the network. Click **Exit** on the setup wizard.



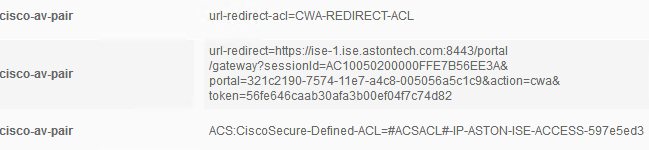
Let’s look at ISE to see what just happened. Head over to the **Live Logs**. We can see that we that first we authenticated via MAB then once the setup wizard finished we switched over to EAP-TLS.



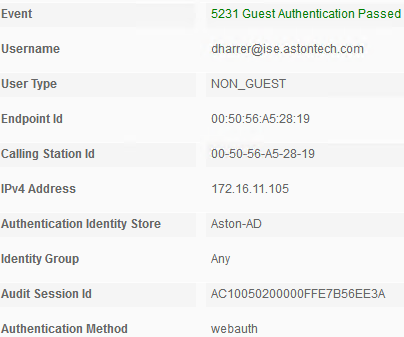
If we look at the details on the first auth we can see that we matched the MAB authC policy, CWA-REDIRECT authZ policy and the result was ASTON-WIRED-CWA.



If we look at the Result section. We see that we are sending the dACL, redirect ACL, and the redirect URL.



Then look if we look at the second one from the top. This is where we authenticated in the web portal.

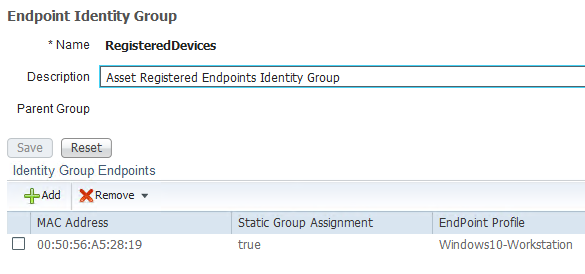


Then finally the last auth we switched to EAP-TLS. Matched the REGISTERED-BYOD authZ policy and we were given ASTON-WIRED-EMPLOYEE authorization profile.

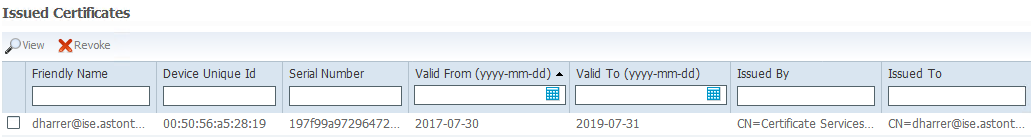




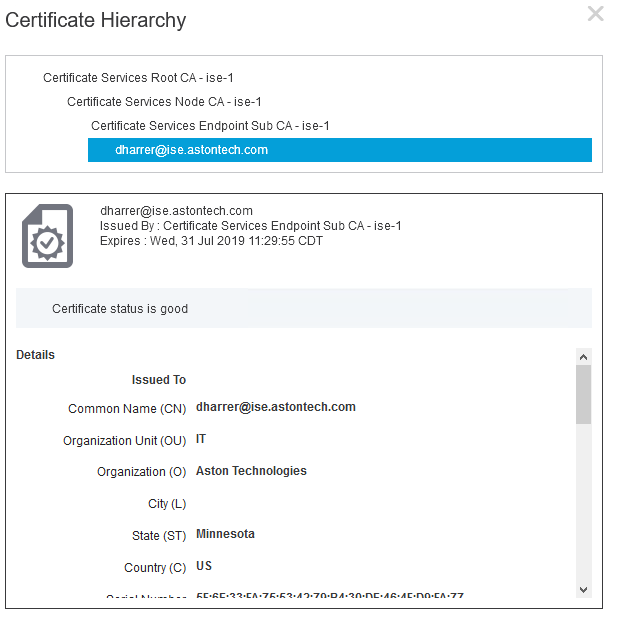
Now our LAB-PC-3 should be in the RegisteredDevices Identity Group. Navigate to **Administartion > Identity Management > Groups > Endpoint Identity Groups > RegisteredDevices**.



We can check the ISE CA and look at the certificate that was issued. Navigate to **Administration > Certificates > Certificate Authority > Issued Certificates**.

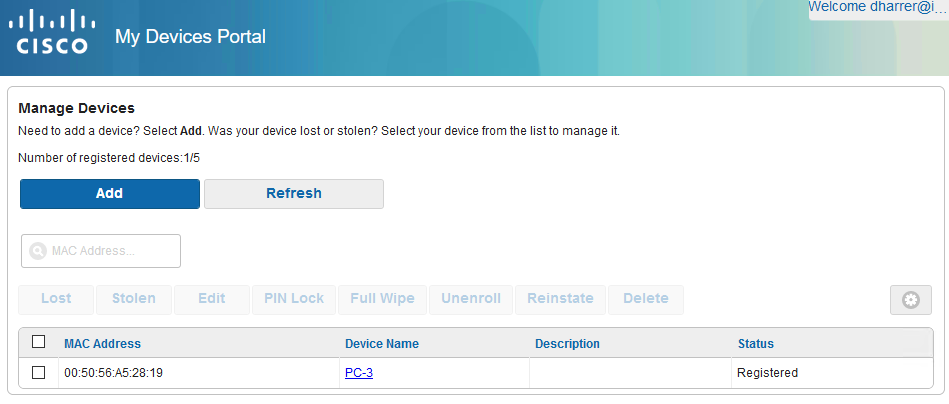


We can view the cert as well. If you click on the checkbox in front of the cert and hit **View**.



Lastly let’s look at the My Devices Portal. In a browser go to <https://mydevices.lab.astontech.com/> and **Login**.

Here we can see our devices, add new ones or we can mark it if it gets lost or stolen to deny network access.



Conclusion

In this lab, we have:

* Created the prerequisite conditions in ISE for our BYOD policy
  + Identity Source Sequence
  + Added BYOD-User AD group
  + Created a Certificate Template for the ISE internal CA
  + Configured NSP client provisioning
* Configured the BYOD My Devices Portal
* Configured a Guest Portal for authentication
* Configured ISE BYOD policy:
  + Created dALCs
  + Authorization Profiles
  + Added the Redirect ACL to the Access-SW
  + Configured Authorization policies
* Tested the wired BYOD onboarding process

In the next lab, we are going to cover wireless BYOD with a single SSID.