|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Wireless BYOD Dual SSID |
| An Aston training document explaining how to deploy wireless BYOD with dual SSIDs |

Contents

[Contents 2](#_Toc37016067)

[Lab Diagram 3](#_Toc37016068)

[WLC Configuration 4](#_Toc37016069)

[Add New SSID 4](#_Toc37016070)

[Create ACL 6](#_Toc37016071)

[ISE Configuration 8](#_Toc37016072)

[Authorization Profiles 8](#_Toc37016073)

[Policy Set 9](#_Toc37016074)

[Onboarding BYOD Devices 10](#_Toc37016075)

[Windows 10 10](#_Toc37016076)

[Android Tablet 15](#_Toc37016077)

[Apple iPad 21](#_Toc37016078)

[Conclusion 28](#_Toc37016079)

Lab Diagram



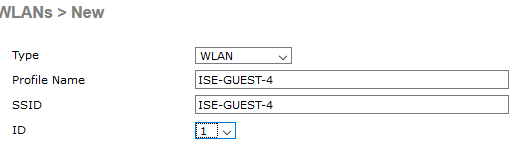
WLC Configuration

Add New SSID

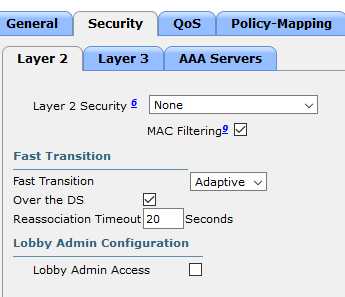
We are going to create an SSID that will be dual purposed as in we are going to use it for Guest access in a later lab as well. Log into the WLC and go to **WLANs**. Select **Create New** then hit **Go**.



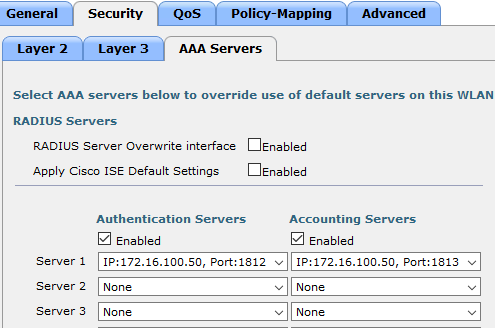
Name it **ISE-GUEST-(x)** then hit **Apply**.



Hit **Apply**. Go to the **Security** tab and set the **Layer2 Security** to **None**. Check the **MAC filtering** checkbox.



Go to **AAA Servers** and add ISE for **Authenticatio**n and **Accounting** Servers.

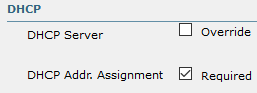


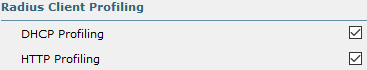
Go to the **Advanced** tab.

Check:

* Allow AAA Override
* DHCP Addr. Assignment Required
* Under Radius Client Profiling check:
  + DHCP Profiling
  + HTTP Profiling
* Change the NAC State to ISE NAC





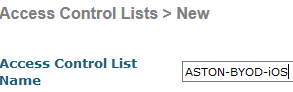




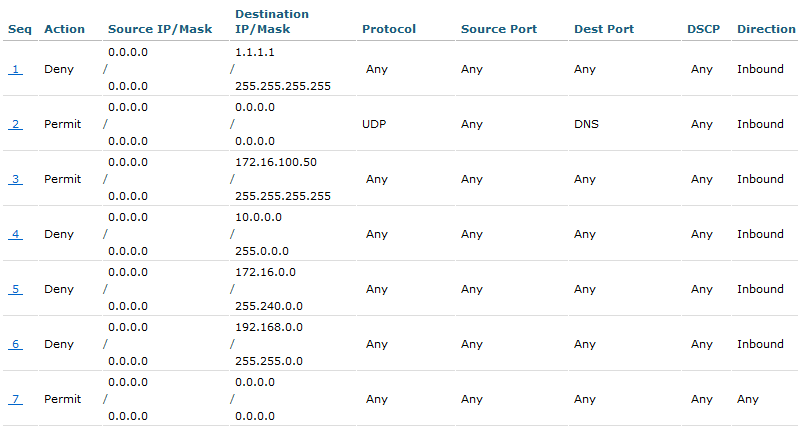
Hit **Apply** and **Save Configuration**.

Create ACL

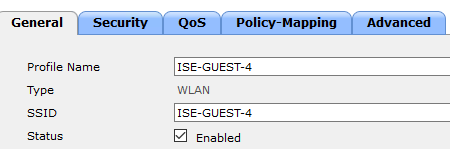
Go to **Security > Access Control Lists** and click **New**. Name it **ASTON-BYOD-iOS** and add the following entries:



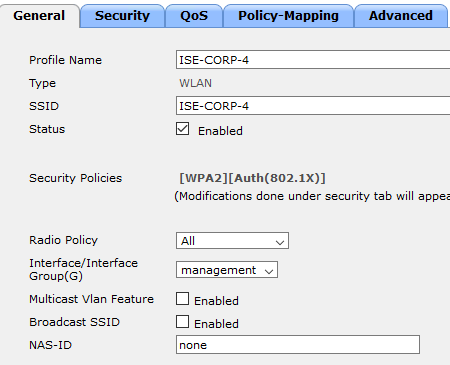
Click into **ASTON-BYOD-iOS** and create the following rules:



Go to **WLANs** click into **ISE-GUEST-(x)** and in the **General** tab, check the **Status Enabled** checkbox.



At this point we can also we can stop broadcasting our **ISE-CORP-(x)** SSID. Click into **ISE-CORP-(x)** and in the **General** tab, uncheck **Broadcast SSID**.



Then **Save Configuration**.

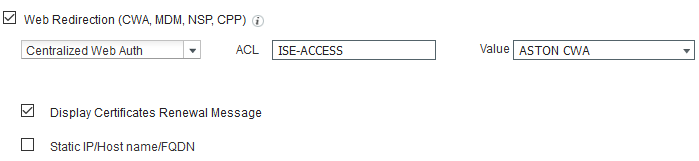
ISE Configuration

Authorization Profiles

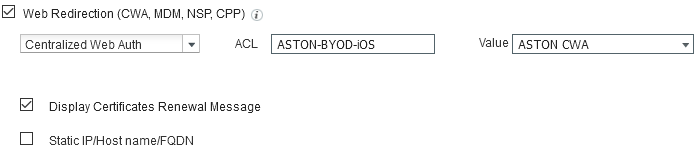
Most of the ISE configuration is already in place from the previous BYOD labs. We only need to add a few Authorization Profiles then build our authC and authZ policies. Log in to ISE and go to **Work Centers > BYOD > Policy Elements > Results > Authorization Profiles**. Click **Add** and name it **ASTON-WIRELESS-CWA**.



In the Common Tasks section check **Web Redirection**. We want to do **Centralized Web Auth**, the redirect ACL is **ISE-ACCESS** that is configured on the WLC and the Value is the guest portal we set up in the wired BYOD lab – **ASTON-CWA**. Then **Submit**.



Duplicate the Profile we just created and name it **ASTON-BYOD-iOS**. All we need to change here is the redirect ACL to match the iOS one we created earlier on the WLC. Then **Submit**.

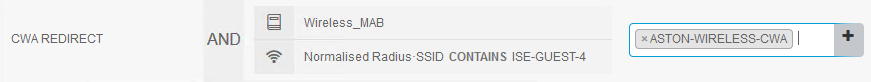


Policy Set

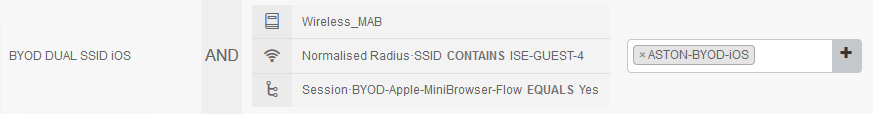
First, we need to add an Authentication policy for wireless MAB. Go to **Policy Sets > WIRELESS** and insert a rule above the **Default**. Name it **MAB**. Conditions we want to match is **Wireless\_MAB** and Allowed Protocols will be **MAB-HOST-LOOKUP**. Then we need to change Identity Source to **Internal Endpoints** and set it to **Continue** If user not found.



We also need to add an Authorization policy to force the redirect to our CWA portal. Insert a rule above the **Default**. Name it **CWA-REDIRECT**. For the conditions we want to match on **Wireless\_MAB AND Normalised Radius:SSID CONTAINS ISE-GUEST-(x)**. Then for Permissions give it **ASTON-WIRELESS-CWA**.



Now we need to create a policy for our iOS devices for the mini browser (CNA). **Duplicate above** the on the **CWA-REDIRECT** rule we just created. Name it **BYOD-DUAL-SSID-iOS**. The Condition we want to add is **Session:BYOD-Apple-MiniBrowser-Flow EQUALS Yes**. Note: This is a new condition in ISE 2.2 for this particular use case. Then for Permissions give it **ASTON-BYOD-iOS**.

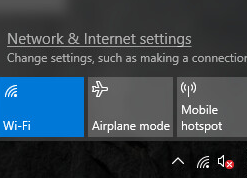


**Save**. That’s it. We already created the **BYOD-REGISTERED** rule that we will match once we get the device gets onboarded.

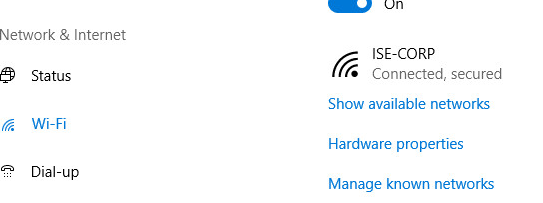
Onboarding BYOD Devices

Windows 10

We are ready to start to test out the dual SSID solution but first we are going to need to remove the credentials that we installed in the last lab. Console into LAB-PC-3. Click on your wireless adaptor in the task bar and click **Network & Internet Settings**.



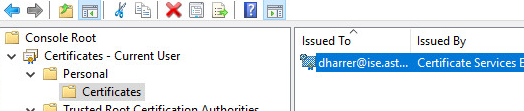
Go to **Wi-Fi** and then click **Manage known networks**.



Click on **ISE-CORP-(x)** and hit **Forget**.



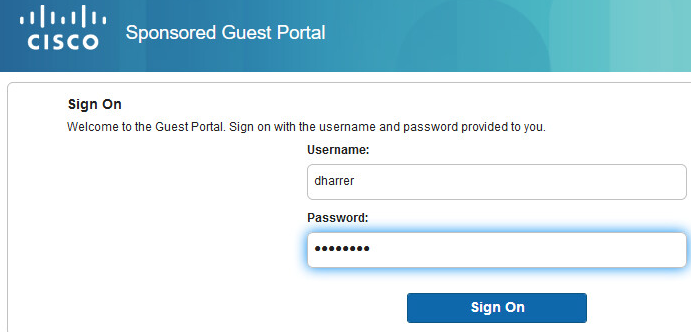
Open MMC and remove the certificate that was installed previously.



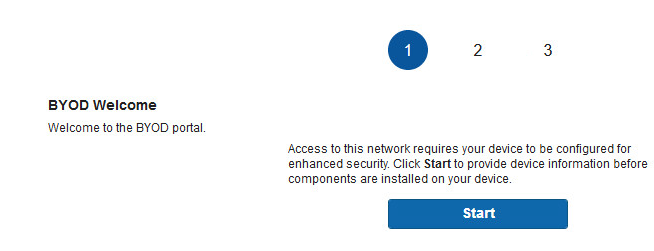
Log in to <https://mydevices.lab.astontech.com/> and Delete all the devices.



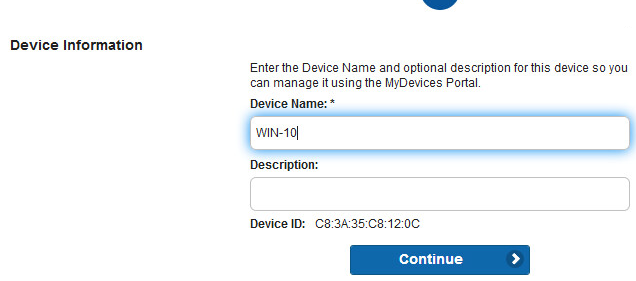
Alright we are ready to test. On ISE-PC-3 connect to the **ISE-GUEST-(x)** SSID, a browser should automatically open and you’ll be redirected to the guest portal. Provide your credentials and hit **Sign On**.



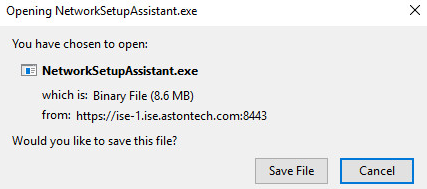
Hit **Start**.



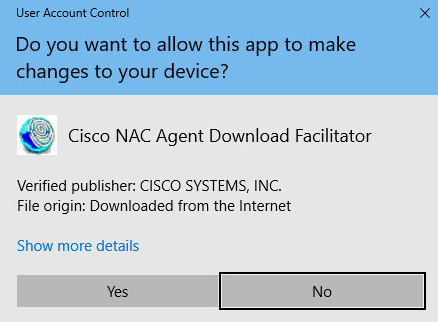
Provide a **Device Name**.



Save the **Network Setup Assistant** and then **Run** it.



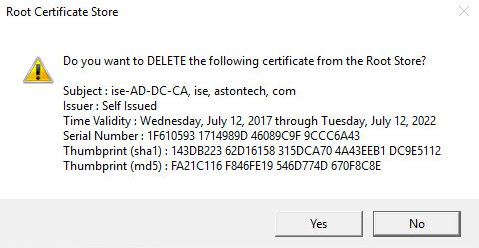
Click **Yes** to continue.



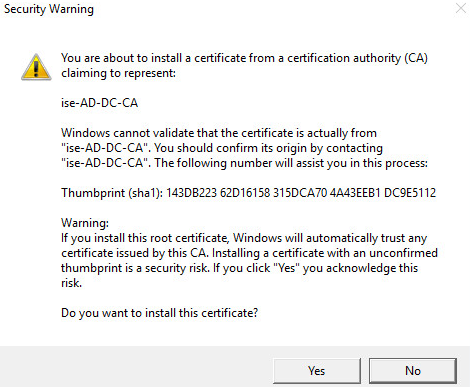
Hit Start to configure the Network Settings.



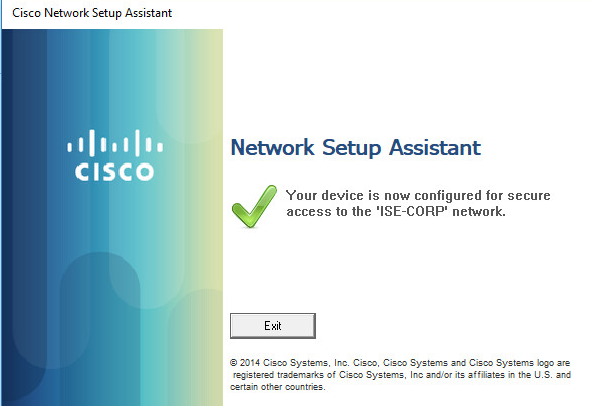
Hit **Yes** to Delete the Root Certificate.

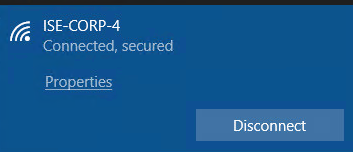


Hit **Yes** to install the Root Cert.



**Boom!** You should be connected to ISE-CORP-(x) now and have full network access.





You can see here we come in authenticating via MAB then after we get onboarded there at the top we are using our cert with EAP-TLS and get the full access profile.

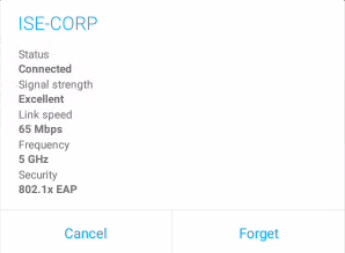


Take a minute to review the ISE logs. Also, look at the client info in the WLC, at My Devices Portal, ISE CA issued certs and Registered devices. Make sure everything is as expected.

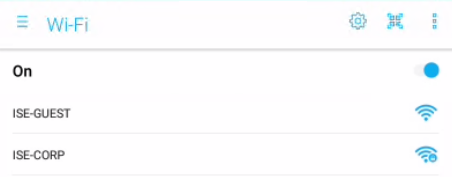
Android Tablet

For this part of the lab just follow along. This is just for you to see the process. We no longer have access to the wireless network for these labs.

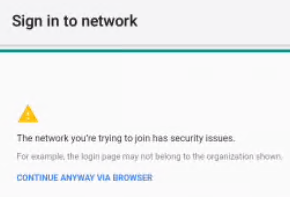
Same as with the Windows host we need to remove the credentials on the Android Tablet from the previous lab. Go to **Settings > Wi-Fi**. Click on **ISE-CORP** and hit **Forget**.



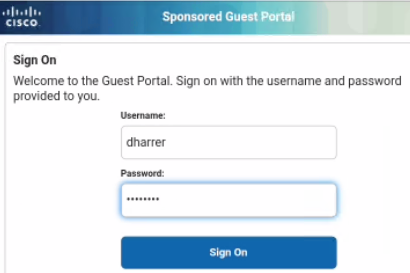
Now Connect to **ISE-GUEST**.



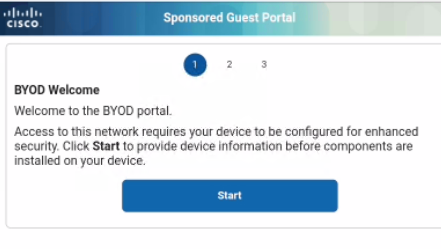
Click **CONTINUE ANYWAY VIA BROWSER**.



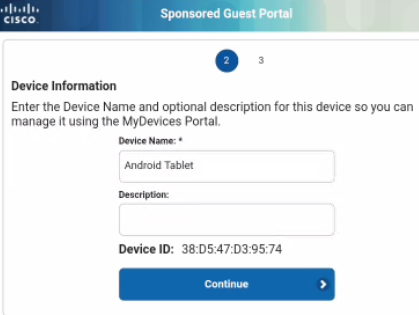
**Sign in** to the portal.



Hit **Start**.



Enter a **Device Name**.



Now hit the home button then Click on the Network Setup Assistance icon.

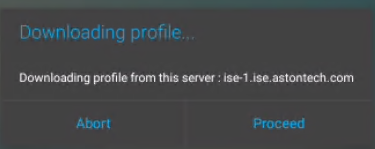




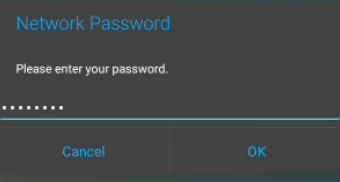
**Start** the Network Setup Assistant.



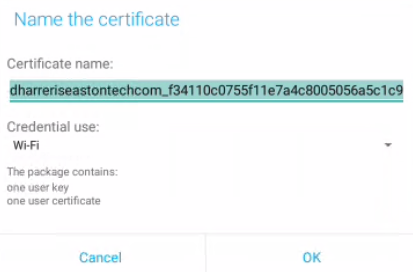
Click **Proceed**.



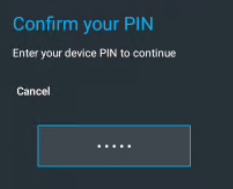
Enter your **AD** password and hit **OK**.



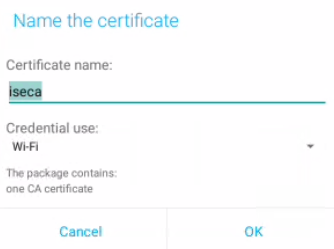
Change Credential use to **Wi-Fi** and hit **OK**.



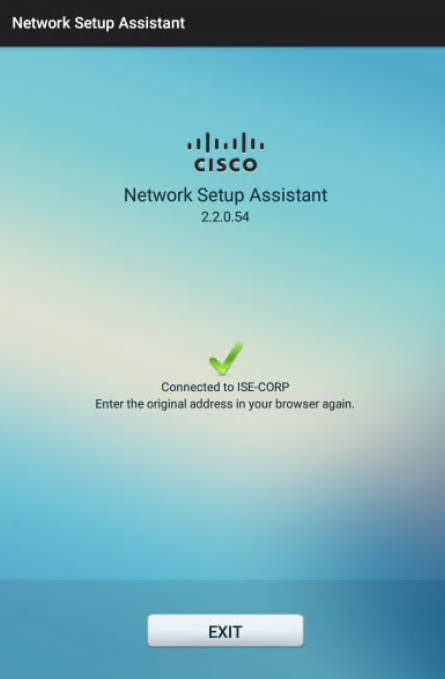
Enter **123456** and hit **OK**.



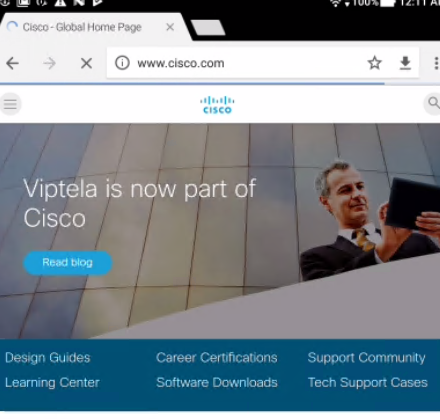
Change Credential use to **Wi-Fi** and hit **OK**.



The onboard process is complete. Hit **Exit**. You should now be connected to ISE-CORP.



Yay, we can get to cisco.com.



A quick look at the Live Logs and we see what we expect to see.



Take a minute to review the ISE logs. Also, look at the client info in the WLC, at My Devices Portal, ISE CA issued certs and Registered devices. Make sure everything is as expected.

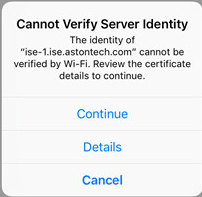
Apple iPad

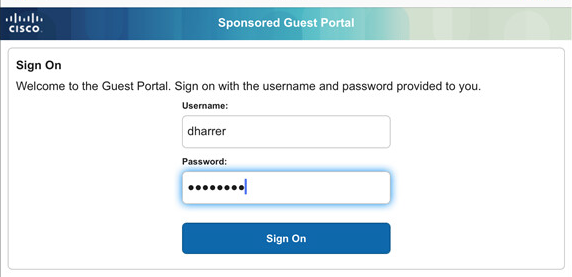
For this part of the lab just follow along. This is just for you to see the process. We no longer have access to the wireless network for these labs.

Before you begin and try to onboard the iPad have your mentor reset it for you. Since we aren’t using well known certificates the iPad seems to have an issue when you delete the profile and try to connect again.

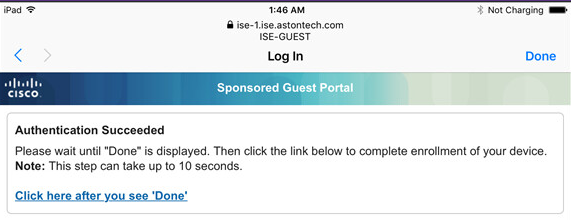
Apple iOS 10.3.x has a few known issues with ISE BYOD onboarding that disrupt the flow which are supposed to be fixed with iOS 11. So for now, we are going to have to deal with it.

Go to **Settings > Wi-Fi** and connect to **ISE-GUEST**. Click **Continue**.

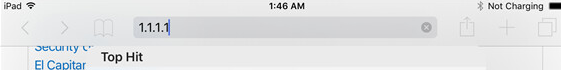


**Sign in** to the Portal.  


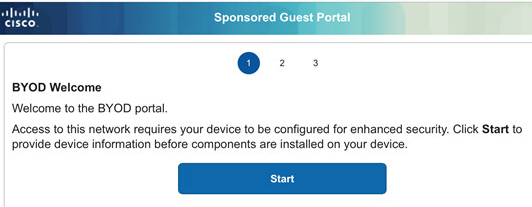
When you get to this screen, just leave it alone and hit the **home** button. You should be able to hit Click here after you see ‘Done’ but this isn’t working with this code version.



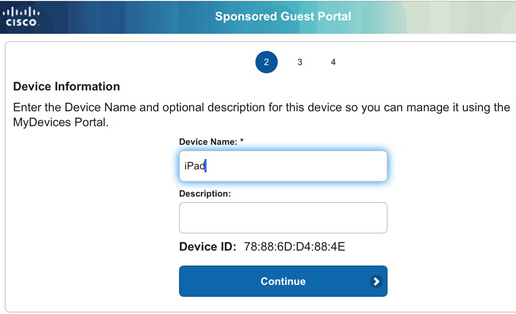
Open **Safari** and go to **1.1.1.1**.



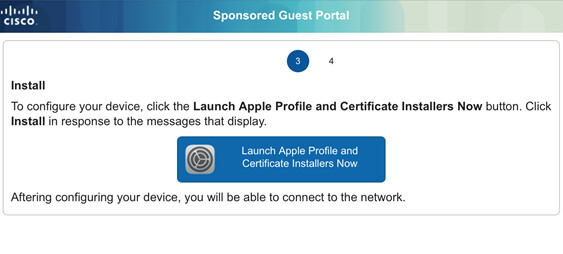
You should get redirected to the Portal Page. Hit **Start**.



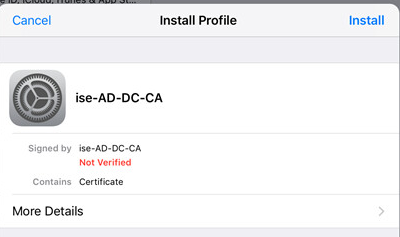
Enter a **Device Name**.



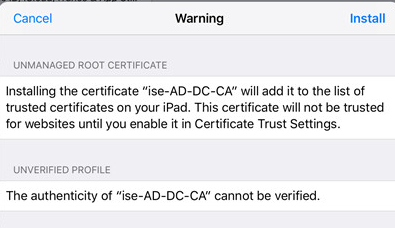
Click **Launch Apple Profile and Certificate Installers Now** button.



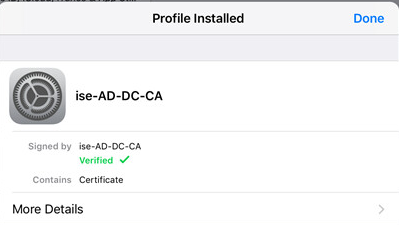
Hit **Install** to install the Root Cert.



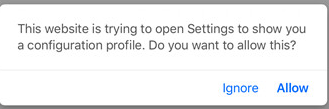
Hit Install again.



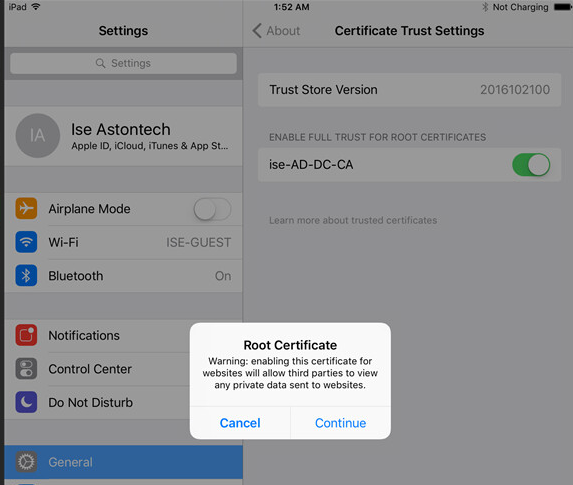
Hit **Done**.



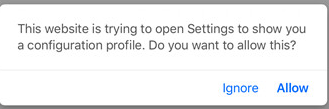
When you see this prompt for the second time go to **Settings > General > About > Certificate Trust Settings** and enable our Root Cert.



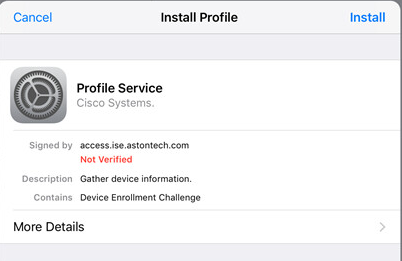
Hit **Continue**.



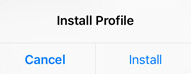
Double tap the Home button and go back to the previous page. Then hit **Allow**.



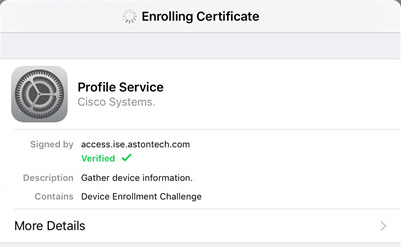
Hit **Install**.



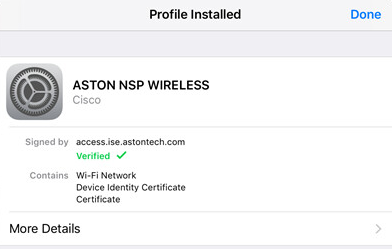
Hit **Install** once more.



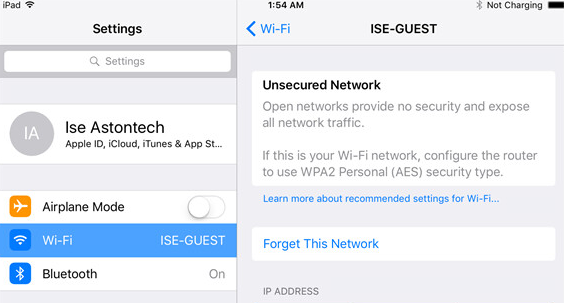
You should see it going through the Enrollment process at this point.



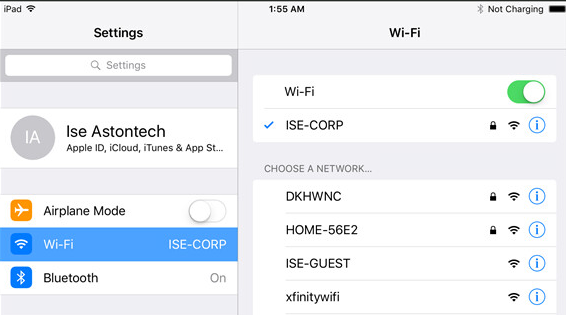
When it’s finished hit **Done**.



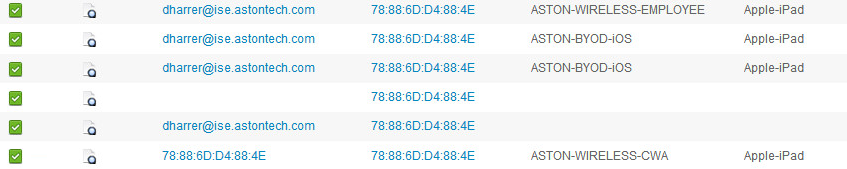
Go to **Settings > Wi-Fi > ISE-GUEST** and hit **Forget this Network**.



Now you automatically connect to ISE-CORP.



A quick look at the Live Logs and we see what we expect to see.



Conclusion

In this lab, we have:

* Configured an SSID for Guest on the WLC
* Added an ACL on the WLC for our Apple iPad use case
* Configured Authorization Profiles for wireless CWA and for iOS devices on ISE
* Created authentication policy for wireless MAB on ISE
* Created authorization policy for CWA redirect and iOS with dual SSIDs
* Onboarded and tested three different common BYOD device types:
  + Windows 10 host
  + Android tablet
  + Apple iPad

In the next lab, we are going to start working on our guest access flows.