|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Sponsored Guest Access |
| An Aston training document explaining how to deploy Sponsored Guest Access on Cisco ISE |

Contents

[Contents 2](#_Toc4756200)

[Lab Diagram 3](#_Toc4756201)

[ISE Configuration 4](#_Toc4756202)

[Identity Groups 4](#_Toc4756203)

[Portals & Components 5](#_Toc4756204)

[Policy Elements 13](#_Toc4756205)

[Policy Set 13](#_Toc4756206)

[Testing Sponsored Guest 15](#_Toc4756207)

[Windows 10 Wired 15](#_Toc4756208)

[Windows 10 Wireless 19](#_Toc4756209)

[Android Tablet 21](#_Toc4756210)

[Conclusion 27](#_Toc4756211)

Lab Diagram

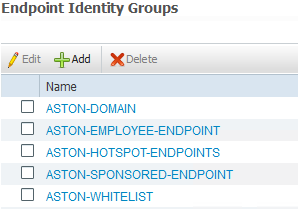


ISE Configuration

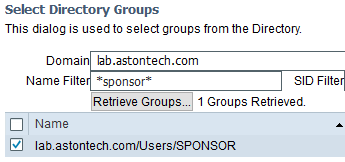
Identity Groups

We are going to add two Identity Groups. One for our Sponsored endpoints and the other for our employee’s guest internet access.

Log in to ISE and go to **Work Centers > Guest Access > Identity Groups > Endpoint Identity Groups**. **Add** one named **ASTON-EMPLOYEE-ENDPOINT** and another named **ASTON-SPONSORED-ENDPOINT**.

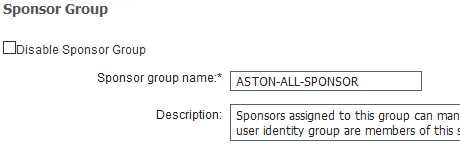


We need to add a group from AD that can “sponsor” guest access. We have a group in AD called **Sponsor**. Go to **Ext Id Sources > Active Directory > Groups** and Add it to list if you haven’t already.

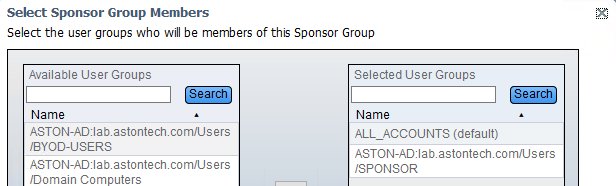


Portals & Components

Go to **Portals & Components > Sponsor Groups**. Click on **ALL\_ACCOUNTS** and **Duplicate**. Name it **ASTON-ALL-SPONSOR**.



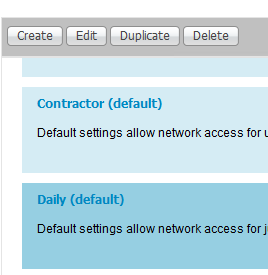
In the **Match Criteria** Section click **Members**. Add the **Sponsors** AD group we just added to ISE.



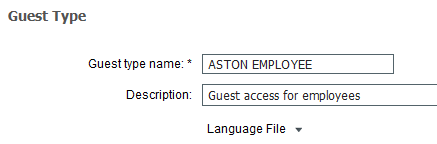
Now we want to add some a couple Guest Types but they haven’t been created yet. However, they were nice enough to put a link to the configuration page. Click the link under **Configure Guest Types at**:



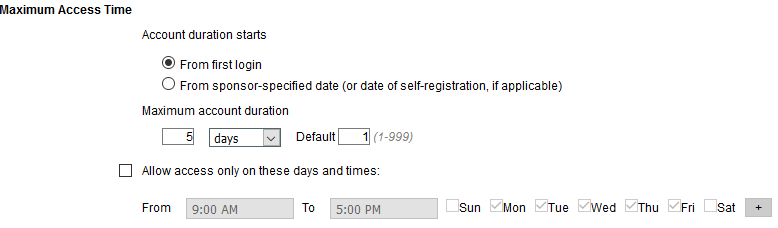
Click on **Daily** and **Duplicate**.



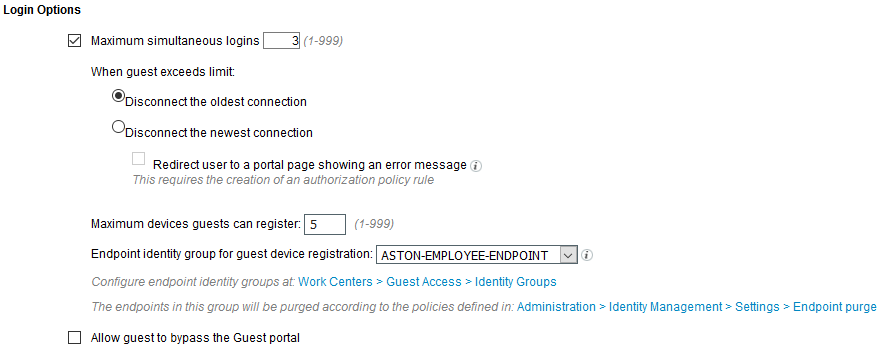
Name it **ASTON EMPLOYEE**.



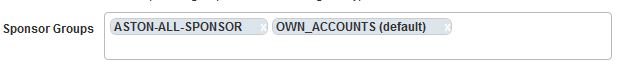
Configure the following for **Maximum Access time**:



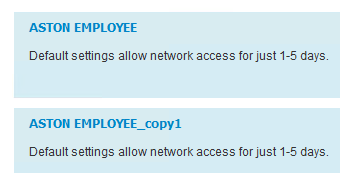
Configure the following for **Login Options**:



**Account Expiration Notification** can remain default since we don’t have an SMS or SMTP server set up. For Sponsor Groups, you can remove all but **OWN\_ACCOUNTS** and **ASTON-ALL-SPONSOR (ALL\_ACCOUNTS (default)\_copy1)**. Then Scroll to the top and **Save**.



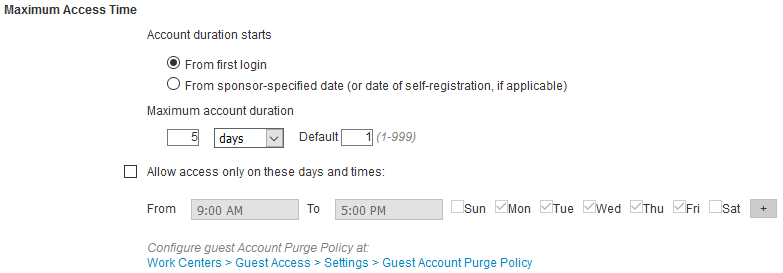
Click **Guest Types** then on **ASTON EMPLOYEE** and **Duplicate** again.



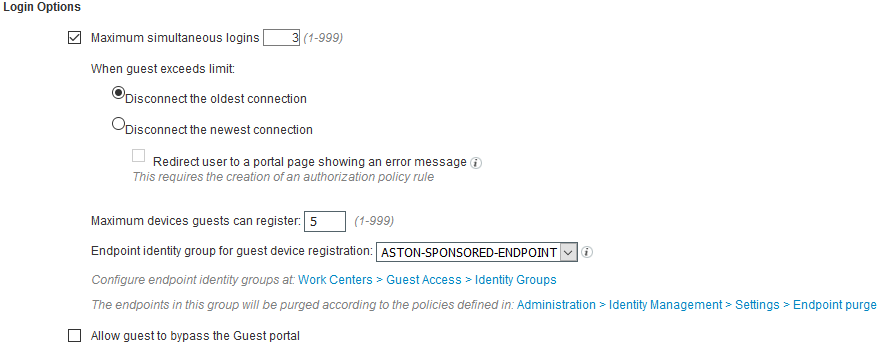
Name it **ASTON 5 DAY PASS**.



Configure the following for **Maximum Access Time**:

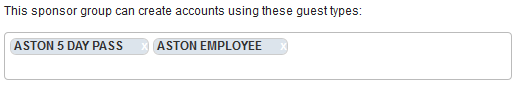


Configure the following for **Login Options**:



**Account Expiration Notification** can remain default since we don’t have an SMS or SMTP server set up. For Sponsor Groups, you can leave default as well. Then Scroll to the top and **Save**.

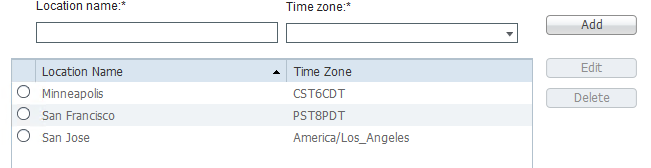
Now go back to the **Sponsor Group ASTON-ALL-SPONSOR** configuration page. Add the **Guest types** we just created. You might have to **Save** then **Close** and click back in for them to show up.



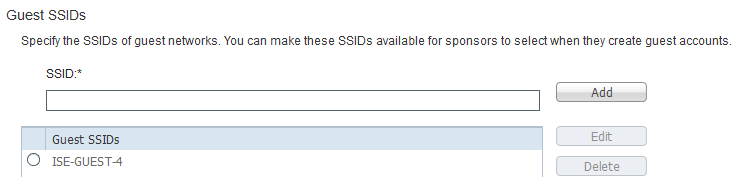
Next, we want to create a couple Guest Location and SSIDs. Again, this is on another page, click the link **Configure guest locations at**:



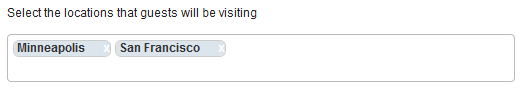
In the new page that has opened for **Guest Locations**, **Add Minneapolis** and **San Francisco**.



In the **Guest SSIDs**, Add our Guest SSID **ISE-GUEST-(x)**. Then **Save**.

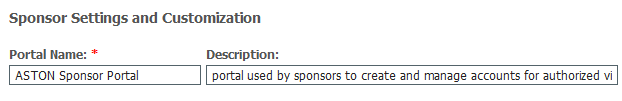


Now back to the **Sponsor Group** page. Add the **Guest Locations** we just created. Again, you might have to **Save** then Close and click back in for them to show up.

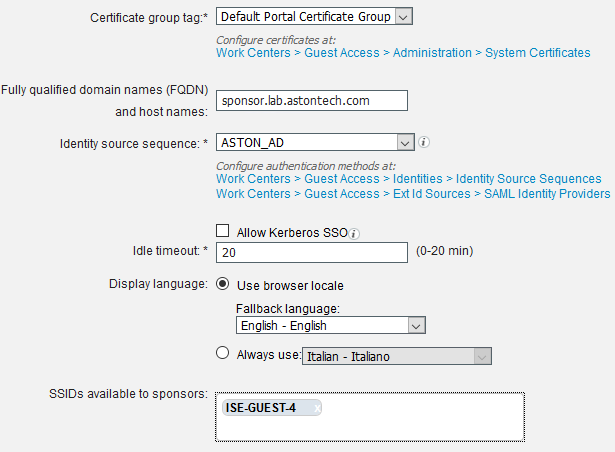


We can leave everything else default since we don’t have SMTP or SMS configured. Scroll to the top and click **Save**.

Let’s create a Sponsor Portal. This is the portal that our sponsors will log in to in order to manage guest accounts. Go to **Sponsor Portals**. Duplicate the default **Sponsor Portal**. Name it **ASTON Sponsor Portal**.



Expand **Portal Settings**. Add a **FQDN** called **sponsor.ise.astontech.com**. Since we only want AD users to manage this portal change the **Identity source sequence** to **ASTON\_AD**. Change the **Idle timeout** to **20**. Add our guest **SSID** to be available to sponsors.



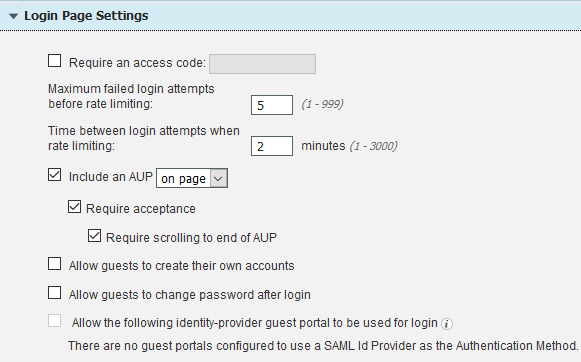
You can choose not to display the AUP if you like otherwise scroll to the top and **Save**.

Before we go any further, the **FQDN** we just added to the sponsor portal needs to be resolvable. Console into your AD server and add it to **DNS**.

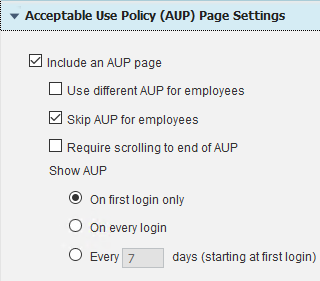
Now let’s configure our CWA portal for Guest Access. Go to **Guest Portals > ASTON CWA**. Expand **Portal Settings** and change **Employees using this portal as** **guests** to **ASTON EMPLOYEE**.



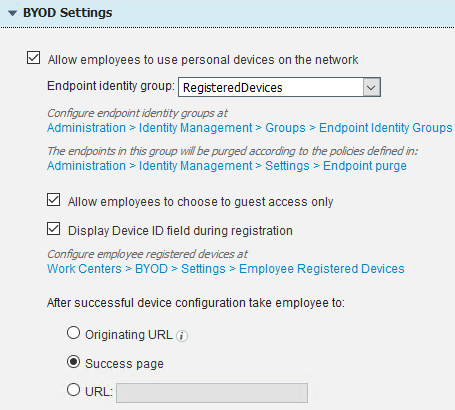
Expand **Login Page Settings** and configure the following:



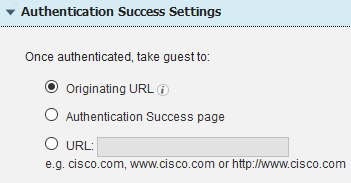
Expand Acceptable Use Policy (AUP) Page Settings and configure the following:



Expand **BYOD Settings** will need to check the box that says **Allow employees to choose to guest access only**.



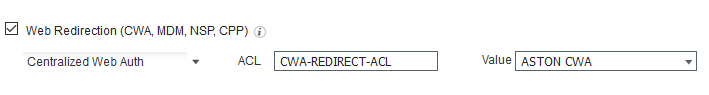
Expand **Authentication Success Settings** and click **Originating URL**.



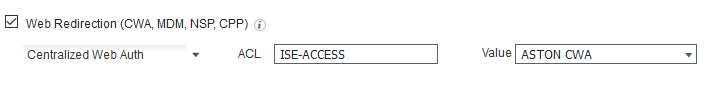
Everything else can remind the default. Scroll up to the top and click **Save**.

Policy Elements

We’ll need to edit our redirect CWA Authorization Policies back to redirect endpoints to the sponsor portal. Go to **Policy Elements > Results > Authorization Profiles**. Click on **ASTON-WIRED-CWA** and change the **Web Redirection** to **ASTON WIRED CWA**. Then **Save**.

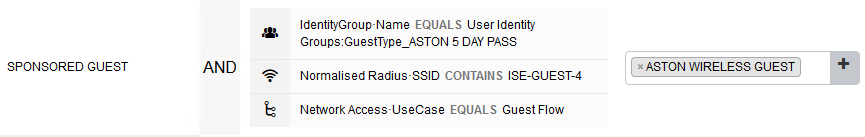


We’ll need to the same for wireless. Click on **ASTON-WIRELESS-CWA** and edit it. Then **Save**.

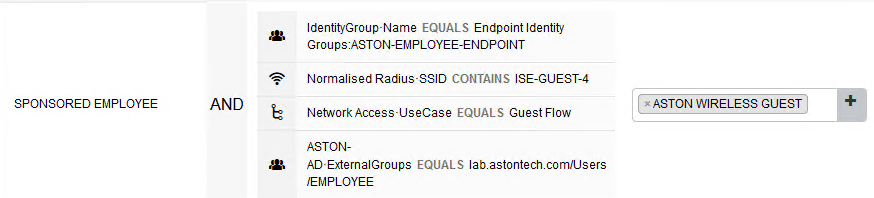


Policy Set

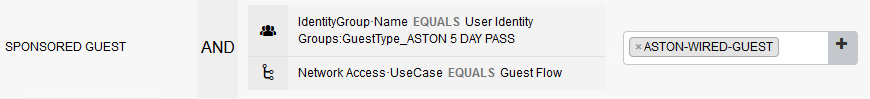
Now we are ready to create our policy. Go to **Policy Sets > WIRELESS**. On our **HOTSPOT** rule click the **Gear icon** and **Insert New Rule Above**. Name it **SPONSORED GUEST**. The Conditions we want to match on are **User Identity Groups:GuestType\_ASTON 5 DAY PASS** AND **Normalised Radius:SSID CONTAINS ISE-GUEST-(x)** AND **Network Access:UseCase EQUALS Guest Flow**. Then for Permissions give it **ASTON-WIRELESS-GUEST**.



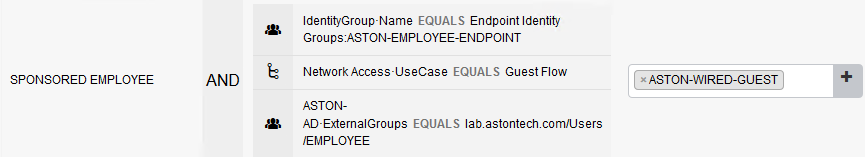
Now for the employee guest. **Insert New Rule Above** SPONSORED GUEST and name it **SPONSORED EMPLOYEE**. The Conditions we want to match are **Endpoint Identity Groups:ASTON-EMPLOYEE-ENDPOINT** AND **Normalised Radius:SSID CONTAINS ISE-GUEST-(x)** AND **Network Access:UseCase EQUALS Guest Flow** AND **Aston-AD:ExternalGroups EQUALS lab.astontech.com/Users/Employee**. Then for Permissions give it **ASTON-WIRELESS-GUEST**.



Now go to the WIRED Policy Set, we need to do pretty much the same thing here. Insert New Rule Above HOTSPOT. Name it **SPONSORED GUEST**. The conditions we want to match on are **User Identity Groups:GuestType\_ASTON 5 DAY PASS** AND **Network Access:UseCase EQUALS Guest Flow**. Thenfor Permissions give it ASTON-WIRED-GUEST.



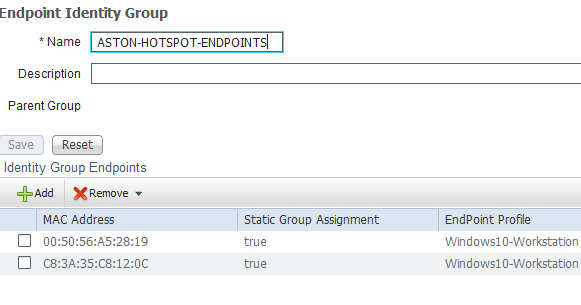
**Insert New Rule Above** SPONSORED GUEST and name it **SPONSORED EMPLOYEE**. The Conditions we want to match are **Endpoint Identity Groups:ASTON-EMPLOYEE-ENDPOINT** AND **Network Access:UseCase EQUALS Guest Flow** AND **Aston-AD:ExternalGroups EQUALS ise.astontech.com/Users/Employee**. Then for Permissions give it **ASTON-WIRED-GUEST**.



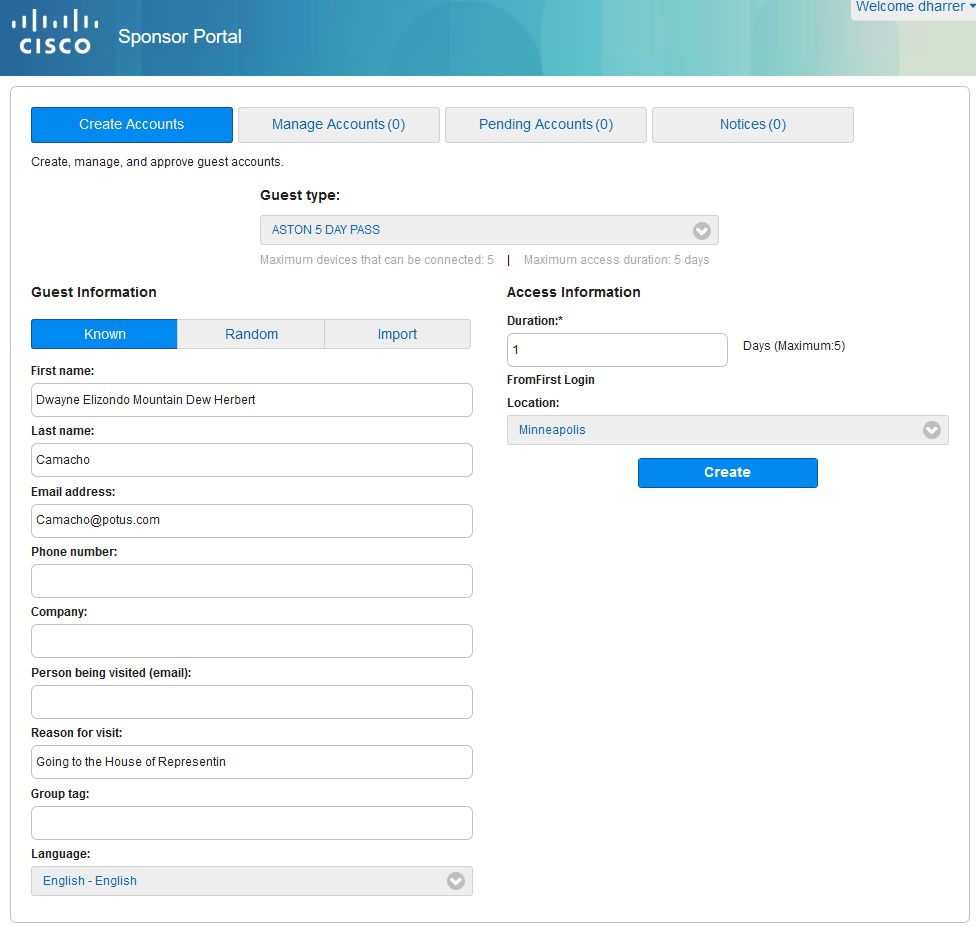
Testing Sponsored Guest

Windows 10 Wired

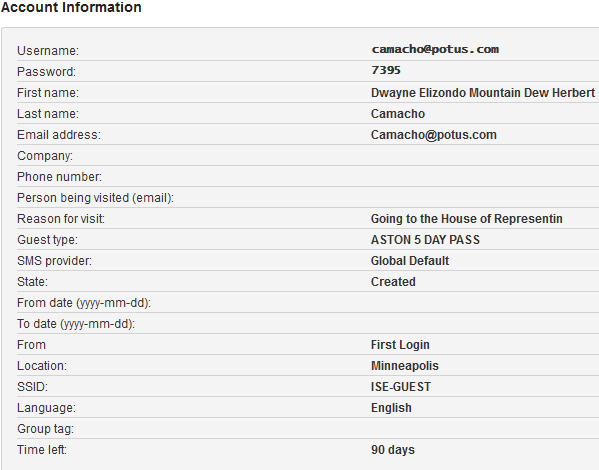
First before we start testing let’s remove any endpoints in **ASTON-HOTSPOT-ENDPOINTS** from the previous lab.



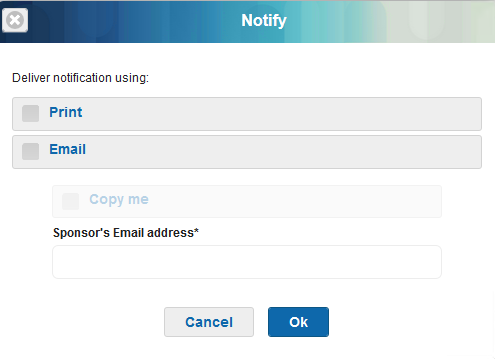
Now go to <https://sponsor.lab.astontech.com/> and sign in with your AD account. Here is where we create/manage guest accounts. You’ll notice that we have the option to select either of our two Guest types, Locations and the Duration for this guest account. Go ahead and create a guest and give them the **ASTON 5 DAY PASS** Guest Type.



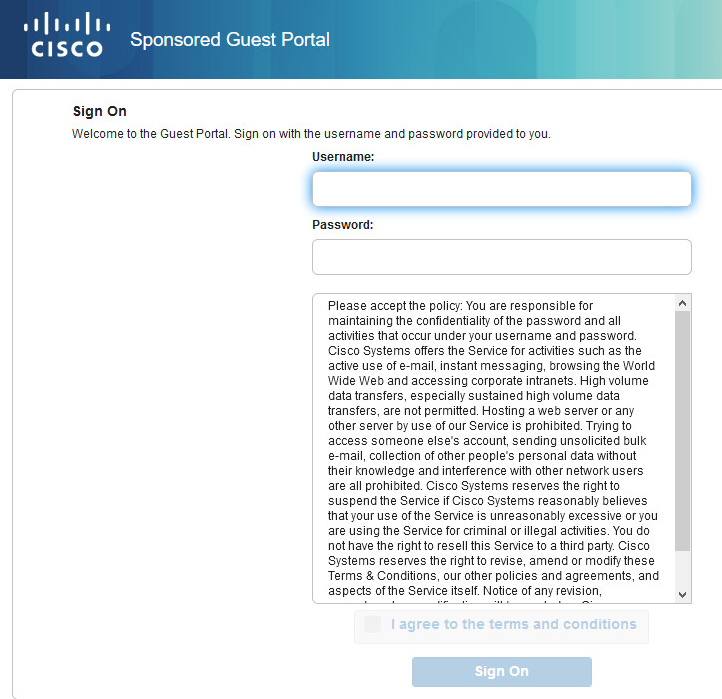
After you create the account you be presented with the **Account information** with Username and Password.



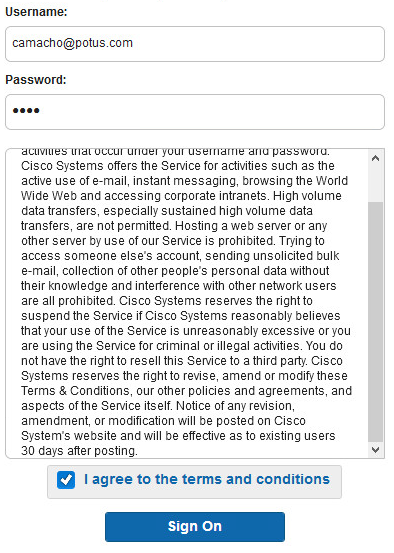
Down at the bottom there is the **Notify** button, you can select to Print or Email. Note this could be set up to send a notification automatically if we had SMTP configured.



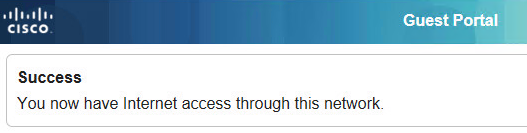
Let’s test this account out on LAB-PC-3. Console into LAB-PC-3 **disable** both the **Ethernet0** and **Wireless** adaptors. Log in to **ISE-ACCESS-SW** and **shut/no shut** port **g1/0/11**. Now on LAB-PC-3 **enable Ethernet0**. You should get a browser popup with the Guest Portal Sign On page.



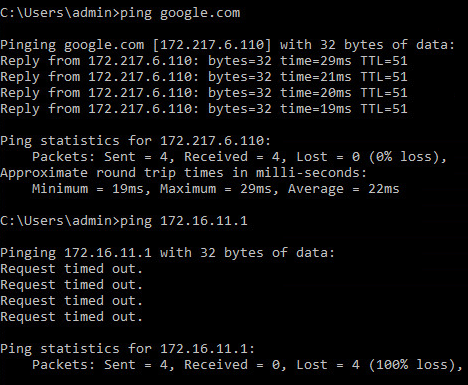
Enter your guest **Username** and **Password**. Agree to the terms and hit **Sign On**.



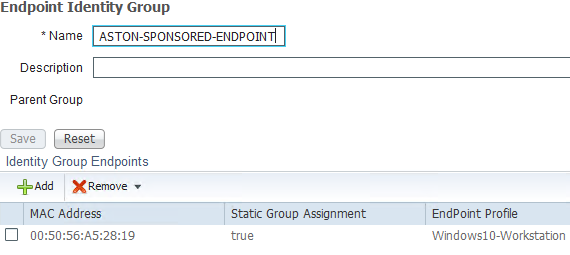
You should get a success page or be redirected to the page that you were on previously.



You should have access to the internet and nothing else. A quick test shows we can get to Google but not our own default gateway.



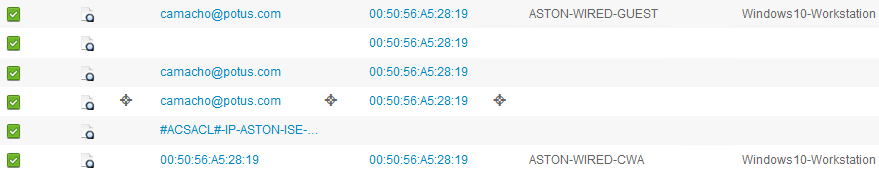
If we look at our **ASTON-SPONSORED-ENDPOINT** Identity Group, we can see that our endpoint has been added.



Now if we go back to the **Sponsor Portal** and look at the guest account we created we can see the clock has started. The **From/To Date** and **Time left** field is now populated.



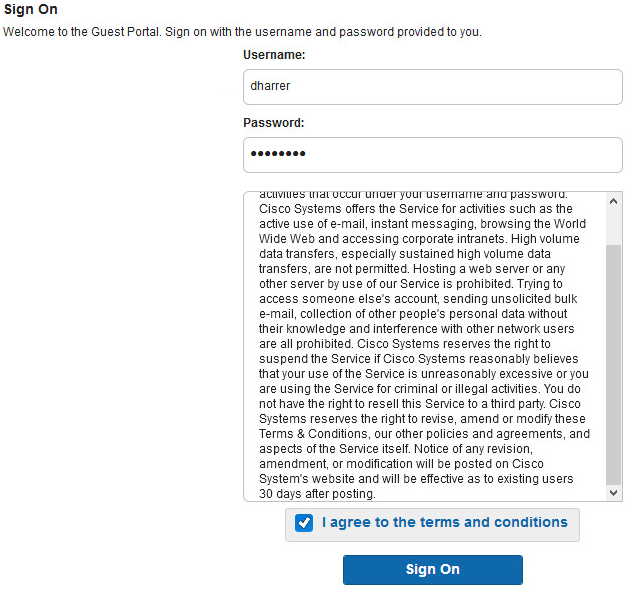
And a quick look at the **Live Logs** shows what we expect to see.



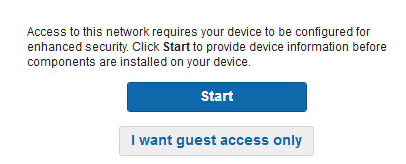
Take a minute to review the ISE logs. Also, run some show commands on the switch to confirm. Make sure everything is as expected.

Windows 10 Wireless

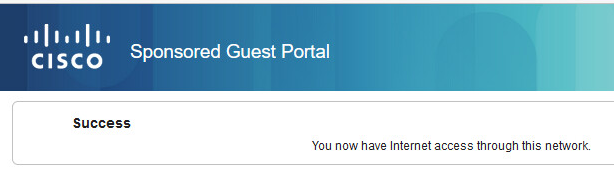
Let’s test our employee guest access policy on this one. Disable **Ethernet0** on LAB-PC-3 and enable the **Wireless** adaptor. Connect to the **ISE-GUEST-(x)** SSID. Again, the portal Sign On page should automatically pop up in a browser. This time enter your **AD** creds and **Sign On**.



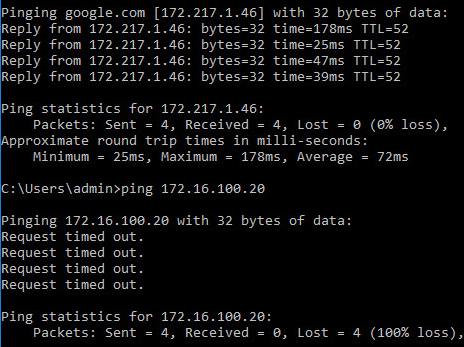
Instead of going through the BYOD onboarding process we just want Internet/Guest access. Click on **I want guest access only**.



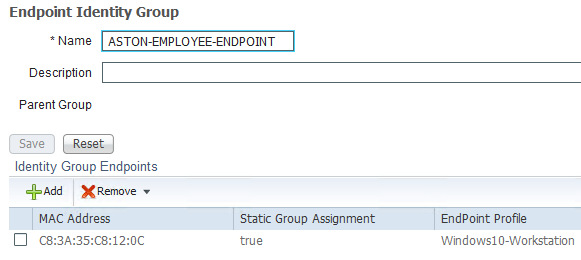
After logging in you should get a success page and you should now have internet access.



A quick test shows we can reach Google but not the AD server.



If we check the **ASTON-EMPLOYEE-ENDPOINT** Identity Group, we see that the endpoint has been added.



And a quick look at the **Live Logs** shows what we are expecting.



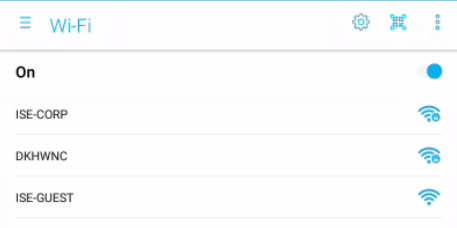
Take a minute to review the ISE logs. Also, look at the client information on the WLC to confirm. Make sure everything is as expected.

Android Tablet

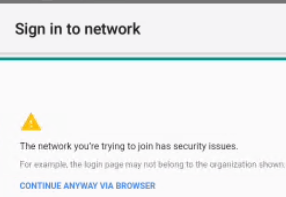
For this part of the lab just follow along. This is just for you to see the process. We no longer have access to the wireless network for these labs.

Let’s try the Android tablet with our guest account. Then we’ll delete the account and see what happens.

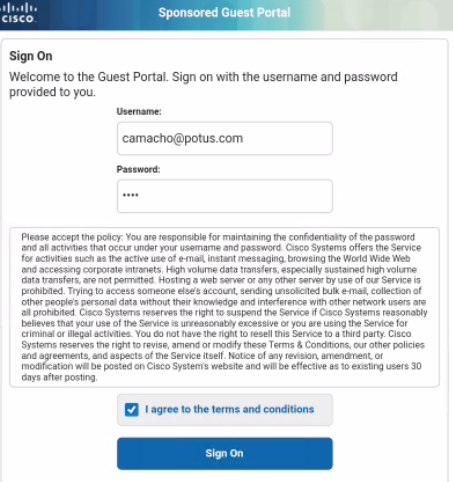
Open the **Vysor** app on your desktop and connect to the tablet. Go to **Settings > Wi-Fi** and connect to **ISE-GUEST** SSID.



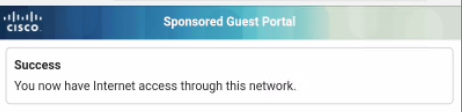
When the browser pops up click **CONTINUE ANYWAY VIA BROWSER**.



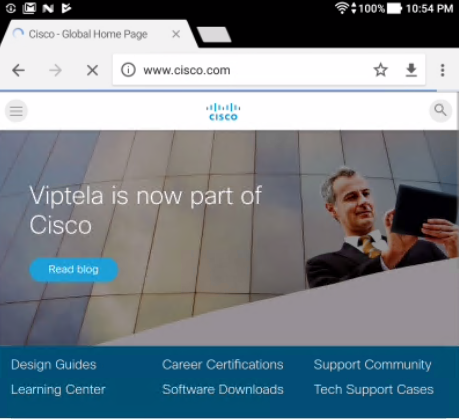
Enter your guest credentials.



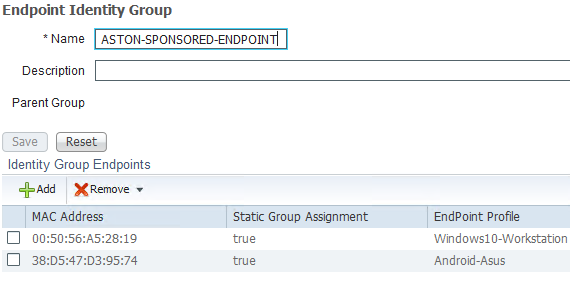
**Success**!



Try accessing a website like cisco.com.



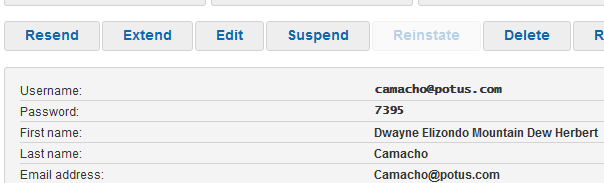
If Check the **ASTON-SPONSORED-ENDPOINT** Identity group, we see its been added.



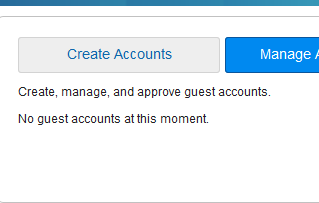
Again, a quick look at the **Live Logs**.



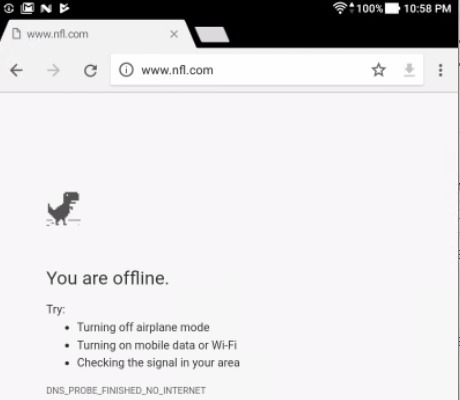
Now let’s go to the portal and **Delete** the account.



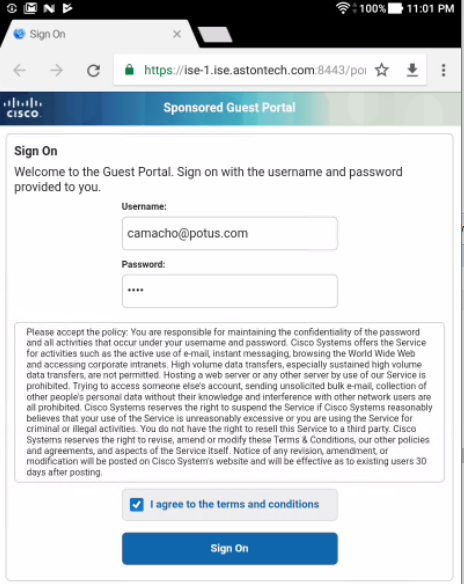
Now it’s gone.



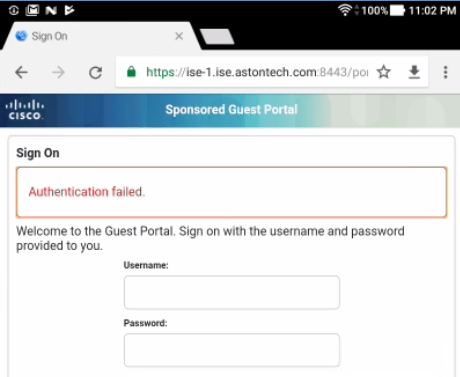
According to the tablet we are still connected to the Wi-Fi but now we can’t access the internet.

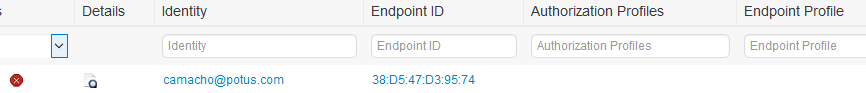


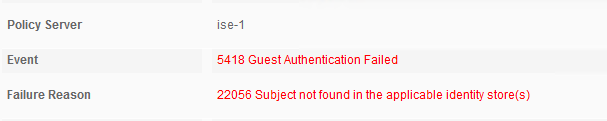
Disconnect from **ISE-GUEST** and reconnect and try to log back in with your guest creds. If you remember what they are.



You can see now we fail.







Conclusion

In this lab, we have:

* Added Identity Groups for our sponsored and employee guest accounts
* Added our Sponsors group from AD to ISE
* Configured Guest types and Sponsor groups
* Configured our Sponsor Portal and added the FQDN to DNS
* Edited our previously created Sponsored Guest portal to support our use case
* Edited our Authorization Profiles for wired and wireless CWA to point to our Sponsored Guest Portal
* Created Sponsored Guest and Employee Guest authorization policy for wired and wireless
* Created a Hotspot authorization policy for wired and wireless
* Tested different our Sponsored Guest use cases with:
  + Windows 10 wired with guest account
  + Windows 10 wireless with employee account
  + Android tablet with guest account
  + Android tablet with guest account is removed

In the next lab, we are going to set up another guest access type, Self-Registered Guest Access.