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

Contents

[Contents 2](#_Toc492641095)

[Introduction 3](#_Toc492641096)

[Lab Diagram 4](#_Toc492641097)

[WLC Configuration 5](#_Toc492641098)

[Add ACL 5](#_Toc492641099)

[ISE Configuration 6](#_Toc492641100)

[Identity Groups 6](#_Toc492641101)

[Portals & Components 6](#_Toc492641102)

[Policy Elements 8](#_Toc492641103)

[Policy Set 10](#_Toc492641104)

[Testing Guest Hotspot 11](#_Toc492641105)

[Windows 10 Wired 11](#_Toc492641106)

[Windows 10 Wireless 14](#_Toc492641107)

[Android Tablet 16](#_Toc492641108)

[Conclusion 19](#_Toc492641109)

Introduction

In this lab, we are going to walk through the first Guest Access use case which is hostspot. This is a quick and easy way to set up guest access.

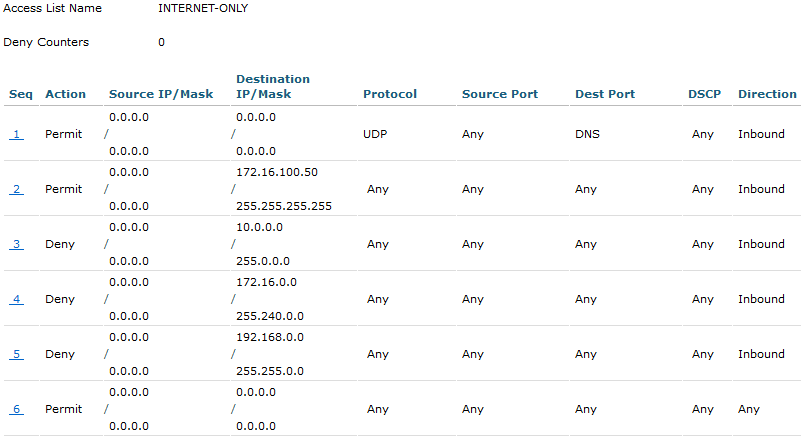
Lab Diagram



WLC Configuration

Add ACL

We need to create an ACL on the WLC to only allow internet access for our wireless guests. Log in to the WLC and go to **Security > Access Control Lists** and add an ACL called **INTERNET-ONLY** with the following entries:

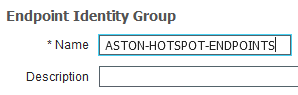


Then **Save** your Configuration.

ISE Configuration

Identity Groups

We could just use the GuestEndpoints group but to provide a little more flexibility we are going to create an Identity Group called **ASTON-HOTSPOT-ENDPOINTS**. Go to **Work Centers > Guest Access > Identity Groups > Endpoint Identity Groups**. Hit **Add** and give it the name stated below. Then **Submit**.



By default, once ISE learns a MAC address it will stay in the database forever. We don’t want a guest who may have been to our site once or twice to waste space in the database. In ISE there something called Endpoint purging. You have other conditions that you can purge endpoints on but we are going to create a rule that purges endpoints after being inactive for 7 days.

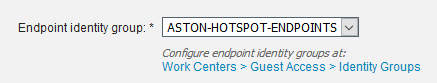
Go to **Administration > Identity Management > Settings > Endpoint Purge**. Insert a new rule in the Purge Policy Set and name it **HOTSPOT-PURGE**. The conditions we want to match on are **Endpoint Identity Group:ASTON-HOTSPOT-ENDPOINTS** and **ENDPOINTPURGE:InactiveDays GREATERTHAN 7**.



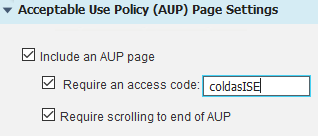
Portals & Components

Go to **Work Centers > Guest Access >** **Portals & Components > Guest Portals**. Click on the **Hotspot Guest Portal (default)** to highlight it and hit **Duplicate** then click into it.

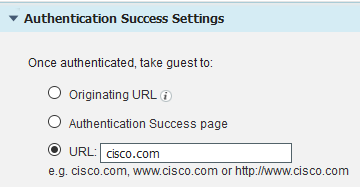
Name the new Portal **ASTON-HOTSPOT-GUEST-PORTAL**. Expand **Portal Settings**. We want to change the **Endpoint Identity Group** to the one we just created **ASTON-HOTSPOT-ENDPOINTS**.



Expand the **AUP** page settings. Let’s make guests use an access code when they log in rather than leaving it wide open. Check all three checkboxes and for the access code use **coldasISE**.



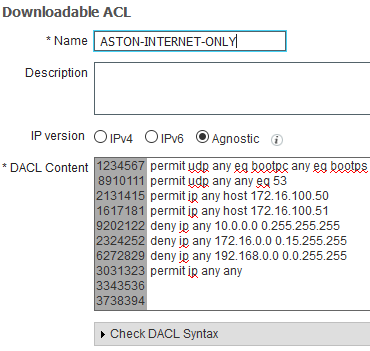
After the Guest authenticates, let’s send the user to astontech.com. Expand **Authentication Success Settings** and hit the **URL** radio button and add **cisco.com**.



Then go to the top and hit **Save**.

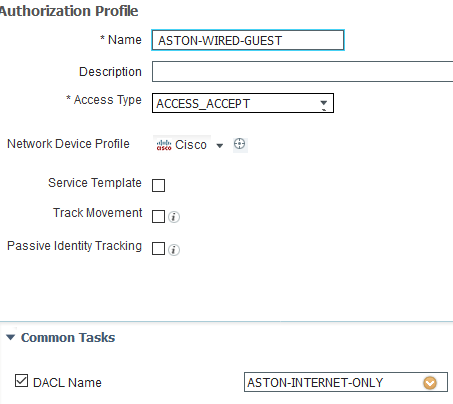
Policy Elements

Just like with the WLC we need an ACL to send to the switch to only allow internet access for wired devices. Go to **Policy Elements > Results > Downloadable ACLs**. Click Add and name it **ASTON-INTERNET-ONLY**. Add the following Content:

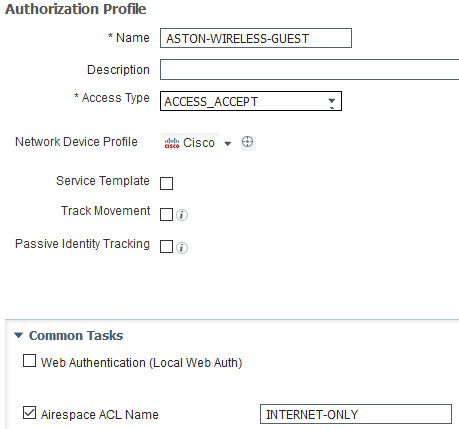


Now we need to create two and edit two Authorization Profiles for our Hotspot policy. The New ones we create are for after the guest get authenticated we need to give them the result of our internet only ACL. We also need to edit the CWA profiles to point to our hotspot portal.

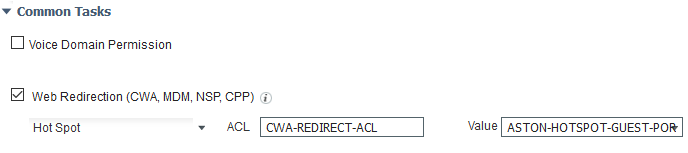
Go to **Authorization Profiles** and hit **Add**. Name it **ASTON-WIRED-GUEST** and check **DACL Name** and apply **ASTON-INTERNET-ONLY**.



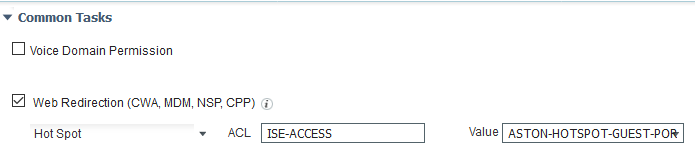
Add another one called **ASTON-WIRELESS-GUEST** and check **Airespace ACL Name** and give it the name of ACL we created on the WLC, **INTERNET-ONLY**.



Now let’s edit the CWA profiles we have. For wired click on **ASTON-WIRED-CWA**. Scroll down in the **Common Tasks** to Web Redirection and change it to Hot Spot and the value to **ASTON-HOTSPOT-GUEST-PORTAL**. Then **Save**.



Now we need to the same thing for our wireless CWA profile. Click on **ASTON-WIRELESS-CWA**. Scroll down in the **Common Tasks** to **Web Redirection** and change it to **Hot Spot** and the value to **ASTON-HOTSPOT-GUEST-PORTAL**. Then **Save**.



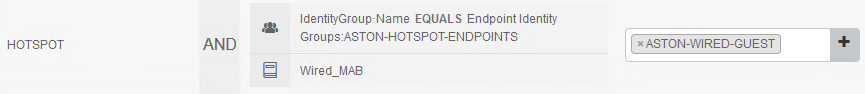
Policy Set

We have already changed the **CWA-REDIRECT** policies by changing the Authorization Profile to point to our new hotspot portal. Now let’s create our policies for after a guest gets authenticated for wired and wireless.

Go to **Policy Sets > WIRELESS**. It’s important where we put this rule since we don’t want it to match on any of the BYOD policies that we have created previously. Click the **Gear** on **BYOD-DUAL-SSID-iOS** and **Inset New Rule Above**. Name it **HOTSPOT** and for conditions we want to match on **Endpoint Identity Group:ASTON-HOTSPOT-ENDPOINTS** and **Normalised Radius:SSID CONTAINS ISE-GUEST-(x)**. Then for **Permissions** give it **ASTON-WIRELESS-GUEST**.



Now go to the **WIRED** Policy Set. Click on the **Gear** on **CWA-REDIRECT** policy and **Insert New Rule Above**. Name it **HOTSPOT** and for conditions we want to match on **Endpoint Identity Group:ASTON-HOTSPOT-ENDPOINTS** and **Wired\_MAB**. Then for **Permissions** give it **ASTON-WIRED-GUEST**.

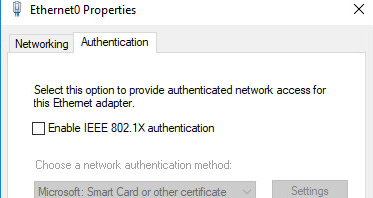


Testing Guest Hotspot

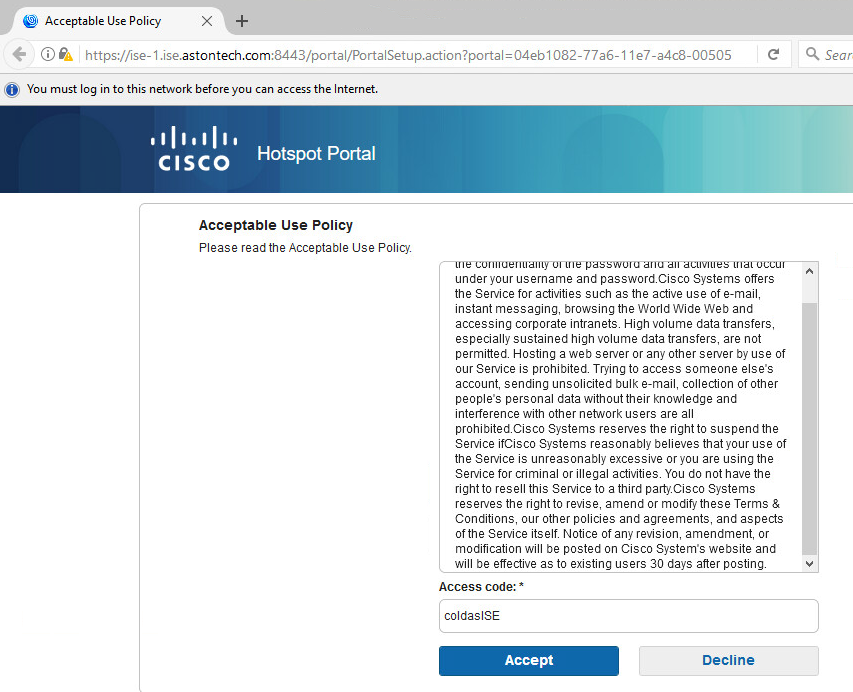
Windows 10 Wired

Before we start we need to make sure that none of our lab devices are in the RegisteredDevices identity group. Log in to <https://mydevices.lab.astontech.com/> and delete all your devices.

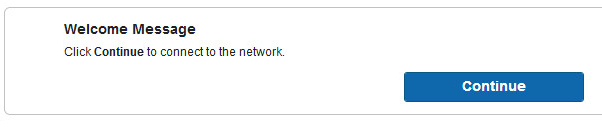
Console into LAB-PC-3. Since we want to test our wired connection disable the wireless adaptor and enable Ethernet0. On Ethernet0 check to make sure dot1x authentication is disabled.



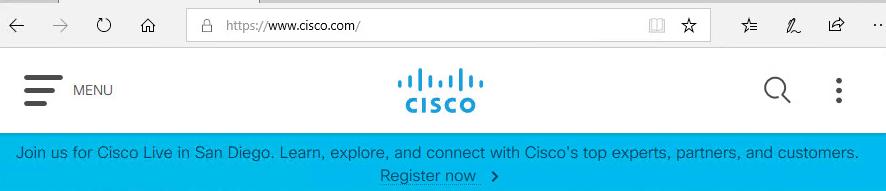
If not redirect automatically, open a web browser and go to cisco.com. You should be redirected the Hotspot Portal. Log in with the access code **coldasISE** and hit **Accept**.



Click **Continue**.



You should get redirected to cisco.com.

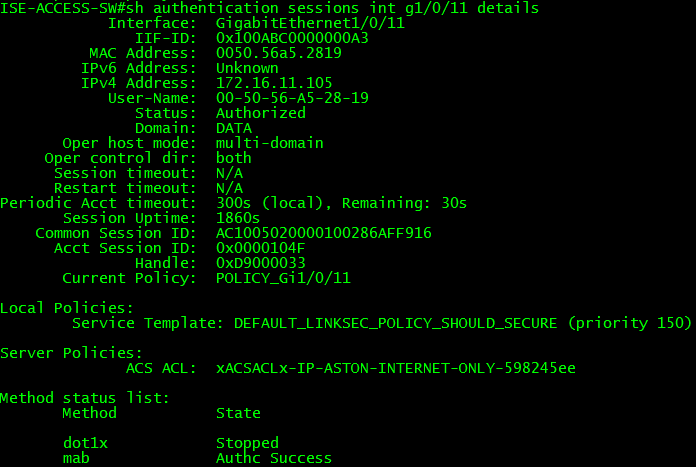


You should have access to the internet but not anything internal except ISE. Try to ping some of our internal IPs like its gateway 172.16.11.1 or the AD server 172.16.100.20.

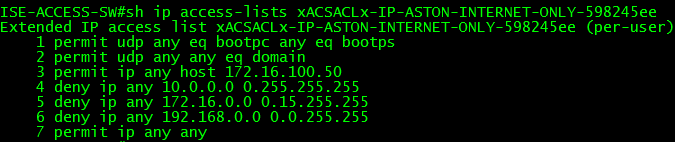
A quick look at the Live Logs and we see that we are coming in via MAB. First hitting the redirect policy then after entering the access code, ISE forces a CoA and we come back and hit the HOTSPOT policy.



We can also look at the switch.



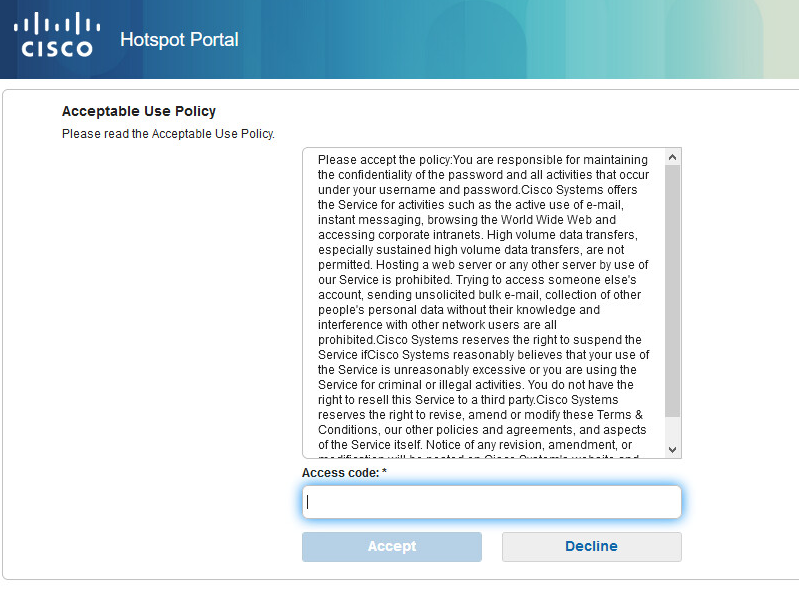
And the ACL that is applied.



Windows 10 Wireless

Let’s try and see if the wireless policy works. Disable Ethernet0 and enable the wireless adaptor then connect to **ISE-GUEST-(x)**.

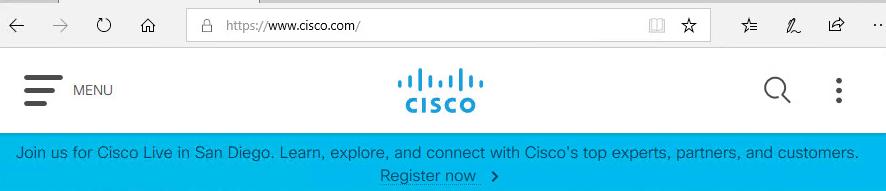
Again, a browser window should pop up with the Hotspot page. Enter the Access code **coldasISE** and **Accept** the AUP.



Then click **Continue**.



Now you should have been redirected to cisco.com

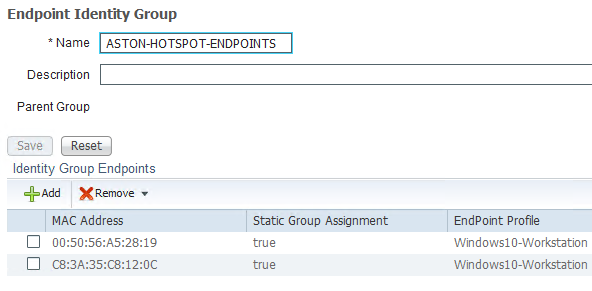


Again, test your network access. You should have access to the internet but not anything internal except ISE. Try to ping some of our internal IPs like its gateway 172.16.100.1 or the AD server 172.16.100.20.

A quick look at the **Live Logs** shows the same result as before except now it’s wireless.



Now if we check our Hotspot identity group both MAC addresses should be in there.

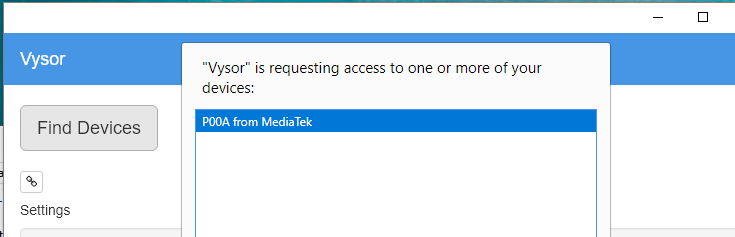


Take a minute to review the ISE logs. Also, look at the client info in the WLC and the switch. Make sure everything is as expected.

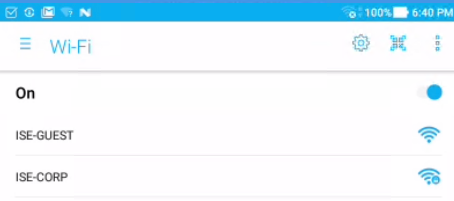
Android Tablet

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.

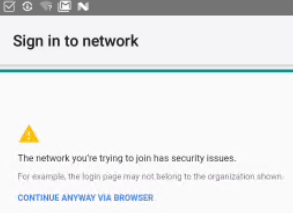
Let’s test out the Android tablet it should be pretty much the same as the Windows was. Open **Vysor** on your jumphost and hit **Find Devices**. Click on the device and hit **Select**.



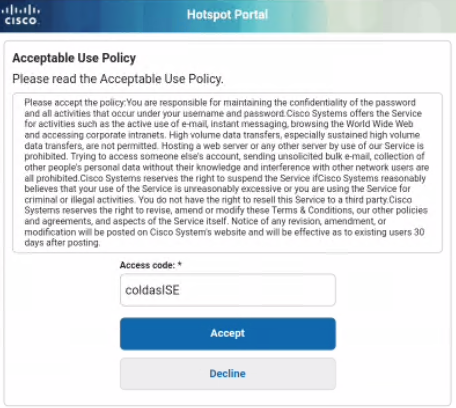
Open the **Settings** go to **Wi-Fi** and connect to **ISE-GUEST**.



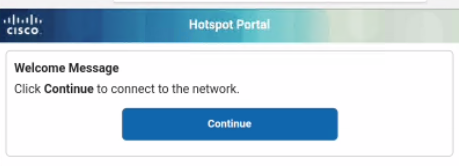
Click **CONTINUE ANYWAY VIA BROSWER**.



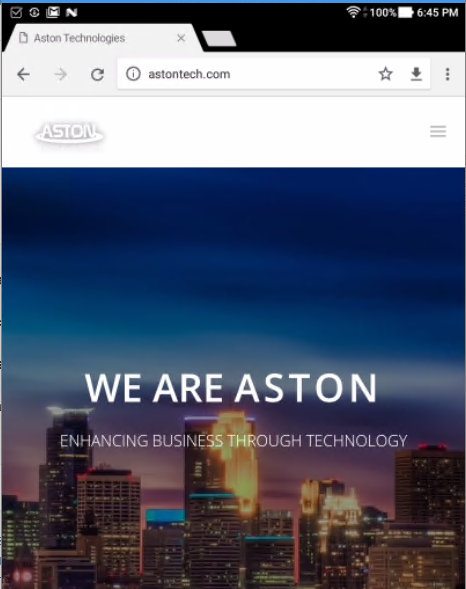
Enter the **Access code** and hit **Accept**.



Hit **Continue**.



You should be redirected to astontech.com.



Conclusion

In this lab, we have:

* Configured an ACL for internet only access on the WLC
* Added an Identity Group for our Hotspot endpoints
* Configured an endpoint purge policy to remove devices after 7 days
* Created a Hotspot portal for guests to input the access code
* Created an ACL for internet only access to be downloaded to the switch
* Added 2 Authorization Profiles for wired and wireless guest
* Edited our CWA Authorization Profile to redirect to the guest portal
* Created a Hotspot authorization policy for wired and wireless
* Tested three different common Guest device types:
  + Windows 10 wired
  + Windows 10 wireless
  + Android tablet

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