|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Posture Assessment with AnyConnect |
| An Aston training document explaining how to deploy basic Posture with ISE AnyConnect Posture Module |

Contents

[Contents 2](#_Toc41396637)

[Lab Diagram 3](#_Toc41396638)

[ISE Configuration 4](#_Toc41396639)

[Client Provisioning 4](#_Toc41396640)

[Policy Elements 8](#_Toc41396641)

[Posture Policy 15](#_Toc41396642)

[Policy Set 15](#_Toc41396643)

[Configure Access SW 16](#_Toc41396644)

[Testing with ISE-PC-2 17](#_Toc41396645)

[Conclusion 31](#_Toc41396646)

Lab Diagram

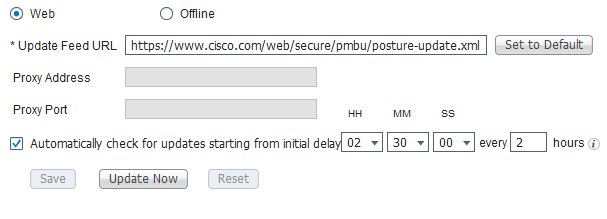


ISE Configuration

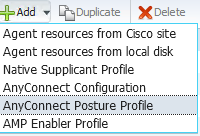
Client Provisioning

For posturing to work with ISE we need to utilize the AnyConnect ISE posture and compliance modules. There are two ways to get AnyConnect on the device. One way would be to use the enterprise’s corporate software distribution system but since we don’t have one we are going to set up ISE to push out the software. Along with Software we need to send a configuration profile like we did we the VPN labs. Let’s get started.

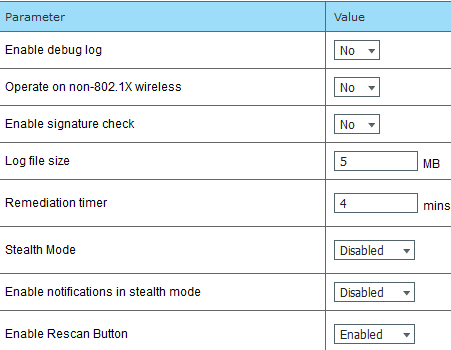
Log into ISE and navigate to **Work Centers > Posture > Settings > Software Updates > Posture Updates** and make sure that your posture information is up to date. You can hit **Update Now** to make sure.



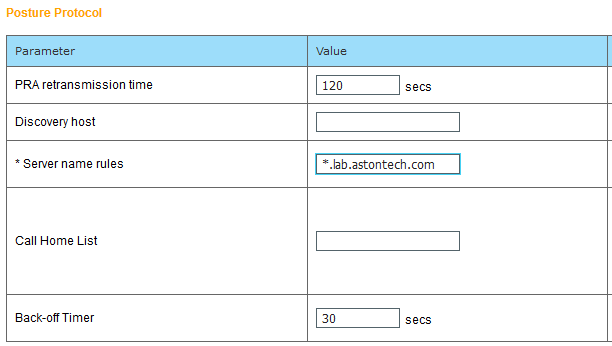
Navigate to **Work Centers > Posture > Client Provisioning > Resources**. Hit **Add** and select **AnyConnect Posture Profile**.



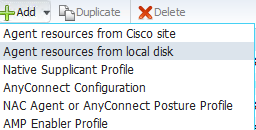
Name it **ASTON\_ISE\_AC\_PROFILE**. For the Agent behavior let’s give ourselves a little more time for the **Remediation timer** also **Enable the Rescan Button**. Configure the following:



Everything else can stay default except under the **Posture Protocol** we need to add a Server name rule. This tells the server what domain it’s allowed to connect to in the case of overlapping IP space. Add **\*.lab.astontech.com**. Then hit **Save**.



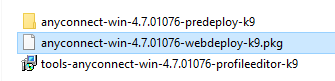
Now we need to upload the AnyConnect software version that we are using to ISE. Hit **Add** and **select Agent resources from local disk**.



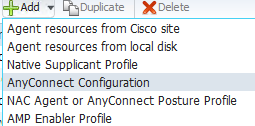
For Category select **Cisco Provided Packages**.



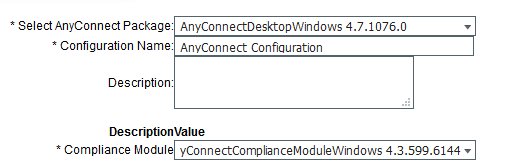
Browse to the AnyConnect version. If you don’t have it locally on your machine you can grab it from our shared drive [\\10.1.249.115\Software\Networking\Data\Security\Cisco\ASA\AnyConnect\4.7](file://10.1.249.115/Software/Networking/Data/Security/Cisco/ASA/AnyConnect/4.7). Then hit **Submit**.



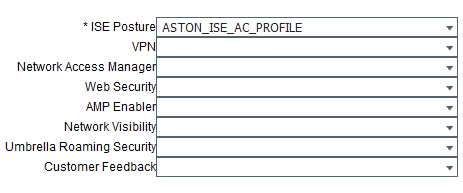
Now hit **Add** again and select **AnyConnect Configuration**.



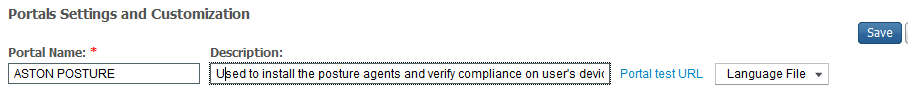
Select the **AnyConnect Package**. Name it **ASTON AnyConnect Windows**. Select the latest **Compliance Module**.



Add the Profile we created under **ISE Posture**. Everything else can stay default. Hit **Save**.



Next go to the **Client Provisioning portal**. Select the **Create**. Name it **ASTON POSTURE** and hit **Save**. Wait tell you see the Saved window popup before moving on.



Navigate to the Client Provisioning Policy. We could use the BYOD policies to push out the Posture software but we have those set up for BYOD-USERS and we want to posture everyone.

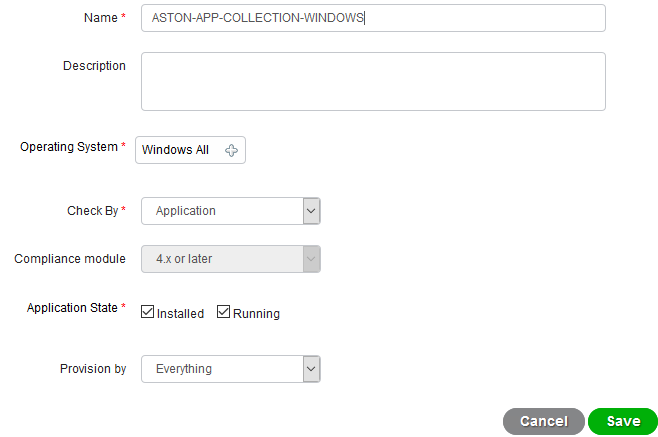
Add a new policy at the top of the list. Name it **ASTON POSTURE WINDOWS**. Operating System is going to be **Windows All** and for the let’s match on dot1x (**Radius:Service-Type EQUALS Framed**) and the **Employee AD group** then for Results under the Agent Configuration select **ASTON AnyConnect Windows**. Then hit **Save**.



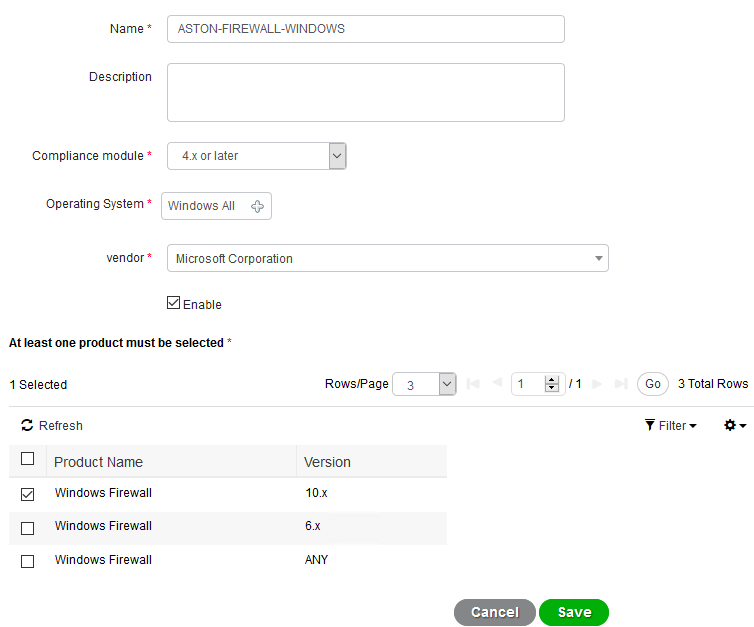
Policy Elements

We are going to create 3 checks for posture. One is not really a check but rather collecting information on what applications are installed and running on the host. For the other two we are going to require that the Windows Firewall is enabled and Windows defender is installed and up to date.

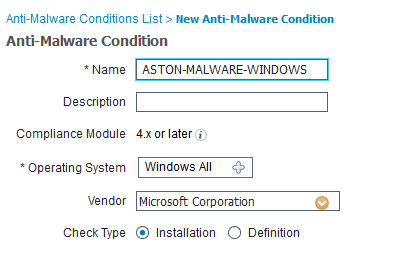
Navigate to **Policy Elements > Conditions > Application** and hit **Add**. Name it **ASTON-APP-COLLECTION-WINDOWS** and configure the following then **Save**:

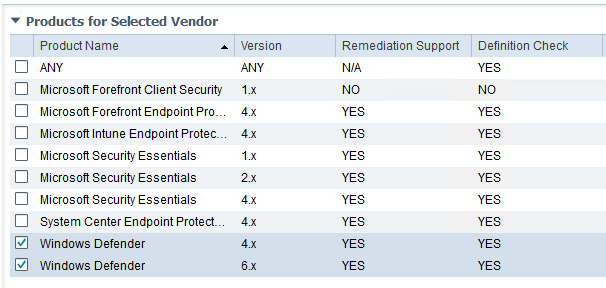


Select **Firewall Condition** and hit **Add**. Configure the following then hit **Save**:



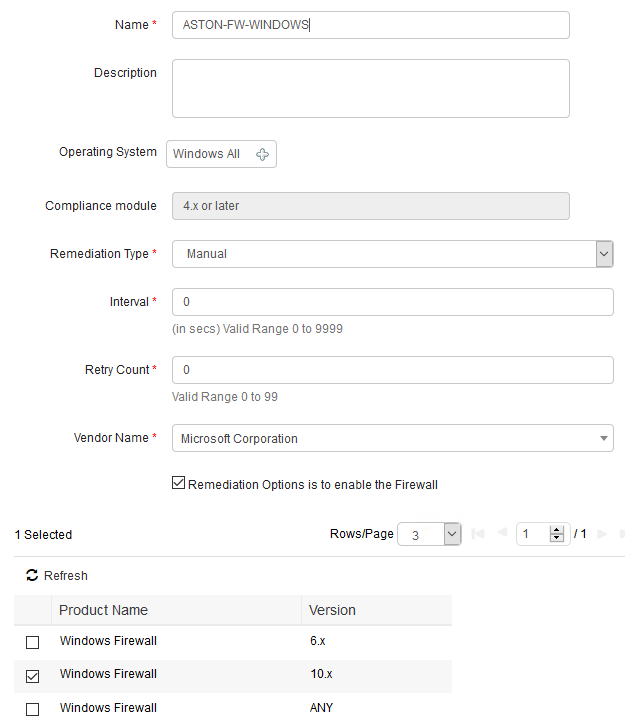
Select Anti-Malware and hit Add. Name it **ASTON-MALWARE-WINDOWS** and configure the following and Save:





Now it’s on to Remediations. For Application since we are just collecting information they isn’t really anything to remediate and there is a default remediation for Anti-Malware we can use. We’ll need to create one for our Firewall check however.

Select Firewall and hit **Add**. Name it **ASTON-FW-WINDOWS** and configure the following then **Save**:



We have it set to manual remediation for now. Later we’ll change that to see how the behavior changes.

Select **Requirements** and **Insert new requirement**, it doesn’t matter where. These requirements aren’t processed in a top down order like you would see within the Policy Sets for example.

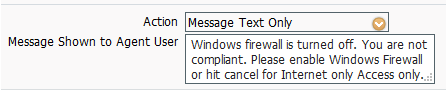
Name this requirement **ASTON APP COLLECTION WIN**. Operating System will be **Windows All**, Compliance module **4.x or later** and conditions select **ASTON-APP-COLLECTION-WINDOWS**.



Duplicate the App requirement we just created and change the name to **ASTON ANTI-MALWARE WIN**. For conditions change to **ASTON-MALWARE-WINDOWS**. For the Remediation Actions select **AnyAMDefRemediationWin**.



Duplicate one of the new requirements and change the name to **ASTON FW WINDOWS**. Change the conditions to **ASTON-FIREWALL-WINDOWS** and then for Remediation Actions configure the following:

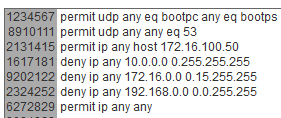




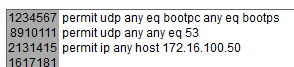
Then hit **Save**.

Now we need to create some dACLs. One for when the posture status is unkown and another for when the host is non-compliant. We’ll use the **ASTON-EMPLOYEE** ACL when the host is compliant.

Select **Downloadable ACLs** and hit **Add**. Name it **ASTON-NON-COMP-POSTURE** and configure the following:

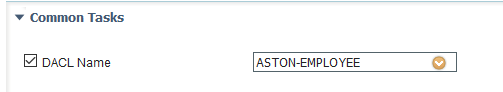


Add another and name it **ASTON-UNKNOWN-POSTURE** and configure the following:

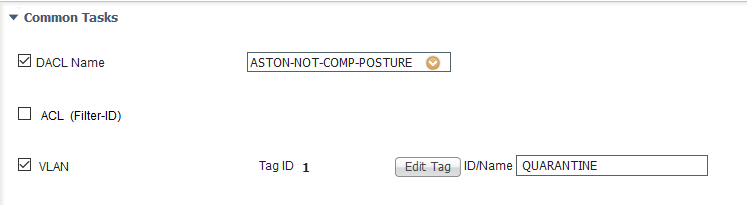


Now we need to make three Authorization Profiles one for each one of our posture states.

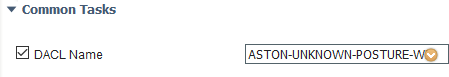
Select **Authorization Profiles** and hit **Add**. Name the first one **ASTON-COMP-POSTURE-WIRED**. All we need to do here is send the dACL.



Add another one and name it **ASTON-NON-COMP-POSTURE-WIRED**. For this profile, we are going to send a **dACL** and change the VLAN to the **QUARNTINE VLAN** we have configured on the switch. You can put the VLAN name or ID which is **35**.



Last one name **ASTON-UNKNOWN-POSTURE-WIRED**. For this profile, we’ll need to set up web redirection the client provisioning portal as well as send a dACL. For the dACL select **ASTON-UNKNOWN-POSTURE**.



For the web redirection select **Client Provisioning (Posture)** and for the ACL type **POSTURE-DISCOVERY** which we will add to the switch a little later. Then select the posture portal that we created - **ASTON POSTURE**.

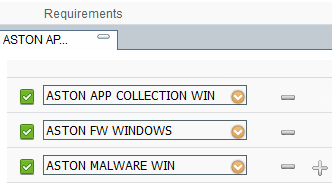


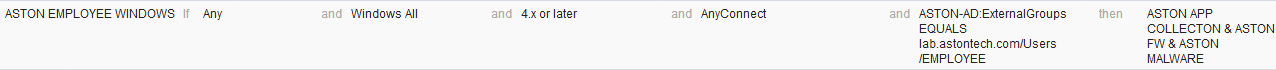
Hit **Save**.

Posture Policy

Navigate to Posture Policy and add a new policy. This is where we are going to say the who, what, when and where for posture.

Name the Policy **ASTON EMPLOYEE WINDOWS**. Operating system will be **Windows All**, Compliance Module – **4.x or later**. Then for the conditions we want to match on our AD group **Employee**. Then we are going to apply the three requirements that we created.

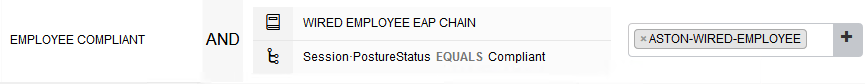




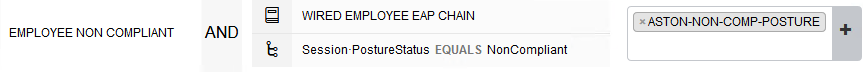
Policy Set

We need to configure some rules in the WIRED policy set. Navigate to **Policy Sets > WIRED**. We are going to use ISE-PC-2 to do the testing so let’s create new rules with EAP-FAST.

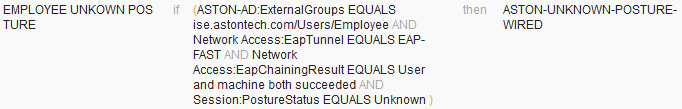
**Duplicate Above** the **EMPLOYEE EAP CHAIN** policy. Name it **EMPLOYEE COMPLIANT**. We are going to add one condition which is **Session:PostureStatus Equals Compliant**.



**Duplicate Above** the **EMPLOYEE COMPLIANT** policy and name it **EMPLOYEE NON-COMPLIANT**. We are going to change the posture status to **NOT EQUALS Compliant** and change the results to **ASTON-NON-COMP-POSTURE**.



**Duplicate Above EMPLOYEE NON-COMPLIANT** and name it **EMPLOYEE UNKNOWN POSTURE**. Change the **Posture Status to EQUALS Unknown**. Then change the results to **ASTON-UNKNOWN-POSTURE**.



Then **Save**.

Configure Access SW

We need to configure redirect ACL for the posture discovery process. Log in to **Access-SW** and configure the following:

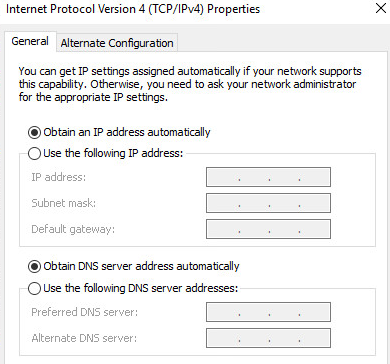
ip access-list extended POSTURE-DISCOVERY

permit tcp any 172.16.0.1 0.0.255.0 eq www

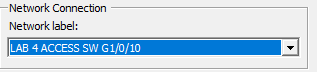
permit tcp any host 72.163.1.80 eq www

Testing with ISE-PC-2

Let’s get the PC ready for testing. Open a console window to PC-2 and log in. Remove the static IP that we added in the VPN lab.

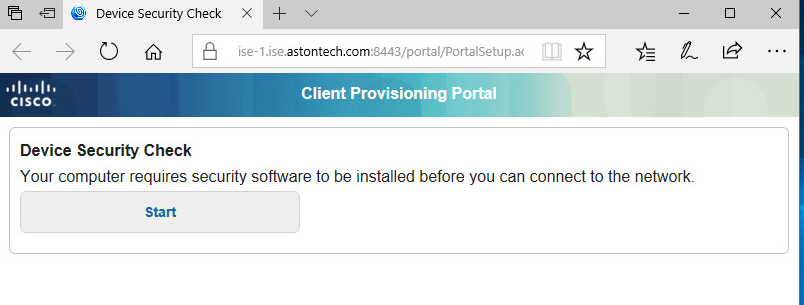


Ok, now we should be ready to connect to the network to test. Change the Network adaptor to **LAB (x) Access SW G1/0/10**.

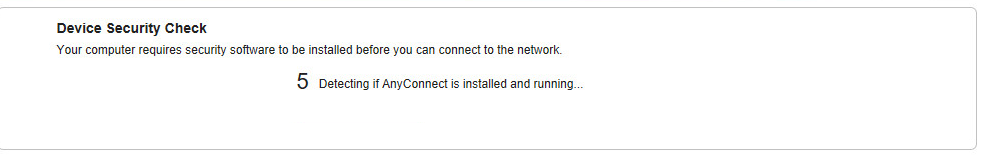


We need to install the ISE posture module; in the real world you would use your enterprise’s software distribution tool but since we don’t have one, we’ll need kick off the install manually.

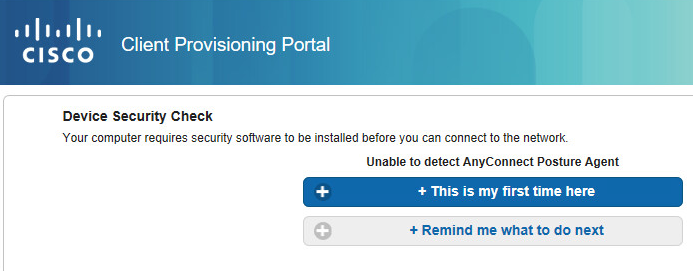
Once you change the interface; open a web browser and type **172.16.11.1**. That should redirect you to the provision portal. Once that page loads click on **Start**.



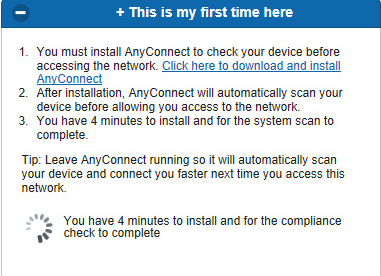
ISE is checking for AnyConnect ISE posture and compliance modules.



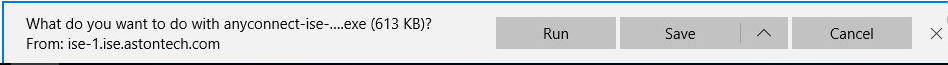
Click **This is my first time here**.



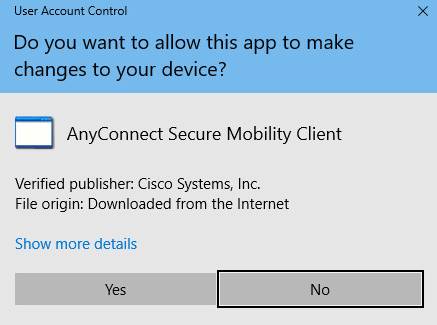
Click where it says, “**Click here to download and install AnyConnect**”.



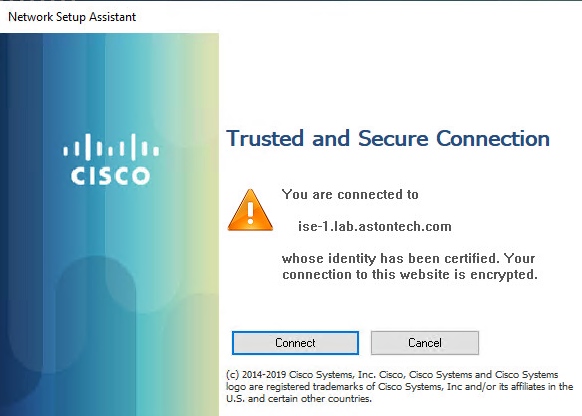
Click **Run**.



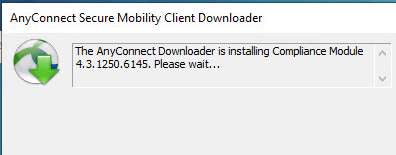
Hit **Yes**.



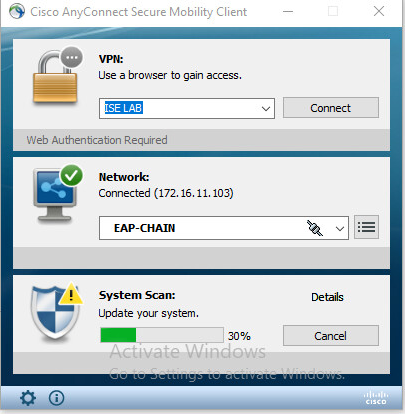
Hit **Connect**.



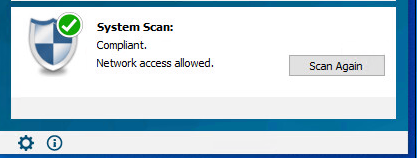
You can see that AnyConnect is installing.



Now AnyConnect is scanning the system.

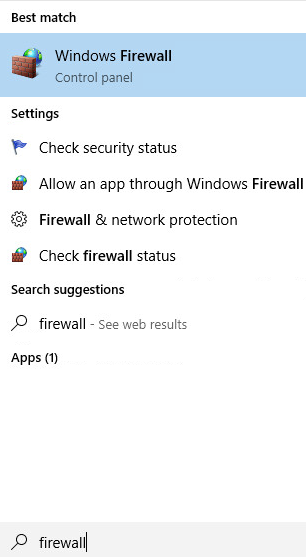


Once that’s finished scanning you should now be compliant and have access to the whole network.

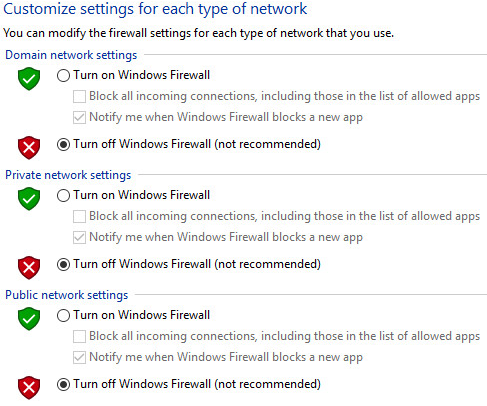


Test access to the internet and Ping the Access-sw.

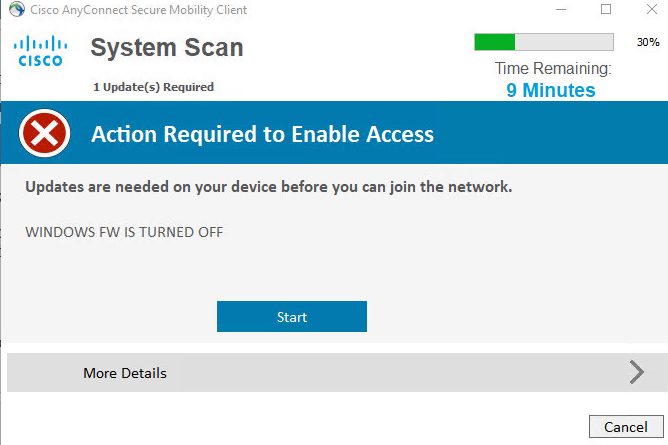
Now we want to fail posture. Let’s disable the Windows Firewall. Hit the **Windows key** and type **firewall** and select **Windows Firewall**.



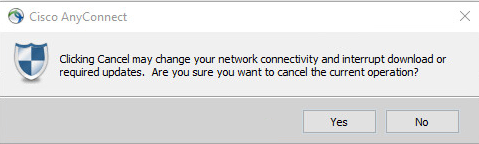
Select **Turn Windows Firewall on or off** on the left-hand side. Then turn off all the Firewalls.



Here we are failing the posture check since we turned off the Windows Firewall. Click **Cancel**.

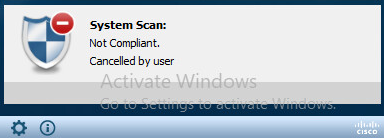


Hit **Yes** to cancel.

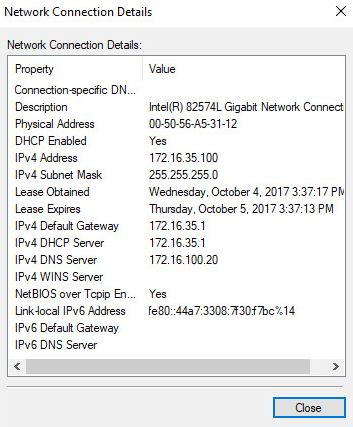


This process will run twice just go through the cancellation process again

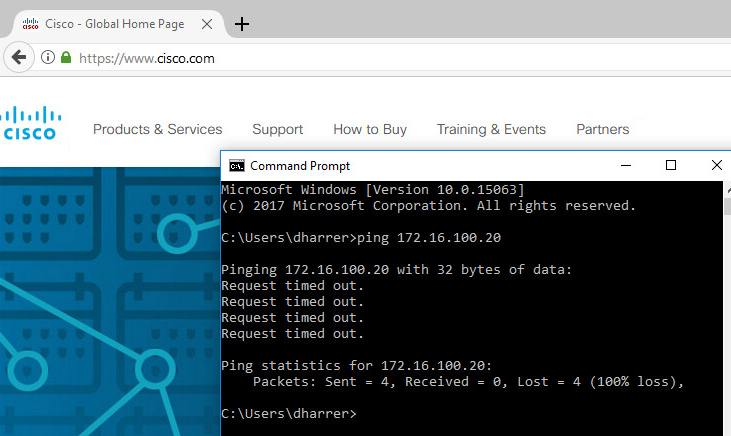
Here we can see that we are not compliant. We should be switched to VLAN 35 and have internet only network access.



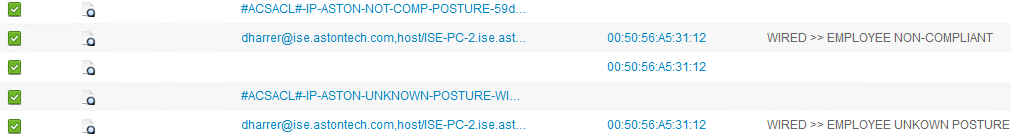
Here we see we got an IP from VLAN 35.



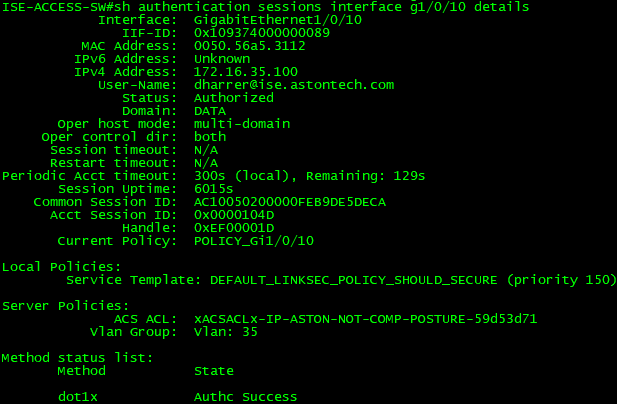
Internet is working but we can’t access internal resources except ISE.



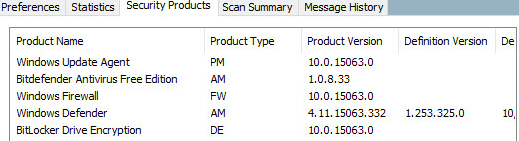
ISE live logs show that we came in unknown then went to non-compliant. Check the details and see what information is there.



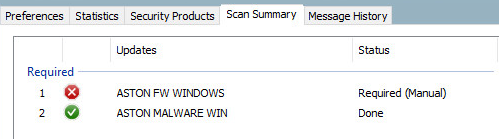
If we look at the switch we can see that we have the correct ACL and are being assigned to VLAN 35.



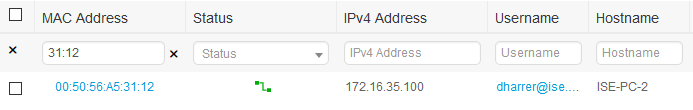
If we go back to **PC-2** and click on the **Gear Icon** on the **AnyConnect Client** then go to **System Scan** take a look at the **Security Products** tab. We can see all the Security products installed on the device.



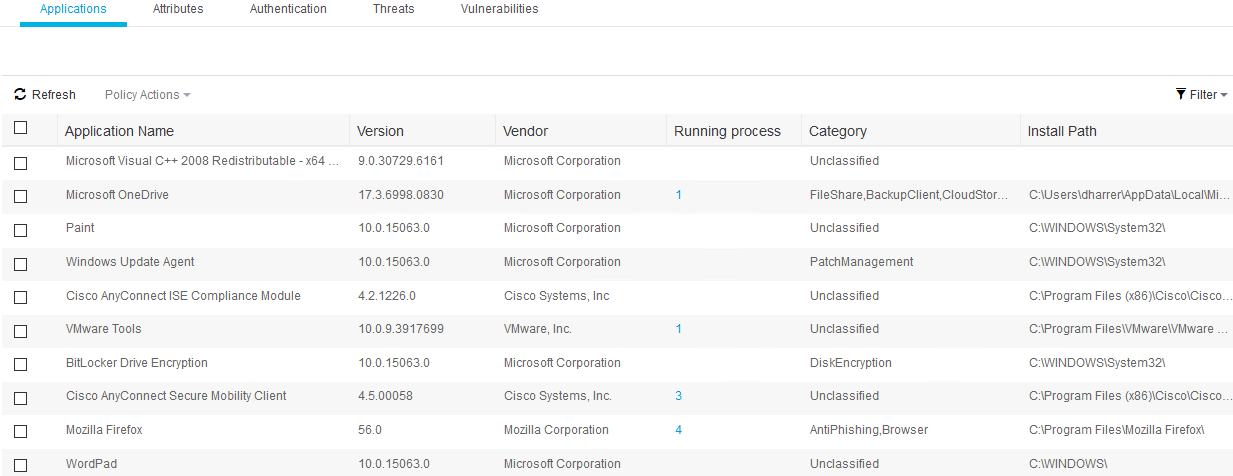
Now move over to the **Scan Summary** tab. Here we can see our 2 checks with the Firewall check failing.



We have one more thing that we configured, that was application collection. To see what we have collected in ISE go to **Context Visibility > Endpoints** and find **ISE-PC-2** and click on its **MAC address**.



Now in the applications tab you should be seeing all the installed and running applications along with other information, version numbers and install path.

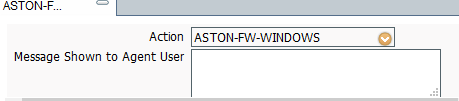


Now we’ve tested our unknown and not-compliant rules. Let’s test the compliant policy but instead of just turning on our Windows Firewall let’s have ISE do that for us.

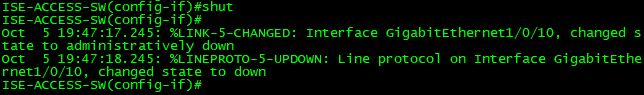
In ISE go to **Work Centers > Posture > Policy Elements > Remediations > Firewall** and **Edit ASTON-FW-WINDOWS**. Change the **Remediation Type** to **Automatic** and hit **Save**.

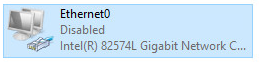


Then go to Requirements and find the **ASTON FW WINDOWS** rule change the Remediation Actions to **ASTON-FW-WINDOWS**.

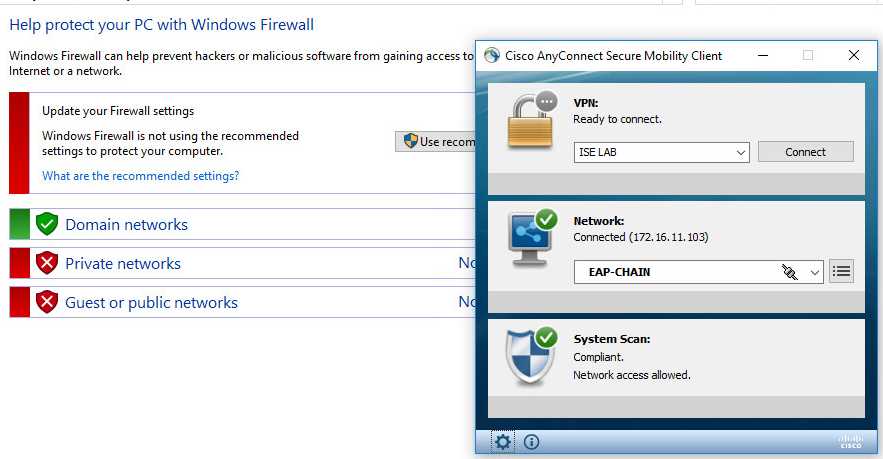


Log into the Access-SW and **shut** the port on G1/0/10 then **disable** the network adaptor on ISE-PC-2.





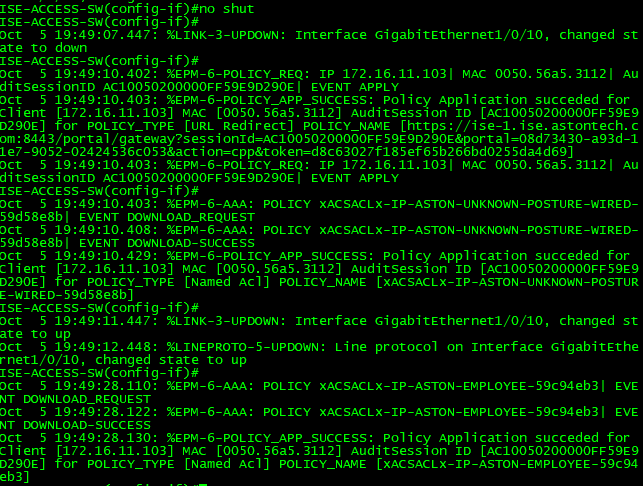
Then **no shut** the port and **enable** the network adaptor. Now you should come back online as compliant and if you check the Firewall you’ll see that it has been automatically enabled.

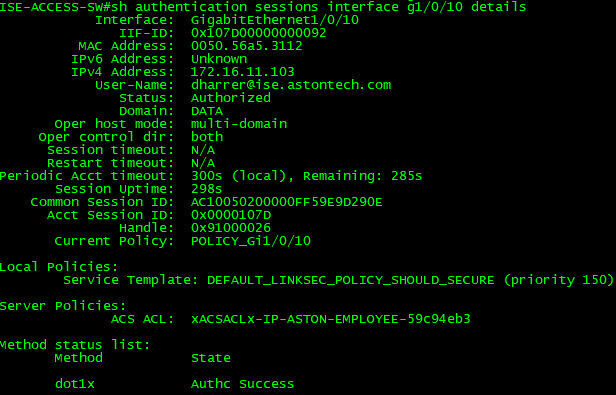


If we look at ISE we see that we get the EMPLOYEE COMPLIANT policy and the EMPLOYEE ACL.



And the switch:





Conclusion

In this lab, we have:

* Configured client provisioning
  + Created an AnyConnect Posture Profile
  + Uploaded an AnyConnect package
  + Created an AnyConnect configuration package
  + Configured client provisioning policy
  + Created a client provisioning portal
* Configured our Policy Elements for Posture
  + Created conditions for App collection, Windows Firewall and Windows Defender
  + Created dACLs for unknown and non-compliant policies
  + Created Authorization Profiles for compliant, non-compliant and unknown
* Configured our Posture Policy
  + Configured our WIRED Policy Set to support Posture
* Tested our posture policies for unknown and non-compliant
* Changed our FW policy and tested for compliant status

In the next lab, we are going to cover posture for guests utilizing the temporal web agent.