|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Remote Access VPN with Certificates |
| An Aston training document explaining how to configure RA VPN with certificates |

Contents

[Contents 2](#_Toc41344807)

[Lab Diagram 3](#_Toc41344808)

[ASA Configuration 4](#_Toc41344809)

[Add RADIUS Server 4](#_Toc41344810)

[Tunnel Group 6](#_Toc41344811)

[Add the Lab Root Certificate 8](#_Toc41344812)

[AnyConnect Client Profile 10](#_Toc41344813)

[Testing RA VPN 11](#_Toc41344814)

[Testing Network admin account 11](#_Toc41344815)

[Testing with Employee account 14](#_Toc41344816)

[Conclusion 22](#_Toc41344817)

Lab Diagram

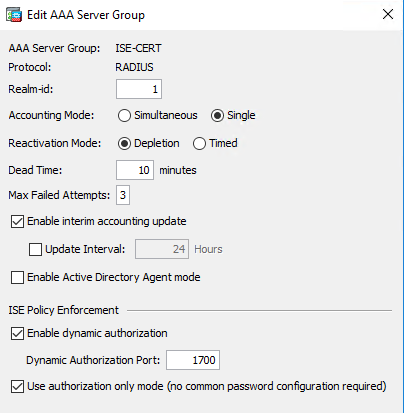


ASA Configuration

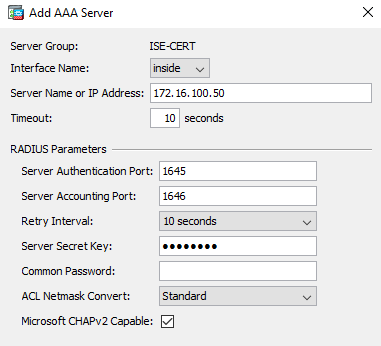
Add RADIUS Server

You might be asking why we are adding another RADIUS server since we added ISE in the last lab. The reason is when you use certificates to authenticate via AnyConnect with the ASA as the gateway. The ASA actually does the authentication, so we need to create a server group that will only send authorization requests to ISE based on the cert presented.

Log into ASDM and go to **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**. Click Add and configure the following:



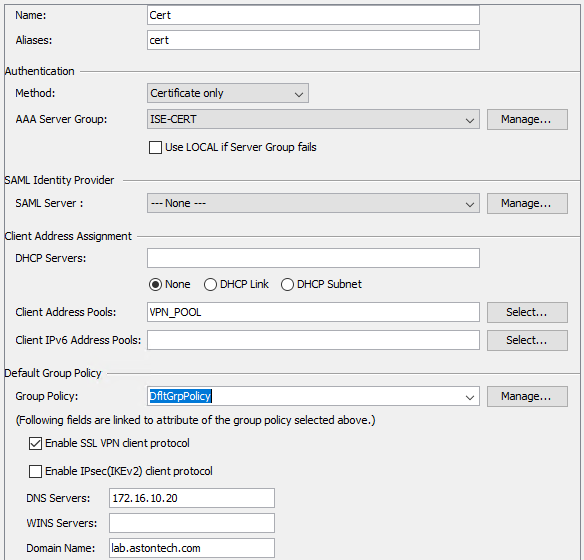
**Add** a server to the group just like before. Hit **OK** and **Apply**.



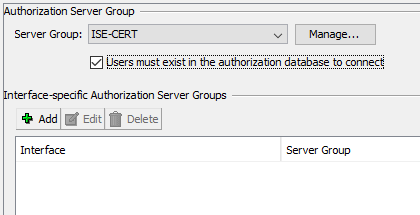
Test Authentication again, in case of any typos.

Tunnel Group

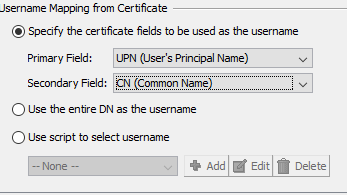
Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** and hit **Add**. Name it **CERT** and configure the following:



Expand the **Advanced** tab and go to **Authorization**. **Add** the new Server Group we created - **ISE-CERT**.

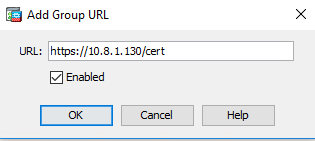


At the bottom of the page for the **Username Mapping from the Certificate**, change the Primary to **UPN** and the secondary to **CN**. Then hit **OK**.



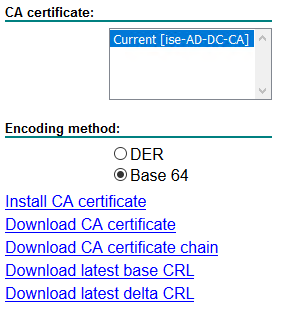
Finally, go to **Group Alias/Group URL** section.

Under Group URL click **Add**. Input <https://your.asa.outside.ip/cert>. Hit **OK** and **Apply**.

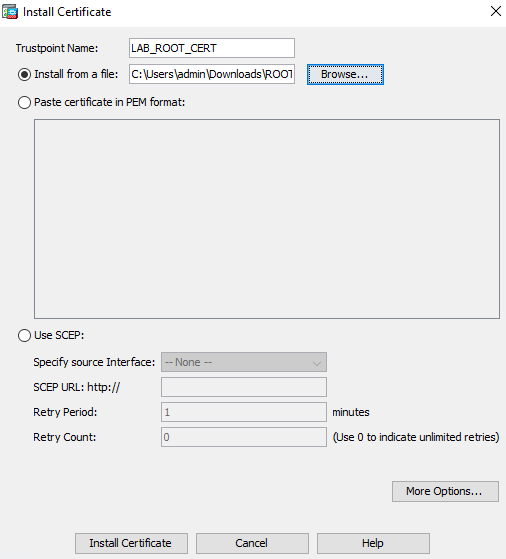


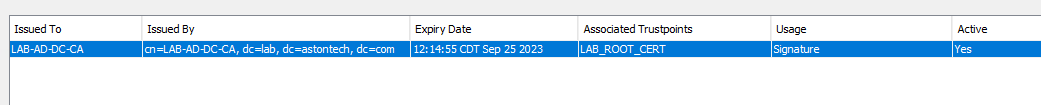
Add the Lab Root Certificate

We’ll need the ROOT cert for our internal CA to add to the ASA for our domain machines. Go to <http://172.16.100.20/certsrv> and download the root cert.



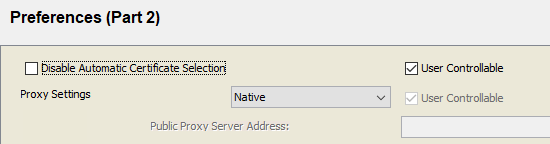
Once you have those go back to ASDM and navigate to **Configuration > Remote Access VPN > Certificate Management > CA Certificates**. Click Add, give them a friendly name and install the root cert we just downloaded.



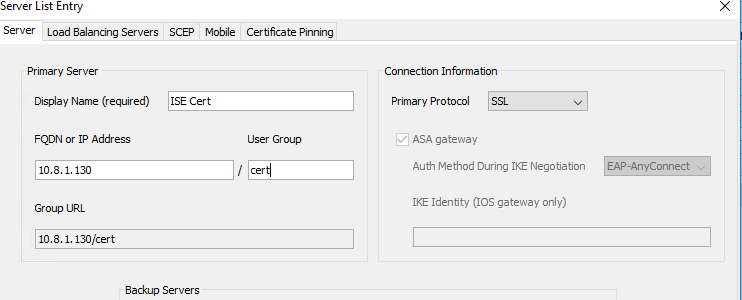


AnyConnect Client Profile

Last thing we need to do a little editing on the Client Profile. Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**. Click on the profile we have and hit **Edit**. Go to the **Preferences Part 2** configuration page and **uncheck** the **Disable Automatic Certificate Selection**.



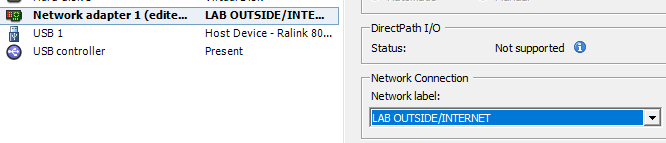
Go down to the **Server List** page. Add a new server for the alias for the certificate tunnel group we created.



Testing RA VPN

Testing Network admin account

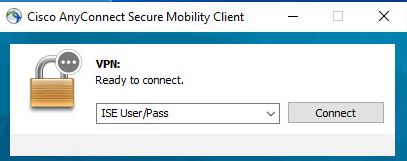
Open a console window to PC-2 and log in. If you haven’t already, change PC-2’s Network Adaptor to the Outside network.



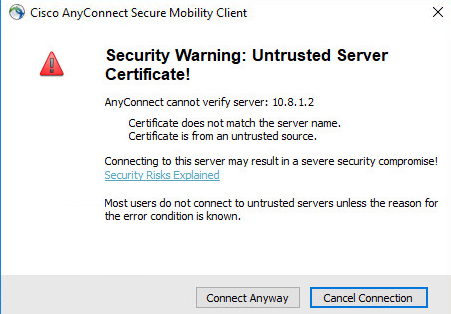
Statically assign your NIC.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Gateway | Lab 1 | Lab 2 | Lab 3 | Lab 4 |
| 10.8.1.225/27 | 10.8.1.226 – 228 | 10.8.1.229 – 232 | 10.8.1.233 – 236 | 10.8.1.237 – 240 |

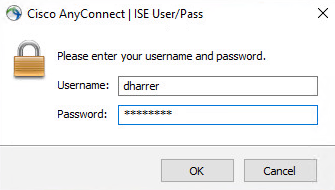
**Connect** to ISE User/Pass so we can pull down the changes to the client profile.



Hit **Connect Anyway** on the popup.

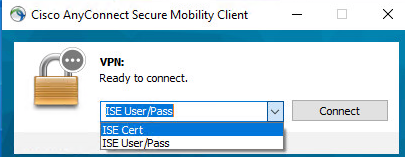


Input your AD Creds.



Once connected, hit **Disconnect.**

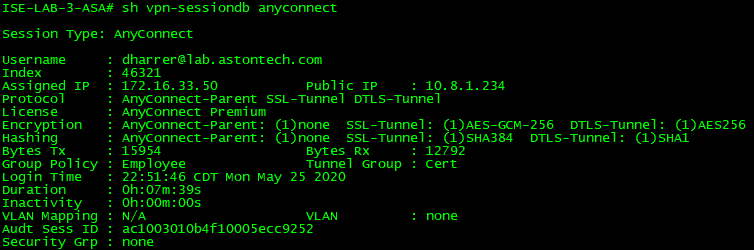
Now you should have the ISE Cert connection profile in AnyConnect.



Connect using ISE Cert. Your VPN session should connect automatically. If we check ISE we can see that passed with our identity being pulled from the certificate and dACL being sent.



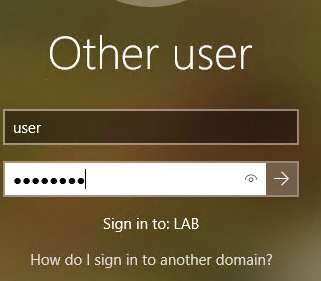
And on the ASA:



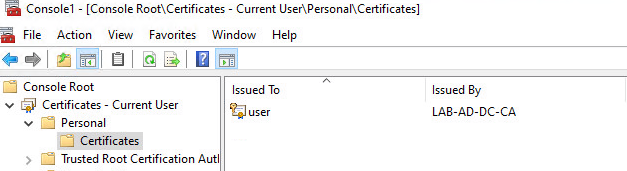
Testing with Employee account

Now let’s try with the User account that we created but first we need to get the certificate and AnyConnect installed on the PC. We are going to have to jump through a few hoops for this.

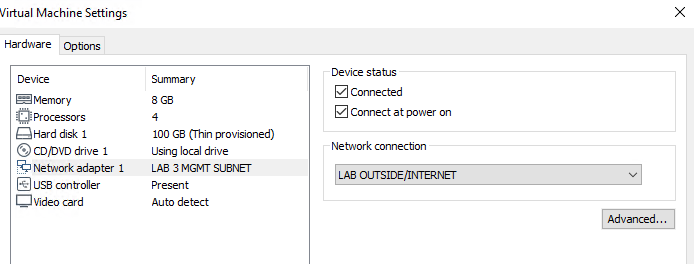
On **PC-1** change the network connection to the **LAB (x) MGMT Subnet**. Log out of your account and log in with the User account.



Open **MMC** and confirm that you have the certificate installed.



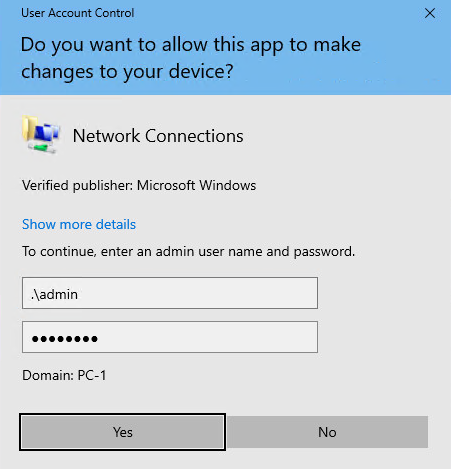
Change the network connection to **LAB OUTSIDE/INTERNET**.



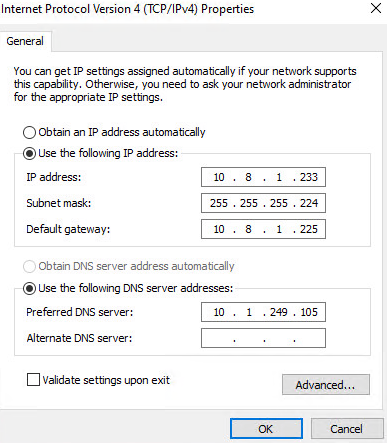
Assign the PC an appropriate IP address. Remember we have PC-2 assigned an address from this subnet.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Gateway | Lab 1 | Lab 2 | Lab 3 | Lab 4 |
| 10.8.1.225/27 | 10.8.1.226 – 228 | 10.8.1.229 – 232 | 10.8.1.233 – 236 | 10.8.1.237 – 240 |

To make this change you might have to elevate privileges. Use the local creds for this (**admin/qwe123$!**).

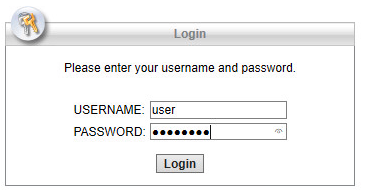


Here is an example for Lab 3:

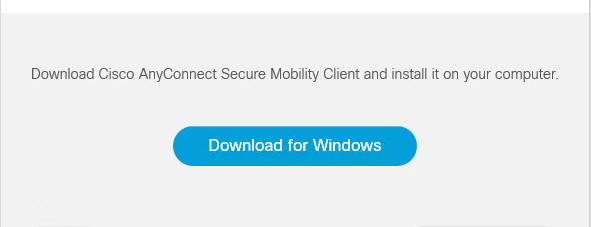


Now we need to install AnyConnect on this PC. Open a web browser and go to <https://your.asa.outside.ip>.

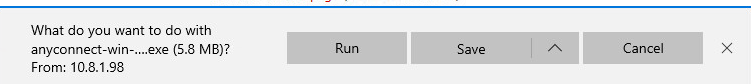
Proceed through the security warnings and log in with the user or your own account.



Click the **Download for windows**.

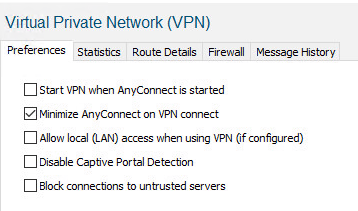


Continue through the security warnings and hit **Run**.

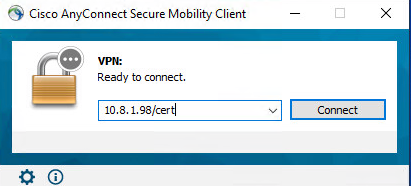


Continue through the install and when prompted for admin user creds use the local again (**admin/qwe123$!**).

Open AnyConnect by clicking on the Windows button and type AnyConnect. Once AnyConnect opens hit the gear icon and uncheck **Block connections to untrusted servers**.



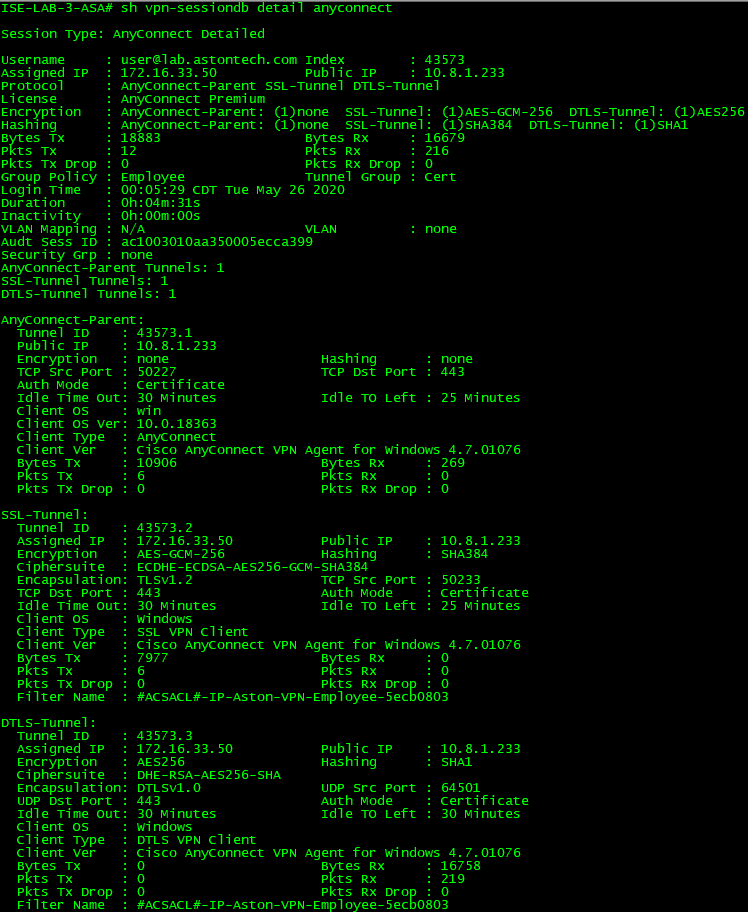
Connect to your ASA using the Cert profile and continue through the security warnings.



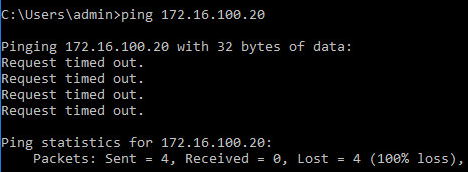
You should now be connected to the VPN. Let’s check the live logs in ISE.

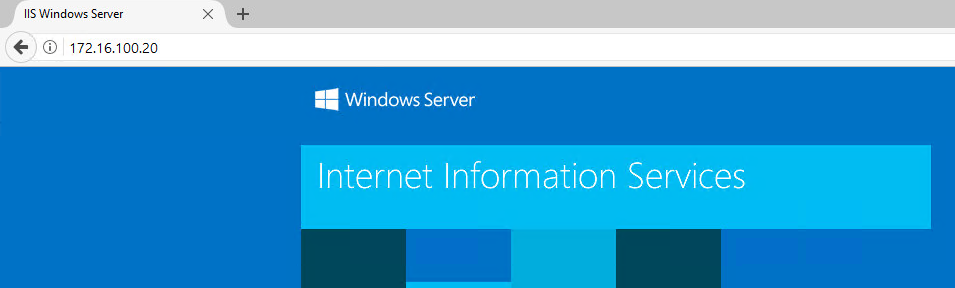


Now if we look at the ASA.



Test pings to the ISE and the DC. Those should fail but you should be able to access them via a web browser.





Conclusion

In this lab, we have:

* Downloaded and installed our internal CA root Certificate
* Added ISE to use as the backend AAA server for RA VPN with authorization only
* Created a new Tunnel Group for certificate authorization
* Edited our AnyConnect Profile to include the new tunnel group for certificate only connections
* Tested both Network Admin and Employee accounts connecting to the VPN with certificates

In the next lab, we will start working on Posturing with ISE.