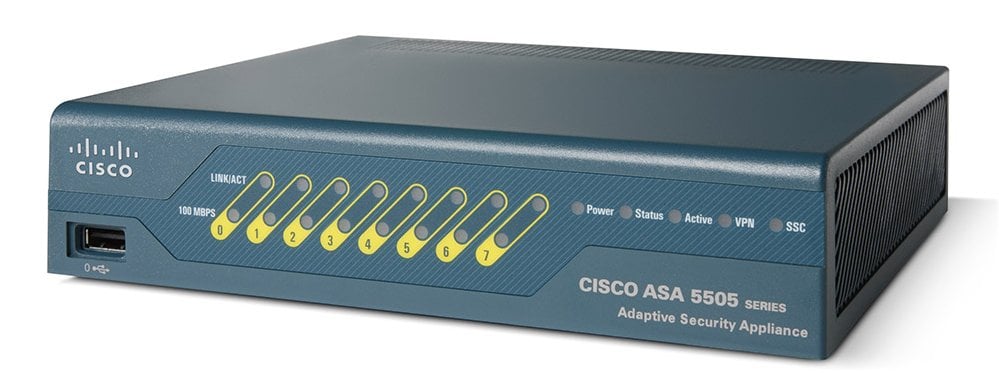
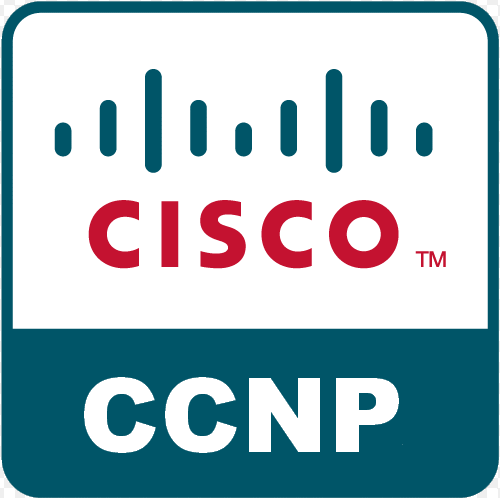
Cisco ASA 5505

Reed Holman | Cybersecurity | 12/1/2022





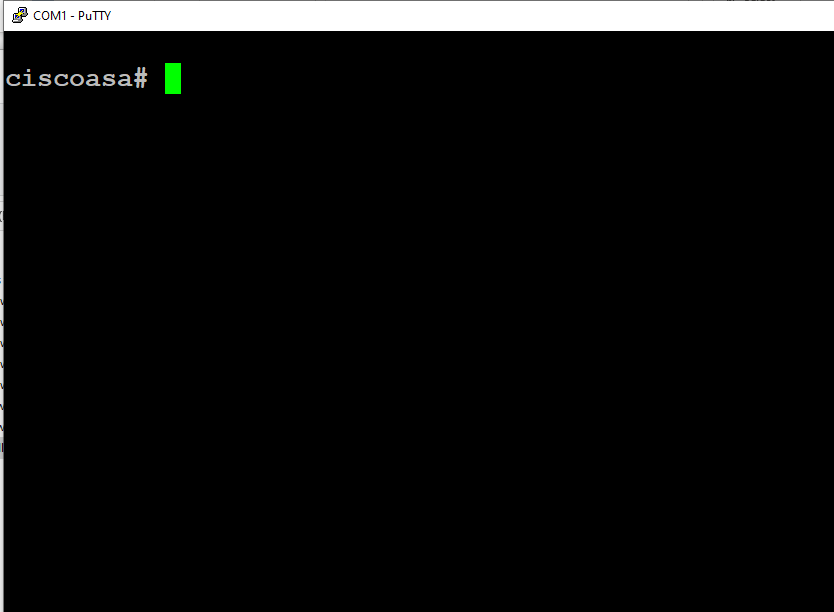
Purpose: To configure a cisco ASA 5505 with SOHO configurations

Background Information:

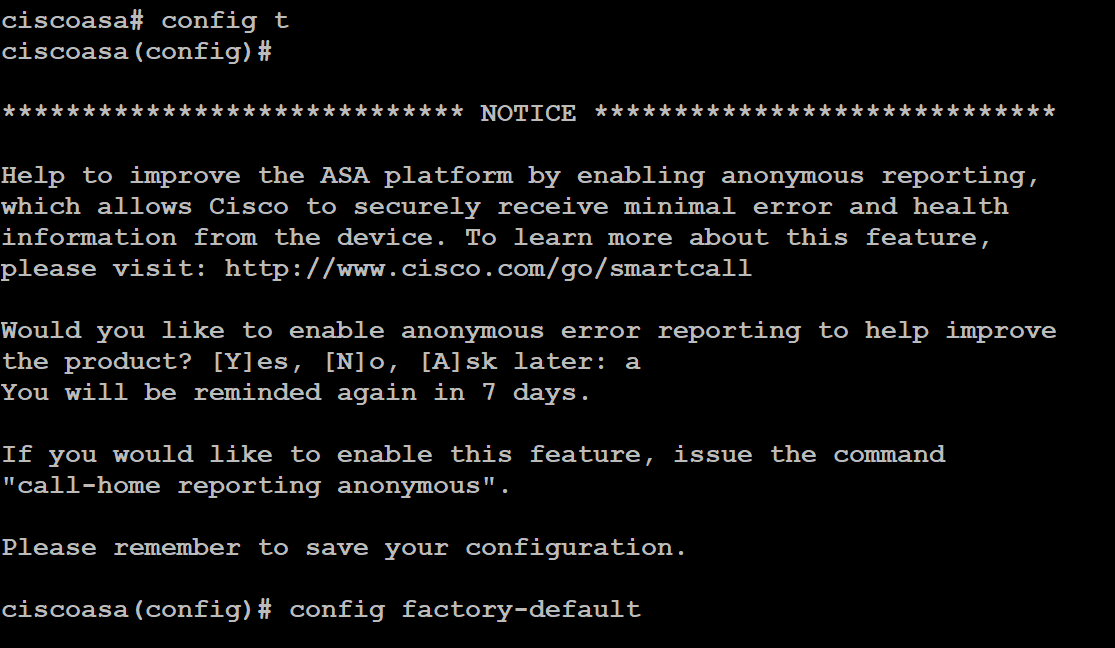
Cisco ASA 5505 or Adaptive Security Appliance is a firewall that is great for small to midsize networks. It has quite a few features like SSL and IPsec VPN, etc. SSL is a a protocol that encrypts and authenticates connects between devices. IPsec VPN is a protocol that also authenticates and encrypts data and will help make your network more secure. One of the major differences between this and the other firewalls we have used is the Cisco Adaptive Security Device Manager (ASDM). It is the program that allows you to manage and make changes to your device. It is the GUI where can monitor and trouble shoot you ASA. It is different from CSM (Cisco Security Manager) because ASDM is more managing a single Cisco ASA while CSM is for managing and setting policies for multiple different devices. All of the other firewalls we used were just directly configured using their web Configurator to make changes. But the Cisco ASA is the only one that required us to install separate software to use it.

Cisco ASA 5505 has two PoE or Power over Ethernet ports which is especially great when setting up Ip phones. You can also upgrade the firewall to get more features with eh Advanced Inspection and Prevention Security Service Card which will give things like intrusion prevention and worm mitigation. You can also upgrade the license to Security Plus. This will support larger networks using a VPN and it has DMZ support. Enabling Cisco AnyConnect client and clientless VPM will help mobile and remote devices connect to your network. That can be a very powerful tool in a network because it allows people working remotely to work on devices that they can’t physically access. Having remote access into your network could potentially be a pretty big security risk. Cisco AnyConnect boast quite a few security features that make it a pretty safe option. One of those features is DNS-Layer security which protects ports from malware, Phishing, and other attacks.

Configurations:



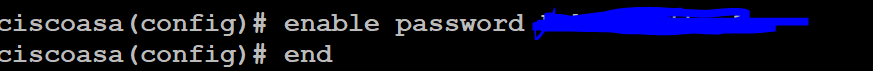
Console into the Cisco ASA



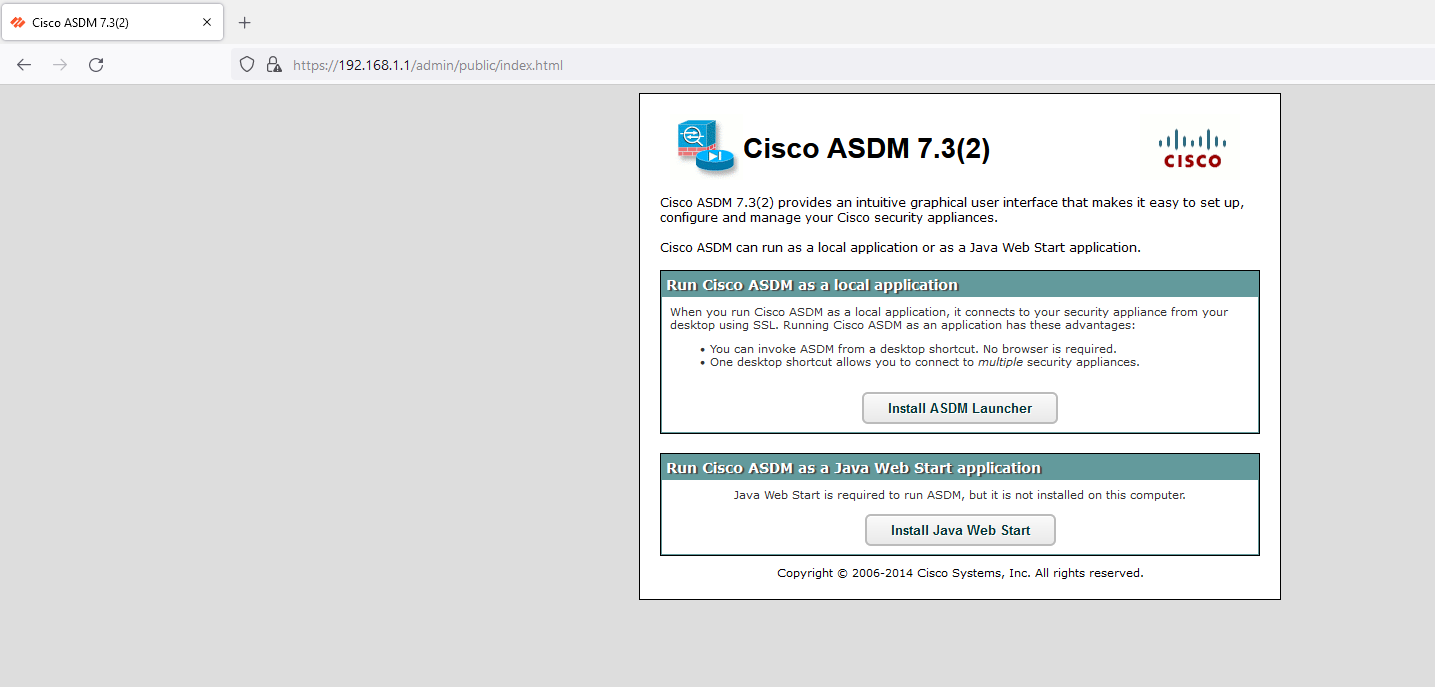
Enter “config factory-default”



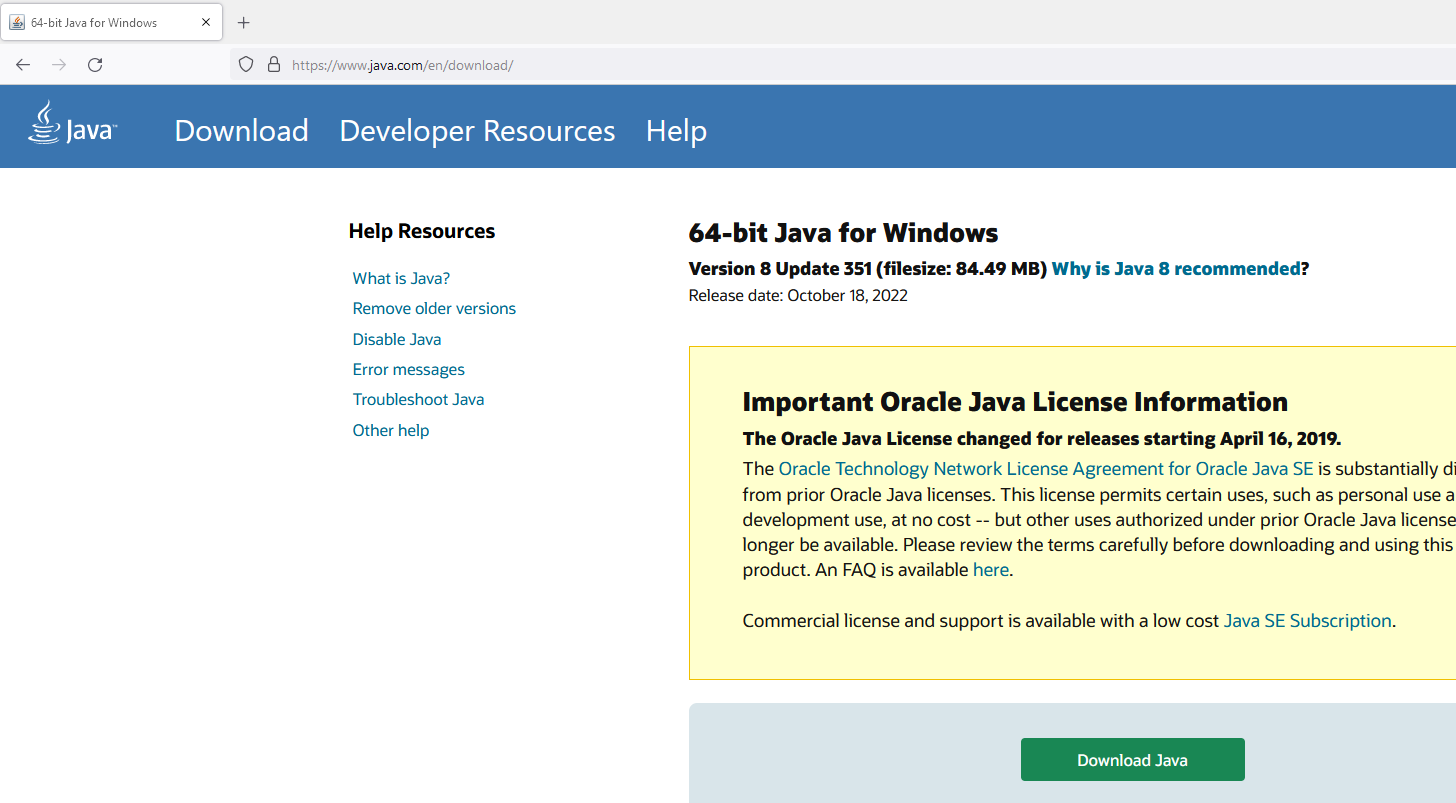
Reload device



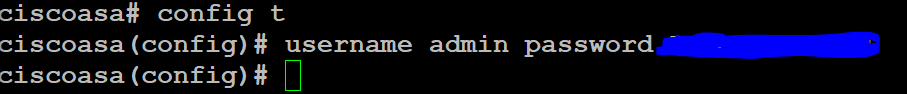
Set a password



Install Cisco ASDM



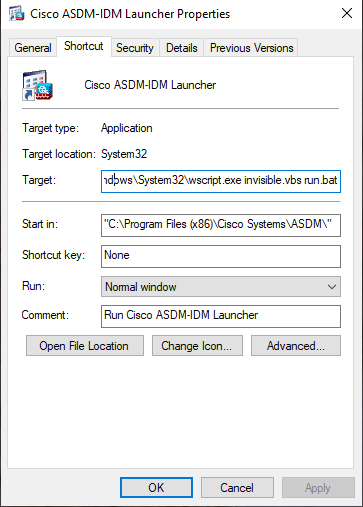
Install Java

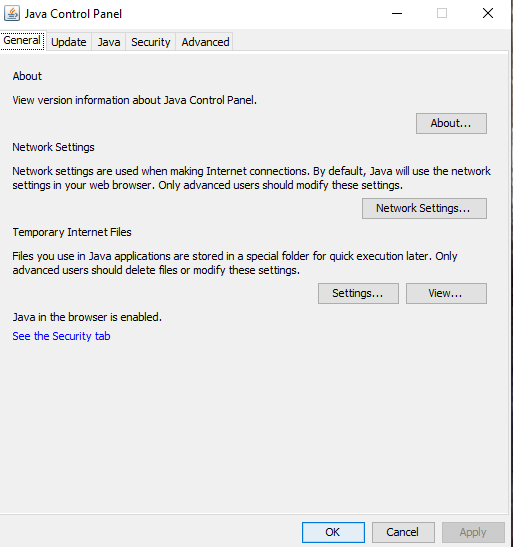


Create a username and password

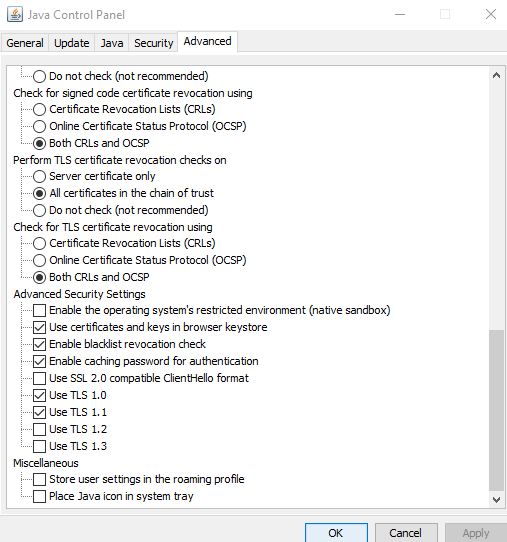
Change Target for ASDM Launcher to

“C:\Windows\system32\wscript.exe invisible.vbs run.bat”

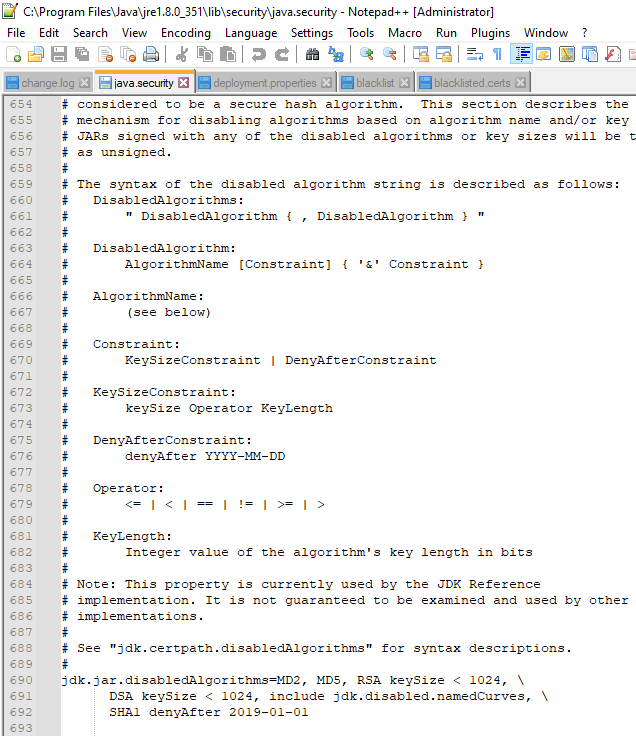




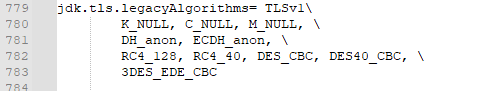
Go to Java Control Panel



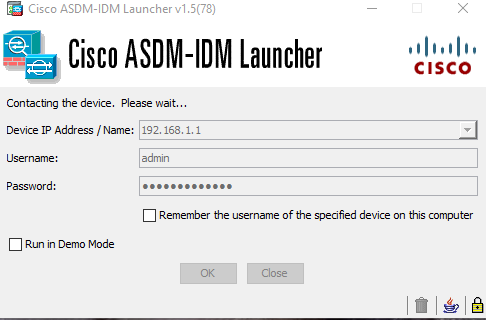
Go to Advanced and check use TLS 1.1



Open Java.security



Allow legacy Algorithms



Login into Cisco ASDM

Problems: We had quite a few problems on this lab. We were not able to launch Cisco ASDM because we needed to change the target for where it was launching to. We also needed to change some of the advanced setting in Java, we didn’t really know why but that is what we found online. We also needed to modify the java.security file to allow certain protocols that were previously blocked. This was kind of hidden and took us a while find but once we did the launcher was able to open.

However, that was not the end of our troubles. Once we were able to open the launcher, we were met with a loading configuration message. It started to load and then the bar got stuck at 17%. We left it alone for a while thinking it might just be slow but after an hour, we conceded that there was in fact something wrong. We tried rebooting our firewall, but it still wouldn’t go past 17%. We tried changing quite a few settings, but nothing changed. We did some research online and learned that we were not the only ones with this problem. It might be an issue with the version that our firewall was running not being compatible with the version of the launcher it told us to install. We tried to install an older version of ASDM software but every time we tried to use it, the launcher would lock us out and prompt us to update to a newer version. Some sources online told us to try and modify our java somehow, but we could never get that to change anything.

Conclusion:

This lab had quite a few problems and was the only lab we were not able to get fulling working. We learned a lot about the process of troubleshooting and scouring the internet for answers. I wish we got to explore the ASDM because it seemed different from the over configurators that we have used. I want to try this lab again, maybe with a different router that is on a newer version.