Implementing Chromebooks with WPA2-Enterprise (802.1x)

Scott Harpster

Southwest Educational Development Center

Purpose:

After following these steps, a user should be able to login to the wireless network through RADIUS using their (LDAP) username and password. The Certificates should be auto deployed via the Google Management Console.

What you need:

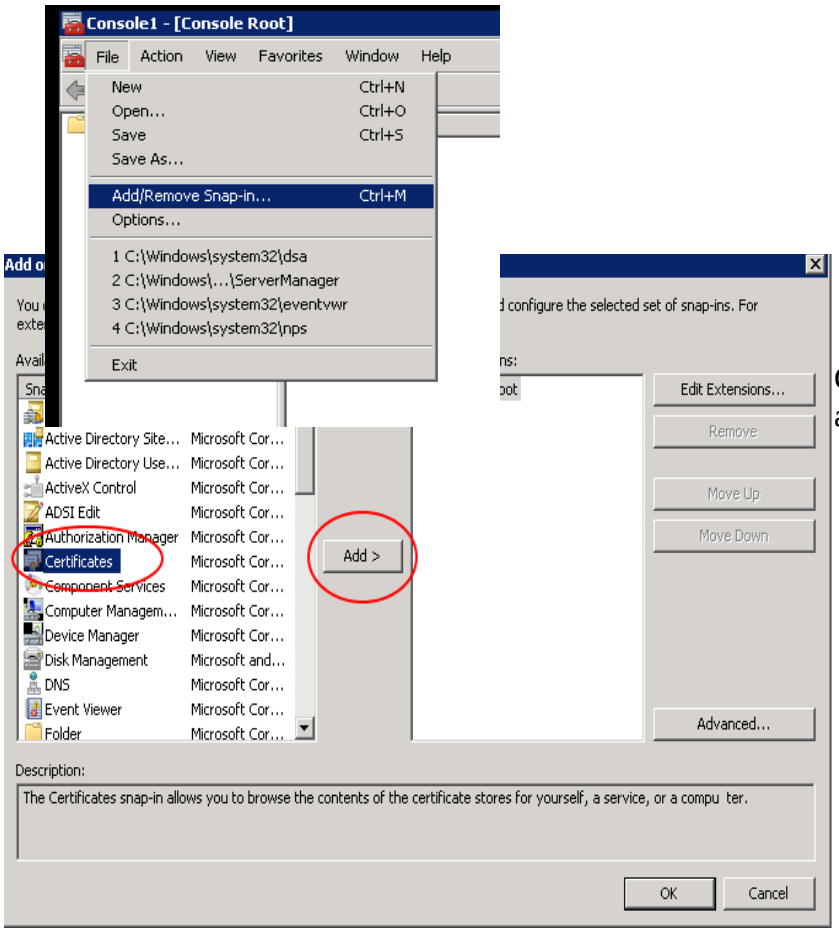
1. A chromebook
2. Access to the RADIUS server (Network Policy Server if your using Microsoft's Solution)
3. Access to the Chromebook Management Console (Optional: For auto deployment of Certification and wireless network settings)

Steps:

RADIUS

Log in to your radius server. Open up Start → run → type in mmc for the Microsoft Management Console.

File → Add / Remove Snap-ins.

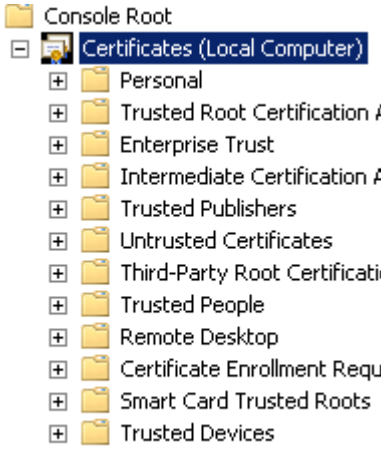


Click on Certificates and then click on add which is in the middle.

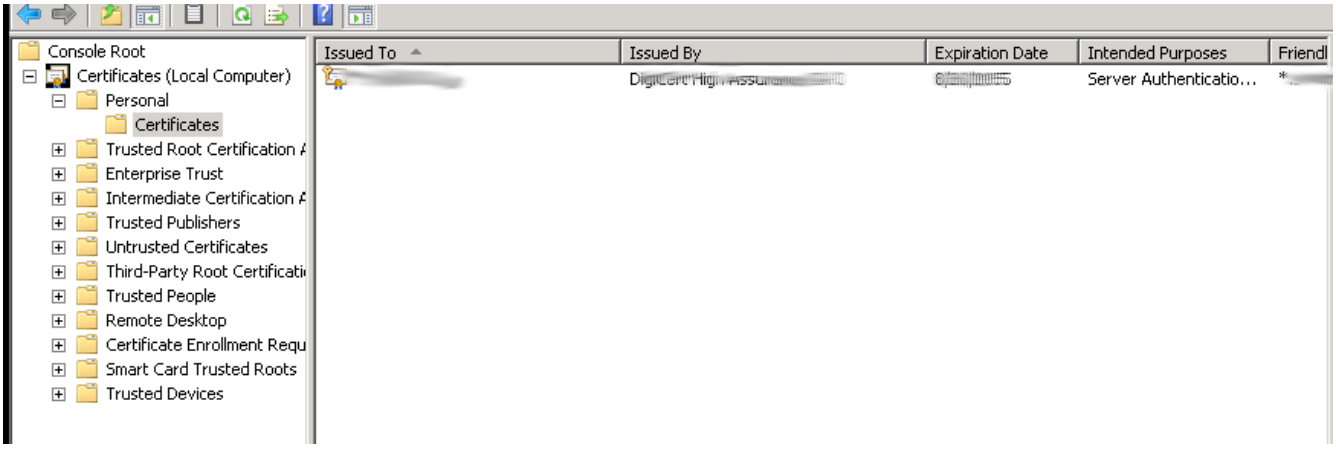
Click on the Computer Account and click Next.

Leave Default and Click Finish.

You should now see a Certificates Folder, expand it. Then expand the Personal Folder, then expand the Certificates Folder.



You should see something like this, with a cert in it that is being used for your RADIUS. You may see more then what I have shown.

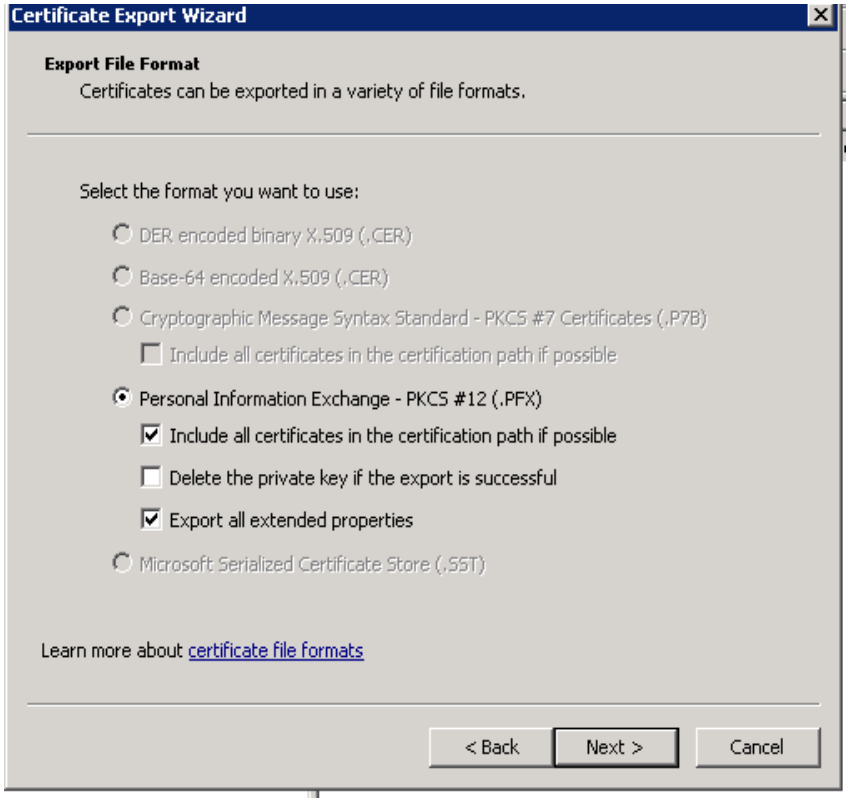


You will want to then right click on it and select

All Tasks → Export.

Click Next → Yes, Export the Private Key. (This will make is a .p12 which is what chrome wants)

Click Next → Check all **EXCEPT DELETE THE PRIVATE KEY.** So in total you have 2 checked.



It will prompt for a password. Type one in and right it down. You will need this.

You now have what the chromebook wants. Save to a USB Drive.

Chromebook Certificate Import

Turn the chromebook on, open up the settings on the chrome browser option box.

Scroll to the bottom and click on “Show Advanced Settings”.

Click on Manage Certificates.

Click on Import → Location the Certificate, make sure you take off the .p12 filter on the bottom right of the filebox and make it say All Files. You should find a .pfx cert and import that. This SHOULD go through and work.

It will prompt for a password, type in the password you wrote down from the export.

Chromebook Wireless Setup

Now that the certificate is installed. Go to the wireless settings. Settings → +Add Connection

Click on Advanced.

Type in the SSID.

EAP Method: PEAP

Phase 2 Authentication: MSCHAPv2

Server CA certficate: Default or if you can pick one pick it.

User Certificate: This should have your certificate, unless the server ca shows up.

Identity: AD Username

Password: AD Password

Now click connect. This **SHOULD** work.

Before you leave the chromebook, go back to the certificate management, do an export of it and save it on your usb drive.

Chromebook Management Console

Login to the management console. Goto Settings-> Devices

Pick the organization you want to have the certificate.

Click on Network → Manage Certificates.

Import that certificate that was exported from the chromebook.

Click on add Wireless, Fill out as much as you can using the previous wireless network settings from the chromebook. For AD authentication, I would leave this blank so students have to use their AD login credentials.

Save it.

This takes a few hours to reach the chromebooks. The chromebooks need internet to get the updates so dont turn off a preshared key wifi until the Chromebooks have been given a chance to get the certificate.

After these steps you should be able to connect to a wireless network that does WPA2-Enterprise with 802.1x Authentication. Your chromebooks should auto receive a certificate allowing users to login with AD.