

# CCPLD WiFi Instructions

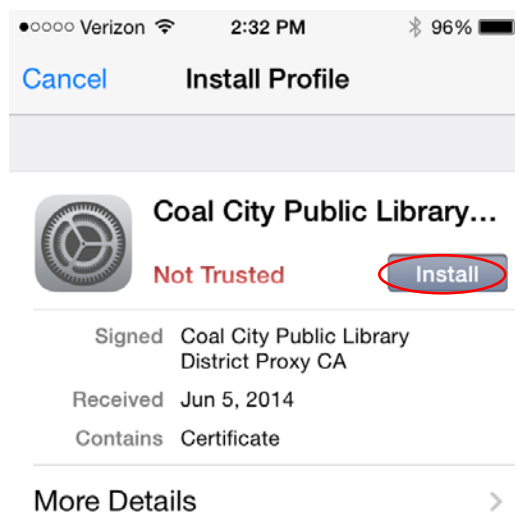
Android Devices .....	1
iPhone/iPad .....	1
Macintosh.....	2
Internet Explorer – Method 1 – Download and OPEN option given.....	3
Internet Explorer – Method 2 – Download and SAVE or SAVE AS option given.....	6
Google Chrome .....	7
Certificate Import Wizard Instructions .....	8
Firefox .....	9
Safari .....	9
Google Chromebook .....	9

## Android Devices

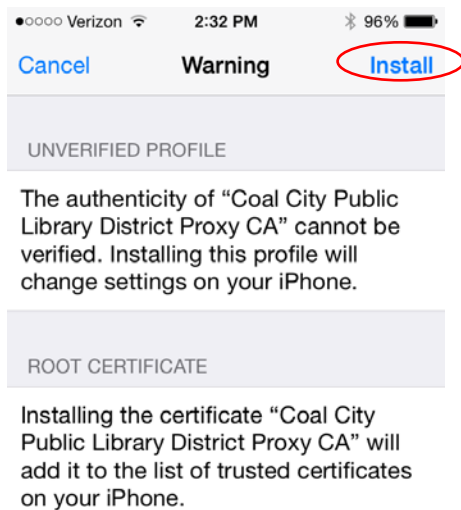
1. Go to: <http://ccpld.org/certs/ccpld.p12> to obtain the certificate
2. The certificate will take a few moments to load.
3. Once the certificate has loaded, it will ask for a password key – the password is 1234
4. Type this in and install the certificate in the Trusted Root Certificates if you are given an option.

## iPhone/iPad

1. Go to: <http://passthrough.fw-notify.net/cacert.pem> to obtain the certificate
2. Click on Install:



- The following screen on the left will appear, click install. You will know the certificate is installed once you see the screen on the right:



## Macintosh

- In any web browser go to : <http://passthrough.fw-notify.net/cacert.pem> and download the certificate to your downloads folder.
- Once downloaded, double click the certificate. This launches Keychain Access and displays a Certificate not Trusted warning.
- Click **Always Trust** to import the certificate into Login Keychain.

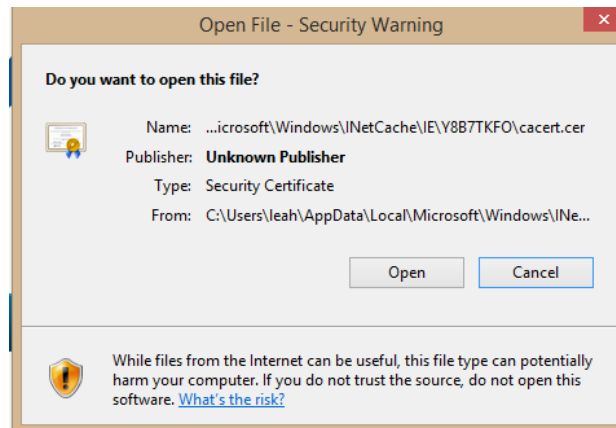
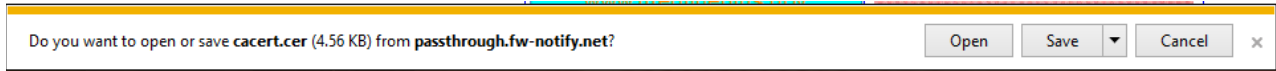
Still having issues? Please read:

The most common reason a certificate isn't accepted is that the certificate authority's root certificate isn't trusted by your computer. To have your computer trust a certificate authority, you must add the certificate authority to a keychain and set the certificate trust settings.

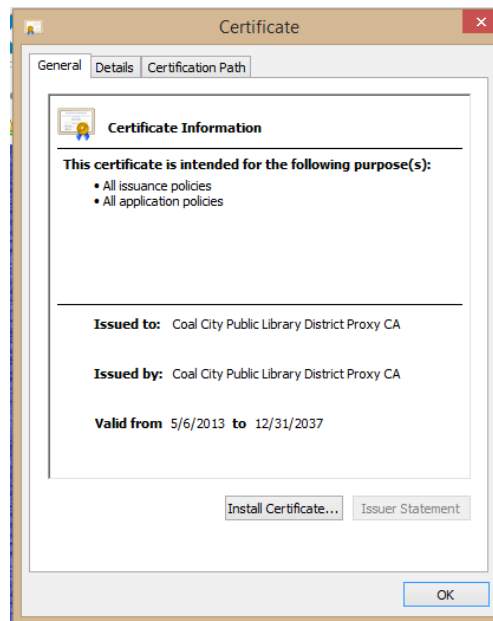
- If an app (such as Safari) displays the root certificate from the certificate authority as part of the message from the certificate authority, drag the root certificate icon to the desktop.
- Drag the certificate file onto the Keychain Access icon, or double-click the certificate file.
- Click the keychain pop-up menu, choose a keychain, then click OK.  
If you're asked, enter the name and password for an administrator user on the computer.
- Select the certificate, then choose File > Get Info.
- Click the Trust disclosure triangle to display the trust policies for the certificate.
- To override the trust policies, choose the trust settings you want to override from the pop-up menus.

## Internet Explorer – Method 1 – Download and OPEN option given

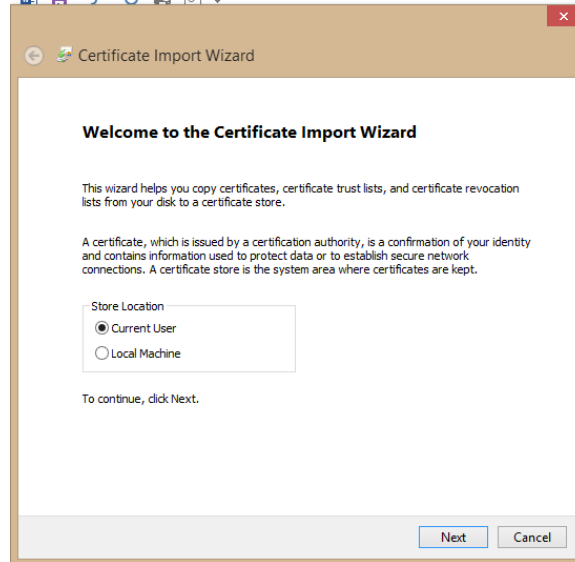
1. In Internet Explorer, go to: <http://passthrough.fw-notify.net/cacert.pem> to obtain the certificate.
2. You may receive security warning(s) like the following, click Open:



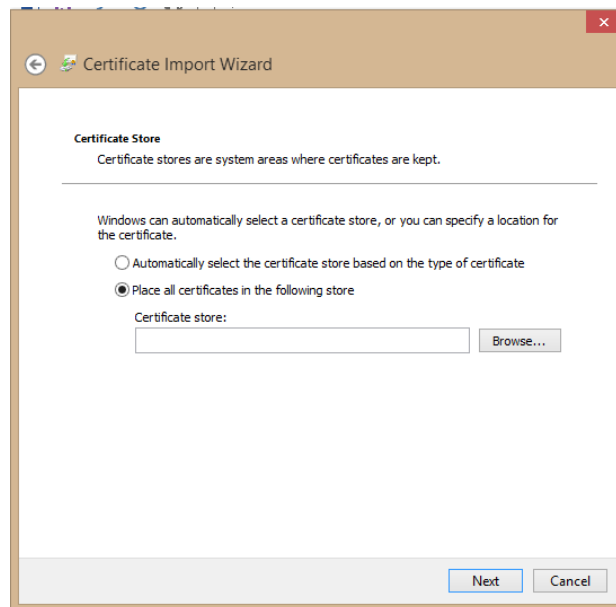
3. Click Install Certificate.



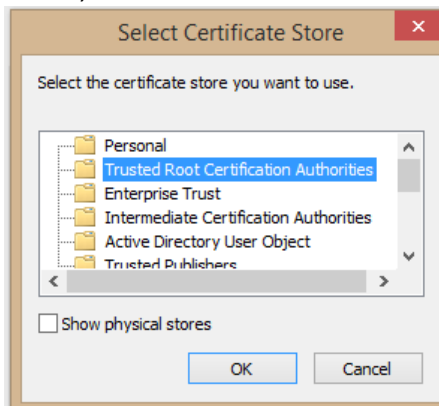
4. In the Certificate Import Wizard window click Next.



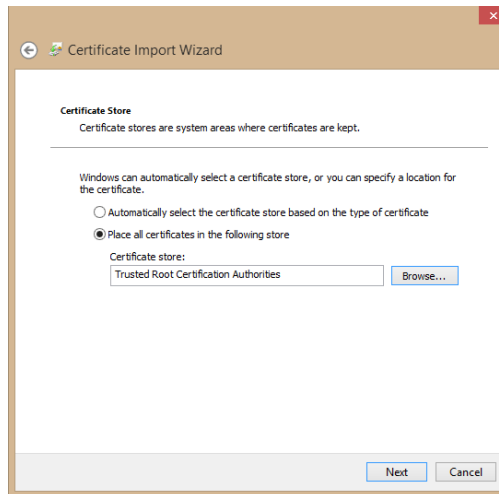
5. In the Certificate Store window, select Place all certificates in the following store and then click Browse.



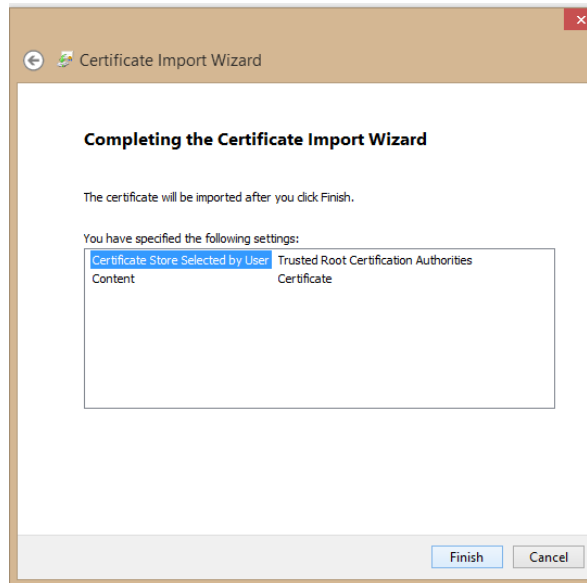
6. In the Select Certificate Store window, select "Trusted Root Certification Authorities" and click OK.



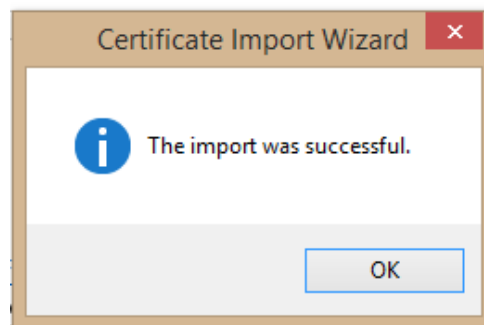
7. In the Certificate Store window, the Certificate store: shows Trusted Root Certification Authorities. Click Next then click Finish.



8. If you have done the steps correctly, you should see a screen similar to this, click Finish.



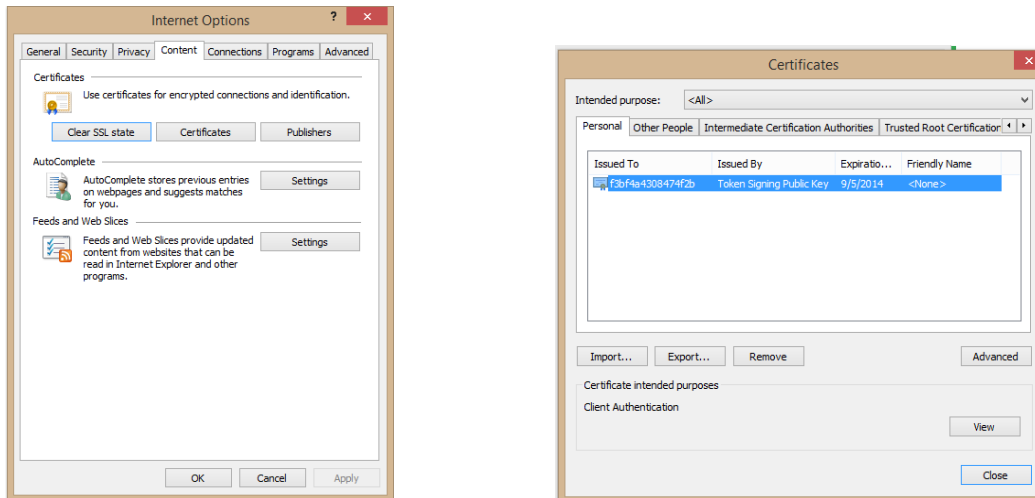
9. The Certificate Import Wizard will notify you that "The import was successful." Click OK to finish.



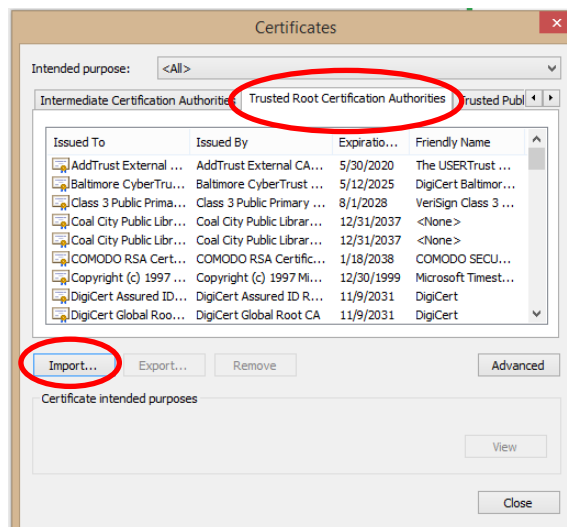
10. Exit Internet Explorer and any other browsers that may be open, and restart your preferred browser.

## Internet Explorer – Method 2 – Download and SAVE or SAVE AS option given

1. In Internet Explorer, go to: <http://passthrough.fw-notify.net/cacert.pem> to obtain the certificate – click Save when prompted.
2. In the Menu Bar, click **Tools > Internet Options** to display the Internet Options window.
3. Switch to the **Content** tab and, under the Certificates section, click **Certificates** to display the Certificates Window.




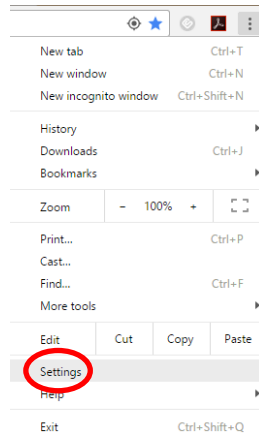
4. Switch to the **Trusted Root Certification Authorities** tab and click the Import button to start Certificate Import Wizard.



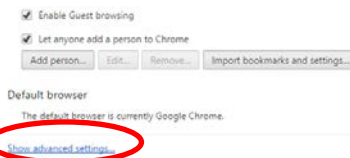
5. Follow the directions for Certificate Import Wizard on page 8 and exit browser and any other browsers that may be open. Restart your preferred browser.

## Google Chrome

1. In Google Chrome, go to: <http://passthrough.fw-notify.net/cacert.pem> to obtain the certificate – it will automatically download.
2. To the right of the Address Bar, click on **Customize and control Google Chrome** button  and click **Settings**.



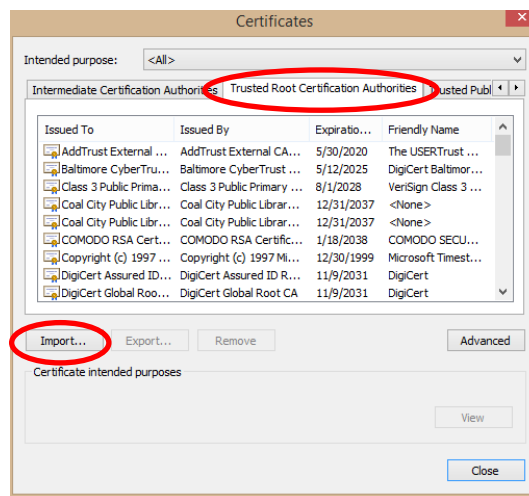
3. Click **Show advanced settings** and scroll down to HTTPS/SSL.



4. Click **Manage Certificates...** to display the Certificates window.



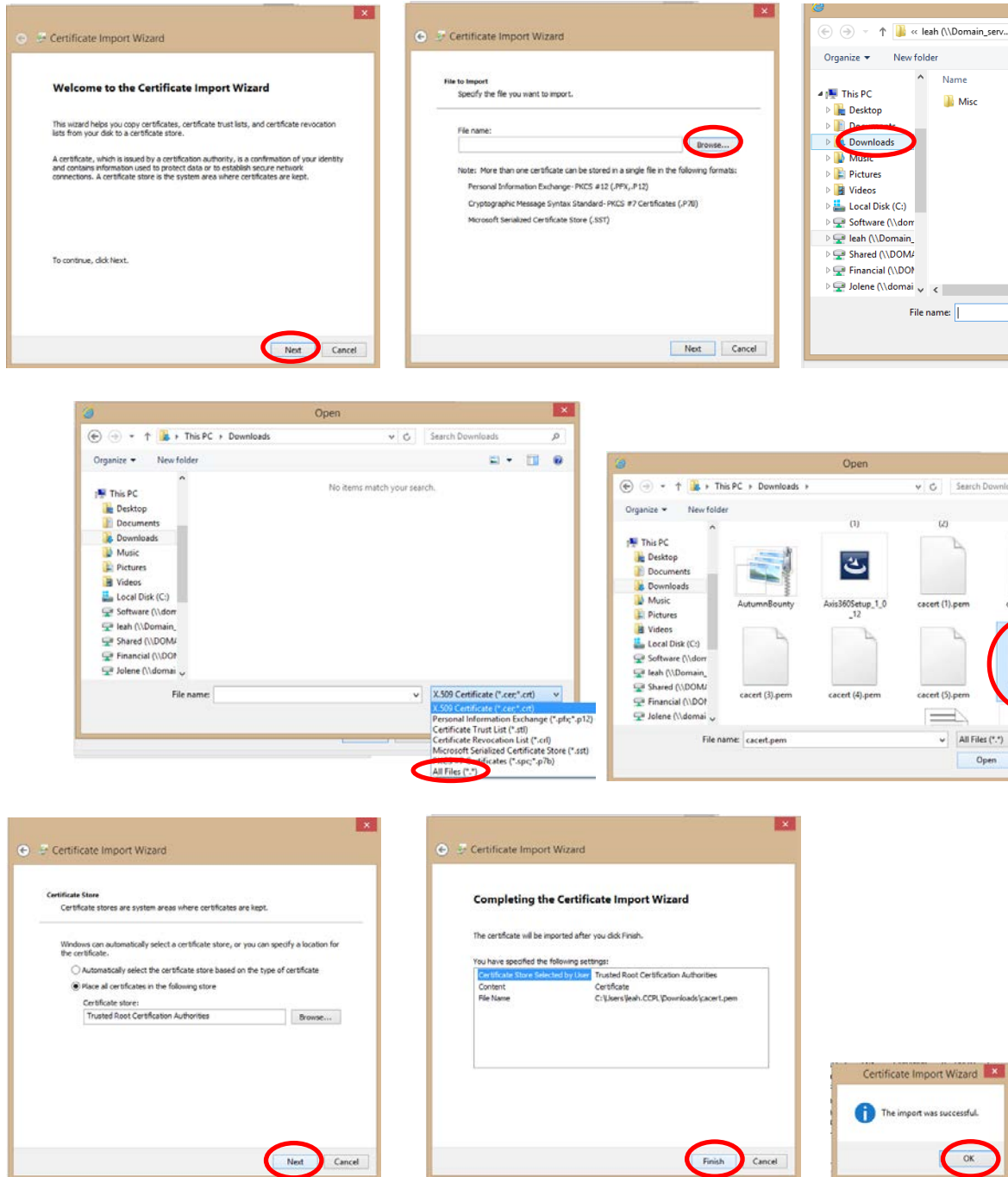
5. Switch to the **Trusted Root Certification Authorities** tab and click the **Import** button to start Certificate Import Wizard.



6. Follow the directions for Certificate Import Wizard on page 8 and exit browser and any other browsers that may be open. Restart your preferred browser.

# Certificate Import Wizard Instructions

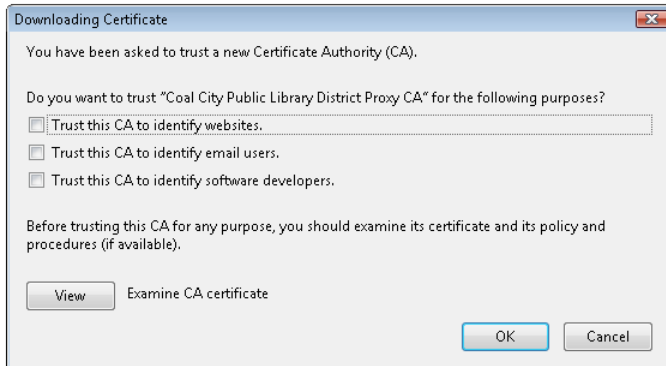
Click Next, then Browse, click on the Downloads file to find the certificate file. You will need to pull down and select ALL Files (\*.\*) in order to find the certificate. Choose the file cacert.pem and click Open. Click Next and then Finish.





## Firefox

1. In Firefox, go to: <http://passthrough.fw-notify.net/cacert.pem> to obtain the certificate.
2. In the Downloading Certificate window, select **Trust this CA to identify websites** and click **OK**.




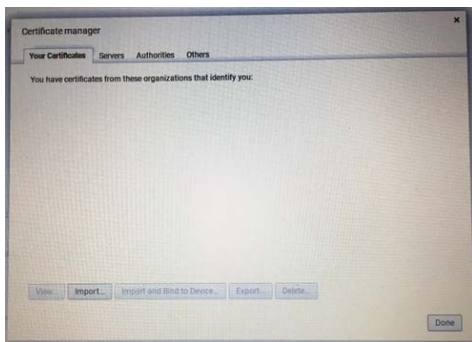
3. Restart the Firefox browser.

## Safari

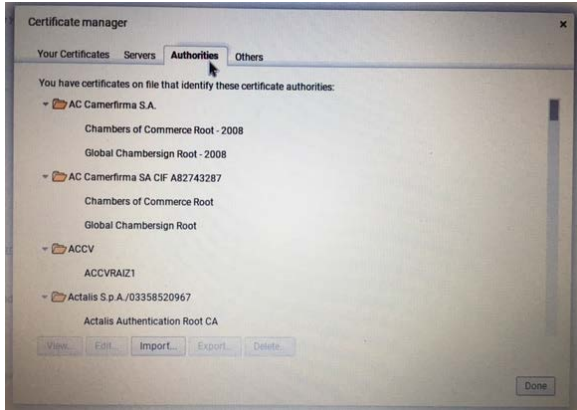
1. In Firefox, go to: <http://passthrough.fw-notify.net/cacert.pem> to download the certificate.
2. Once downloaded, double-click the Certificate. This launches Keychain Access and displays a Certificate Not Trusted warning.
3. Click **Always Trust** to import the certificate into Login Keychain.

## Google Chromebook

1. In Chrome, go to: <http://passthrough.fw-notify.net/cacert.pem> to download the certificate.
2. Open a new tab in Chrome .
3. In the address bar, enter <chrome://settings/certificates>



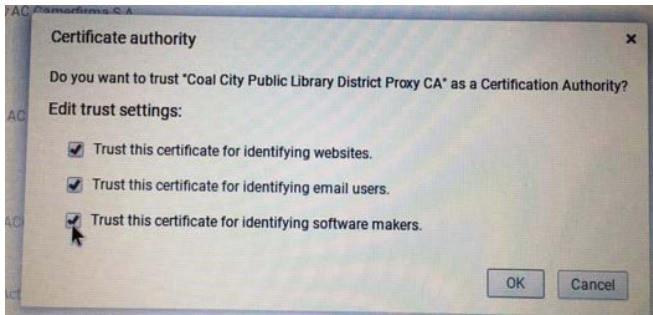
4. Click the **Authorities** tab.



5. Press the **Import** button and choose the X.509 certificate file, which is usually a file with a .pem, .der, .crt, or .p7b extension.



6. In the box that appears, fill out the information on how this certificate should be trusted. None of these trust settings need to be enabled, so we recommend that you leave these unchecked.



7. The certificate will open and install itself on your Chromebook.