

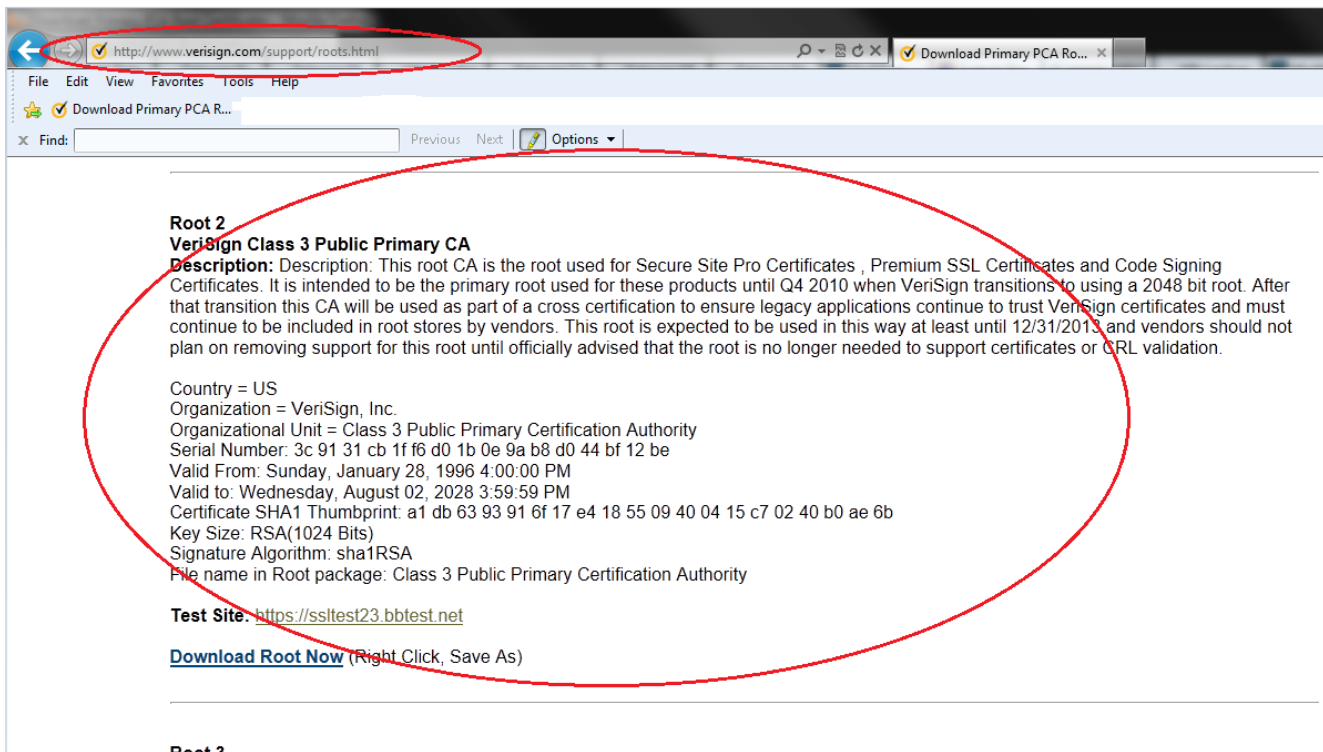
# How to Download and Install SSL Certificates - Windows

This guide lists the steps to Download and Install the SSL Certificates using Windows for your Datawire API to work with the Datawire systems.

To connect to the Datawire Network, the below SSL Certificates are required:

- Root 2 VeriSign Class 3 Public Primary CA (exp 8/2/2028)
- Root 3 VeriSign Class 3 Primary CA - G5 (exp 7/16/2036)
- Equifax Secure Certificate Authority (exp 8/22/2018)

1. Go to <http://www.verisign.com/support/roots.html> and look for “Root 2 VeriSign Class 3 Public Primary CA” (exp 8/2/2028) and “Root 3 VeriSign Class 3 Primary CA - G5” (exp 7/16/2036).



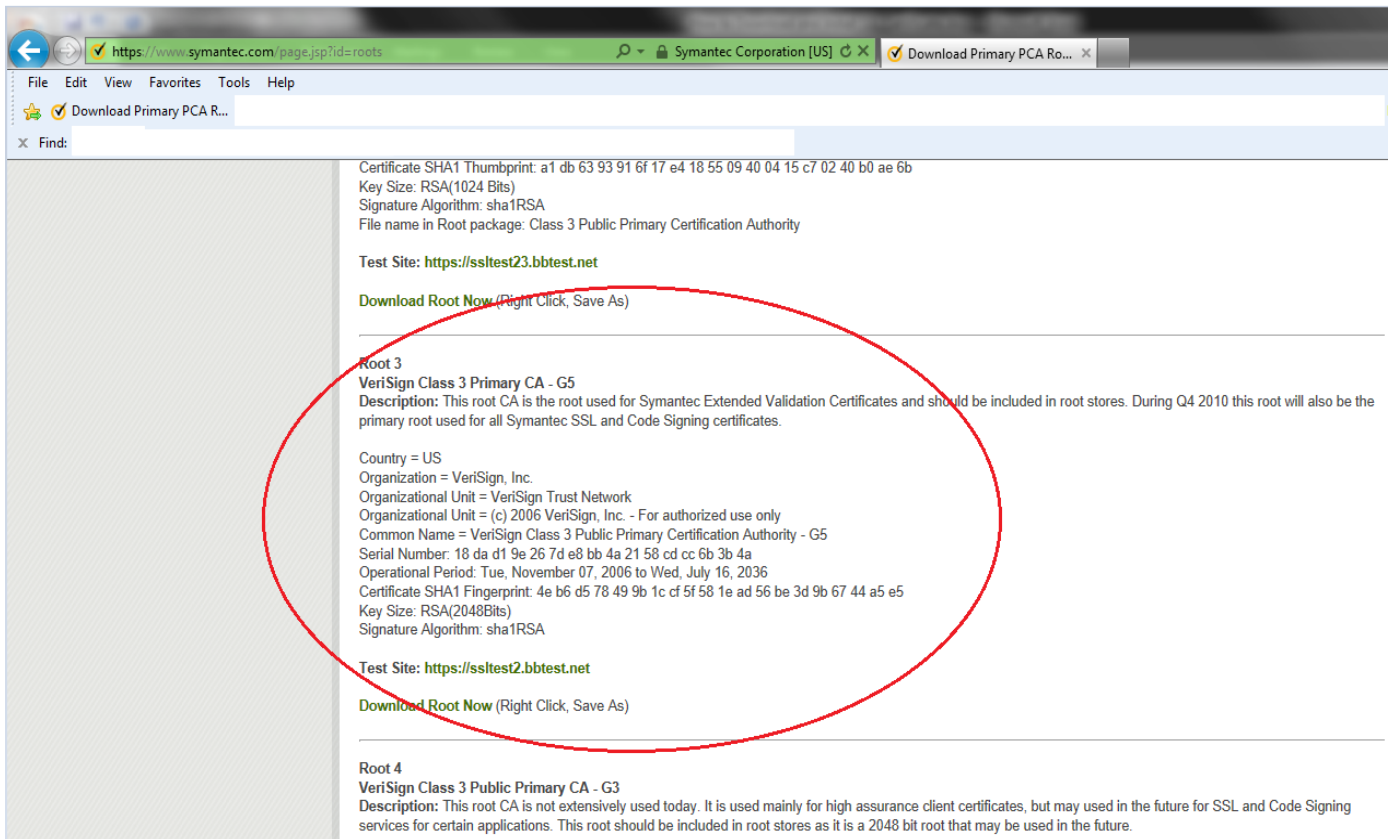
**Root 2**  
**VeriSign Class 3 Public Primary CA**  
**Description:** Description: This root CA is the root used for Secure Site Pro Certificates , Premium SSL Certificates and Code Signing Certificates. It is intended to be the primary root used for these products until Q4 2010 when VeriSign transitions to using a 2048 bit root. After that transition this CA will be used as part of a cross certification to ensure legacy applications continue to trust VeriSign certificates and must continue to be included in root stores by vendors. This root is expected to be used in this way at least until 12/31/2013, and vendors should not plan on removing support for this root until officially advised that the root is no longer needed to support certificates or CRL validation.

Country = US  
Organization = VeriSign, Inc.  
Organizational Unit = Class 3 Public Primary Certification Authority  
Serial Number: 3c 91 31 cb 1f f6 d0 1b 0e 9a b8 d0 44 bf 12 be  
Valid From: Sunday, January 28, 1996 4:00:00 PM  
Valid to: Wednesday, August 02, 2028 3:59:59 PM  
Certificate SHA1 Thumbprint: a1 db 63 93 91 6f 17 e4 18 55 09 40 04 15 c7 02 40 b0 ae 6b  
Key Size: RSA(1024 Bits)  
Signature Algorithm: sha1RSA  
File name in Root package: Class 3 Public Primary Certification Authority

**Test Site:** <https://ssltest23.bbtest.net>

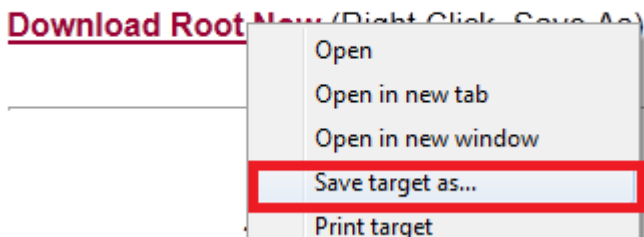
**Download Root Now** (Right Click, Save As)

**Root 3**

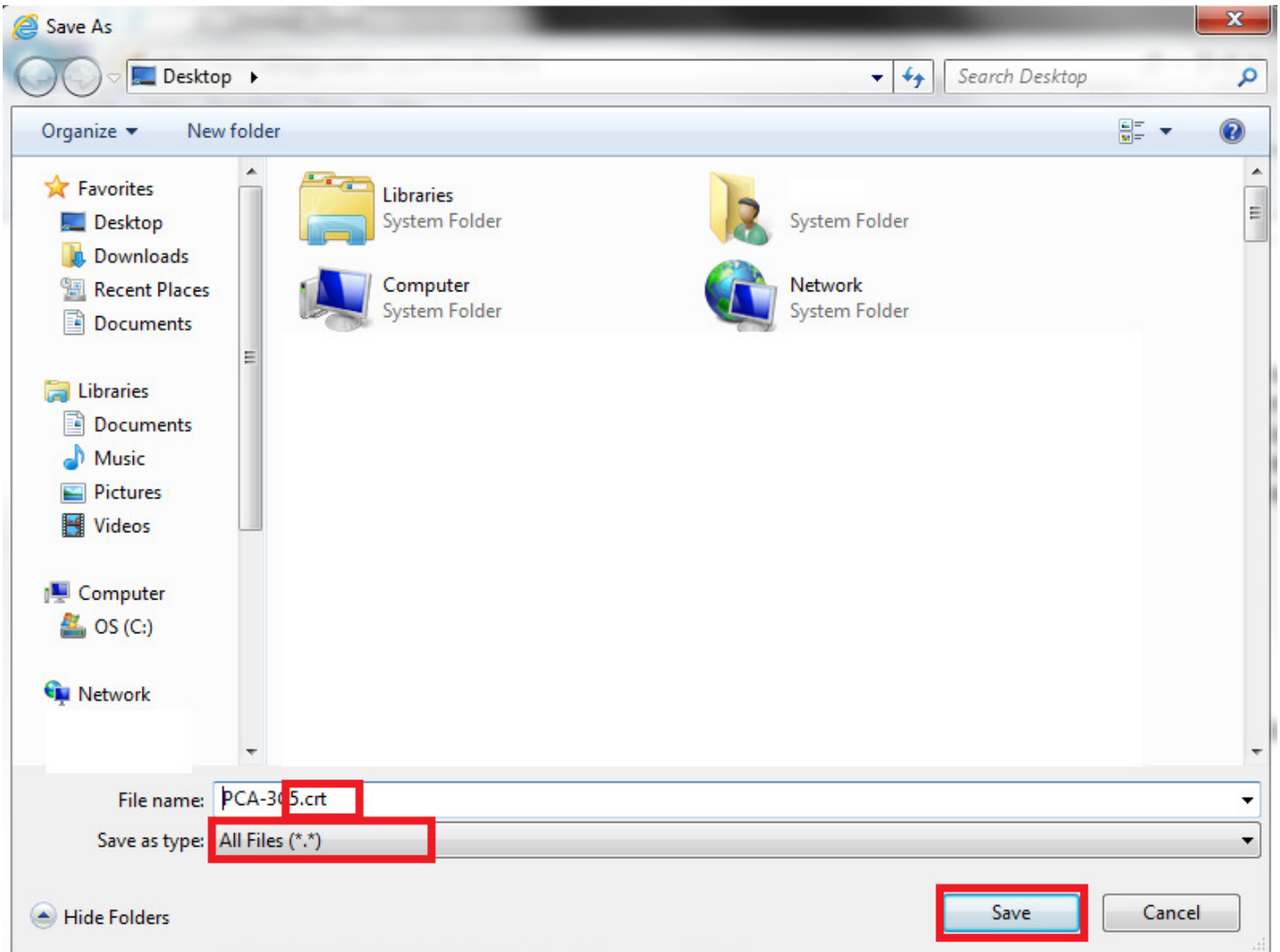


2. Right Click on “Download Root Now” and ‘Save As’

**Test Site:** <https://ssltest23.bbtest.net>

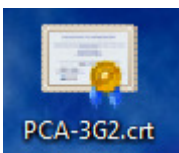


3. Change the ‘Save as Type’ to ‘All Files (\*.\*)’ and rename the file extension from ‘.htm’ to ‘.crt’.



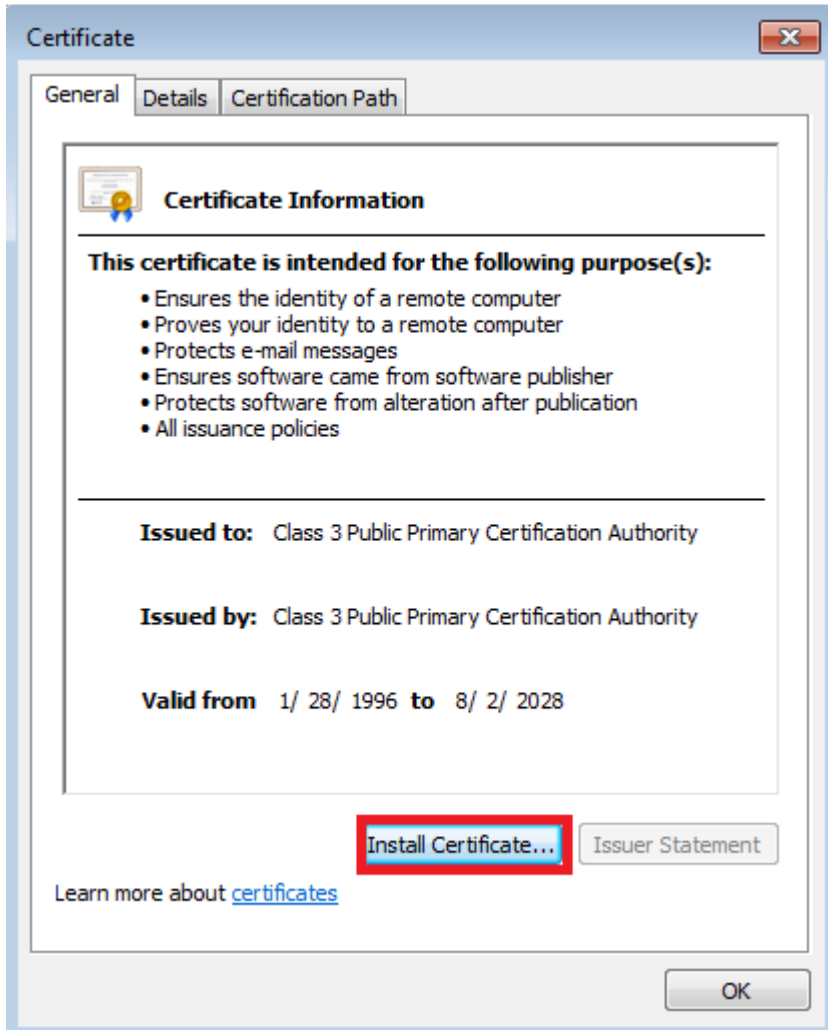
4. Click 'Save'.

If the file was saved in the correct format, the icon should appear as below:



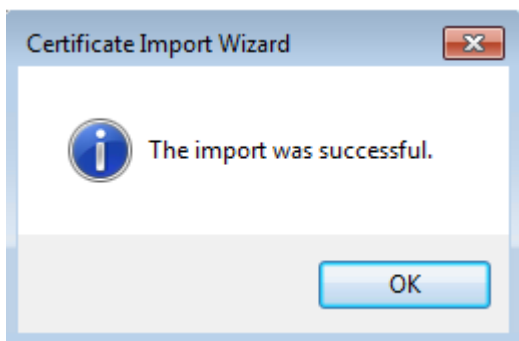
To Install:

- Using an ADMIN privilege account, double click on the icon. You should see the below.

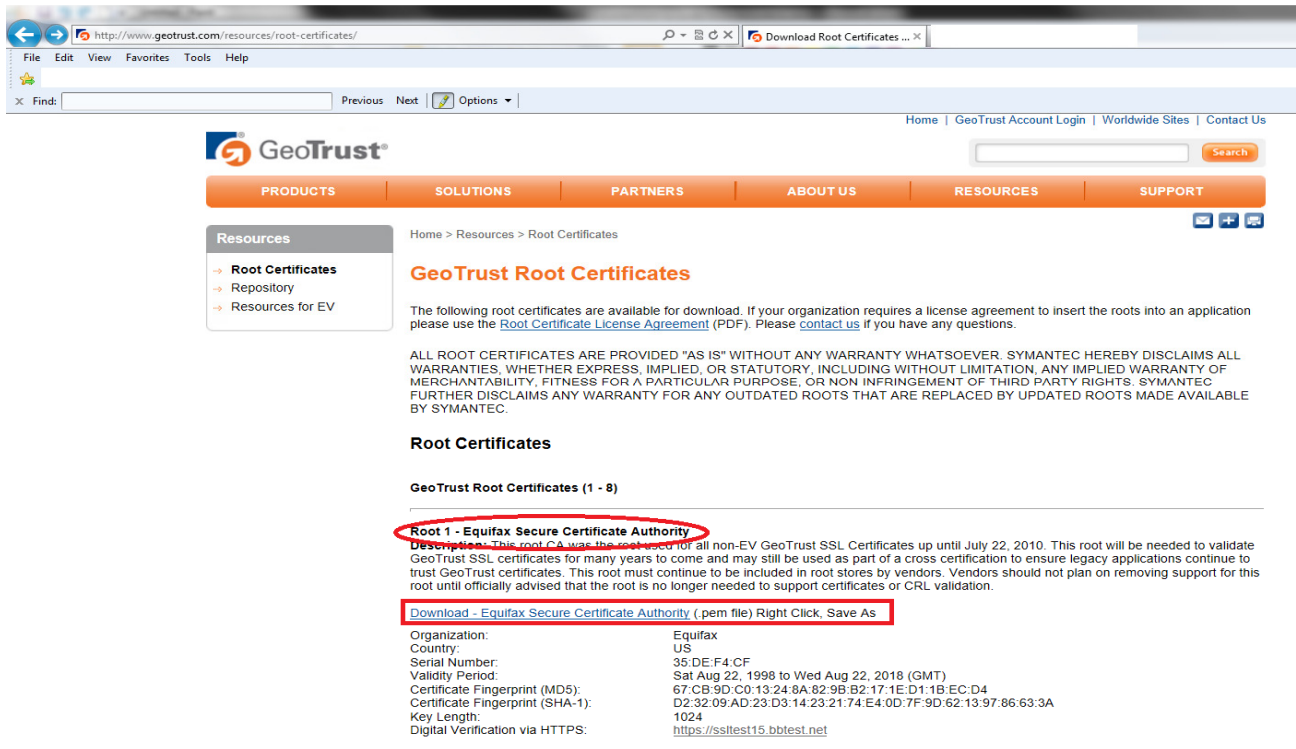


- Click on "Install Certificate..." (Note, if you're not logged in as 'admin' the 'install certificate' option will be grayed out).
- Go through the Set Up Wizard and follow the defaults.

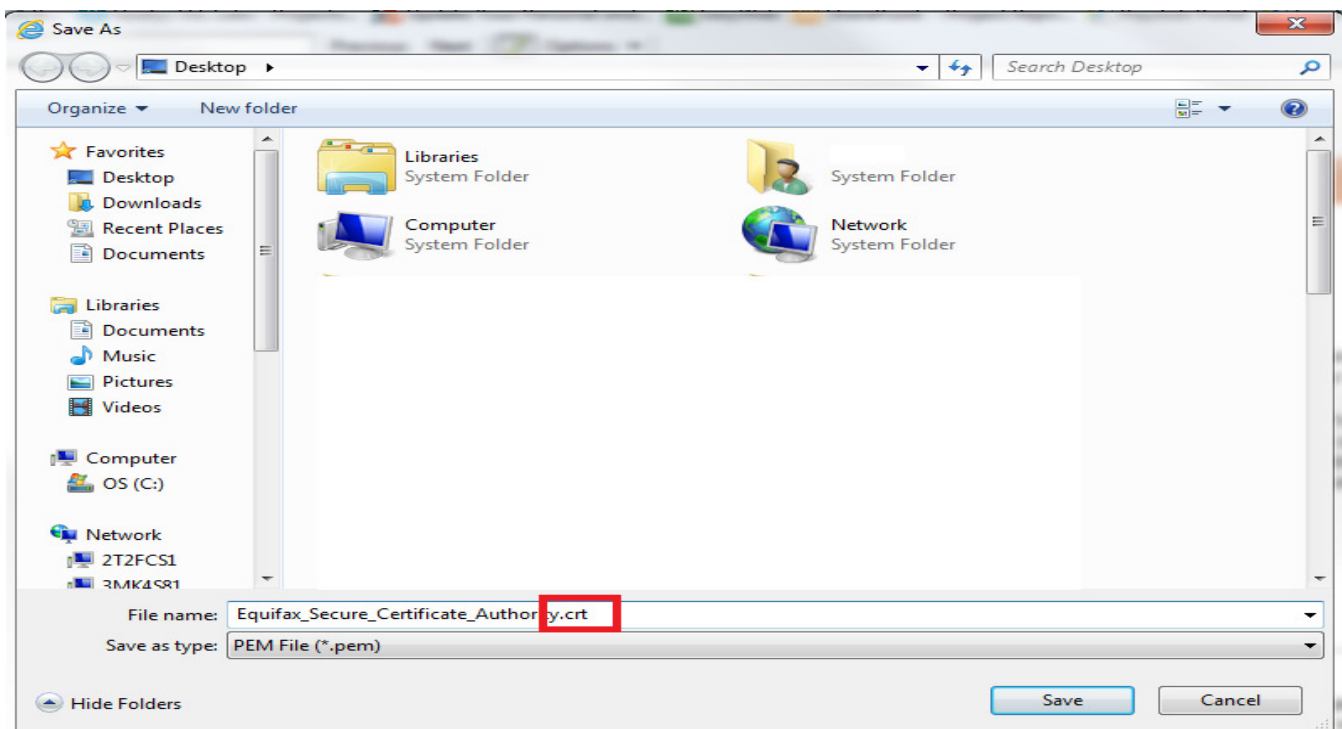
If completed successfully, you should see this:



1. Go to <http://www.geotrust.com/resources/root-certificates/> and look for “Root 1 – Equifax Secure Certificate Authority” (exp 8/22/2018).



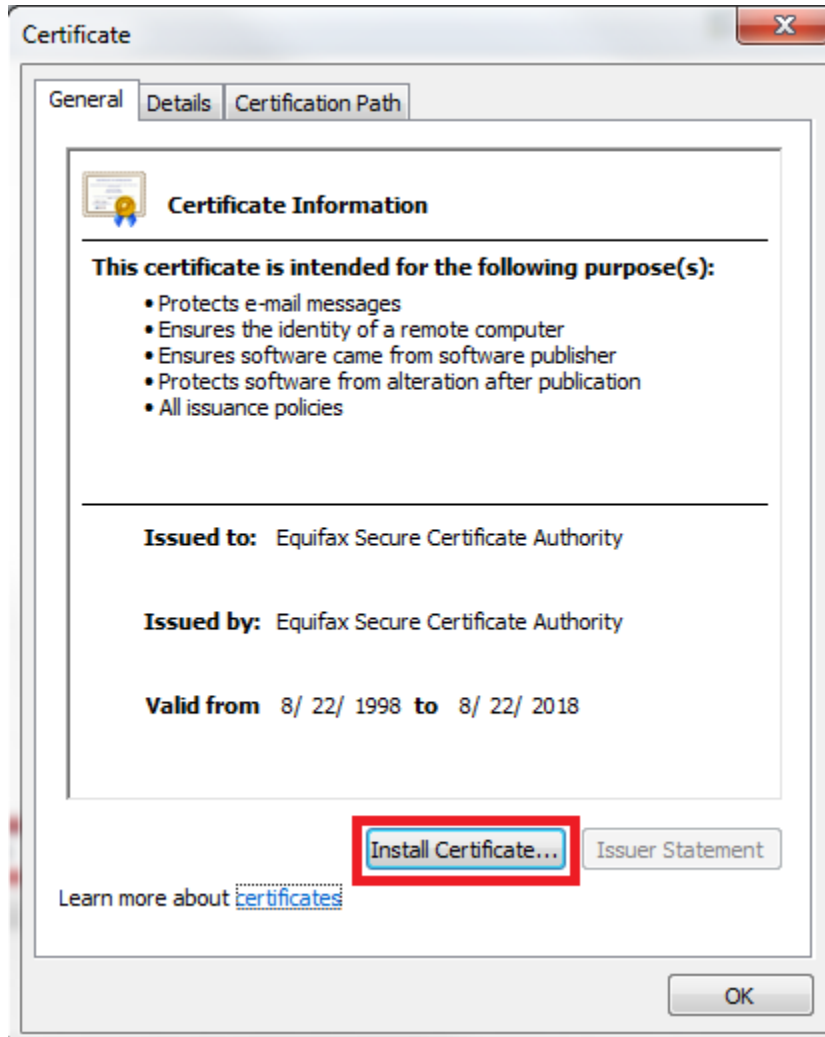
2. Right Click on “Download – Equifax Secure Certificate Authority” and “Save Target As”. Manually change the file extension from .pem to .crt (screen shot below).



If the Certificate was save in the right format the icon should look like this:



3. Double click icon and "Install Certificate". Note: if they're not logged in as 'Admin' this option will be grayed out.



4. Complete the set up wizard using the defaults.
5. System now has the require SSL Certificate in his Root Store.
6. Re-start POS application
7. Try test transaction.