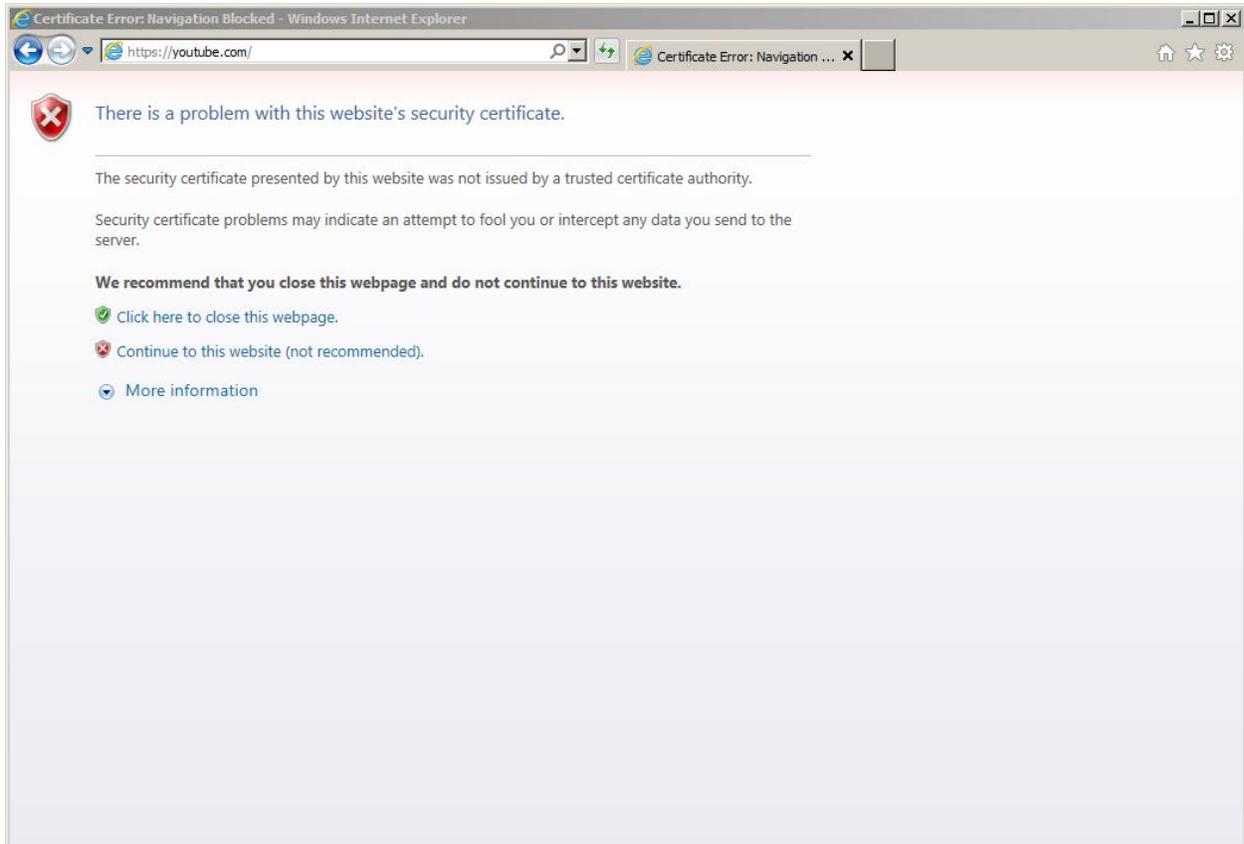
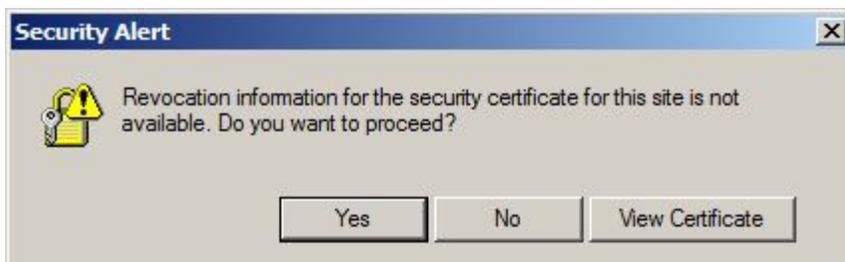


## Windows 7 – Enterprise Root Certificate Authority Import

1. Visit a website that uses SSL. You can tell when the site is using SSL when there is an “S” after the “HTTP” in the URL. <https://www.youtube.com> will be used in this example.
2. When receiving this error click **Continue to this website (not recommended)** twice.



3. The following Security Alerts may be presented. Click **Yes** to both.





4. Click the **Certificate Error** button next to the address bar.



5. Information about the certificate error will be presented here. Click **View certificates**.



6. The **Certificate** dialog box is shown.



7. Click on the **Certificate Path** tab, select the **ccps-AP1-CERTSRV-001-CA** certificate, and click **View Certificate**. Notice the small red “X” on the certificate and the **Certificate status:** indicating that this CA Root certificate is not trusted.



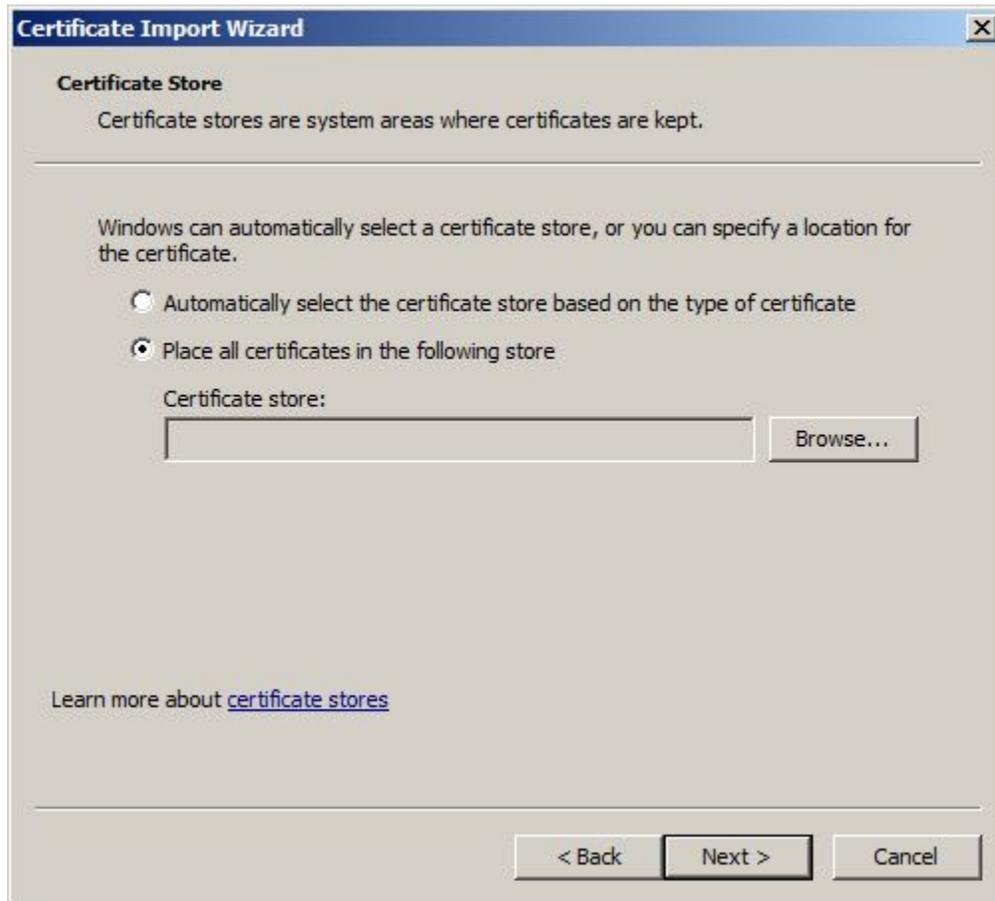
8. The **Certificate Information** is shown. Click **Install Certificate...**



9. The **Certificate Import Wizard** is shown. Click **Next**.



10. Select **Place all certificates in the following store** and click **Browse....**



11. The **Select Certificate Store** dialog box is shown. Check **Show physical stores** and expand the **Trusted Root Certification Authorities**. Select **Local Computer** and click **OK**.



12. Make sure the **Certificate store:** says **Trusted Root Certification Authorities\Local Computer**. Click **Next >**.



13. Click **Finish**.



14. The following Security Warning may be displayed. Click **Yes**.



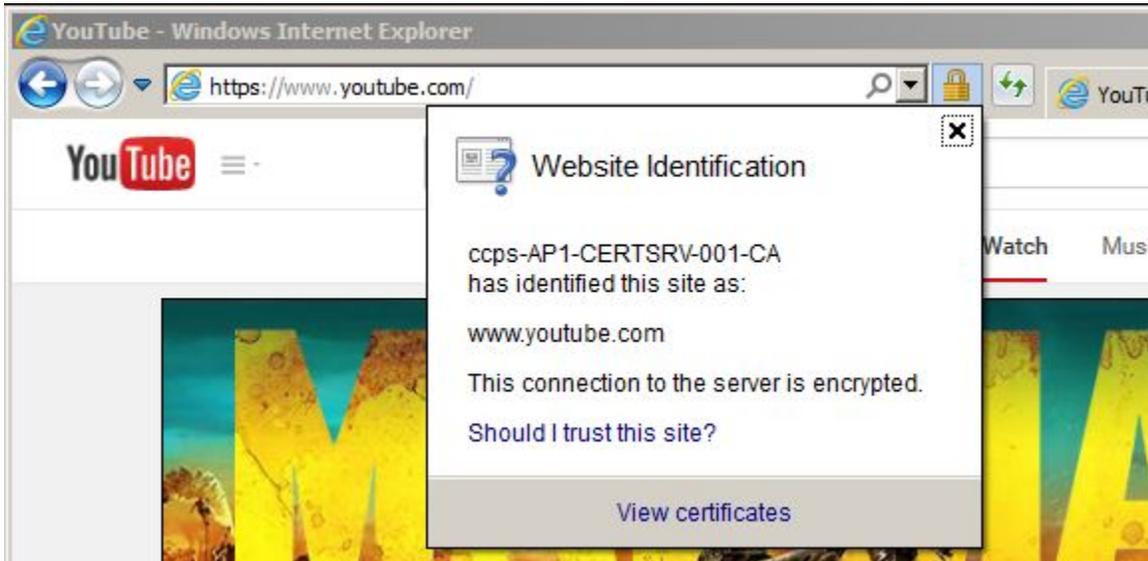
15. Click **OK**.



16. Close all web browsers. Reopen the browser and attempt to visit the same website using SSL.



17. Instead of a **Certificate Error** there should be a small closed padlock next to the address bar. Click the lock icon to display certificate information.



18. Clicking **View certificates** and the **Certificate Path** tab now will show the trusted certificate. Notice the small red "X" is no longer present and the **Certificate status:** indicates this certificate is OK.

