Removing the Federal Bridge cross certification certificates.

These instructions are intended to help you remove the Federal Bridge certificates from the Microsoft Certificate store on your computer. The objective of the Federal Bridge is to 'cross certify' the different certificate policies of all the federal agencies. The Federal Bridge has succeeded in getting Microsoft to include the Federal Bridge certificates in the Microsoft Certificate Store through initial operating system installation (it comes from the factory that way) and/or software updates.

Unfortunately, cross certification does not always work well in implementation. If you are trying to connect to a server (for instance, JPAS) and the server is not configured to account for the efforts of the Federal Bridge (perhaps because it is an old server), then it could cause an SSL Transaction (certificate log-on) to fail.

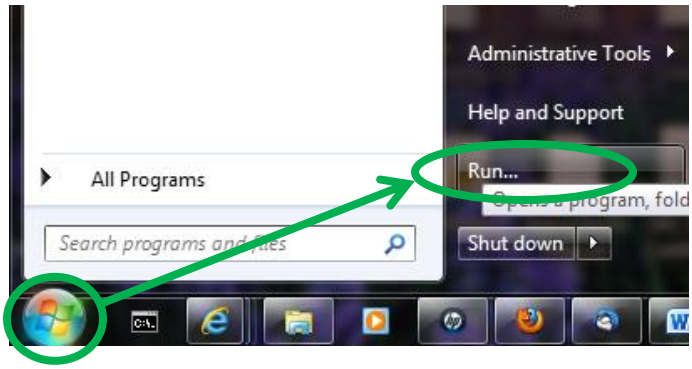
Before you remove the FBCA Certificates, please trust the DoD and ECA PKIs (http://eca.orc.com/wp-content/uploads/ECA_Docs/Trusting_DoD_PKIs.pdf). This will ensure that the Trust path created by the DoD is installed into the Microsoft certificate store. Microsoft might try to 'hold onto' the FBCA certificates if they form the only possible Trust Path that Microsoft has available. By installing the DoD's trust path, we ensure that Microsoft has an alternative to the FBCA certificates that we are trying to delete.

The DoD has created a tool to automatically remove these certificates. You can find instructions on using that tool, here:

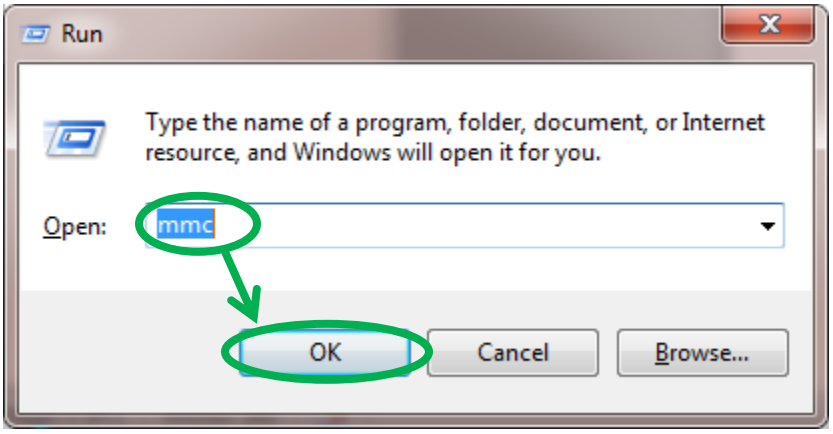
http://eca.orc.com/wp-content/uploads/ECA_Docs/Removing_Federal_Bridge_certificates_Tool.pdf

In order to remove these certificates from the Microsoft Certificate Store in Windows 7, you will need to use the Microsoft Management Console.

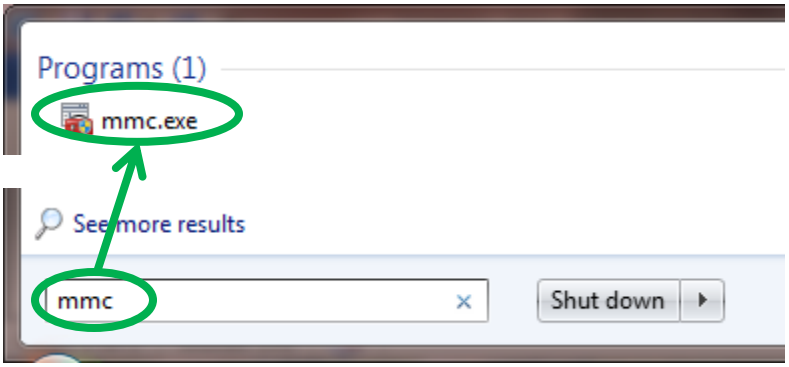
Click on the **Start** button and then click **Run**.



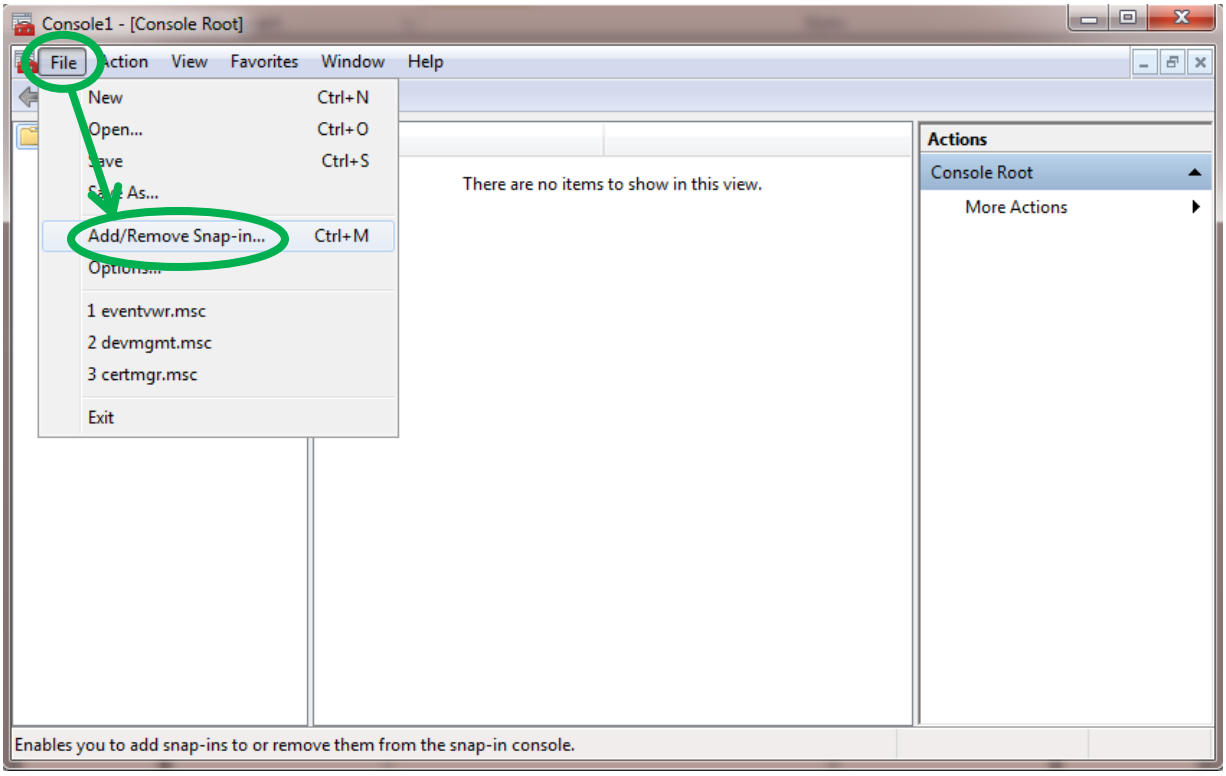
Enter “mmc” in the text field and click OK



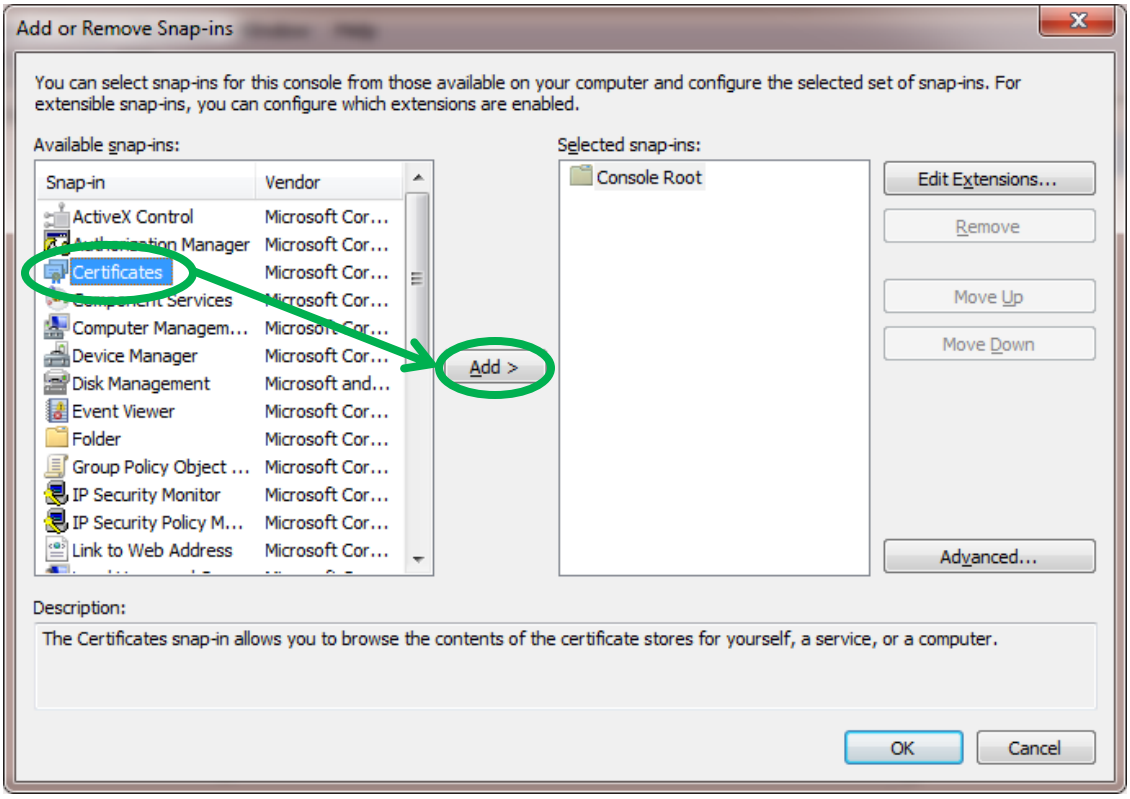
Alternatively, you can enter “mmc” in the search test field, and then double click the mmc.exe entry



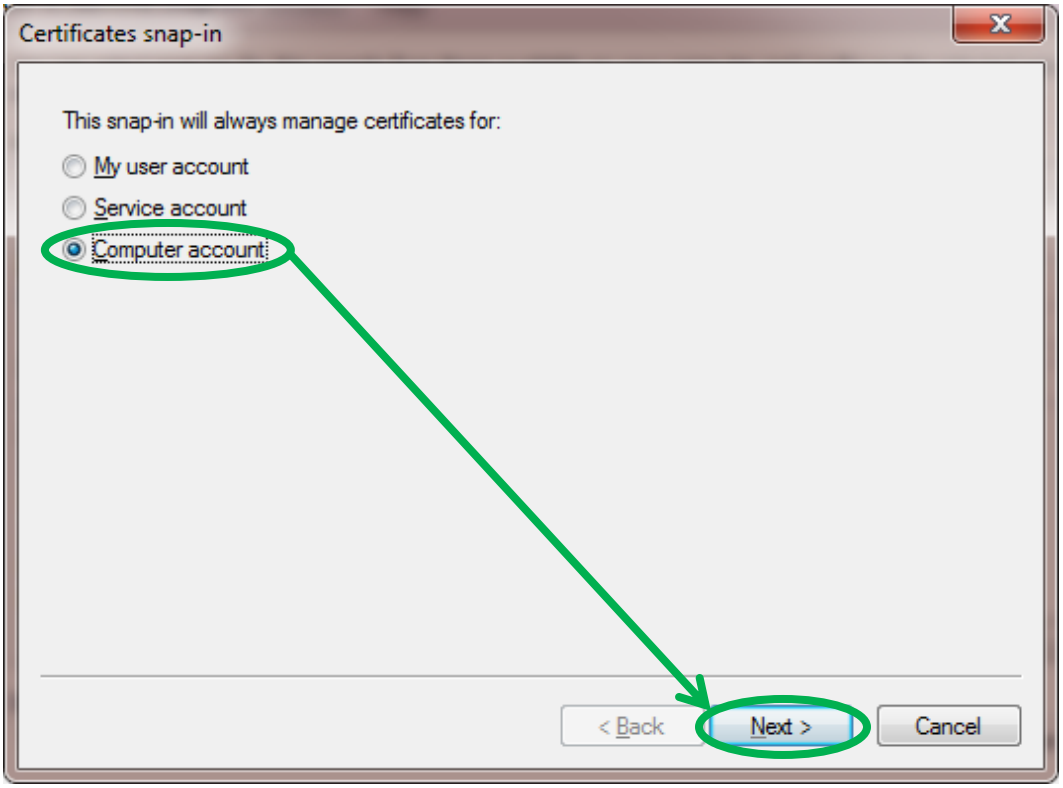
When the Management Console opens, select **File**, then **Add/Remove Snap-in…**



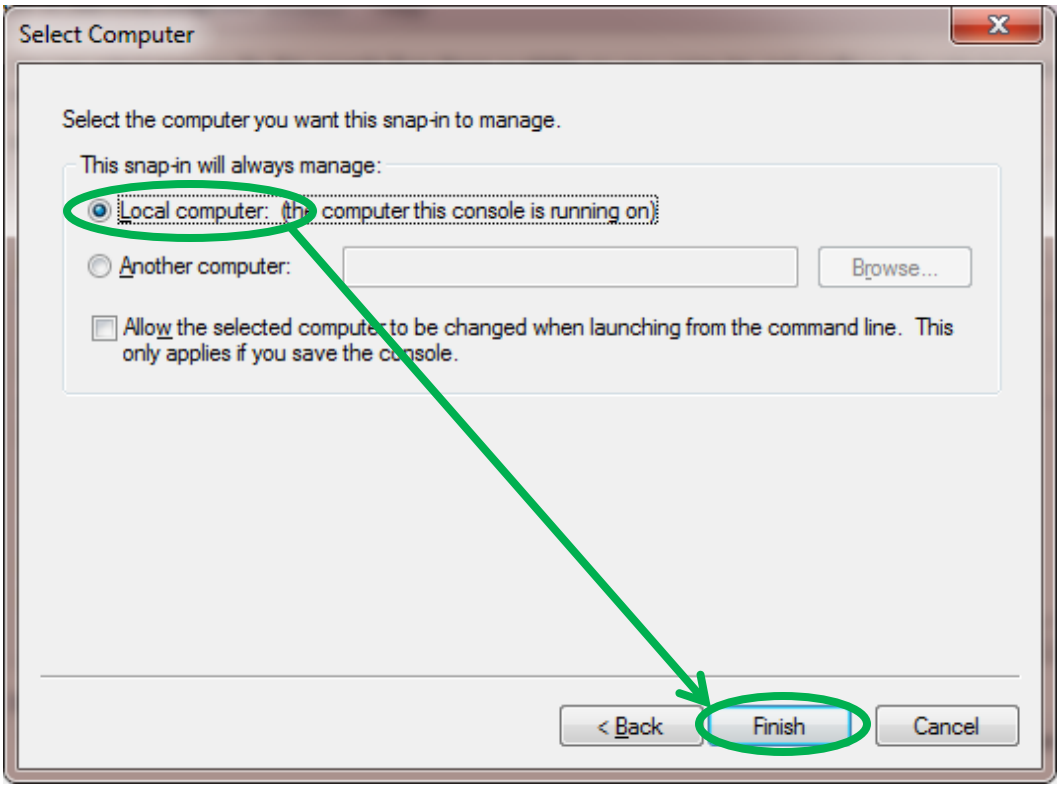
Select Certificates and click the **Add** button



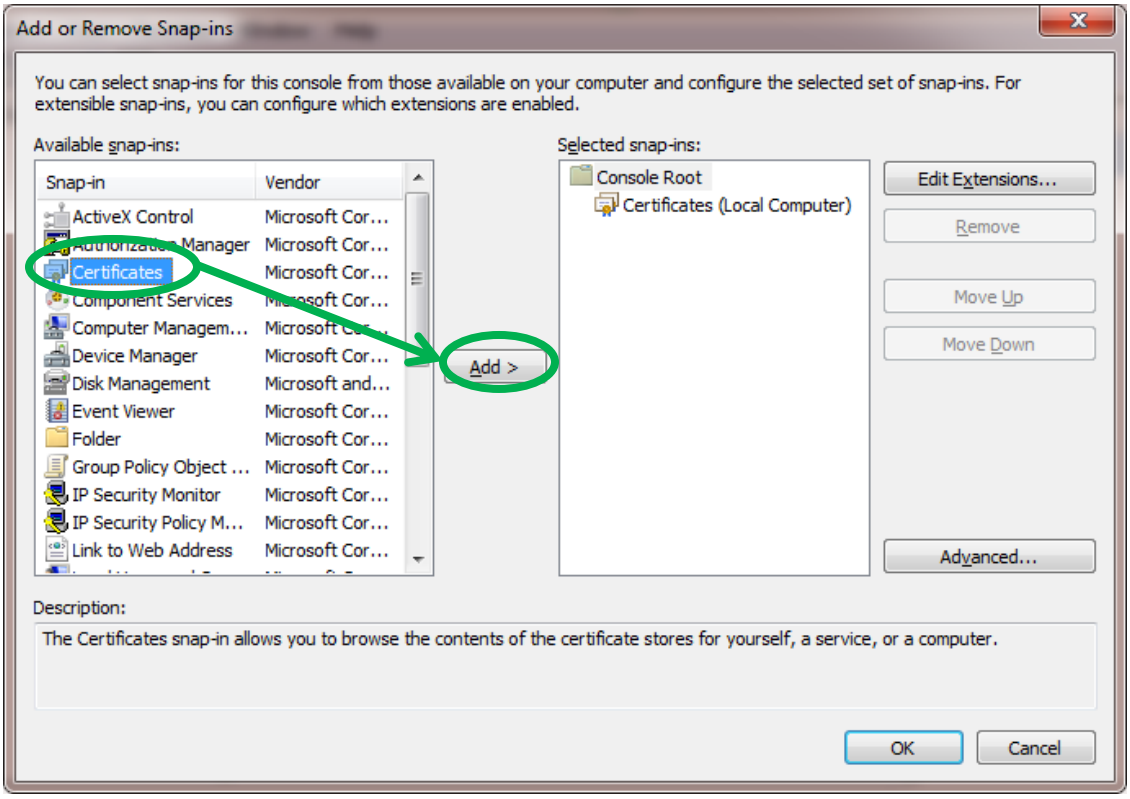
Select **Computer account** and click **Next**



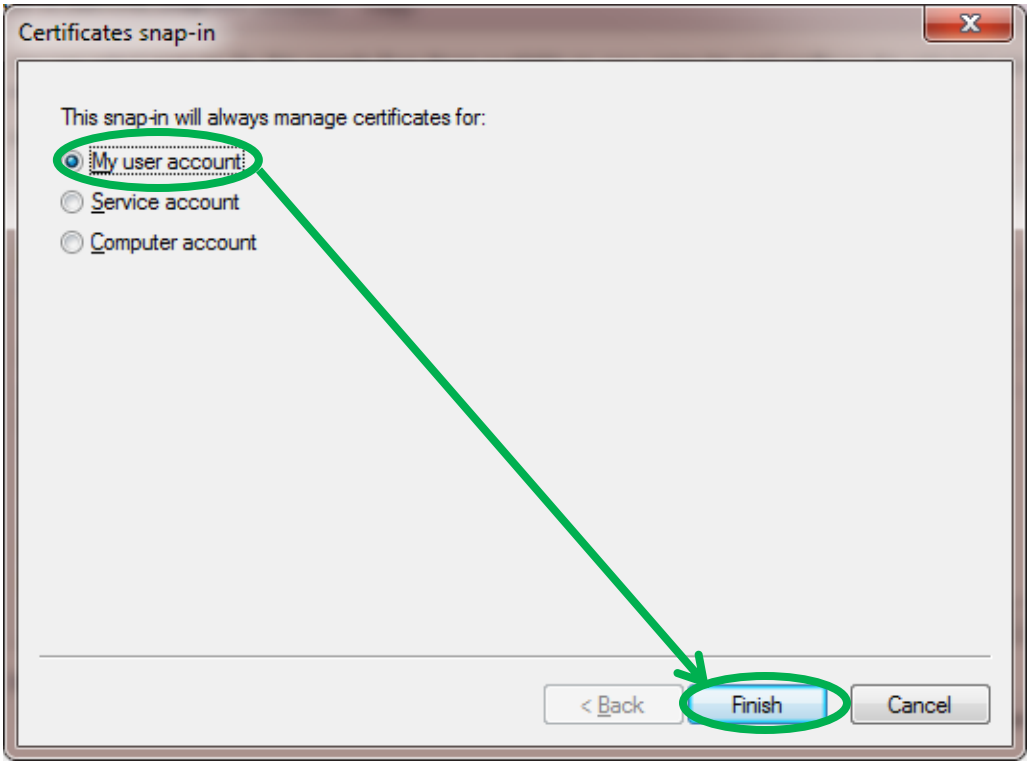
Select **Local computer account** and click **Finish**



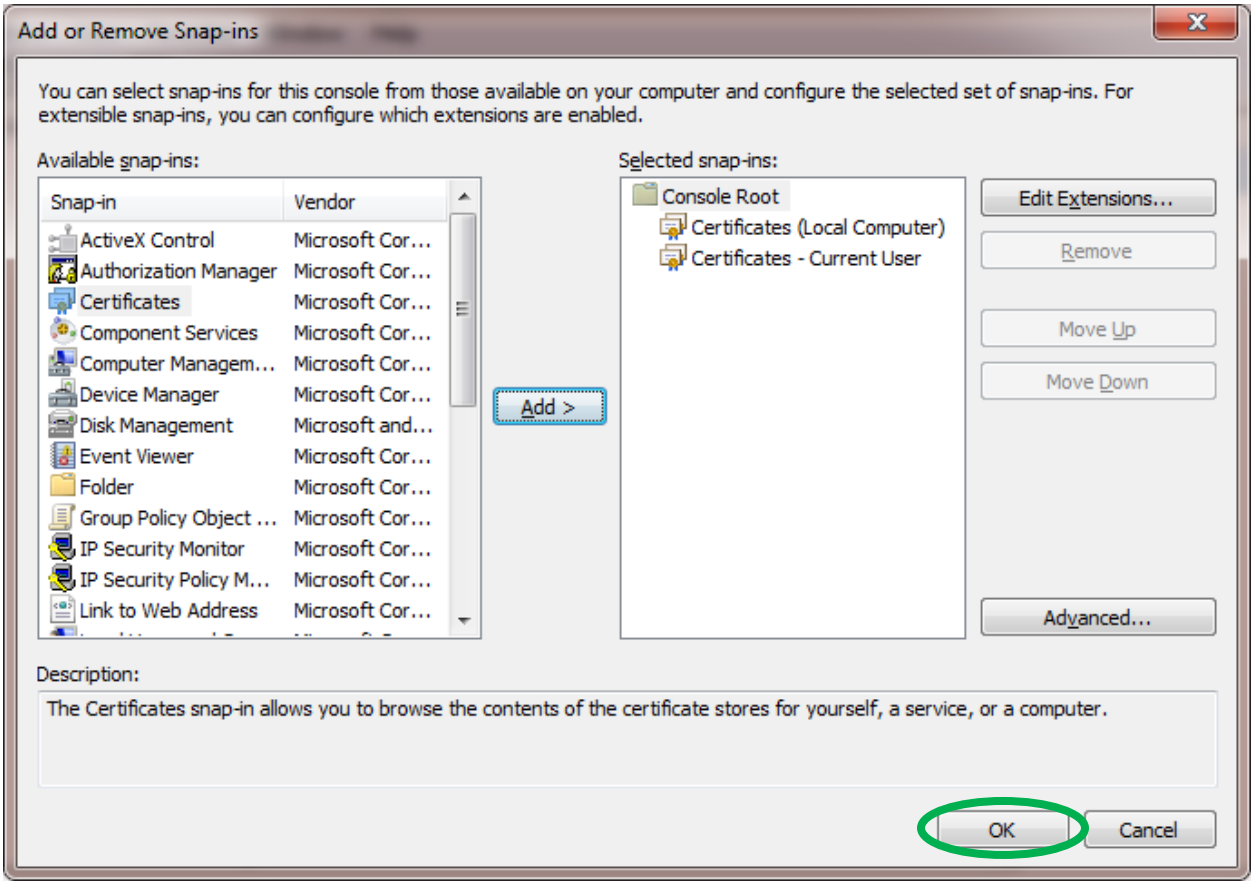
Select Certificates and click the **Add** button, again



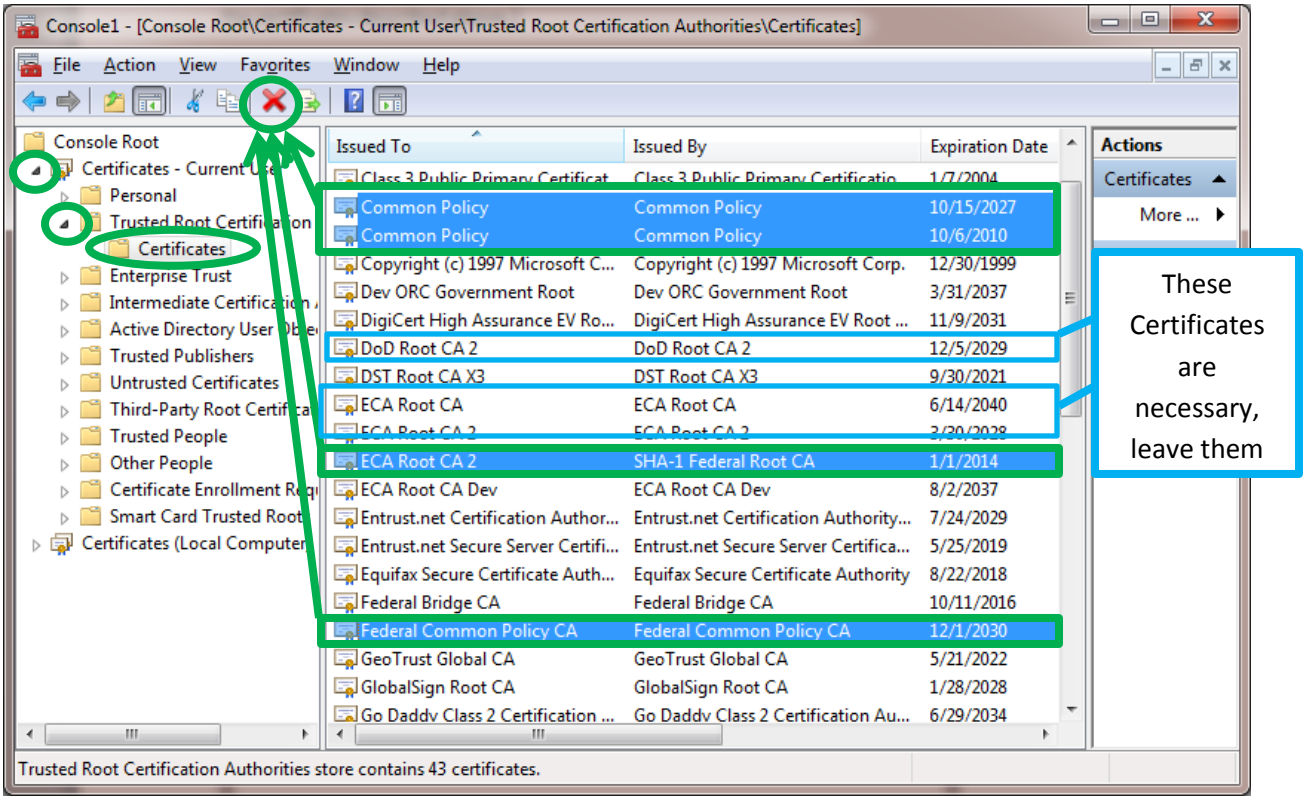
This time, select **My user account** and click **Finish**



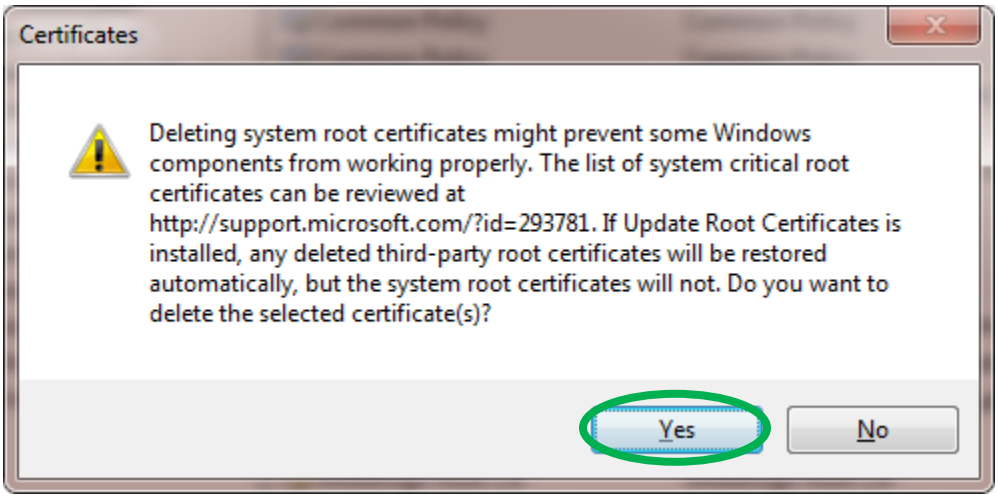
Click the OK button



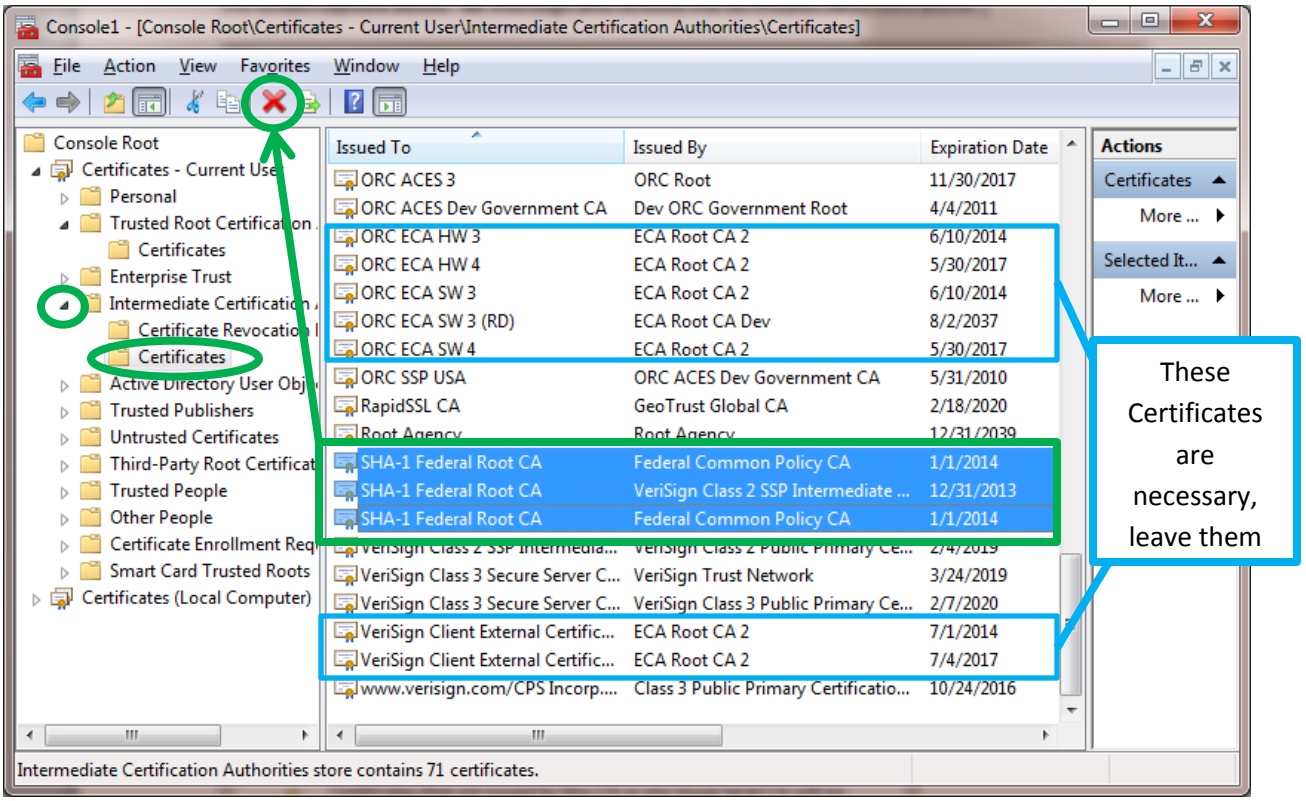
Click on the arrow by Certificates (Local Computer), then click the arrow by Trusted Root Certification Authorities, then select the Certificates folder under Trusted Root Certification Authorities. Then, scroll through the listings and select all certificates the have the phrases," Common Policy", "Federal Bridge", "Federal Common Policy", "SHA-1 Federal Root CA" in either the Issued To or Issued By columns. Then, click the red X delete button. You may need to do this several times, to get them all. [Note: Not every certificate that needs to be removed is shown in the screen capture below. Be thorough and remove the certificates described above.]



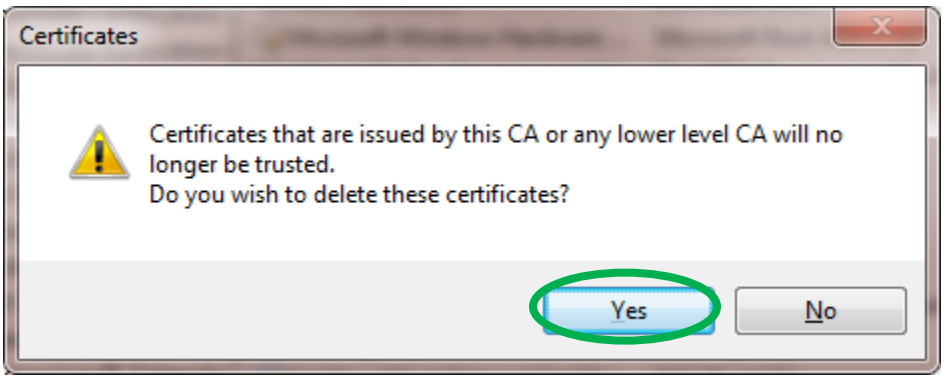
The computer will produce the following warning message. Click the **Yes** button.



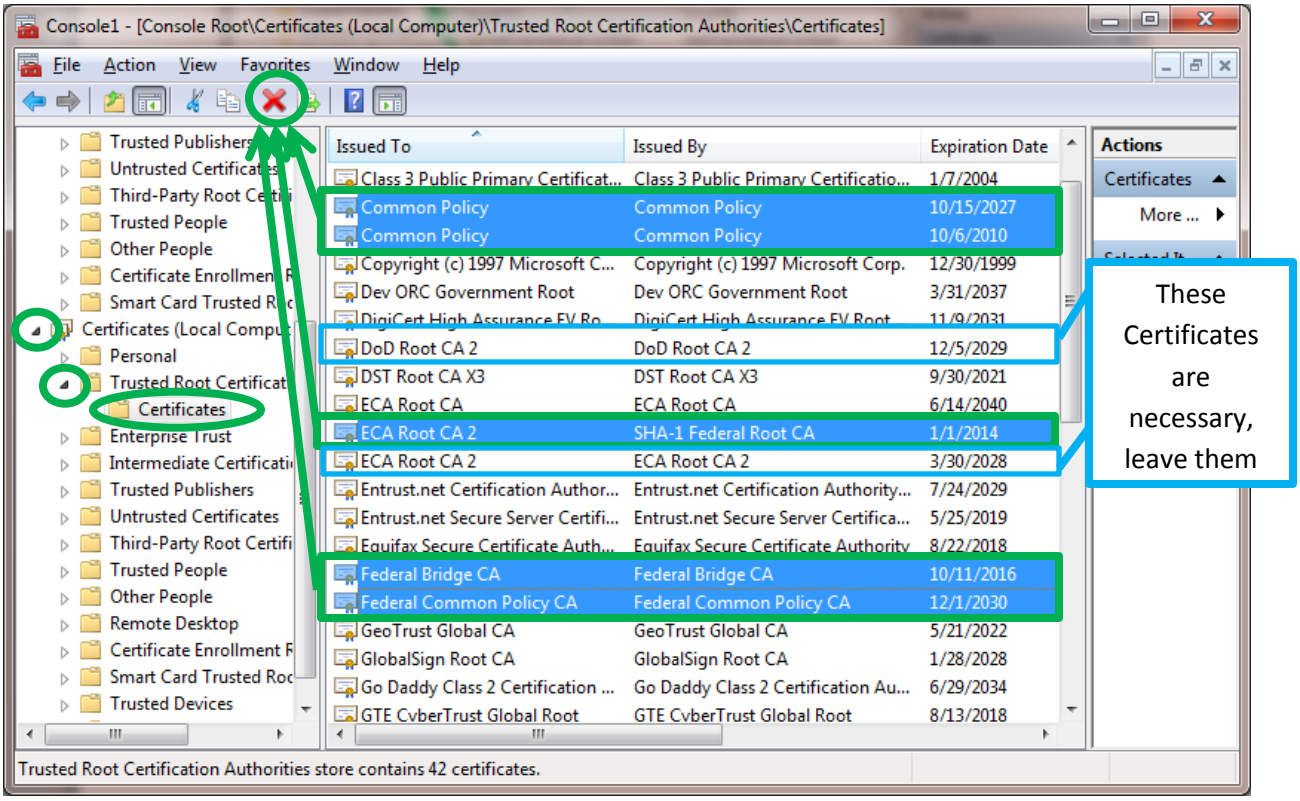
Then, click the arrow by Intermediate Certification Authorities, then select the Certificates folder under Intermediate Certification Authorities. Then, scroll through the listings and select all certificates the have the phrases," Common Policy", "Federal Bridge", "Federal Common Policy", "SHA-1 Federal Root CA" in either the Issued To or Issued By columns. Then, click the red X delete button. You may need to do this several times, to get them all. [Note: Not every certificate that needs to be removed is shown in the screen capture below. Be thorough and remove the certificates described above.]



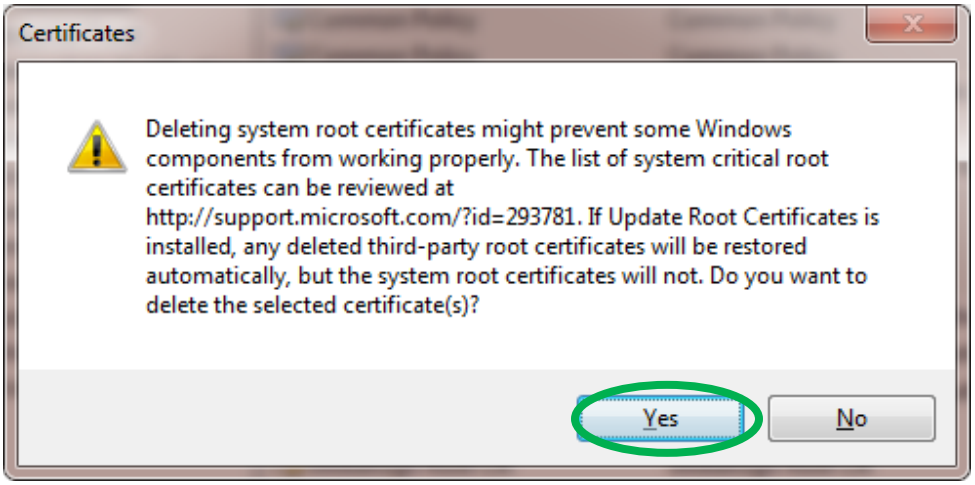
The computer will produce the following warning message. Click the **Yes** button



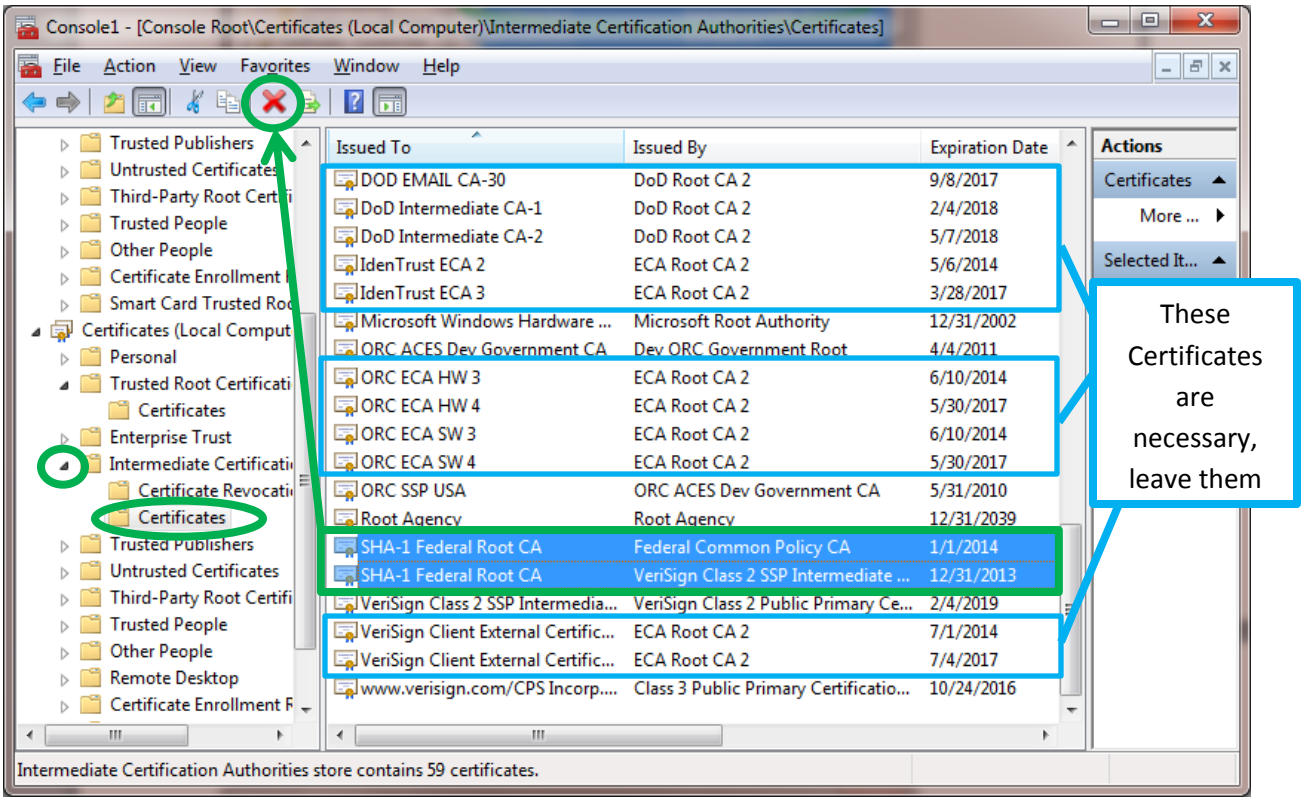
Click on the arrow by Certificates - Current User, then click the arrow by Trusted Root Certification Authorities, then select the Certificates folder under Trusted Root Certification Authorities. Then, scroll through the listings and select all certificates the have the phrases," Common Policy", "Federal Bridge", "Federal Common Policy", "SHA-1 Federal Root CA"in either the Issued To or Issued By columns. Then, click the red X delete button. You may need to do this several times, to get them all. [Note: Not every certificate that needs to be removed is shown in the screen capture below. Be thorough and remove the certificates described above.]



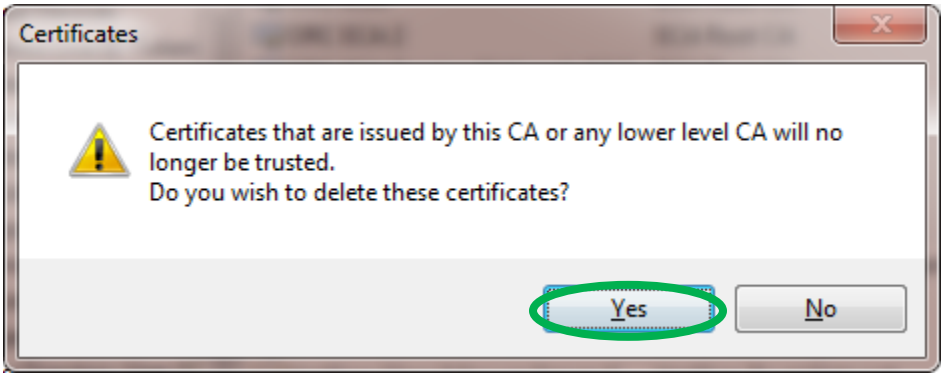
The computer will produce the following warning message. Click the **Yes** button



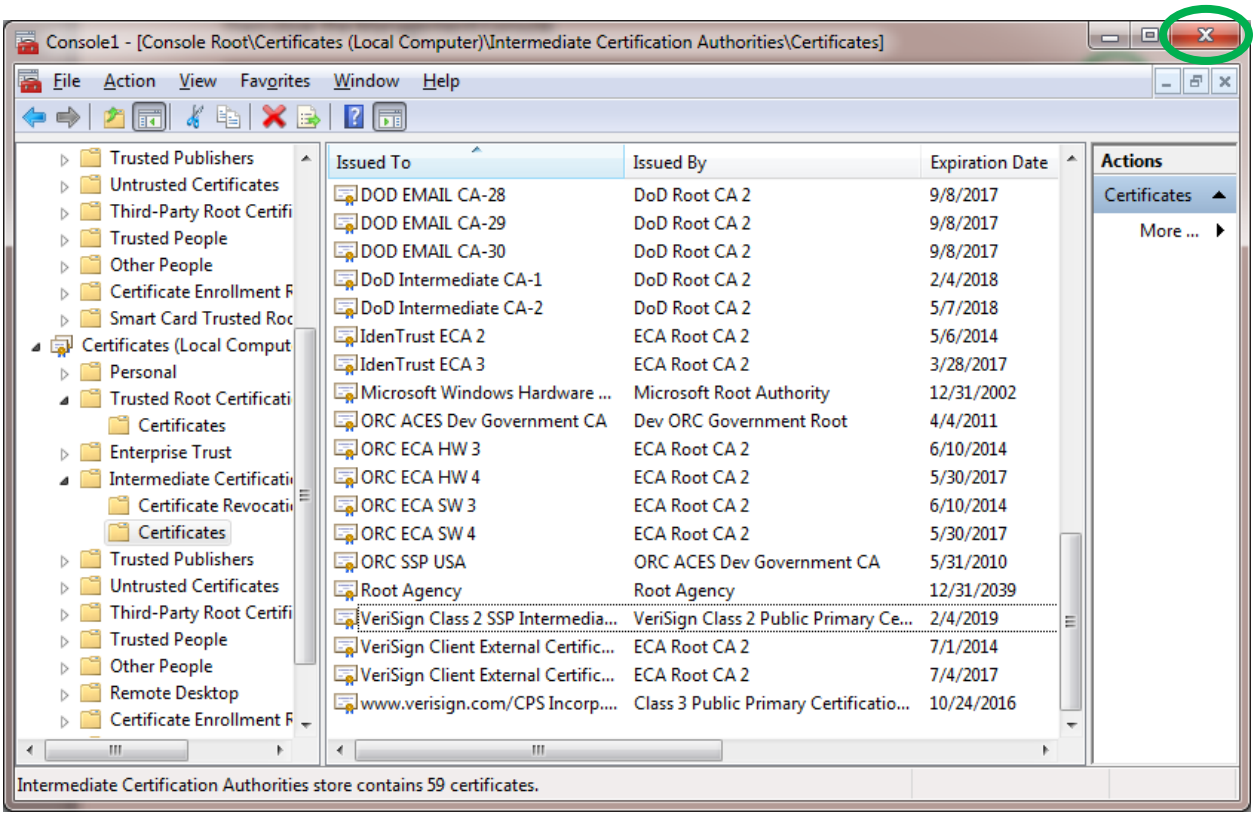
Then, click the arrow by Intermediate Certification Authorities, then select the Certificates folder under Intermediate Certification Authorities. Then, scroll through the listings and select all certificates the have the phrases," Common Policy", "Federal Bridge", "Federal Common Policy", "SHA-1 Federal Root CA"in either the Issued To or Issued By columns. Then, click the red X delete button. You may need to do this several times, to get them all. [Note: Not every certificate that needs to be removed is shown in the screen capture below. Be thorough and remove the certificates described above.]



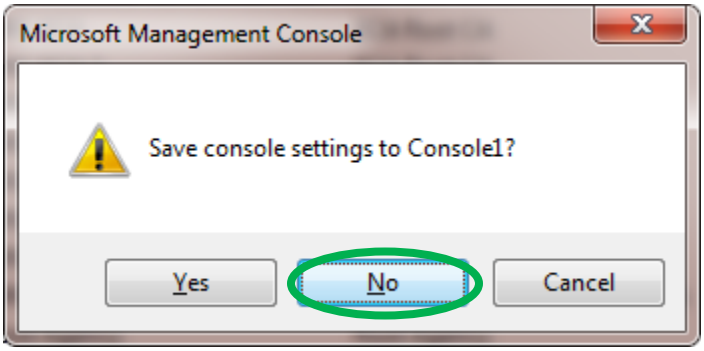
The computer will produce the following warning message. Click the **Yes** button



Then close the Management Console



When your computer asks you if you want to save the Console settings click **No**.



You should now be ready to put back (only) the certificates required to trust the DoD and ECA PKIs by running the **Trust DoD PKIs** instruction. Then try to access your web site (JPAS) again.