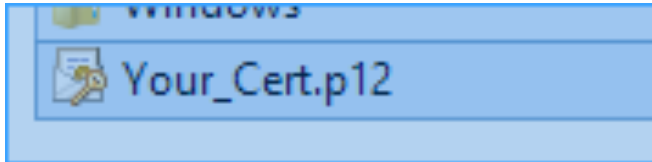


Obtaining Your Certificate

You should have been issued a digital certificate from your organization in order to leverage the new Anaplan Connect 1.4X release. The cert is in an industry standard .p12 format and should look similar to the pic below.

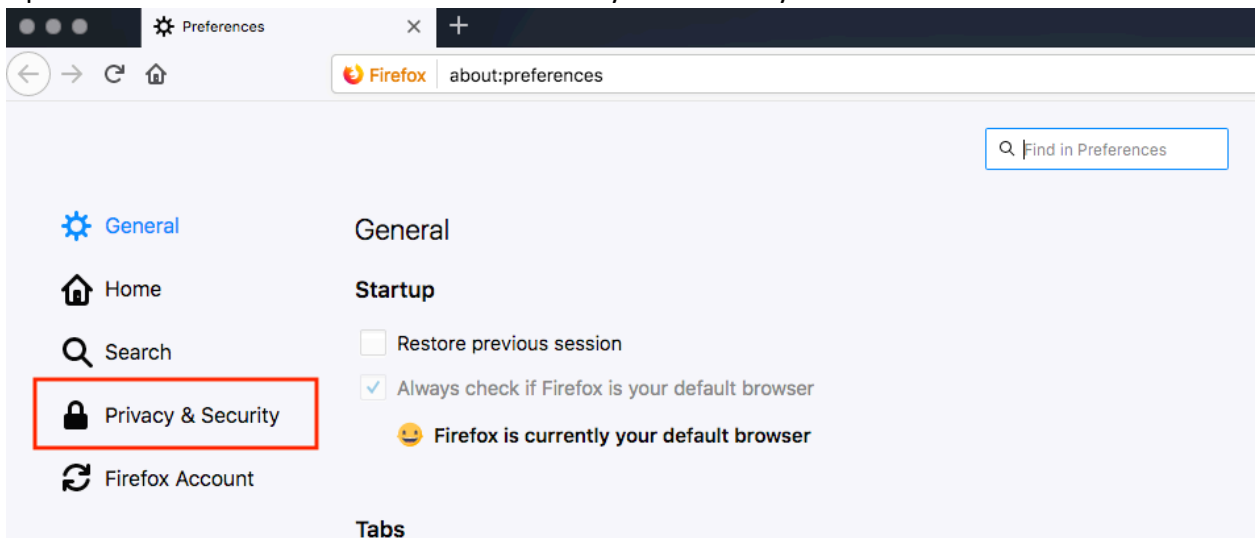


If you have the cert but imported it into your chosen web browser and need to export it follow the steps below. If you have the cert and are ready to create your KeyStore then skip to the next section for brief explanation of the Wizard.

Exporting from your web browser

Depending on your chosen web browser this procedure may be slightly different, I am going to use Firefox because it is one of the most commonly used web browsers.

1. Open the Preferences menu and select “Privacy and Security” from the left menu



2. Scroll down to the Certificates section at the bottom and click View Certificates

Certificates

When a server requests your personal certificate

☐ Select one automatically

☒ Ask you every time

☒ Query OCSP responder servers to confirm the current validity of certificates

[View Certificates...](#)

[Security Devices...](#)

3. Under the “Your Certificates” tab single click on your cert so it is highlighted and then click the “Backup” button.

Certificate Manager

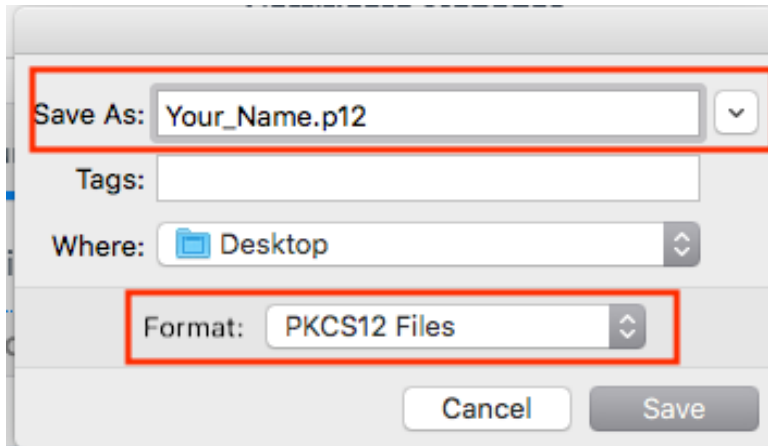
[Your Certificates](#) [People](#) [Servers](#) [Authorities](#)

You have certificates from these organizations that identify you

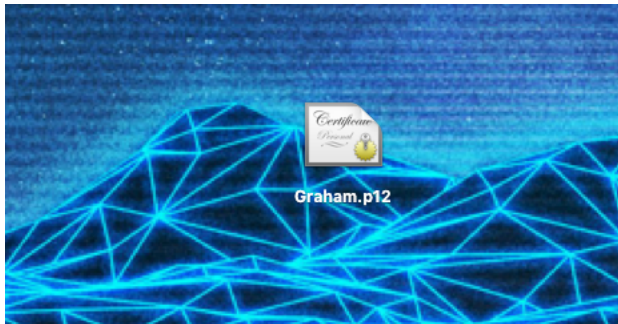
Certificate Name	Security Device	Serial Number
▼ DigiCert Inc		
Graham Gronhoff	Software Security Device	0A:76:38:41:50:60:8C:F3:85:...

[View...](#) [Backup...](#) [Backup All...](#) [Import...](#) [Delete...](#)

4. Enter a specific name for your certificate (usually its best to just use your name) making sure to put “.p12” (without the double quotes) at the end to save it as the proper file type. Ensure the format is PKCS12 Files and then click the save button, you will be prompted to enter a password for the cert so make sure you retain it because it will be required later.



5. Once complete your certificate should be saved to the location specified, in my case it saved directly to my desktop.



6. The export is complete and you can now move on to placing the cert in the required location.

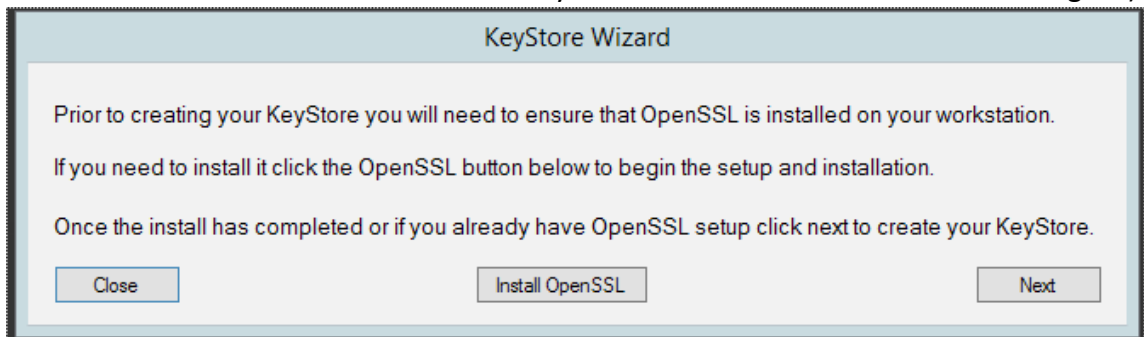
Placing The .p12 File

In order for Windows to perform the correct actions and steps required to create the KeyStore you will need to copy the .p12 file to the root of your C drive or C:\ To do this simply copy and paste it to that location.

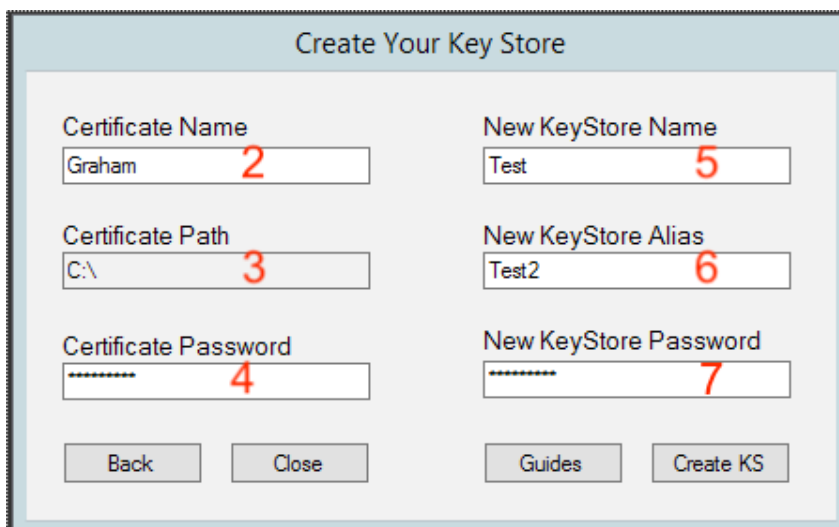
Using the KeyStore Wizard Utility

With the certificate in the correct location we can now use the KeyStore Wizard to install OpenSSL (if it has not been installed already) and then, by entering a few pieces of information, create the Java KeyStore.

1. IN the main window of the application you will be given the choice to install OpenSSL. This is required to extract the proper files and prep everything for the creation process. If it is already installed on your workstation you can skip this step and click next. If not Install OpenSSL before proceeding (this is the light version and has been configured by me to run without interaction so it will only take a few seconds to run after clicking OK).



The KeyStore Wizard dialog box has a title bar "KeyStore Wizard". The main text area contains the following instructions: "Prior to creating your KeyStore you will need to ensure that OpenSSL is installed on your workstation. If you need to install it click the OpenSSL button below to begin the setup and installation. Once the install has completed or if you already have OpenSSL setup click next to create your KeyStore." At the bottom, there are three buttons: "Close", "Install OpenSSL", and "Next".



The "Create Your Key Store" dialog box has a title bar "Create Your Key Store". It contains six input fields arranged in two columns. The left column has "Certificate Name" (value: "Graham", with a red "2" next to it), "Certificate Path" (value: "C:\", with a red "3" next to it), and "Certificate Password" (masked with dots, with a red "4" next to it). The right column has "New KeyStore Name" (value: "Test", with a red "5" next to it), "New KeyStore Alias" (value: "Test2", with a red "6" next to it), and "New KeyStore Password" (masked with dots, with a red "7" next to it). At the bottom, there are four buttons: "Back", "Close", "Guides", and "Create KS".

2. Enter the certificate name (note you do not need to add the .p12 just the name like in the example shown below).

3. The path is hardcoded so skip over it and enter the password for the cert that you created in the previous section.
4. Enter the password that you created for your cert.
5. New KeyStore Name will be the newly created KeyStore.
6. The KeyStore Alias is required so enter a unique name.
7. The password in the last box needs to be at least 6 characters long and cannot contain any special characters such as & % ^ @ /
8. Once you have entered all the information click the Create KS button to start the creation process.
9. After the KeyStore has been created a PDF file will open with final instruction on importing your .pem file into Anaplan and web browser.

If you have any issues or want to review the procedures in detail from start to finish click on the documentation button to view a complete installation guide for Anaplan Connect 1.4 KeyStore creation.