Certificate Manual

We remind you that this manual is unique and exclusive, this manual will explain the steps taken in the last certificate exchange.

***WARNING**: We remind you once that the steps described on the document reflect the work performed on the last certificate renewal. It does not necessarily mean the next time it will be the same case. There might be different or additional steps.*

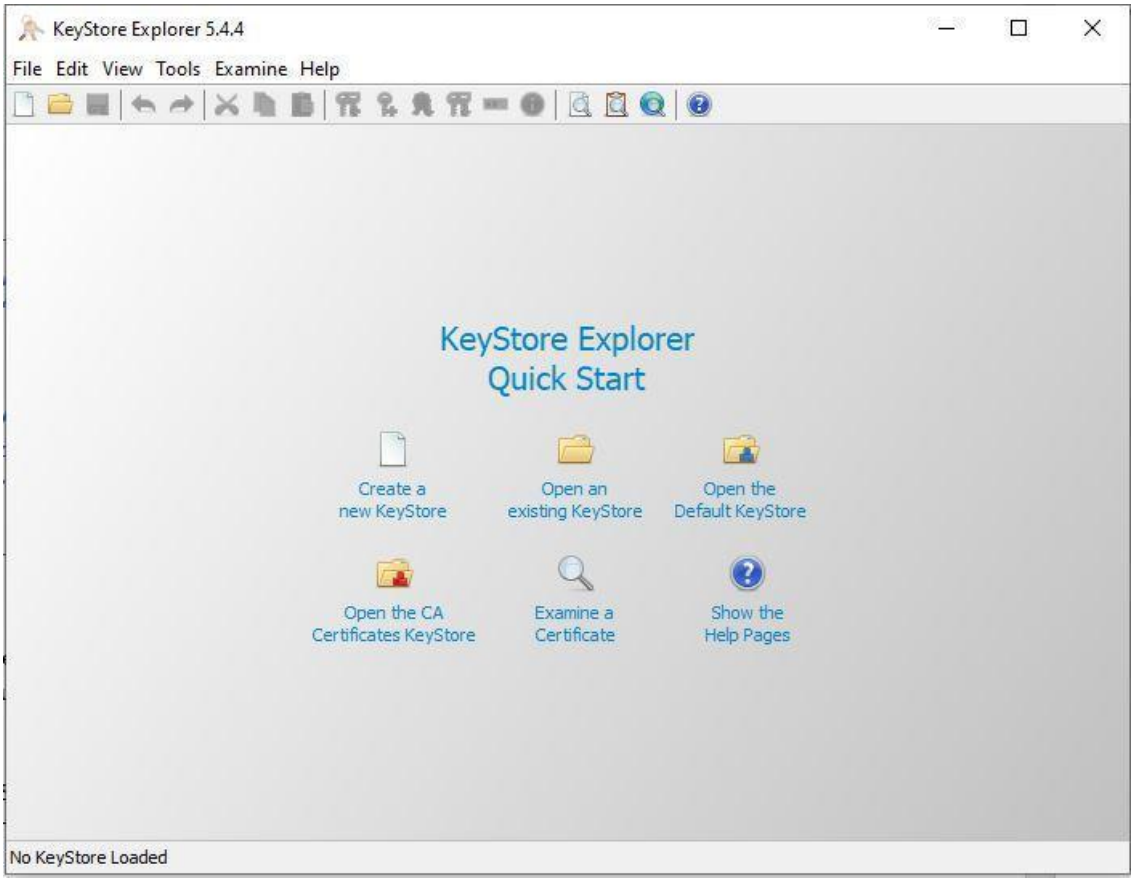
We will proceed with the steps we performed last time to change the certificates, and next, we will show you images of how to do all these steps.

1. Keystore Explorer application.
2. WinSCP/FileZilla application.
3. New certificate.
4. Import the old ".keystore" file into the Keystore Explorer application.
5. Go to the Keystore Explorer application where the old ".keystore" will be and we will exchange the old certificate for the new one inside that ".keystore" key.
6. Import the Root certificate and the Intermediate one.
7. Save the new ".keystore" to a folder.
8. Import the new ".keystore" into the appliance.
9. Access the appliance by putty or other SSH.
10. Import the certificate from the CMI menu.
11. Restart Tomcat for the import to be successful.
12. Check if Tomcat is running, and verify that everything is working normally after importing the new certificate.

1. Keystore Explorer Application.

You can download the Keystore Explorer application for free from the official site:

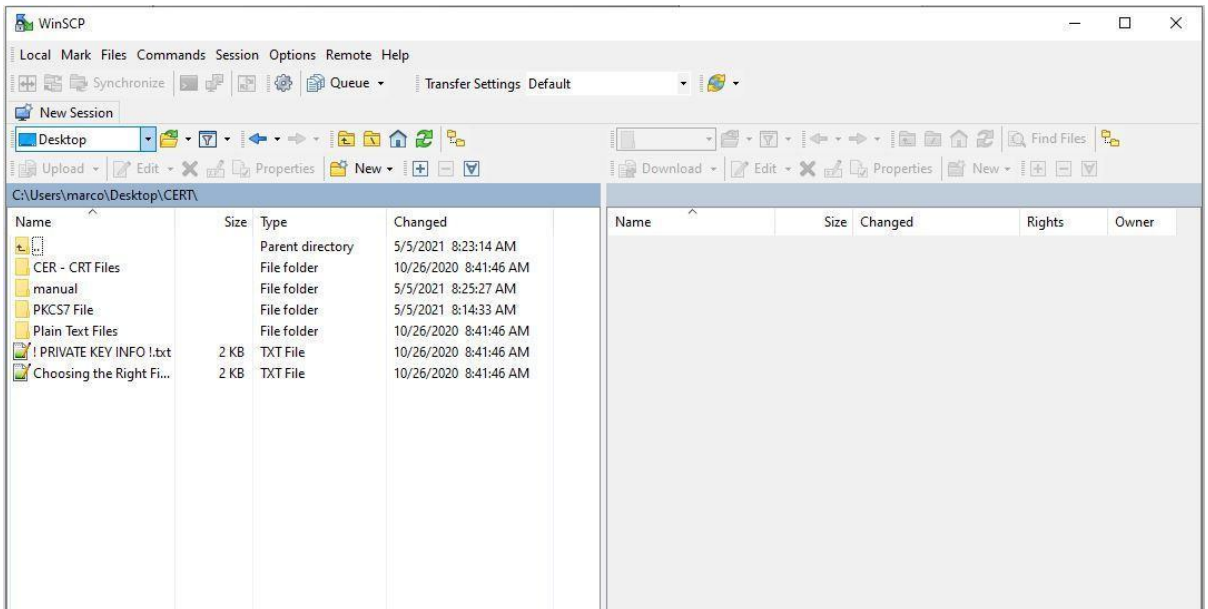
https://keystore-explorer.org/downloads.html



2. WinSCP Application.

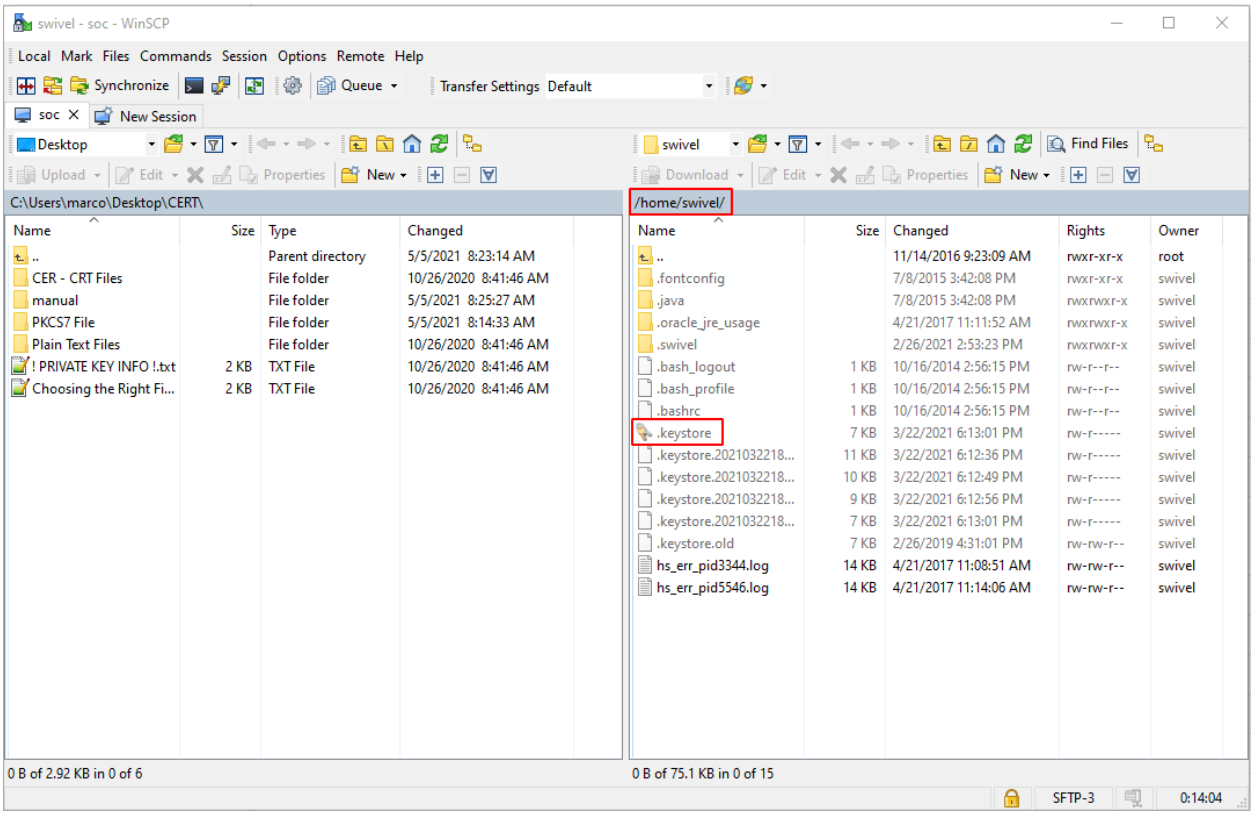
You can download the WinSCP application for free from the official site:

https://winscp.net/eng/download.php

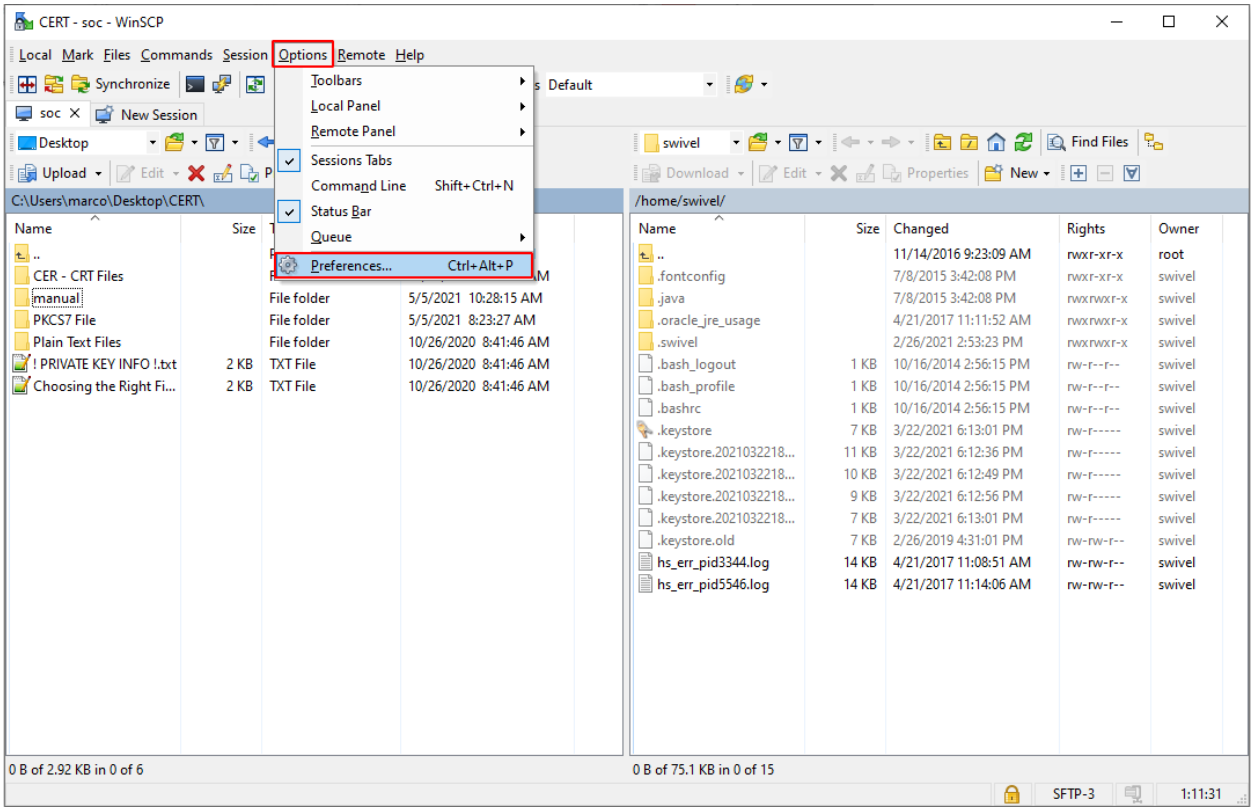


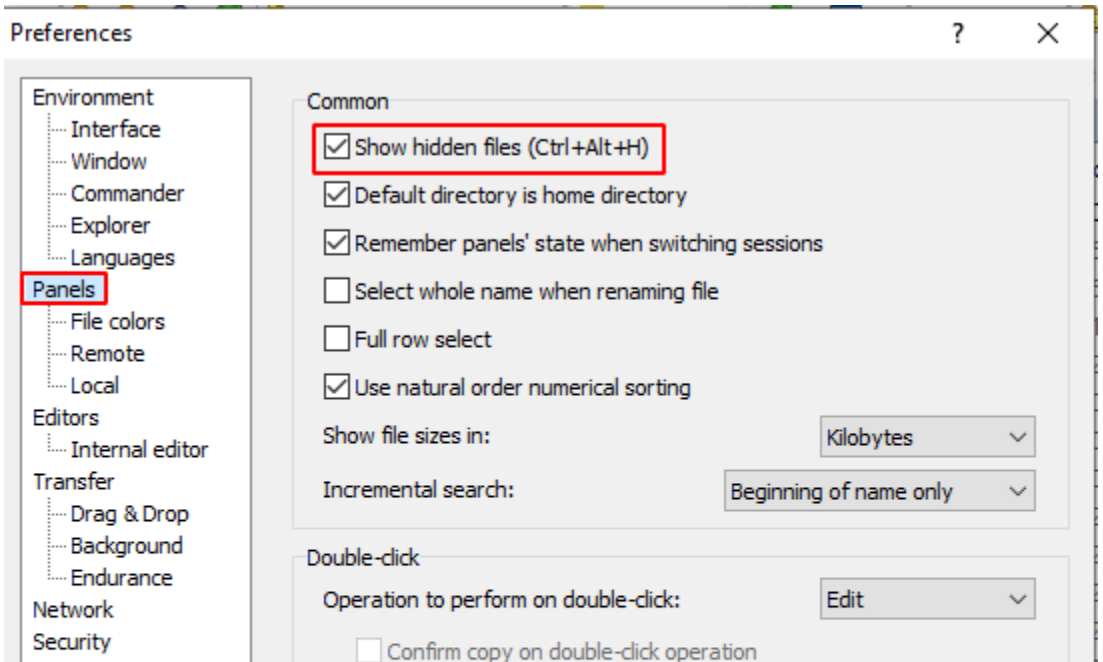
Log into the appliance via WinSCP to fetch/grab the “.Keystore” file.

The old/in-use .keystore that needs to be renewed is in the “**/home/swivel**” folder.

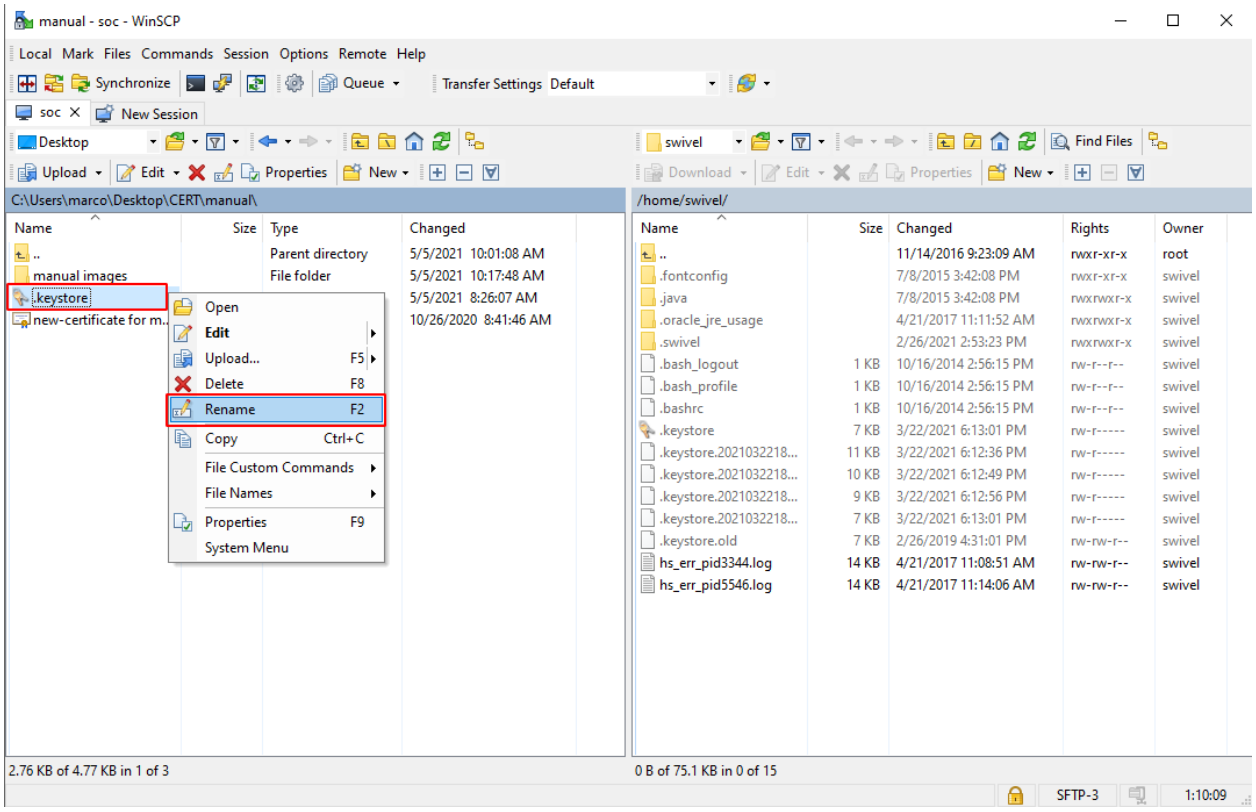


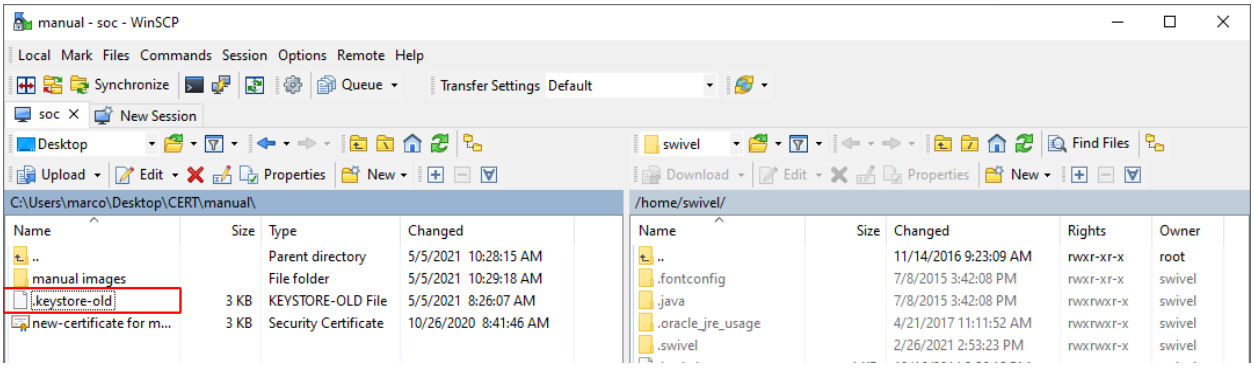
We remind you that if you are not seeing the .keystore, it is because you have to activate the option "Show Hidden Files - (Ctrl+Alt+H) in the "Panels" menu in the settings.





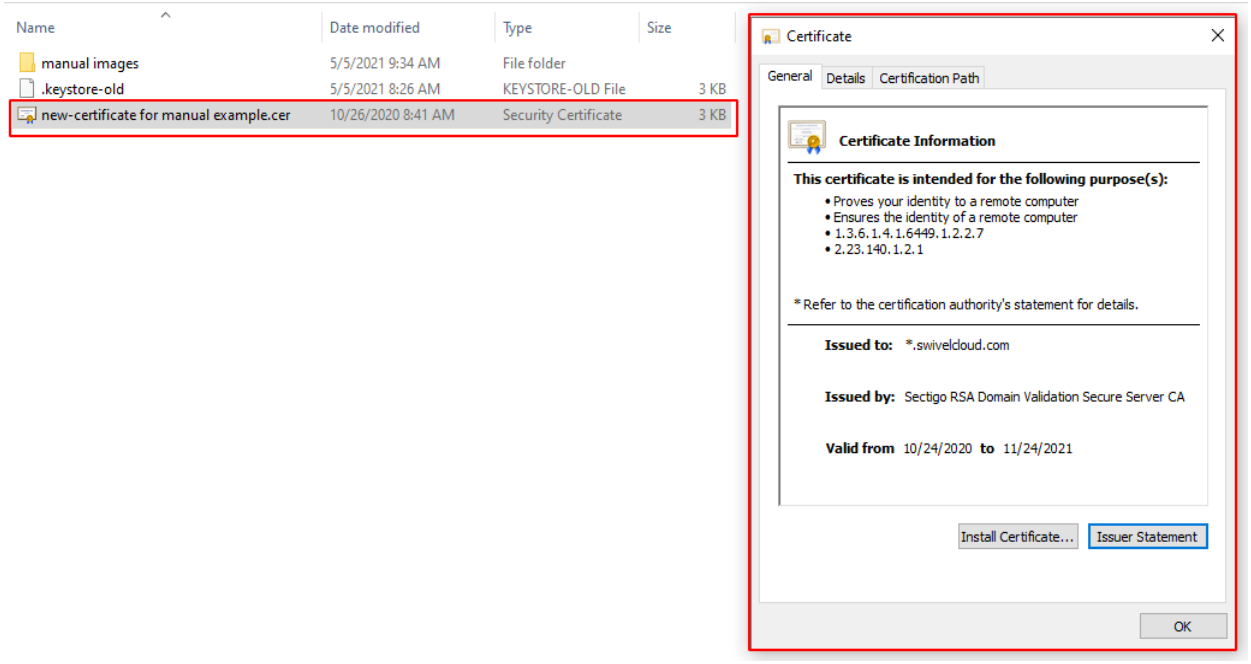
After getting the ".keystore" into your computer, rename it to ".keystore-old" so we can identify it and differentiate it from the future new ".keystore".



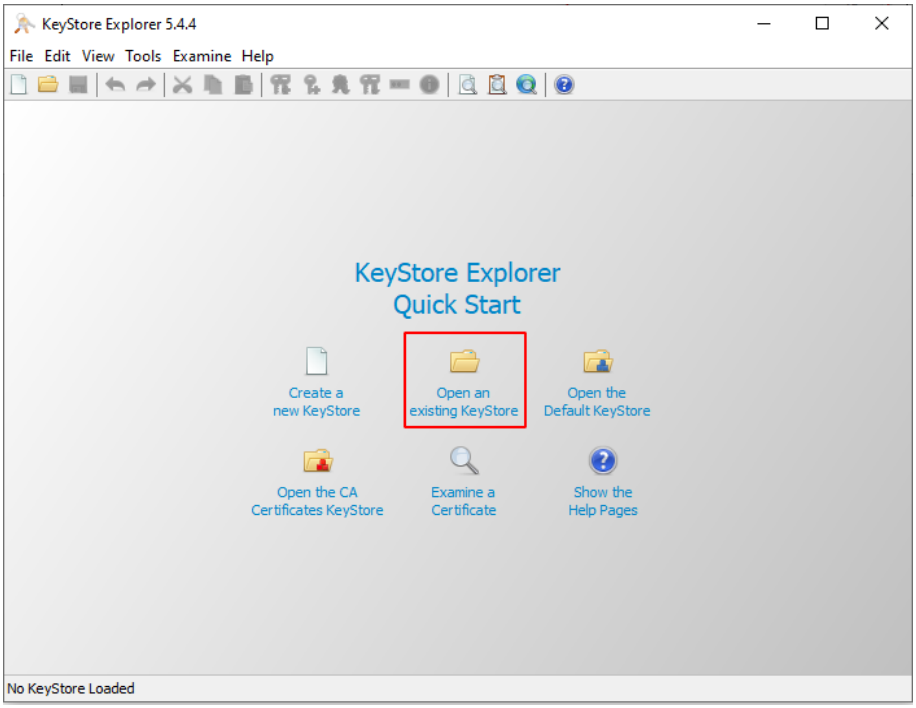


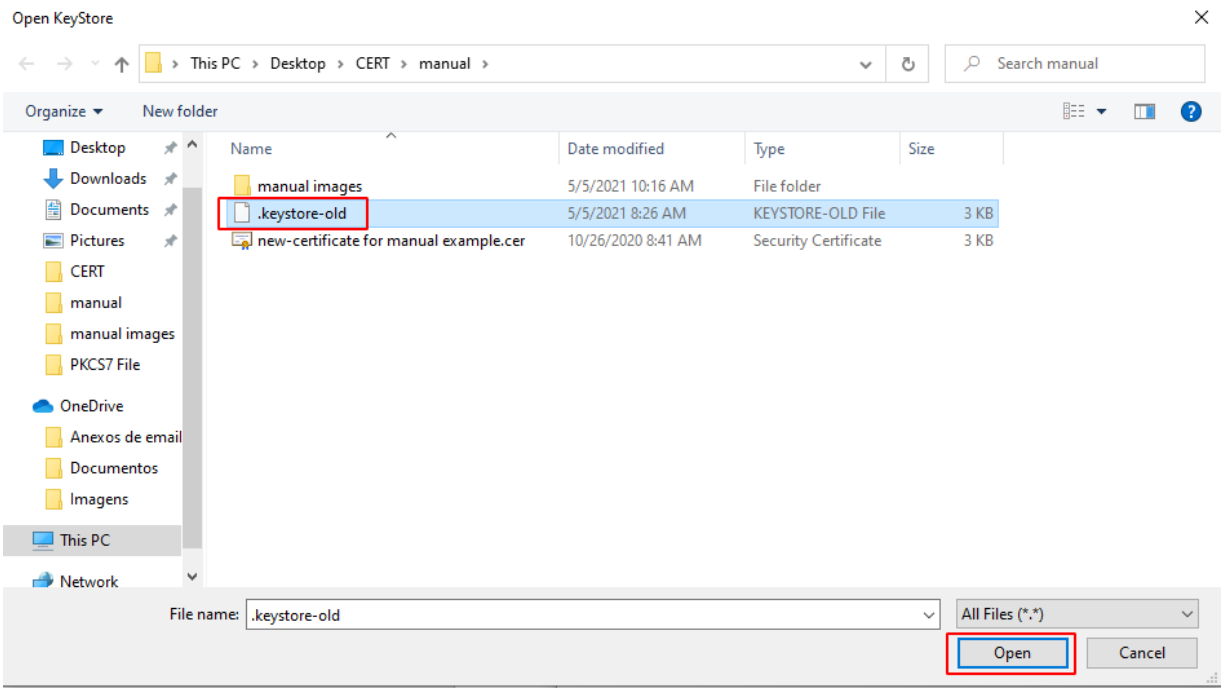
3. Need to have the new certificate.

Warning: The certificate we will show in this manual, is just an example of a certificate.

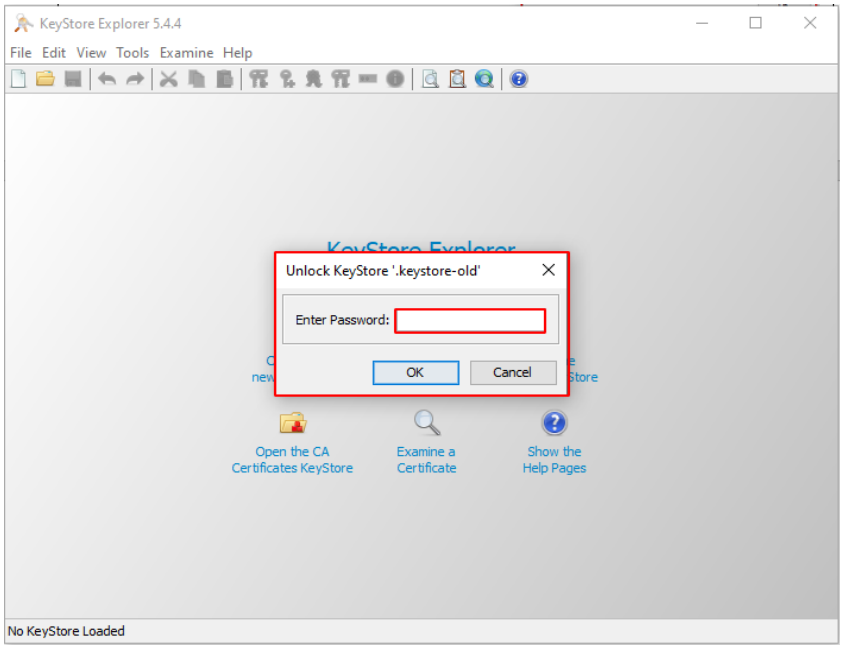


4. Import the old ".keystore" into the Keystore Explorer application.

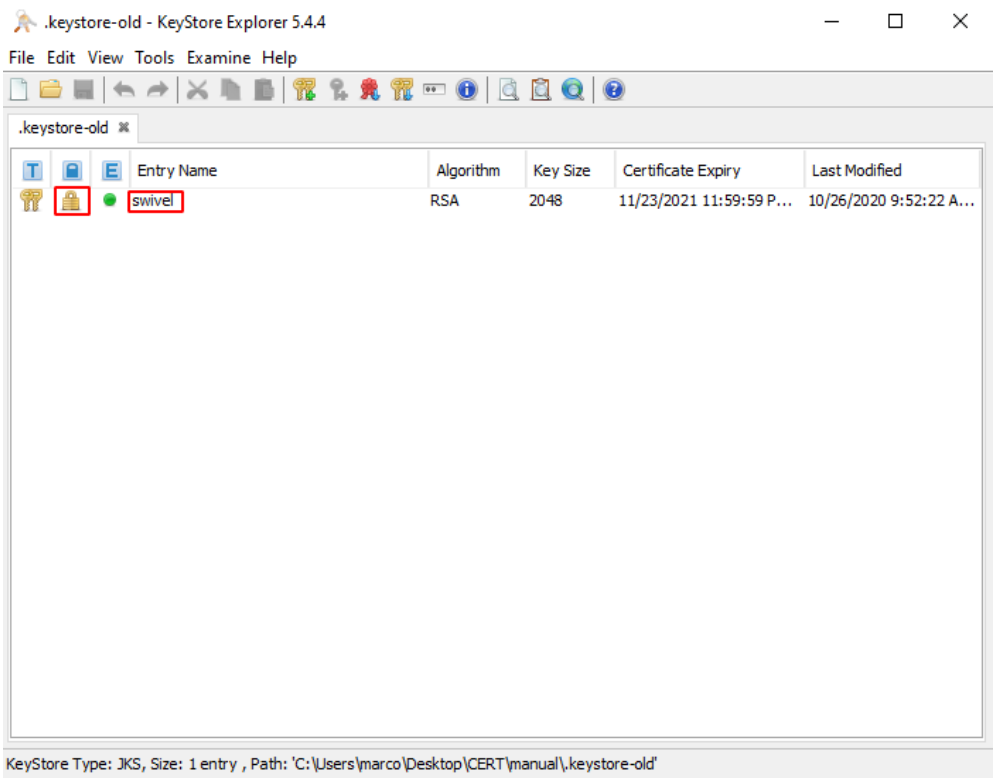




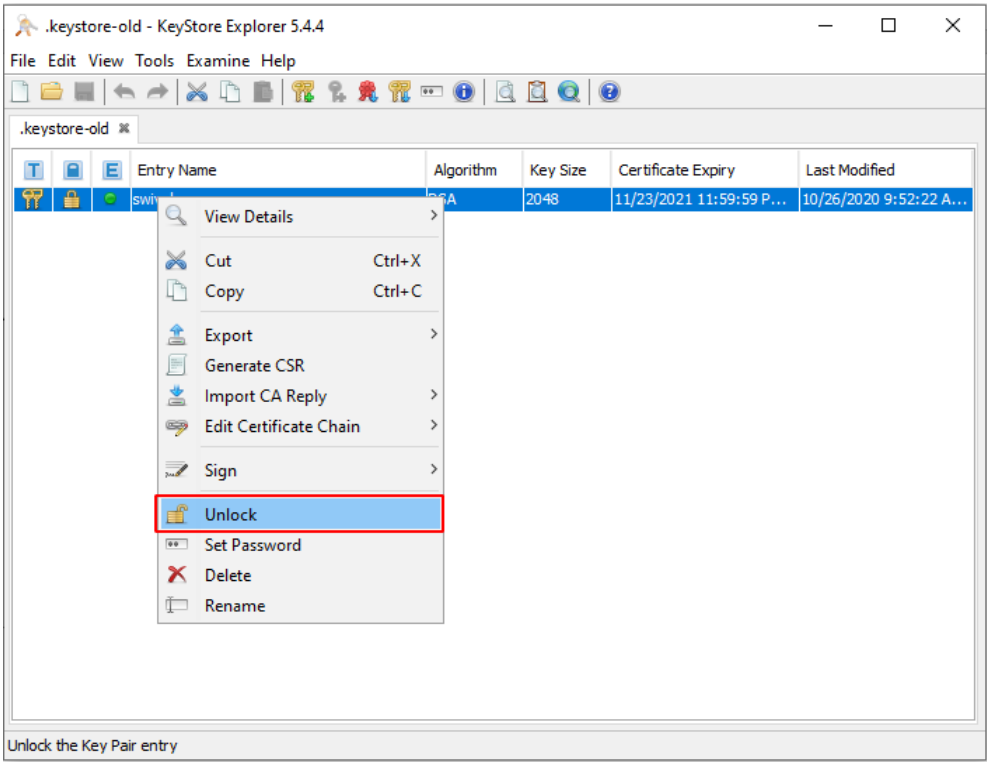
It will ask you for the Keystore password, which by default by SwivelSecure is "**lockbox**".



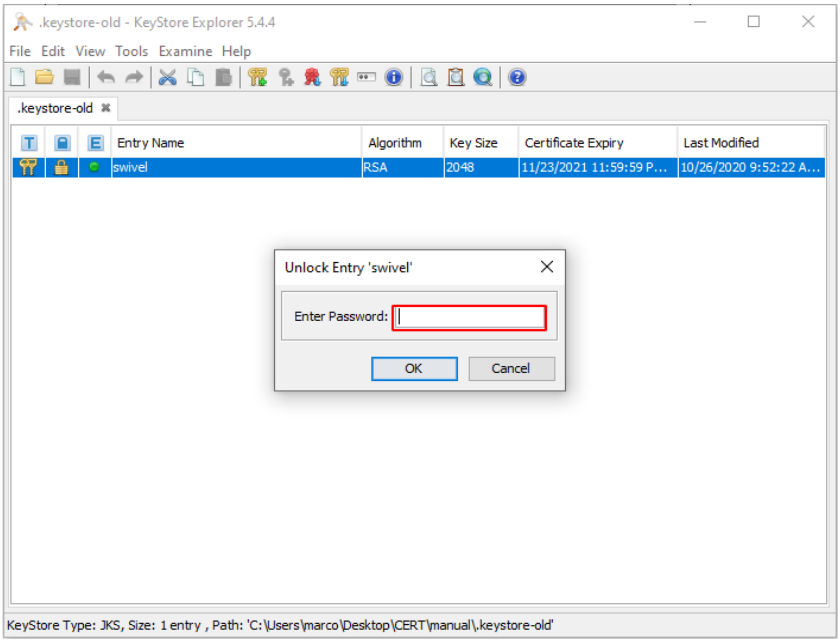
When you enter the password and open ".keystore-old", it should look like this:



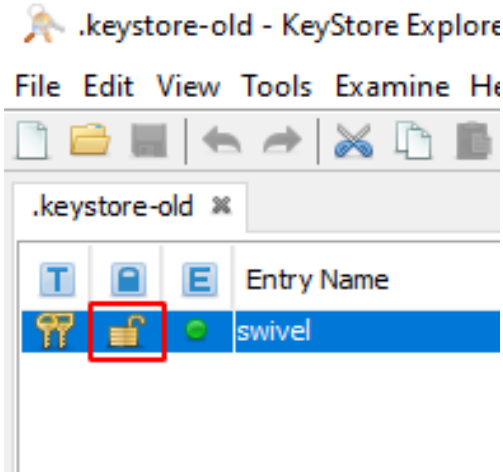
Next, we have to unlock the Keystore entry by doing the following steps:



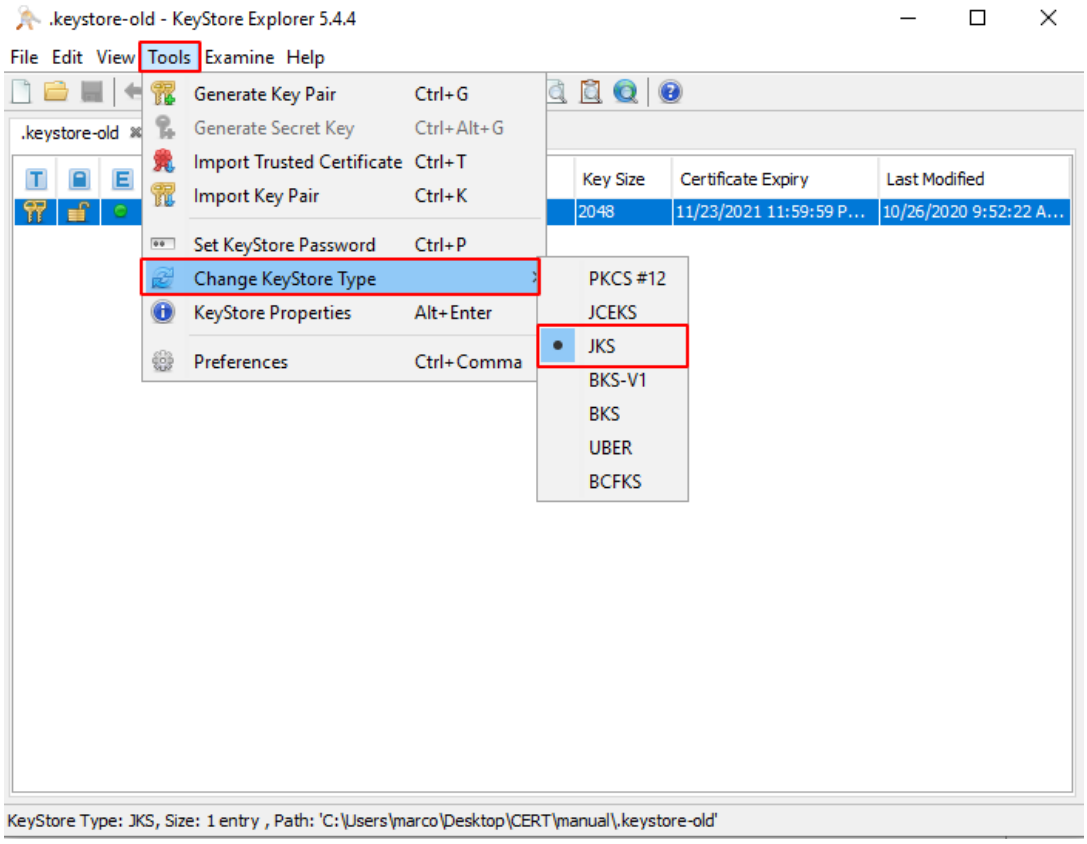
It will ask for a password that should be "lockbox" by default



After entering the password, we can confirm that the Entry has been unlocked by the Padlock symbol:



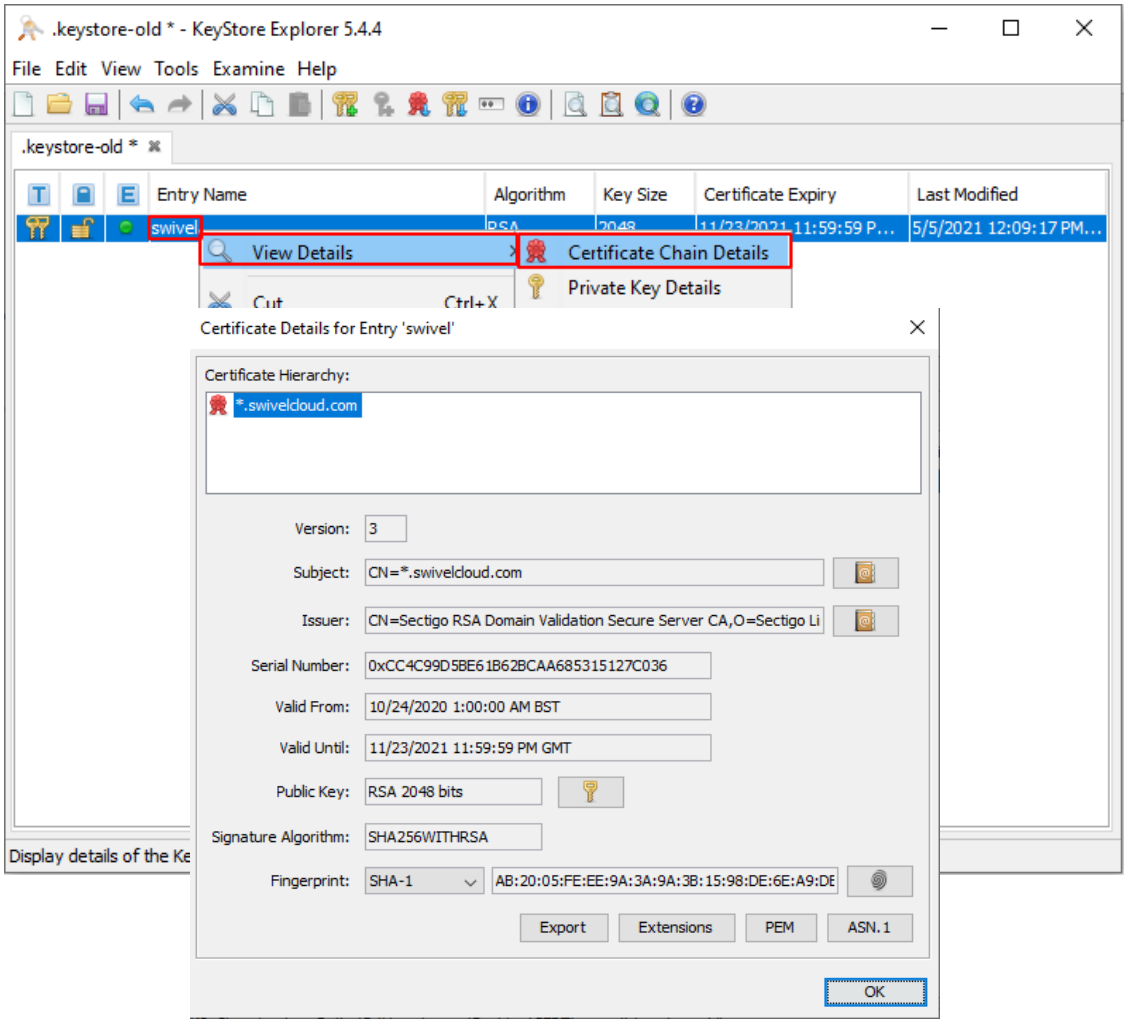
We recommend that you also check the KeyStore Type, which should be **JKS**, you can see in the following image where to check the Type:



5. Export the old certificate to a folder.

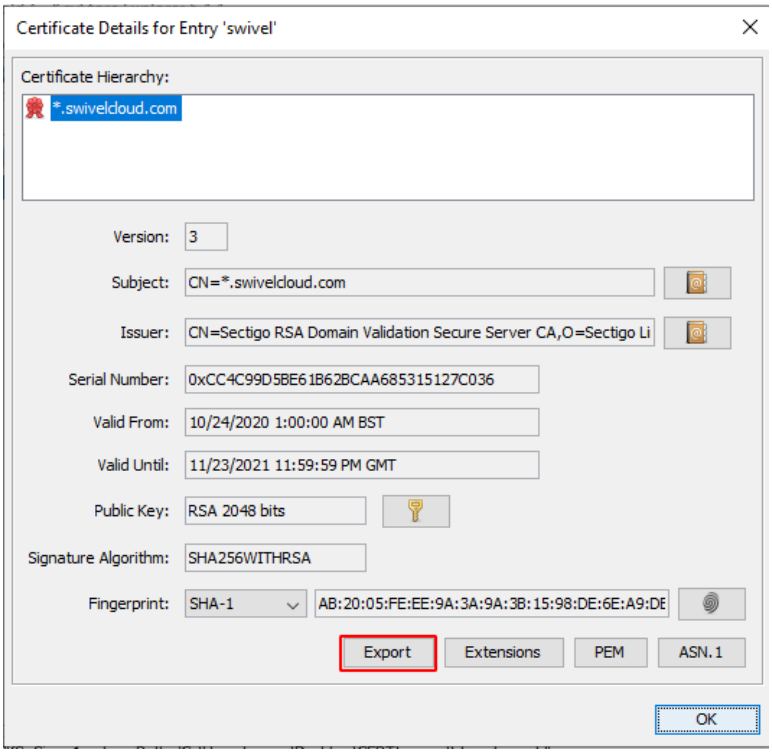
After checking the KeyStore Type, it's time to export the certificate from the Keystore to a folder.

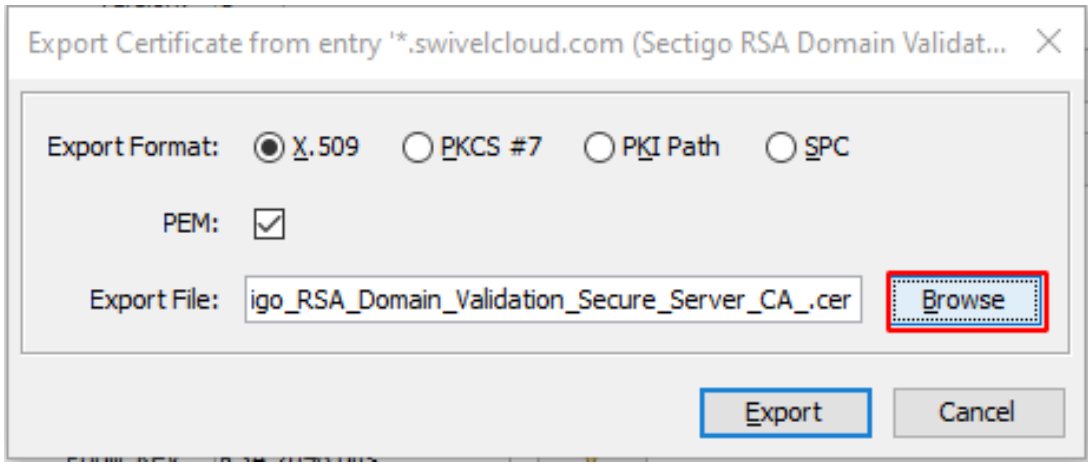
We can do this by accessing the **Certificate Chain Details**, and this can be done in two ways, we can **right-click** on the Keystore Entry Name "**swivel**", go to "**View Details**" and click on "**Certificate Chain Details**" or we can just **double-click** on the KeyStore Entry Name "**swivel**" and the Certificate Chain Details will open.



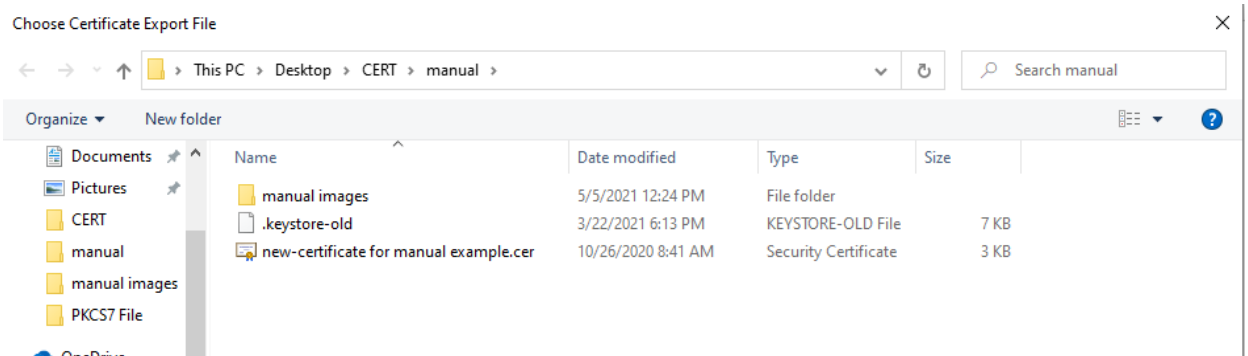
We remind you that this certificate in the manual was generated just for this purpose.

Now we have to export the certificate to a folder.



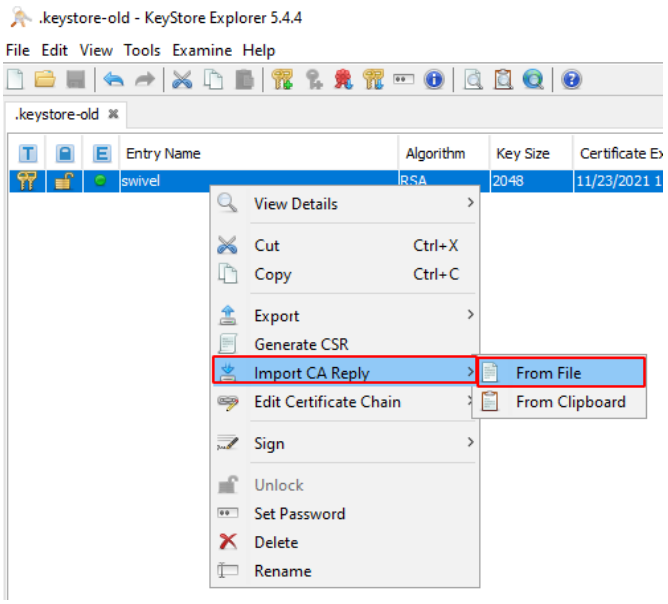


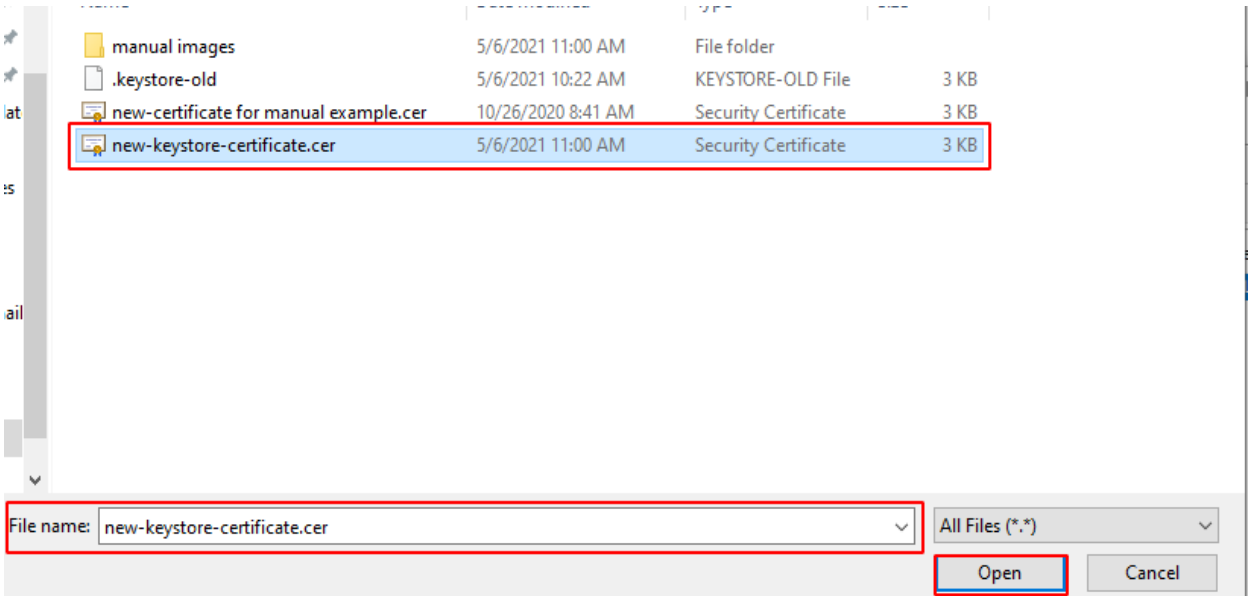
Chose the fold you want to export the ".Keystore-old" certificate and rename it.

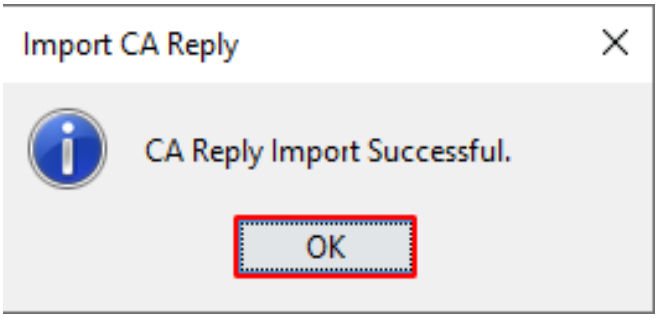


6. Go to the Keystore Explorer application where the old “.Keystore” will be and we will exchange the old certificate for the new one inside the old “.Keystore” key.

Now you have to exchange the old certificate for the new one we made.





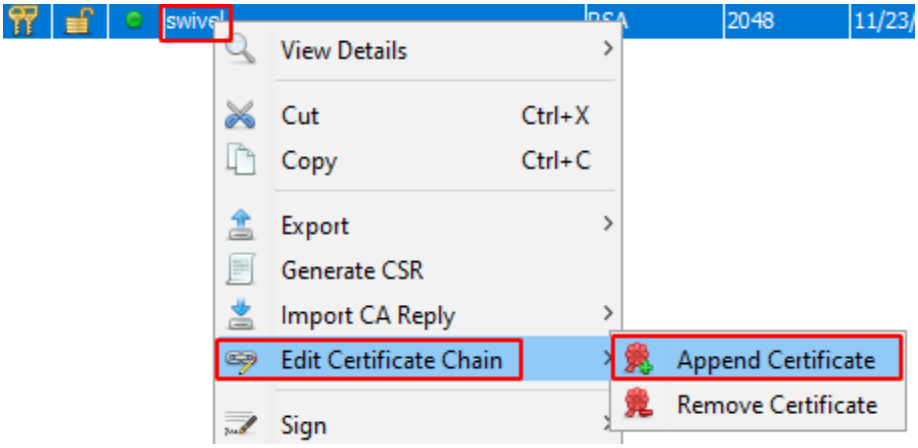


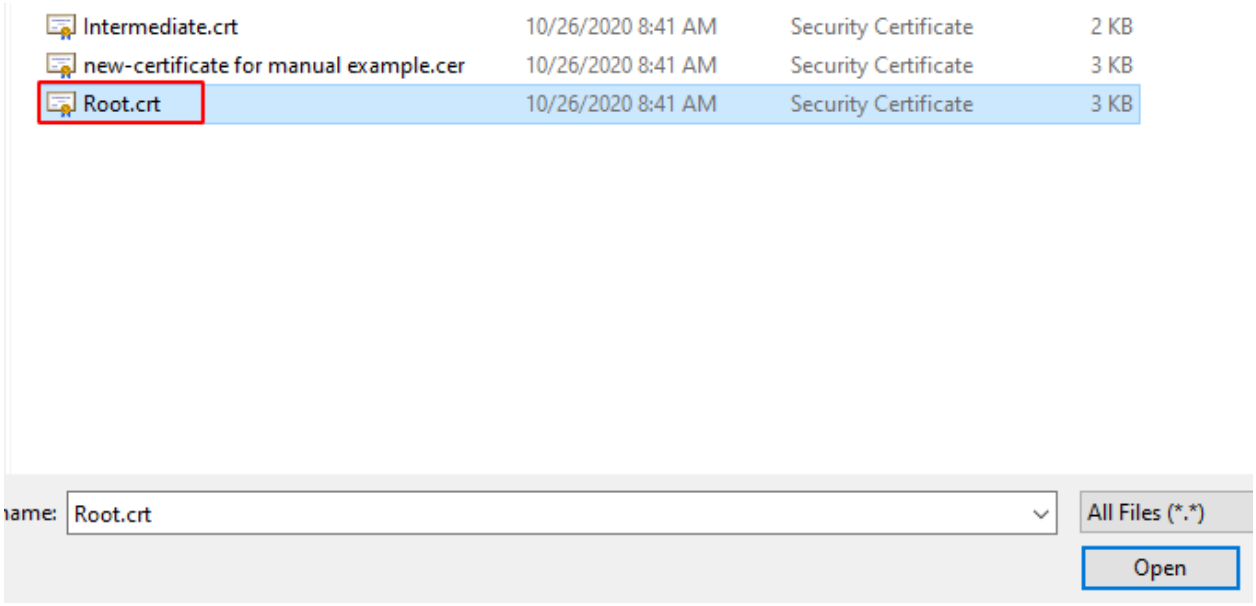
Now we have the new CA in the Keystore.

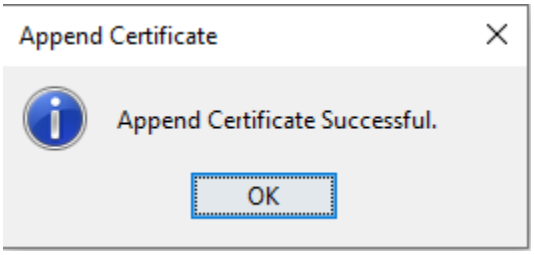
Import the Root certificate and the Intermediate one

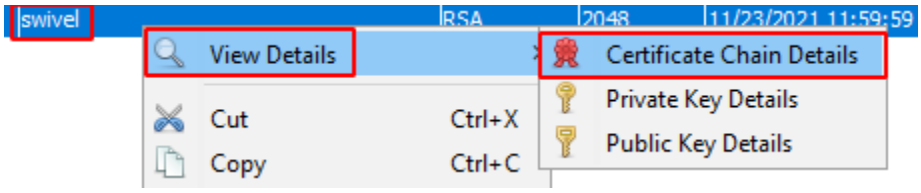
You have to import the root certificate and the intermediate to complete the certificate path for it to be complete for importing into the appliance.

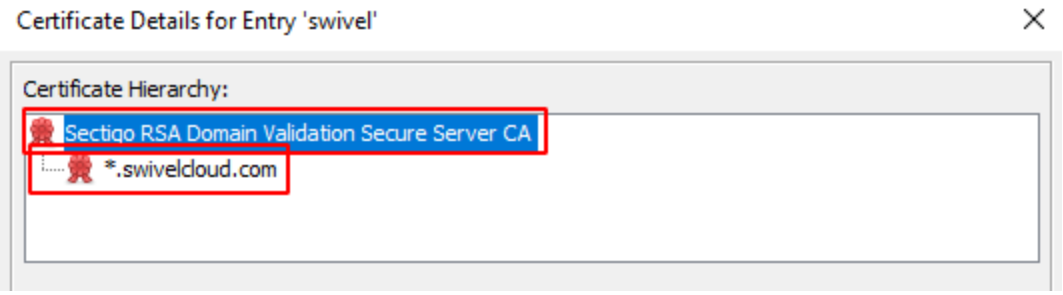
The steps are as follows:



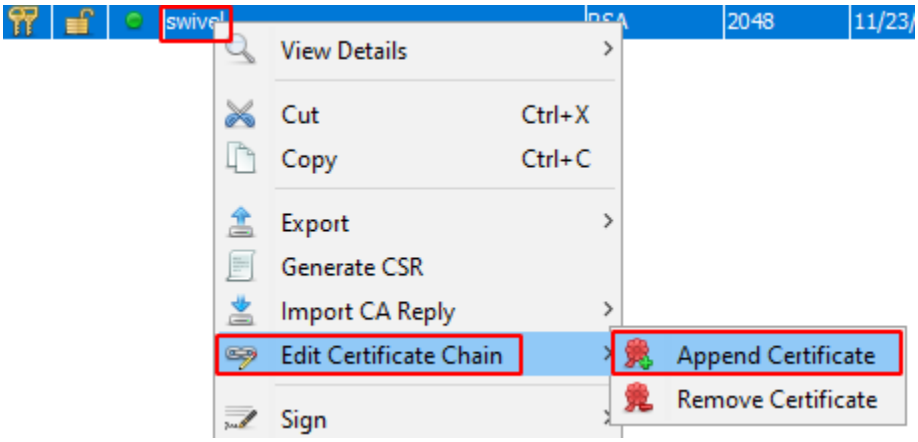

Intermediate.crt 10/26/2020 8:41 AM Security Certificate 2 KB
new-certificate for manual example.cer 10/26/2020 8:41 AM Security Certificate 3 KB
Root.crt 10/26/2020 8:41 AM Security Certificate 3 KB
ame: Root.crt
All Files (*.*)
Open

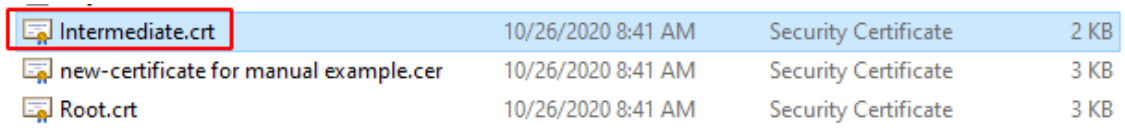

Append Certificate
Append Certificate Successful.
OK

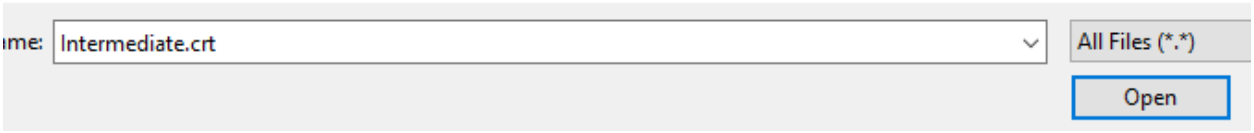

swivel
RSA
2048
11/23/2021 11:59:59
View Details
Cut Ctrl+X
Copy Ctrl+C
Certificate Chain Details
Private Key Details
Public Key Details

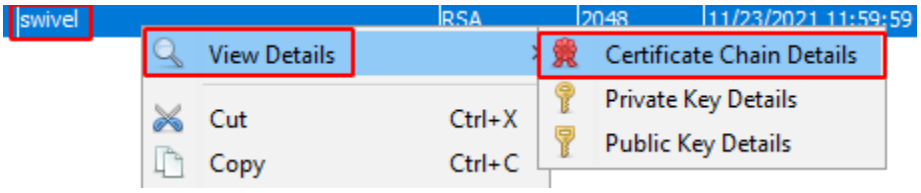


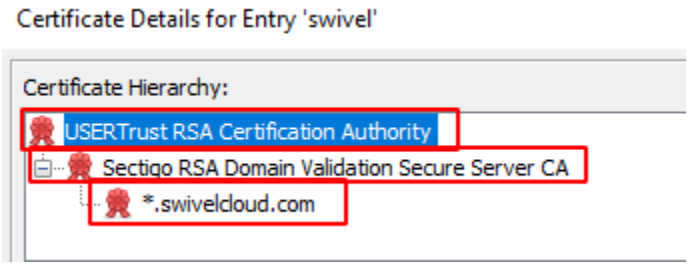
Now the Keystore already has the Root certificate, but the intermediate still missing:







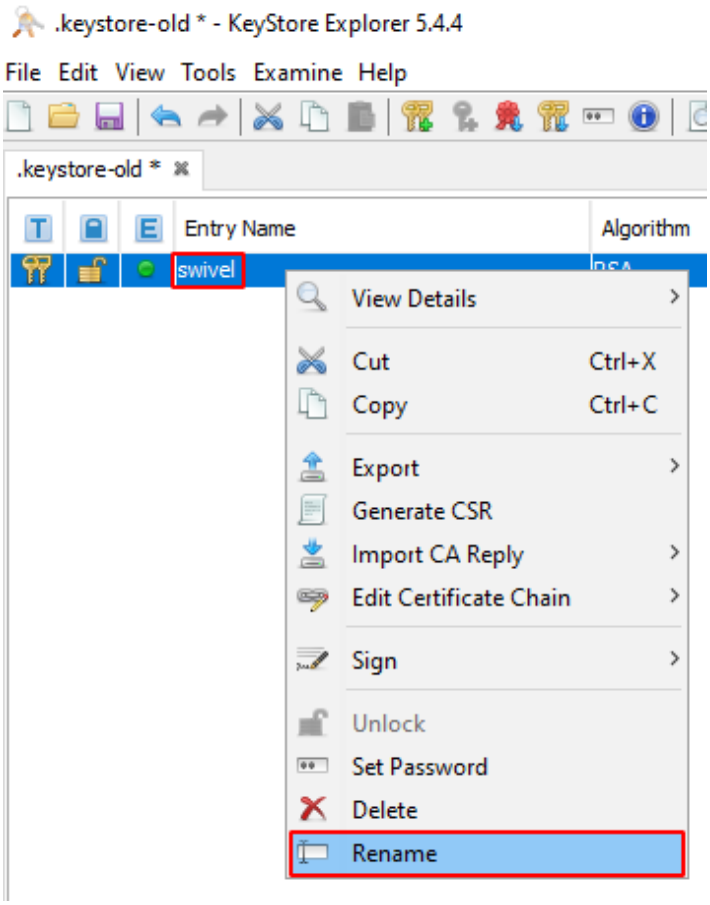




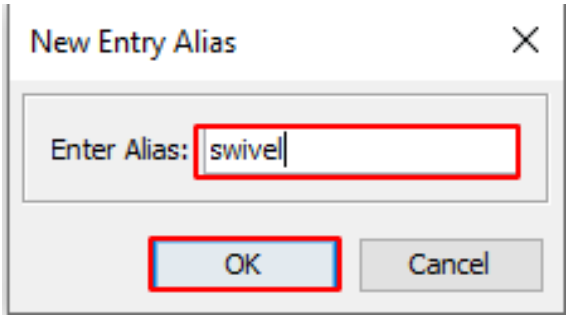
Now the Keystore is compiled and almost ready to be stored and imported into the appliance.

Now we recommend doing some important steps before saving our new ".keystore".

We will start by checking the "Entry Name - Alias" of the certificate and the password of the certificate and the “.keystore”.

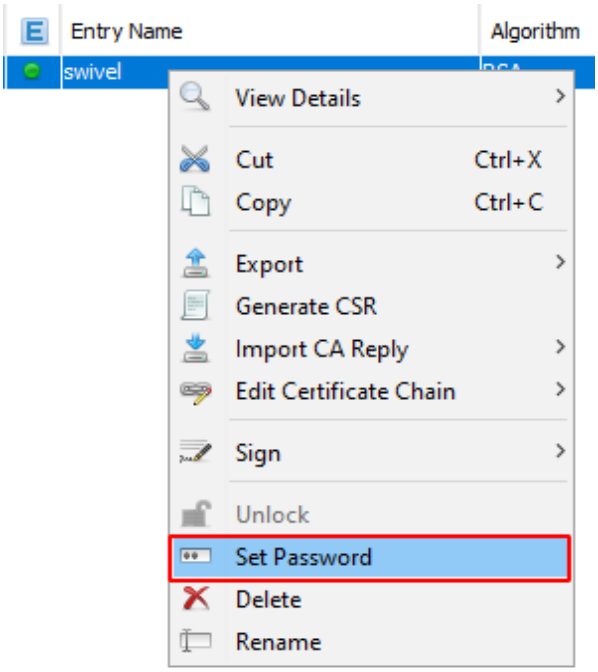


You will have to rename the alias to "**swivel**”

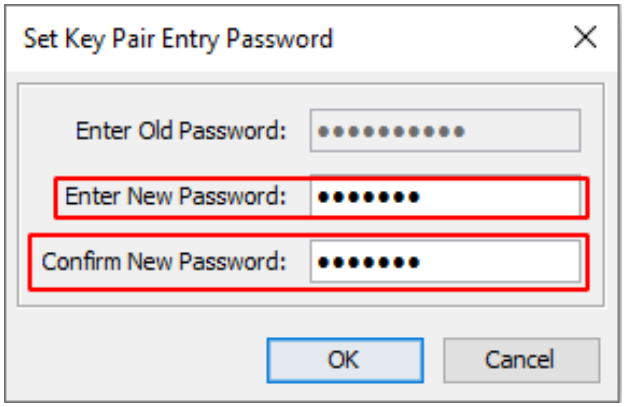


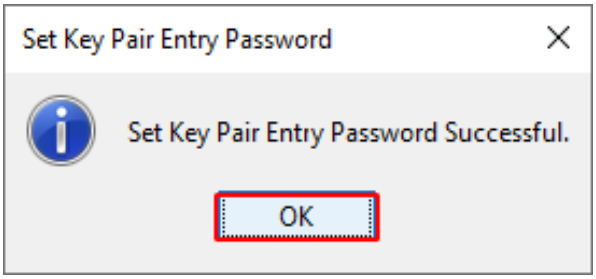
Next, you have to verify the passwords.

Start with the "Key Pair Entry Password":

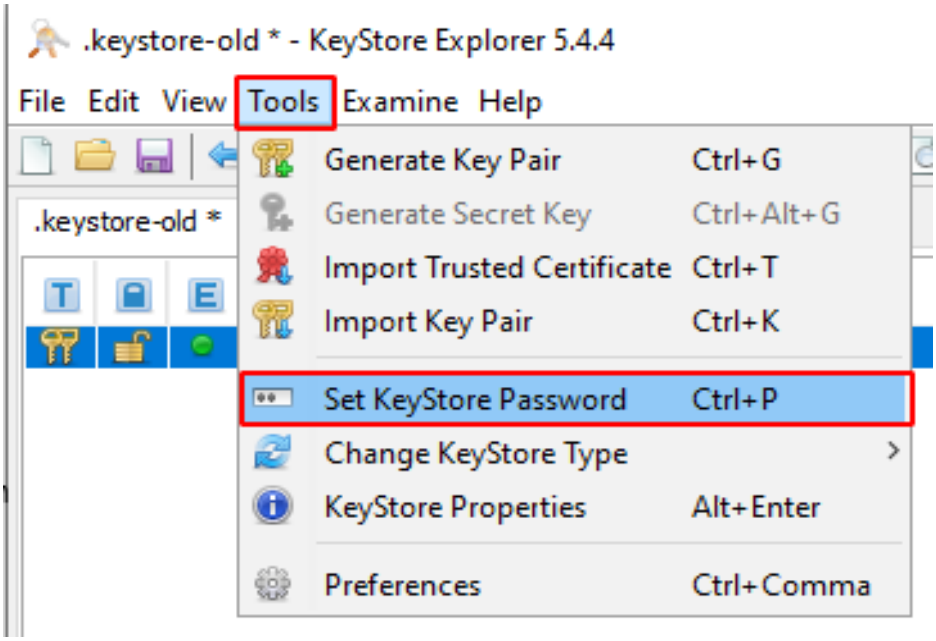


The “Key Pair Entry Password” must be "**lockbox**”.

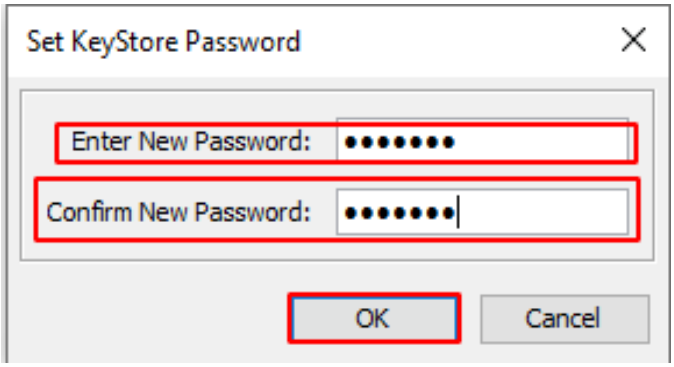


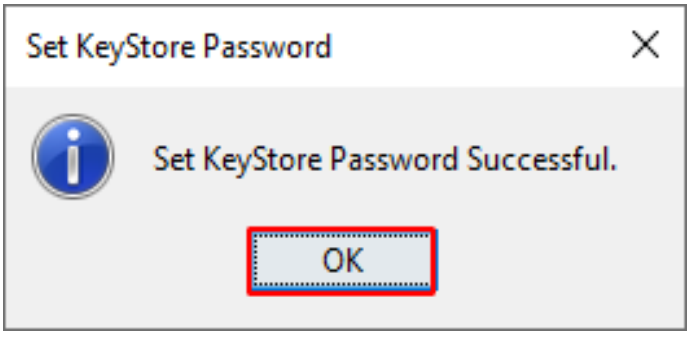


Then check the Keystore password:



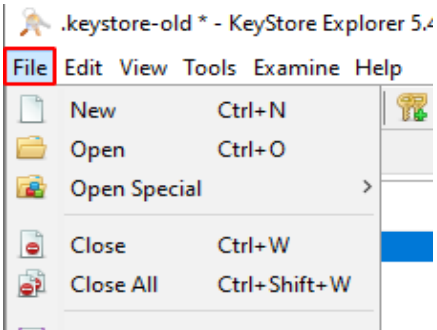
The “KeyStore Password” must be "**lockbox**”.



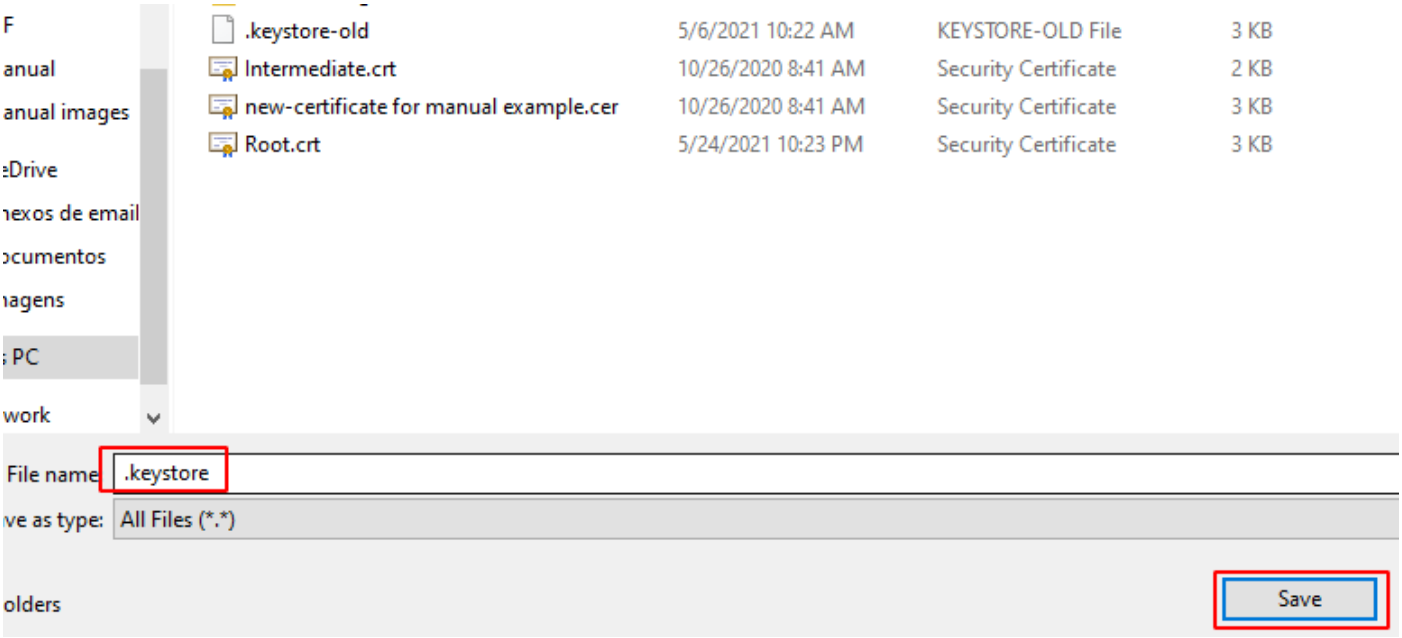


Now the certificate is ready, all you have to do is save it.

7. Save the new ".keystore" to a folder.



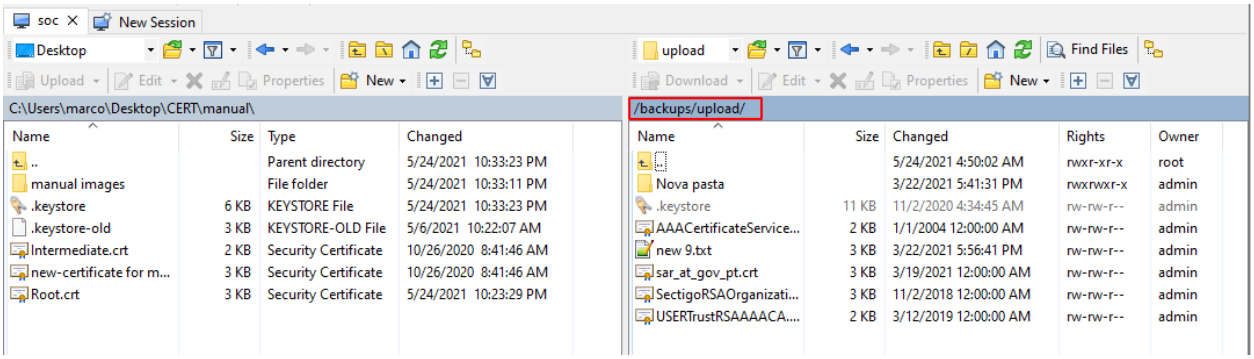
The certificate should be named "**.keystore**".



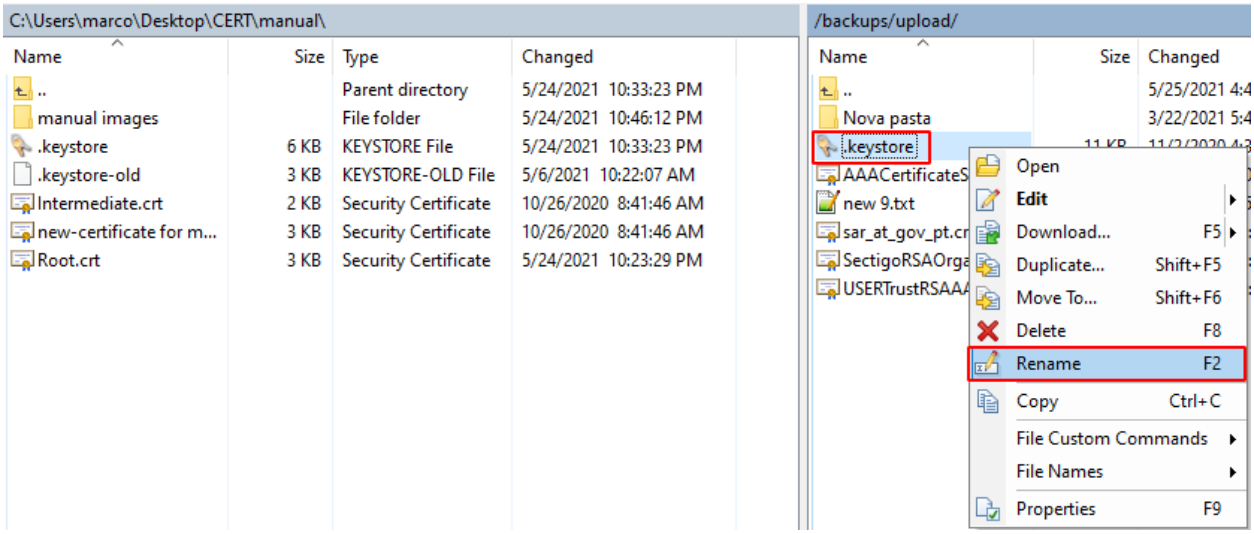
Now you will have the certificate ready to be imported into the appliance.

8 Import the new .Keystore to the appliance

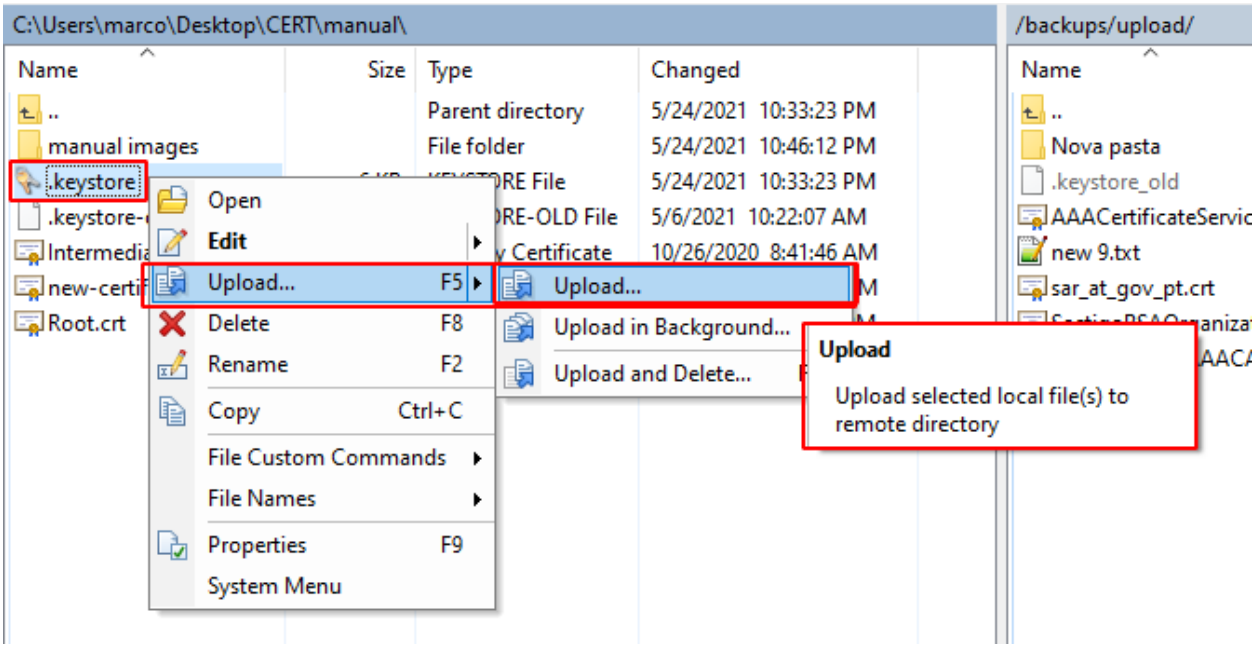
Now by WinSCP, we have to access the appliance and go to the folder /backups/upload.

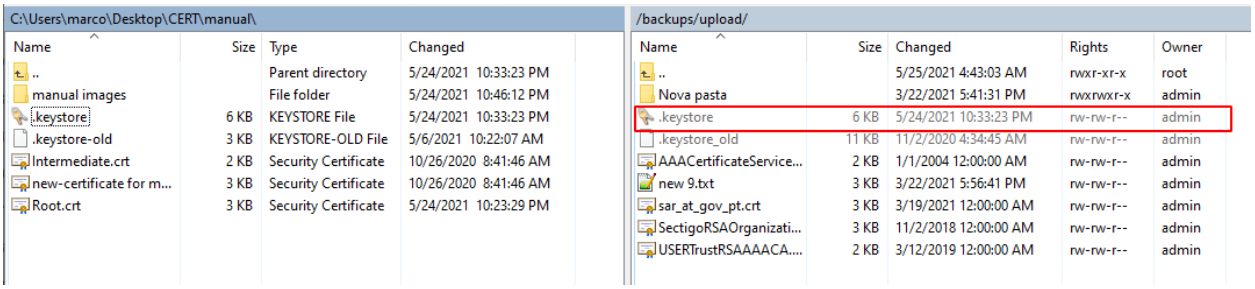


Rename the old ".Keystore" file to ".Keystore_old".



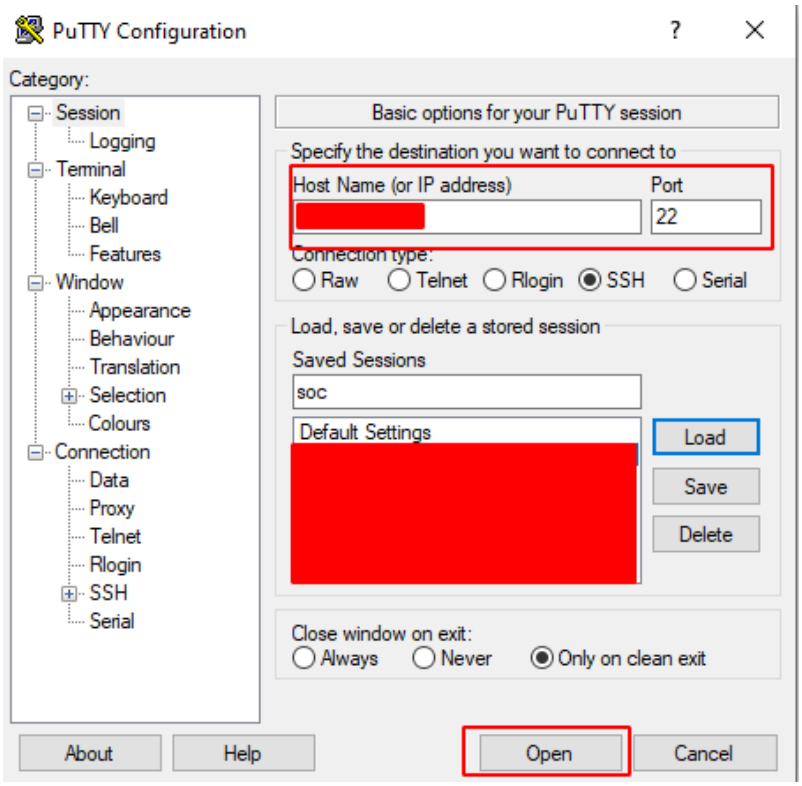
Upload the new ".Keystore" file to the appliance (/backups/upload).





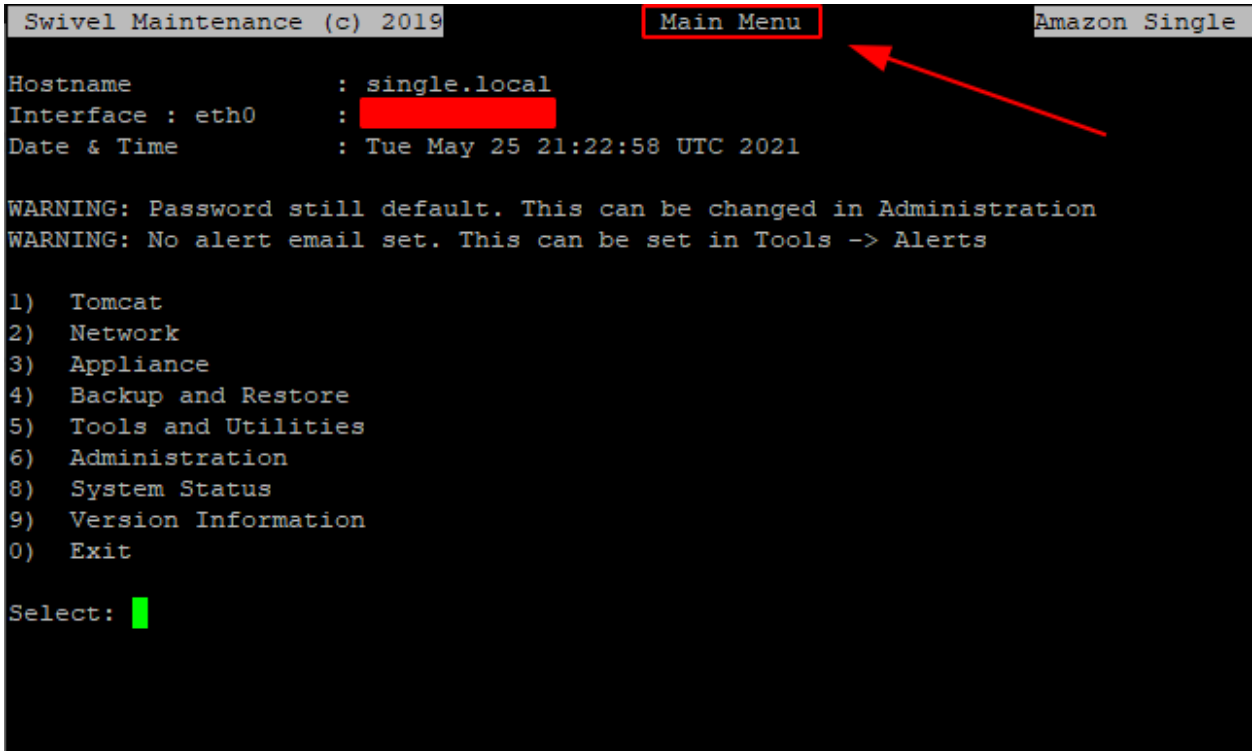
9. Access the appliance by putty or other SSH.

you must access the appliance

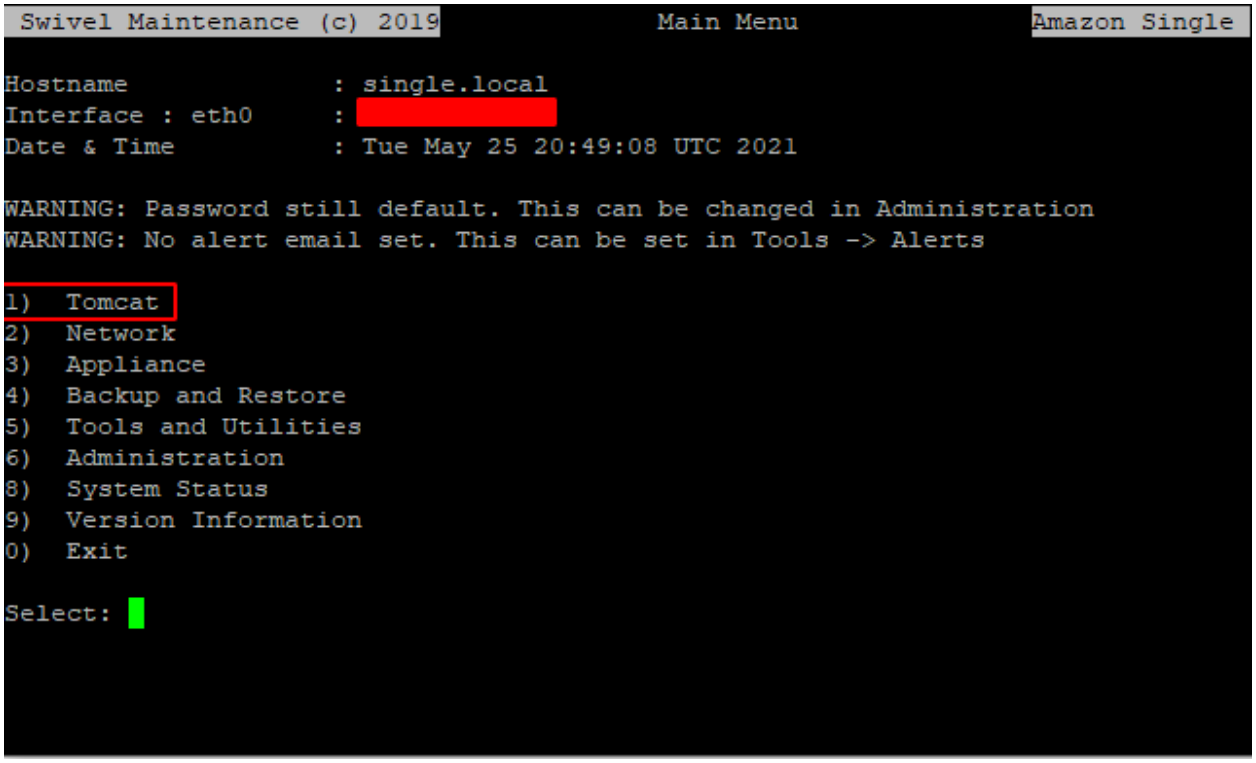


Sign in

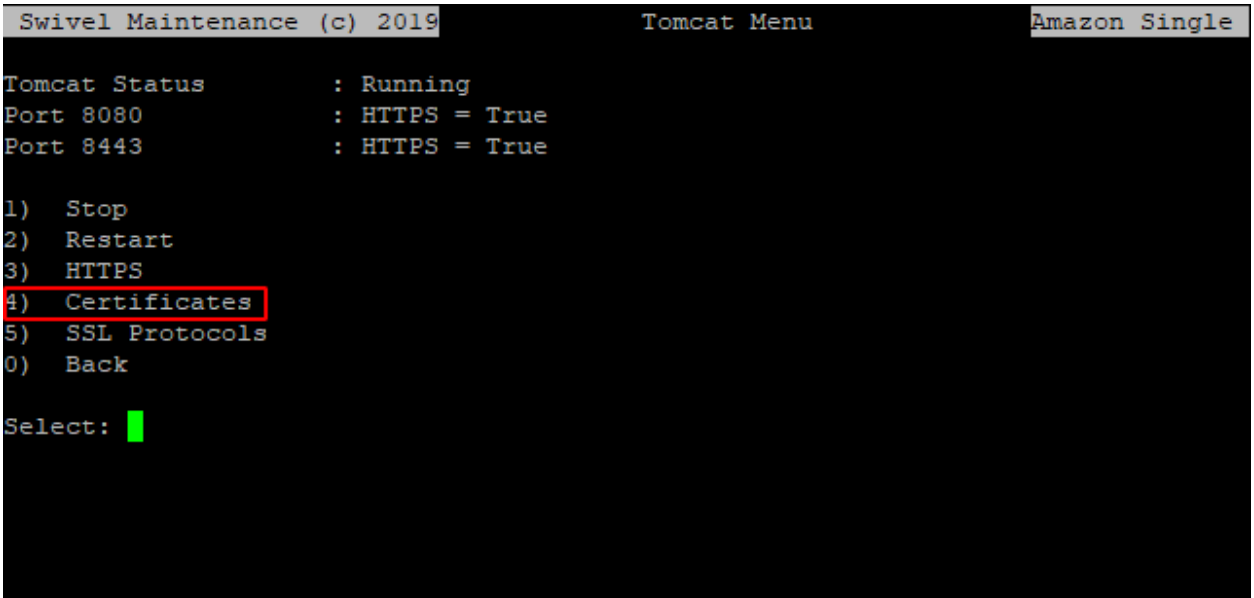
Once inside the appliance in the CMI menu, you can orient yourself and see which menu you are in in the upper right corner.



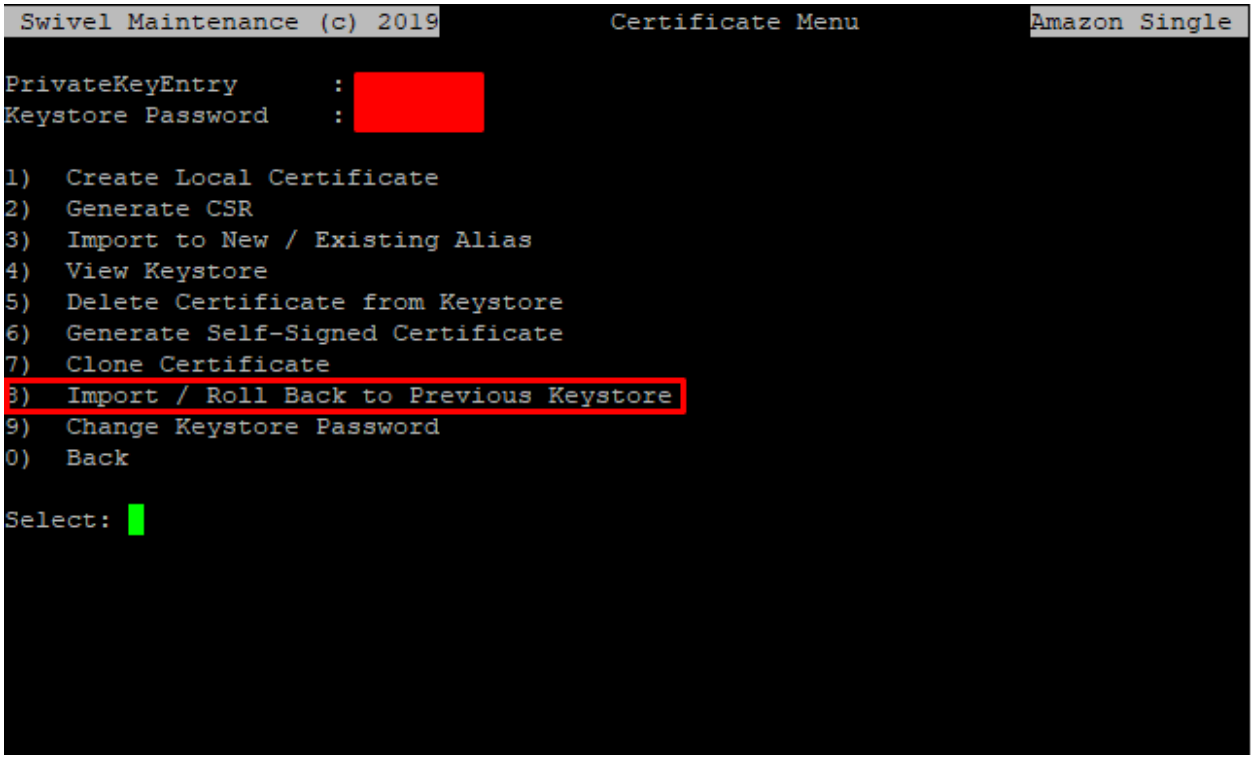
now in the CMI menu, go to menu 1 "Tomcat”



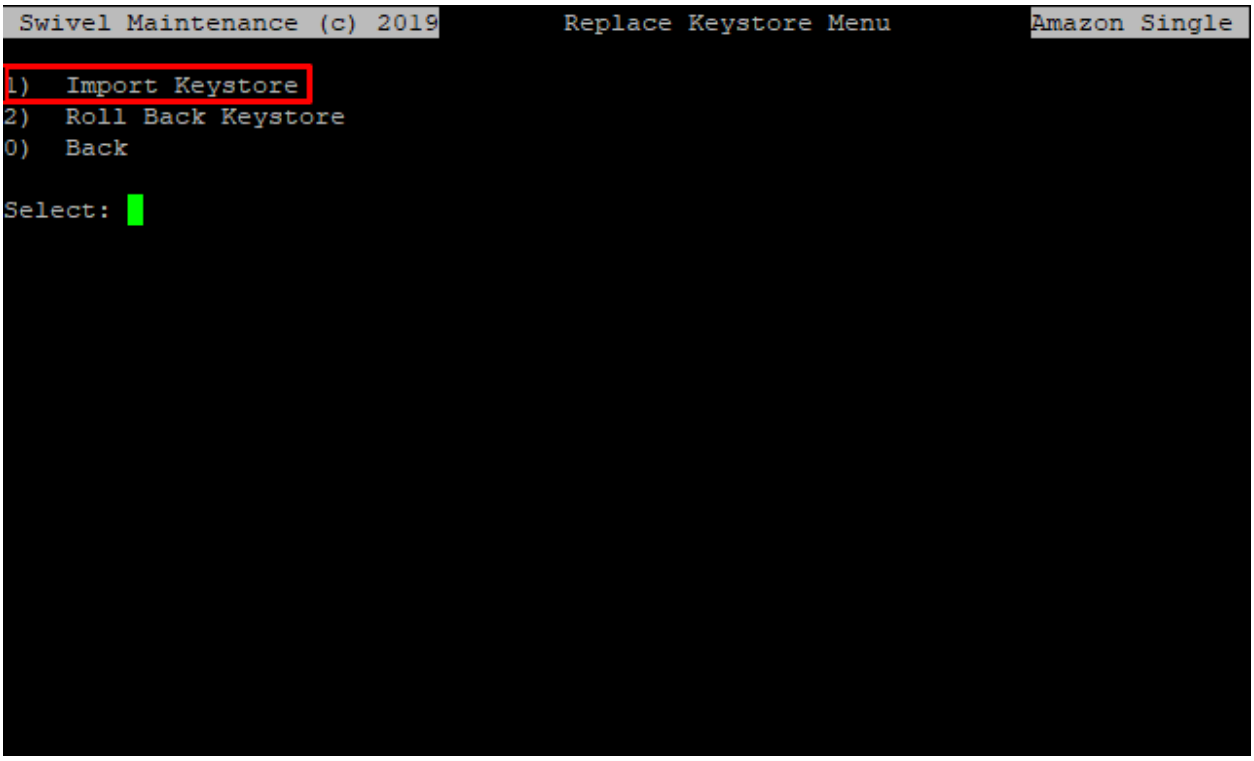
Then go to menu 4 "Certificates”



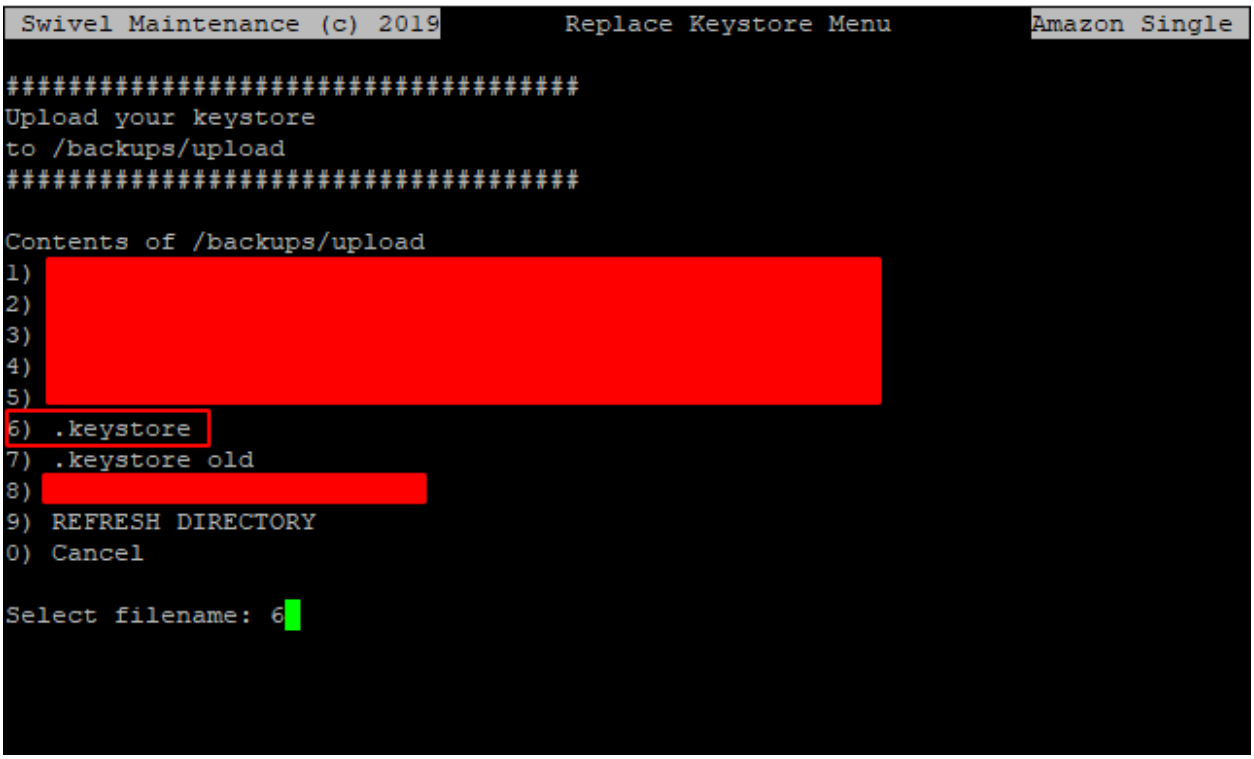
Enter menu 8 “Import / Roll Back to Previous Keystore”



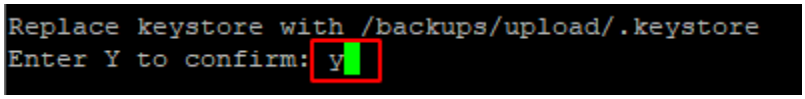
Enter menu 1 “Import Keystore”



Chose the new certificate “.Keystore”, in this example it turned out to be option number 6, but it all depends on what files are in the "/backups/upload" folder.



You will ask to confirm the “Replace Keystore” you should say/type “y” or “Y”

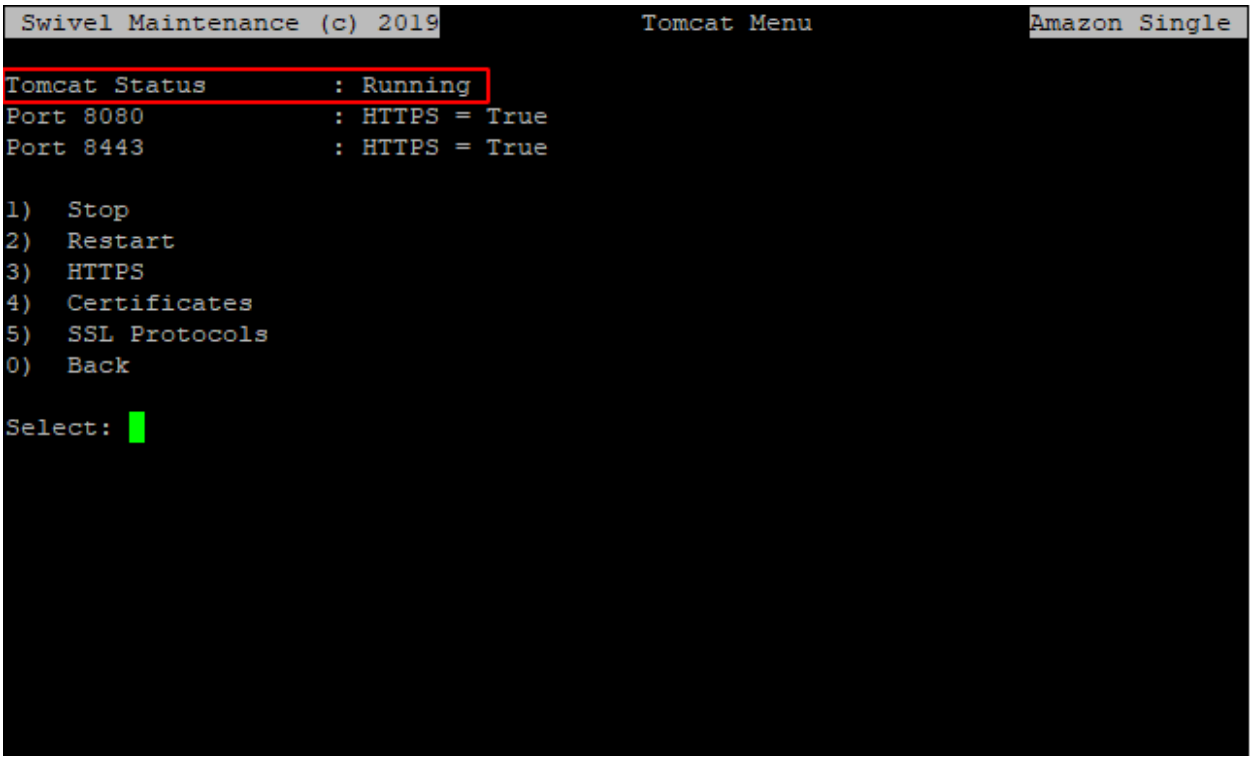


After you have confirmed the replacement of the new “.Keystore” on the appliance, you will be asked if you want to restart Tomcat immediately to apply the changes.

This choice is made by you since you can choose these options since restarting Tomcat will bring the system down for the 30s - 3m, not affecting those who are already authenticated, but it will affect users who want to authenticate themselves in that period of Tomcat restart:

- You can choose to restart Tomcat and apply the changes you made to the “.keystore” immediately;
- You can choose not to restart Tomcat right away and go check if the new “.Keystore” is correct in the "Certificate Menu" by choosing option number 4 "View Keystore" and then choose the aliases that should be the one we chose when making the new “.keystore” which was "swivel", and you will be able to see all the information about the new “.keystore”
- You can choose not to restart Tomcat right away and just do it when it suits you best.

After restarting Tomcat, check that it is "Running" in the "Tomcat Menu.



If it is in "Running" everything should be running fine as expected and you only need to check if you can access the platforms and log in to them.

We take this opportunity to indicate that if you have any questions or problems, you can contact our SOC team by sending an email to ***supportdesk@swivelsecure.com*****.**