

Import, convert and export certificates

Note: Repeat this section for both the Push and Distribution (code-signing) certificates. For this step there are three options shown. Choose which option is most familiar:

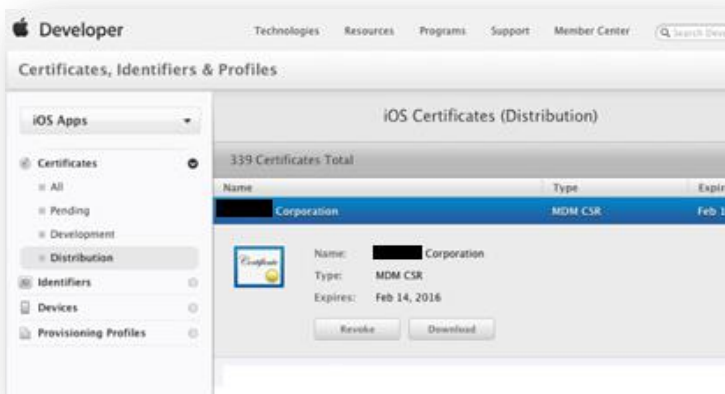
[OSX-Method:](#)

[Linux-Method:](#)

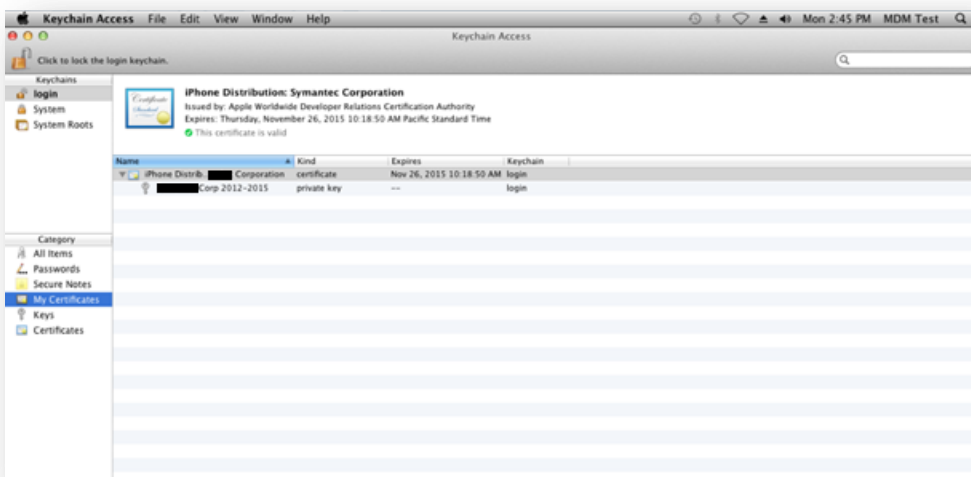
[IIS-Method](#)

OSX-Method:

1. Download the newly created certificate (ios_distribution.cer or aps_distribution.cer) and install it to the keychain by opening the certificate with the Keychain application or manually importing the cert using the Keychain application:



2. The private key should be visible; associated with the certificate on the keychain, see below:



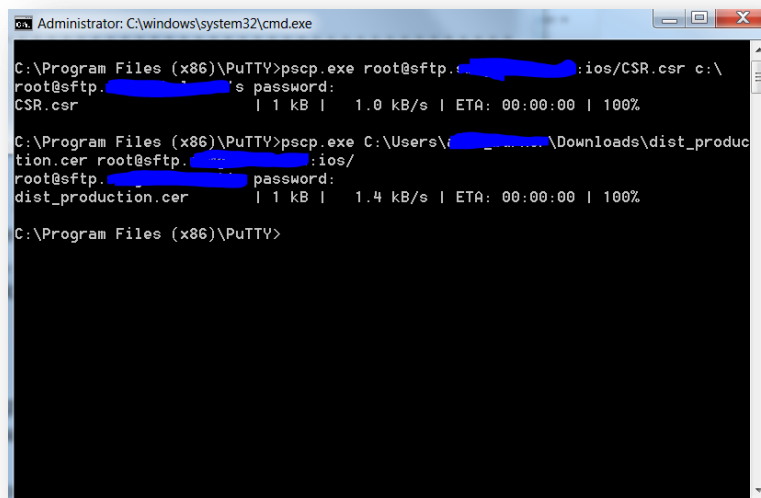
3. Right-click on the certificate and select **Export**. Save the exported Cert as a Personal Information Exchange.
4. Once the certificate has been successfully exported upload the certificate to the Mobility **Admin console** > **Settings** > **Certificates** > **Apple/iOS certificates** under its respective area.

Tip: If it is the ios_distribution.pfx/p12; then upload it to the code-signing area. If it is the APNS (Push) aps_production.cer upload to to the Push section.

5. Remember to update the provisioning profile used to build the iOS Work Hub client after regenerating the ios_distribution and apn_production certificates. See [Renewing the Provisioning Profile](#)

Linux-Method:

1. Download the certificate (ios_distribtuion.cer or aps_production.cer) from the Apple Developer site, to the workstation and upload it to the same Linux machine used to create the CSR.csr using a command like:
pscp.exe C:\CSR.csr root@<remoteHOST>:<remotePath>
For Example:



```
Administrator: C:\windows\system32\cmd.exe
C:\Program Files (x86)\PuTTY>pscp.exe root@sftp.ios:ios/CSR.csr c:\
root@sftp.ios's password:
CSR.cer | 1 kB | 1.0 kB/s | ETA: 00:00:00 | 100%
C:\Program Files (x86)\PuTTY>pscp.exe C:\Users\Downloads\dist_produc
tion.cer root@sftp.ios:/
root@sftp.ios password:
dist_production.cer | 1 kB | 1.4 kB/s | ETA: 00:00:00 | 100%
C:\Program Files (x86)\PuTTY>
```

2. From the Linux machine use openssl to convert the ios_distribution.cer or aps_production.cer to PEM format using:

openssl x509 -inform der -in ios_distribution.cer -out ios_distribution.pem

For example:

```
[root@localhost ios]# openssl x509 -inform der -in dist_production.cer -out dist
production.pem
```

3. Convert the ios_distribution.cer or aps_production and privateKey.key file into a p12 using the following command, entering a complex password to secure the file:

openssl pkcs12 -export -out ios_distribution.pfx -inkey privateKey.key -in ios_distribution.pem

For example:

```
[root@localhost ios]# openssl pkcs12 -export -out dist_certificate.pfx -inkey privateKey.key -in dist_production.pem
Enter Export Password:
Verifying - Enter Export Password:
[root@localhost ios]#
```

4. Download the ios_distribution.pfx or aps_production.pfx to the workstation using PSCP, WinCP or Filezilla. From the workstation download the ios_distribution.pfx.

Tip: For instruction on how to transfer files between a Linux and Windows, see [HOWTO110248](#).

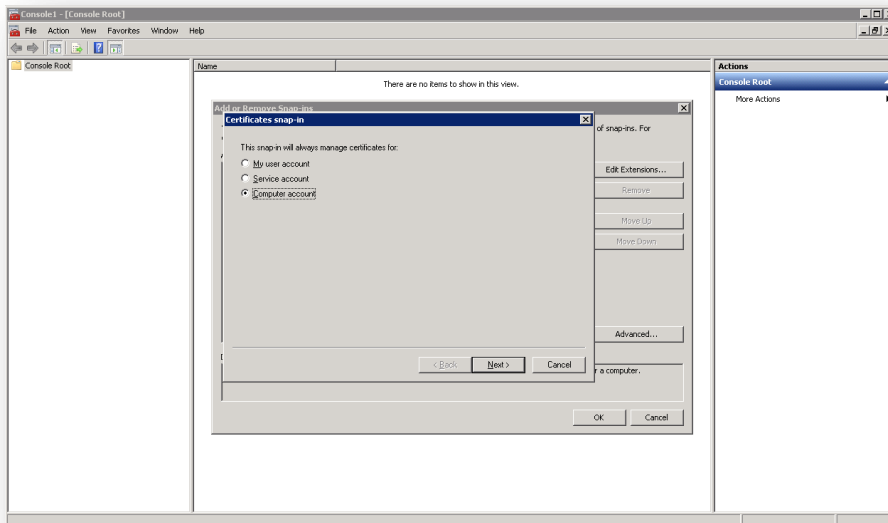
5. Once the certificate has been successfully exported upload the certificate to the Mobility **Admin console** > **Settings** > **Certificates** > **Apple/iOS certificates** under its respective area.

Tip: If it is the ios_distribution.pfx/p12; then upload it to the code-signing area. If it is the APNS (Push) aps_production.cer upload to the Push section.

6. Remember to update the provisioning profile used to build the iOS Work Hub client after regenerating the ios_distribution and apn_production certificates. See [Renewing the Provisioning Profile](#).

IIS-Method

1. From the same windows machine used to generate the CSR, go to **Start** > search for **MMC** and open MMC.
2. From within MMC go to **File > Add/Remove Snap-in > Certificates** and click **Add**.
3. Select **Computer account** and **Next**.



4. Ensure that **Local computer** is selected and click **Finish**.
5. Now **OK** to create the new snap-in.
6. Expand the **Certificates (Local Computer) > Personal > Certificates**.

7. Right click on certificates and select **All Tasks > Import**.
8. Browse to the ios_distribution.cer or aps_distribution.cer created by uploading the CSR from [How to create a CSR](#).
9. Ensure that **Place all certificates in the following store: Personal** is selected and click **Next**.
10. Review the import information and click **Finish**.

Note: If asked, mark the key as exportable and include all extended properties.

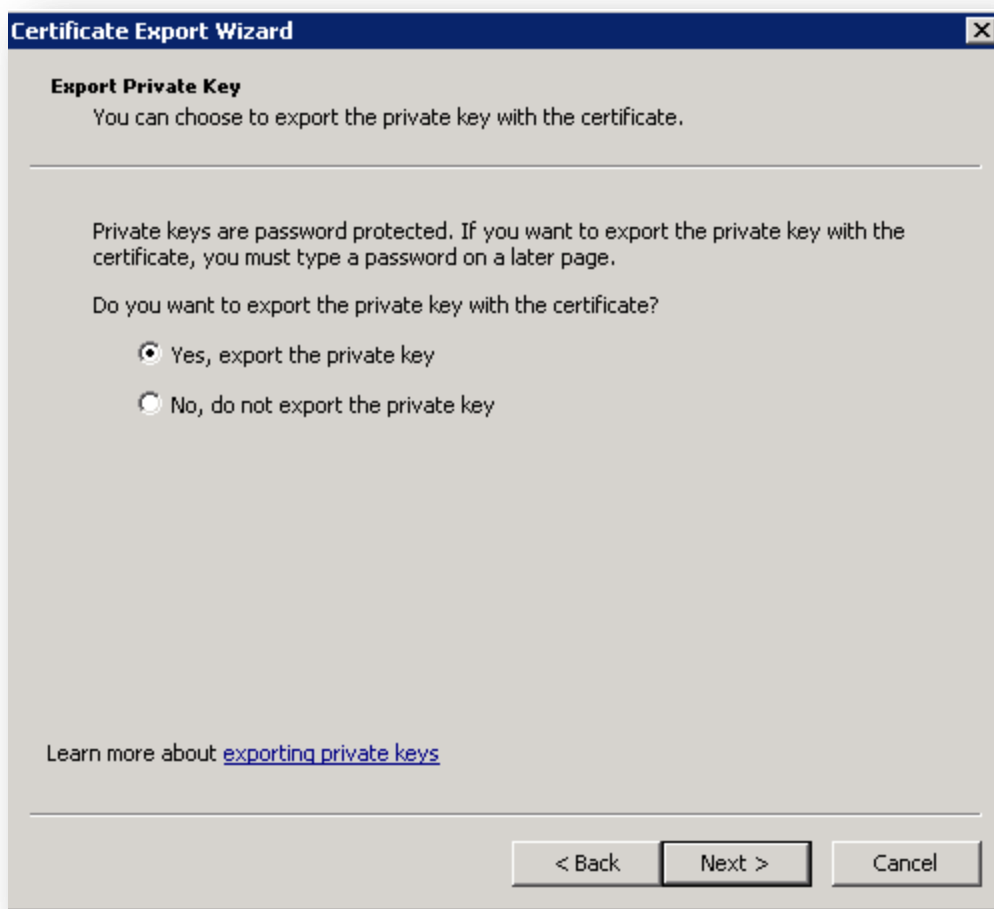
11. Allow up to 1 minute for the import to complete.
12. Verify that the private key has been associated with the certificate by looking for a small key symbol over the certificate as shown below:



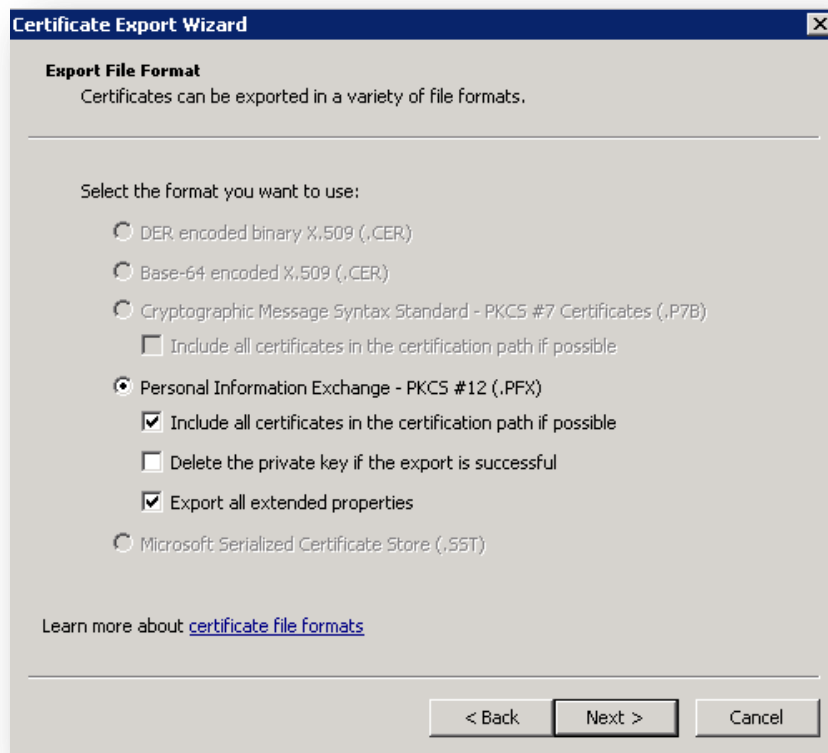
13. If no key icon is showing be sure that the machine has Apple's root [certificate](#) authority added as a trusted Root Certificate and repeat 1-14.

Tip: If the key is still now shown, recreate the [CSR](#) via IIS and repeat.

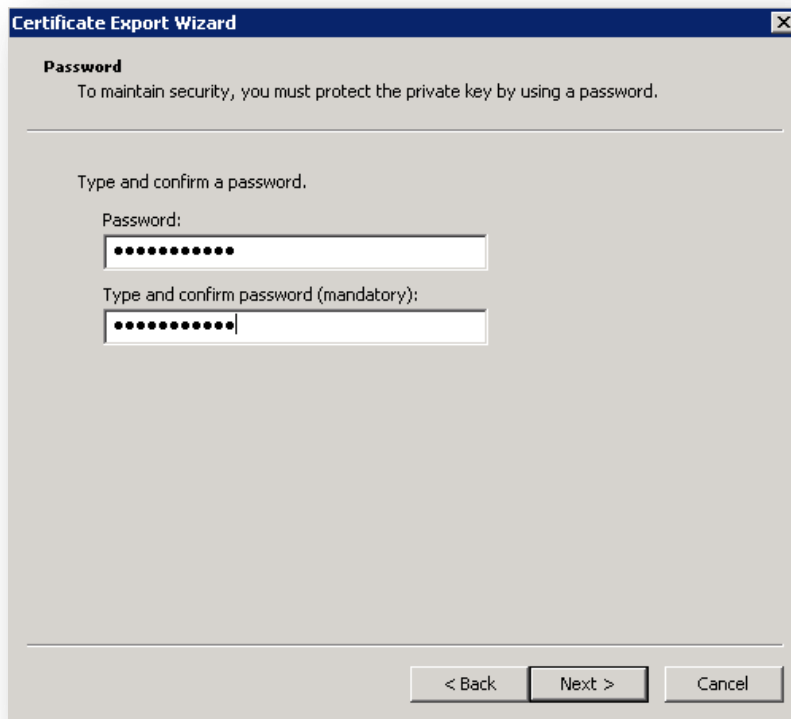
14. If a key is shown, right click on the certificate and go to **All Tasks > Export**.
15. Click **Next**.
16. Select **Yes, export the private key** and click **Next**.



17. Ensure that **Personal Information Exchange – PKCS #12 (.PFX)** is selected and **Include all certificates in the certificate path if possible** and **Export all extended properties** are checked and click **Next**.



18. Set a complex password for the PFX file and **Next:**



19. Name and Save the file to a ubiquitous location.
20. Once the certificate has been successfully exported upload the certificate to the Mobility **Admin console** > **Settings** > **Certificates** > **Apple/iOS certificates** under its respective area.

Tip: If it is the ios_distribution.pfx/p12; then upload it to the code-signing area. If it is the APNS (Push) aps_production.cer upload to to the Push section.

21. Remember to update the provisioning profile used to build the iOS Work Hub client after regenerating the ios_distribution and apn_production certificates. See [Renewing the Provisioning Profile](#).