## 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:

iOS Apps 🔹 👻	iOS Certificates (I	Distribution)
Certificates	339 Certificates Total	
= All	Name	Type Expir
= Pending	Corporation	MDM CSR Feb 1
Development		
Distribution	Ringlink Name: Corporation	
B Identifiers 0	G Type: MDM CSR	
Devices 0	Expires: Feb 14, 2016	
D. Remissioning Realities (2)	Revoke Download	

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

0			Keucha	n Access	
0			Keychai	n Access	
Click to lock the l	opin keychain.				Q
Keychains	1				
login	iPhone Distribution	Symantec Cor	poration		
for the second	Crystifeate Issued by: Apple Worldw	ide Developer Relat	ions Certification Authority		
System Basts	Expires: Thursday, Nove	mber 26, 2015 10:	18:50 AM Pacific Standard Time		
system koots	This certificate is valid	d			
	Name	A Kind	Expires	Keychain	
	v 🔄 iPhone Distrib.	certificate	Nov 26, 2015 10:18:50	AM login	
	© Corp 2012-2015	private key	**	login	
Category					
All Items					
Passwords					
Secure Notes					
My Certificates					
Keys	1				
Certificates					

- 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 <u>Renewing the Provisioning Profile</u>

## Linux-Method:

 Download the certificate (ios\_distribution.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:



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 pr
ivateKey.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.

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.

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 <u>Renewing the Provisioning Profile</u>.

## **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.

File Action View Favorites Window	нер	X
Console Root	Name	Actions
	There are no items to show in this view.	Console Root 🔺
	The area for done for the view	More Actions
		<u> </u>

- 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 <u>How to create</u> <u>a CSR</u>.
- 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:

GiPhone Distribution: Generation or Apple Worldwide Developer Relation	Code Signing	iPhone Distribution:
--	--------------	----------------------

13. If no key icon is showing be sure that the machine has Apple's root <u>certificate</u> authority added as a trusted Root Certificate and repeat 1-14.

Tip: If the key is still now shown, recreate the <u>CSR</u> 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.

Y	ou can choose to export the private key with the certificate.			
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.				
D	o you want to export the private key with the certificate?			
	• Yes, export the private key			
	O No, do not export the private key			
earn i	nore about <u>exporting private keys</u>			

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**.

Cert	ificates can be exported in a variety of file formats.
Sele	ct the format you want to use:
	C DER encoded binary X.509 (.CER)
	C Base-64 encoded X.509 (.CER)
	🔿 Cryptographic Message Syntax Standard - PKCS #7 Certificates (,P7B)
	$\square$ Include all certificates in the certification path if possible
	Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
(	C Microsoft Serialized Certificate Store (.SST)
arn mo	re about <u>certificate file formats</u>
	< Back Next > Cancel

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

To maintain security, you must prote	act the private key by using a password.	
Type and confirm a password.		
Password:		
•••••		
Type and confirm password (man	idatory):	
•••••		
	A Database Marshare	Cancel

- 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 <u>Renewing the Provisioning Profile</u>.