How do I export and convert a pfx CA root certificate and key from a Microsoft CA server

Document ID: 118339

Contributed by Cisco TAC Engineers.

Aug 22, 2014

This Knowledge Base article references software which is not maintained or supported by Cisco. The information is provided as a courtesy for your convenience. For further assistance, please contact the software vendor.

The following are instructions to export a CA signing root certificate and key from a Microsoft CA server 2003. There are several steps in this process. It is crucial that each step is followed.

Exporting the Certificate and private key from MS CA server

1. Go to ***'Start'*** −> ***'Run'*** −> ***MMC***

2. Click on ***'File'*** −> ***'Add / Remove Snap−in'***

3. Click the ***'Add...'*** button

4. Select ***'Certificates'*** then click ***'Add'***

5. Select ***'Computer Account'*** −> ***'Next'*** −> ***'Local Computer'*** −> ***'Finish'***

6. click ***'Close'*** −> ***'OK'***

The MMC is now loaded with the Certificates snap−in.

7. Expand ***Certificates*** −> and click on ***'Personal'*** −> ***'Certificates'***

8. Right click the appropriate CA cert and choose ***'All Tasks'*** −> ***'Export'***

The Certificate Export Wizard will launch

9. Click ***'Next'*** −> Select ***'Yes, Export the private key'*** −> ***'Next'***

10. Uncheck all of the options here. PKCS 12 should be the only option available. Click ***'Next'***

11. Give the private key a password of your choice

12. Give a filename to save as and click ***'Next'***, then ***'Finish'***

You now have your CA signing certificate and root exported as a PKCS 12 (PFX) file.

Extracting the Public key (certificate)

You will need access to a computer running OpenSSL. Copy your PFX file over to this computer and run the following command:

```
openssl pkcs12 −in <filename.pfx> −clcerts −nokeys −out certificate.cer
```

This creates the public key file named "certificate.cer"

Note: *These instructions have been verified using OpenSSL on Linux. Some syntax may vary on the Win32 version.*

Extracting and decrypting the Private key

The WSA requires that the private key be unencrypted. Use the following OpenSSL commands:

```
openssl pkcs12 −in <filename.pfx> −nocerts −out privatekey−encrypted.key
```

You will be prompted for "***Enter Import Password***". This is the password created in ***step 11*** above.
You will also be prompted for "***Enter PEM pass phrase***". The is the encryption password (used below).

This will create the encrypted private key file named "privatekey−encrypted.key"

To create a decrypted version of this key, use the following command:

```
openssl rsa −in privatekey−encrypted.key −out private.key
```

The public and decrypted private keys can be installed on the WSA from ***'Security Services'*** −> ***'HTTPS Proxy'***

Updated: Aug 22, 2014 Document ID: 118339