Est. USA 1981

www.AKCP.com

Uploading SSL security certificates

Manual

Browser Connections & Log in Issues

Please note that currently the only supported browsers are Google Chrome and Mozilla Firefox. With other unsupported browsers, the Web UI might not load correctly.

Important Note: All of the newer versions (from 2020 on) of the third party web browsers, including Chrome will eventually include new security restrictions for HTTPS that will affect your connections to all of our units and also our AKCPro Server web interface.

You have two options to avoid the browser connection issues when connecting to our units' web interfaces:

The first is to simply use HTTP and not HTTPS.
The second is to replace or upload your own valid, trusted HTTPS certificate and if necessary adding this certificate to your trusted certificate lists within the browser.

HTTPS

The HTTPS port on the units and APS is always enabled. You can change its listening port, if necessary. On the SP+ family, the HTTPS supports TLS v1.1 and v1.2.
The HTTPS cypher suites are not customizable.

To eliminate browser warnings about the self-signed SSL certificate, you'll need to replace it.
Using the "Upload Certificate File" option you can upload an SSL certificate that will be used by the unit's or APS Web UI for HTTPS connection (see below).

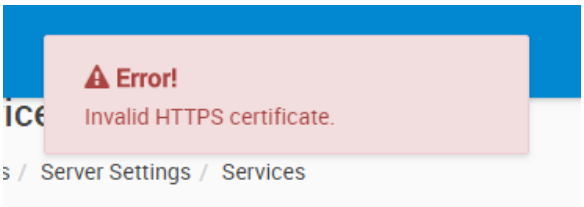
SSL Certificate

SSL certificates are generated for DNS host names and not IP addresses. Therefore, you should set a host name for the SP+ unit in your local DNS server or DHCP server, and then generate the SSL certificate for that hostname. APS on Windows will use the computer's hostname, and L-DCIM can customize the hostname in the settings menu.

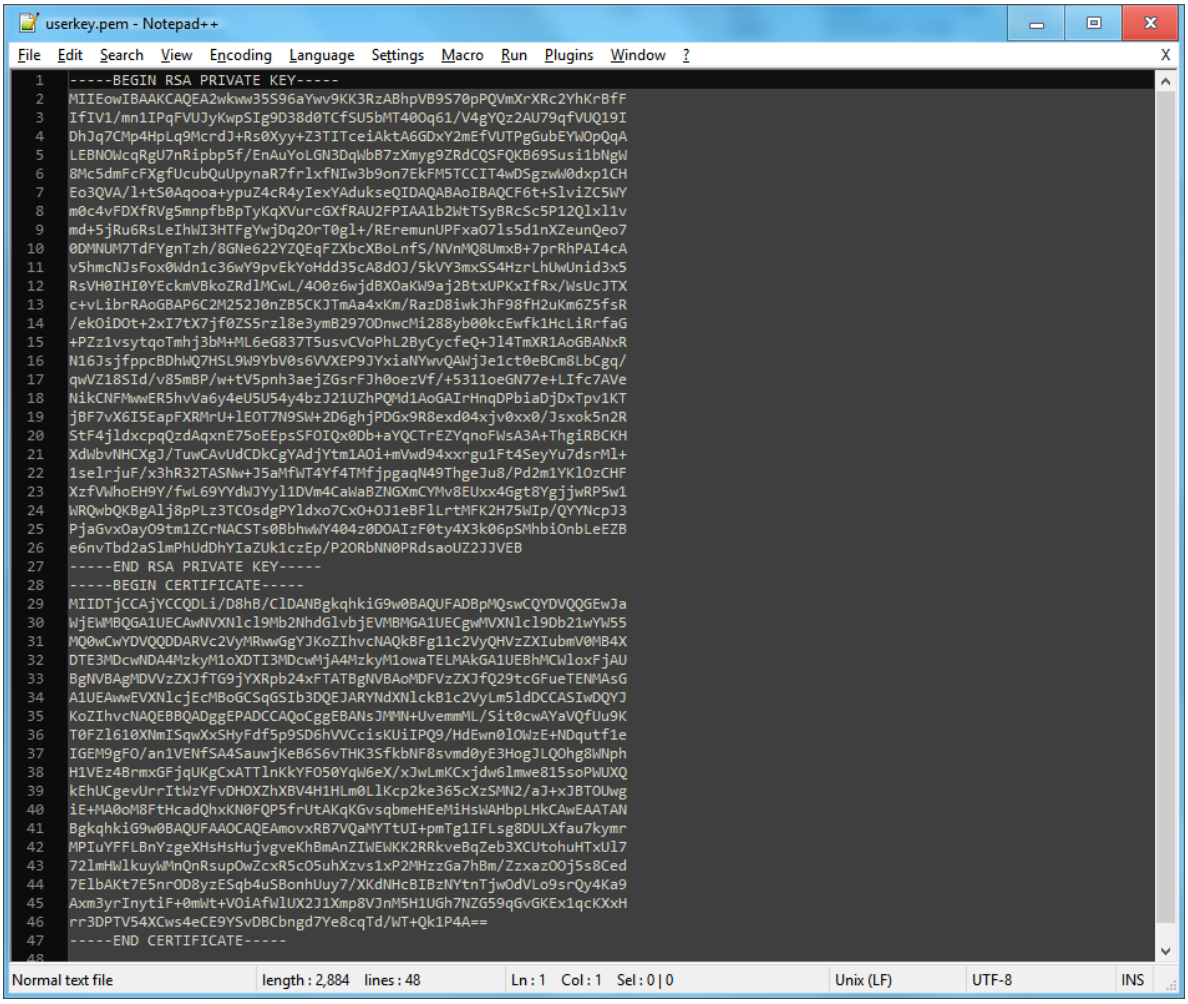
Example full hostname: spplus.mycompany.org

Wildcard SSL certificates should also work (*.mycompany.org), but this hasn't been tested.
If the name doesn't match with the one in the certificate, the browser will still show a security warning.
You can purchase a certificate from a trusted, verified Certificate Authority such as GoDaddy or use your company's own CA if you have one.
Please note that only non-password protected certificate files are supported.

When you select the file for uploading, you'll get a warning if the file is not in the correct .PEM format:



The web server used in SP+ and APS WebUI is using a special Linux format (PEM) for the certificate. **The .PEM file is the private key + certificate combined in one file** (key on the top and cert right below it). You can copy them to one file using Notepad++ if you have 2 separate files, as shown below (it has to be in Unix Line Format and not Windows):

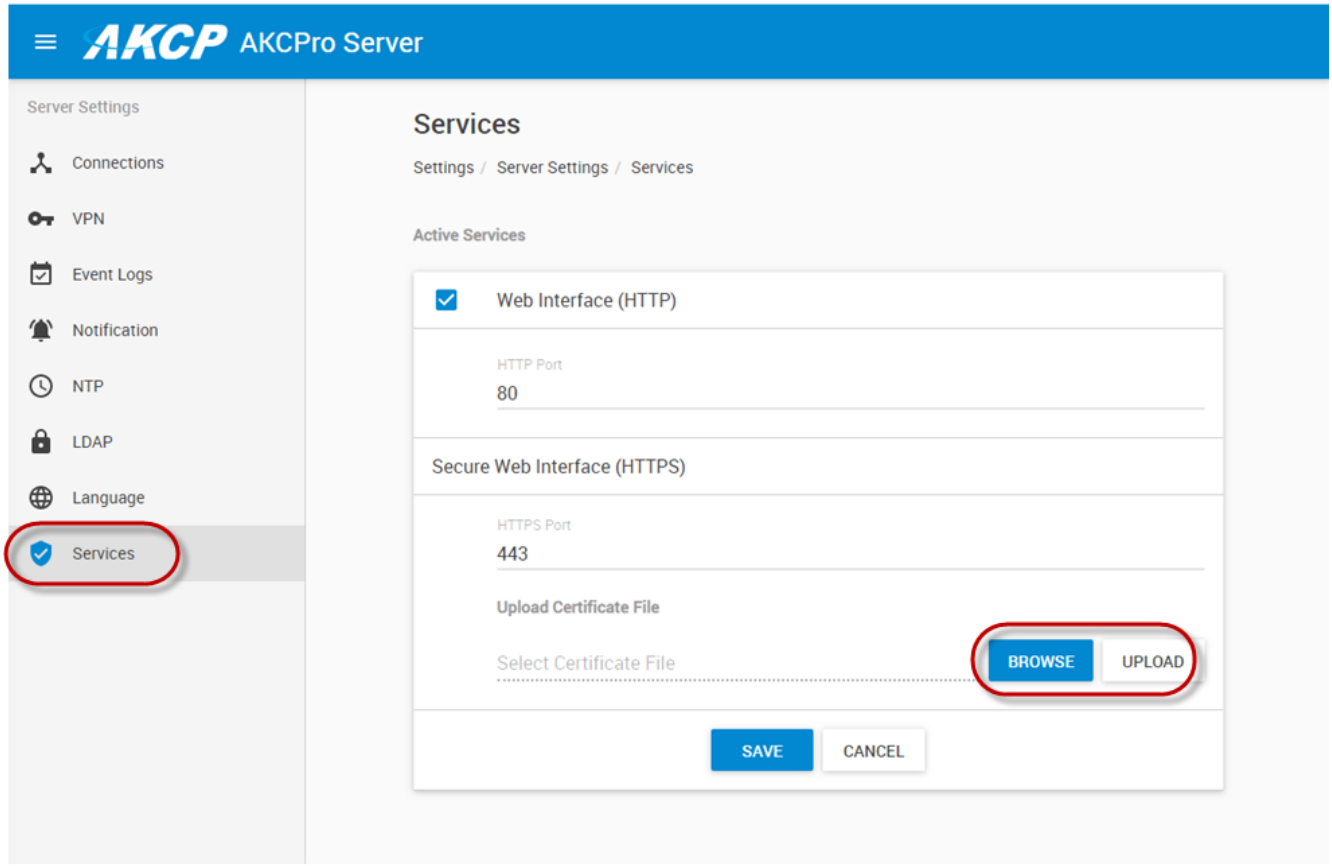


If you don't upload a certificate, the built-in certificate will be used. You'll get a browser warning upon opening the Web UI about an incorrect certificate. This is normal and you should add it as an exception or proceed, depending on your browser.

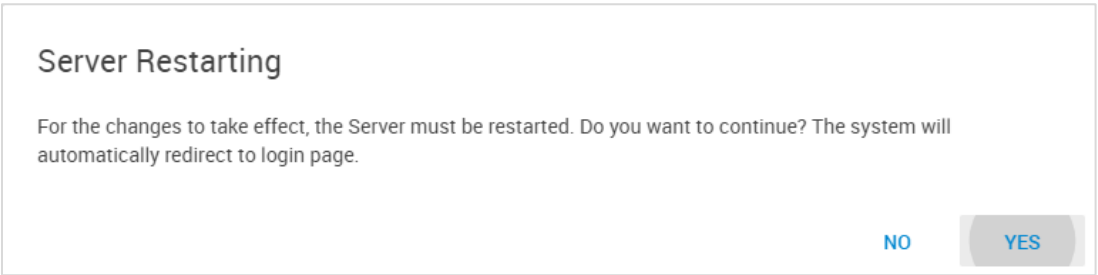
A) Uploading the .PEM for APS WebUI

Note that L-DCIM units are also using APS WebUI.

You can upload the .PEM file in the Server Settings / Services menu as shown in the screen shot below:



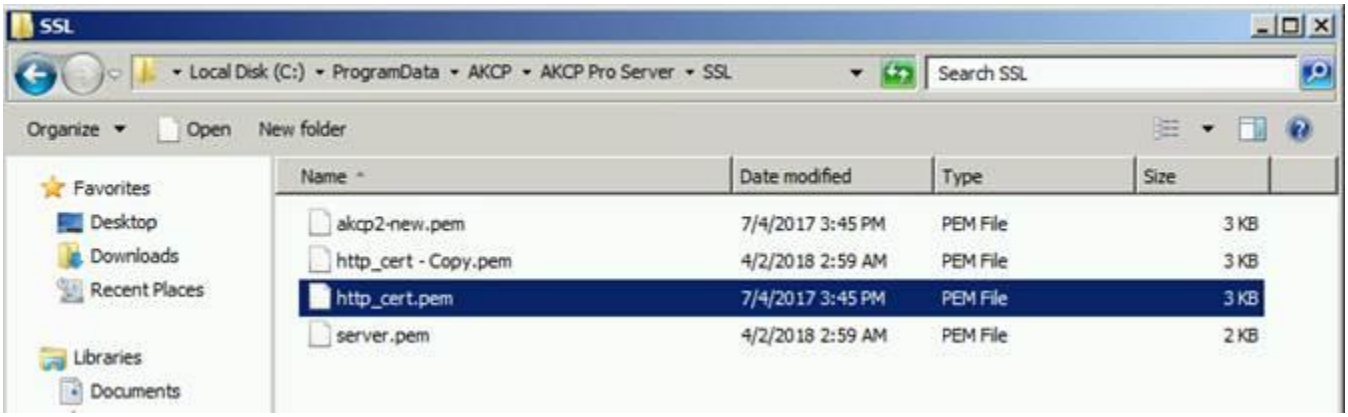
Browse your .PEM file and upload it.
Press “Save” then you’ll be asked to restart the APS service in order to proceed with the new certificate:



Manually replacing the HTTPS certificate for APS

If you're still having problems with uploading the .PEM here are the steps to manually replace the HTTPS certificate of APS HTML UI on Windows:

1. Create the correct PEM file (ask your local system admin for help with this or see above).
2. Stop all APS services using the Server Manager: Service menu / Stop service.
3. Navigate to C:\ProgramData\AKCP\AKCPro Server\SSL.
4. Make a backup of the existing http_cert.pem file.
5. Copy your custom .pem file there (in the screenshot it's akcp2-new.pem).
6. Delete the old http_cert.pem file (don't touch server.pem!).
7. Rename your custom .pem to http_cert.pem.
8. Start all APS services again using the Server Manager.
9. Open the APS HTML UI and verify your SSL certificate has been replaced.

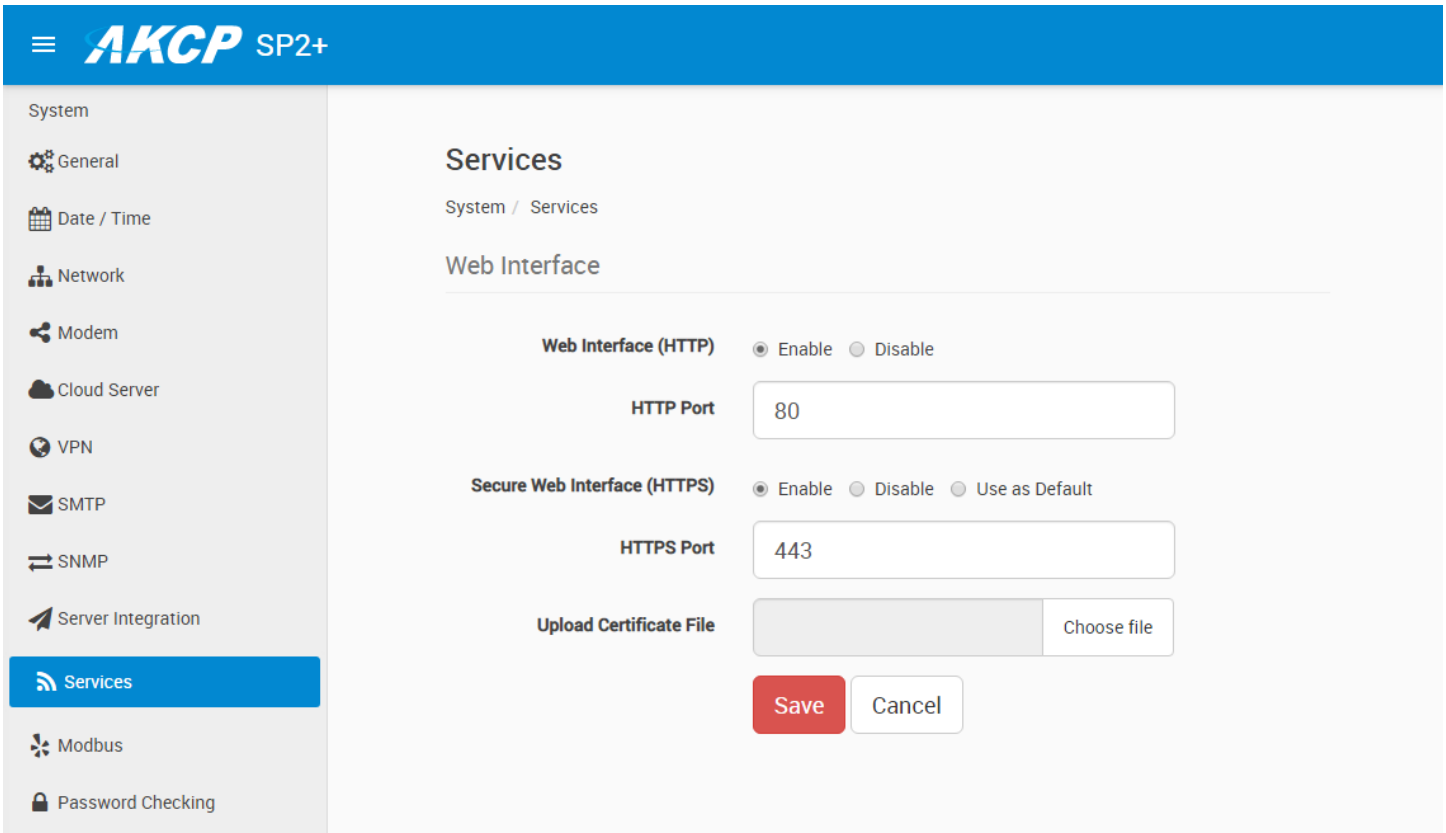


Regarding these HTTPS issues noted above, please be aware that this is not a problem with our AKCPro Server software, L-DCIM or any AKCP base unit. This is a generic security feature in these third party web browsers that we have no control over.

Moreover, it is important to note that if you decide to use this manual replace method, this is the customer's responsibility to manage their own HTTPS certificates in order to access our products web user interface.

B) Uploading the .PEM for SP+ WebUI

Open the Settings / Services menu as shown in the screenshot below:



Click on “Choose file” button next to the “Upload Certificate File” field.

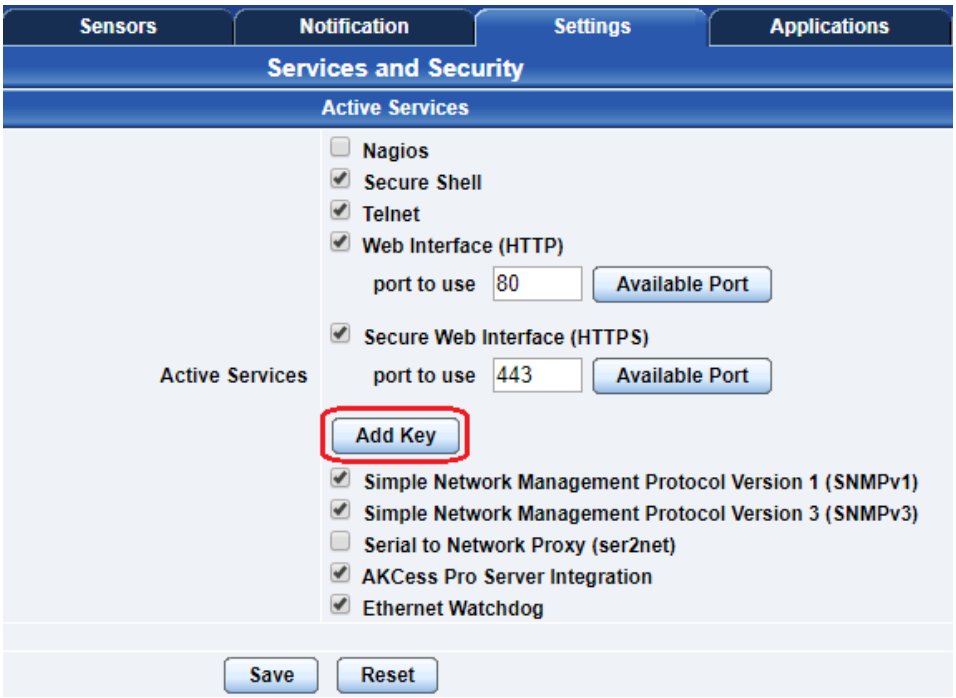
If the file format is correct (see instructions below) then your certificate can be used immediately. You can open WebUI with HTTPS and verify your SSL certificate is used.

If there’s a problem with the certificate and WebUI doesn’t open with HTTPS, open it again using HTTP and replace the .PEM file again.

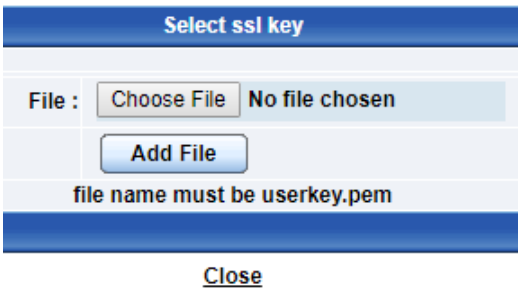
Important note: on the older F4 platform SP+ units, the .PEM’s total file size must be less than 4KB, regardless of the used private key size. If you exceed this file size, the unit won’t be able to use the certificate and the WebUI won’t load over HTTPS.
Also note that using a very large private key can cause WebUI slowdown.
The newer F7 platform units doesn’t have this limitation.

B) Uploading the .PEM for SEC5 WebUI

Open the Settings / Services and Security menu as shown in the screenshot below:



Click the “Add Key” button to upload the .PEM file. It will show a popup window as shown below:



When you select the file for uploading in the popup window, you’ll get a warning if the file is not in the correct .PEM format (see below).

<u>Very Important Note:</u> The file name MUST be userkey.pem, rename the file if necessary.

Also note that using a very large private key can cause WebUI slowdown.

See below for troubleshooting instructions, in case the unit’s WebUI no longer loads.

How to troubleshoot a failed Web UI on the SEC5

Note: these steps are only for troubleshooting a bad SSL certificate file, which prevents the unit's Web UI from appearing because the Apache service cannot start.

The SSL certificate which you can upload from the Web UI will be stored as this file:

```
/flash1/user/init.d/userkey.pem
```

If this file doesn't exist, then the unit's built-in certificate will be used as a fallback. So if the uploaded certificate is a broken file, you just need to remove it and restart Apache to get a working Web UI.

1. **Log in to the unit's SSH console** as the `root` user (the password is the SNMP write community). You have two options:

a) Remove the corrupt .pem file, then the default certificate will be used as a fallback:

```
rm /flash1/user/init.d/userkey.pem
```

b) Overwrite the corrupt .pem file with a known good one:

The following `cat` command will open the file and save it when you press CTRL-D. Insert the new contents and then save it with CTRL-D:

```
cat >/flash1/user/init.d/userkey.pem
```
->now copy the certificate contents and press Enter, then CTRL-D

2. After removing or overwriting the certificate, **restart Apache** and try to log in again to the Web UI:

```
/etc/rc.d/init.d/apache restart
```

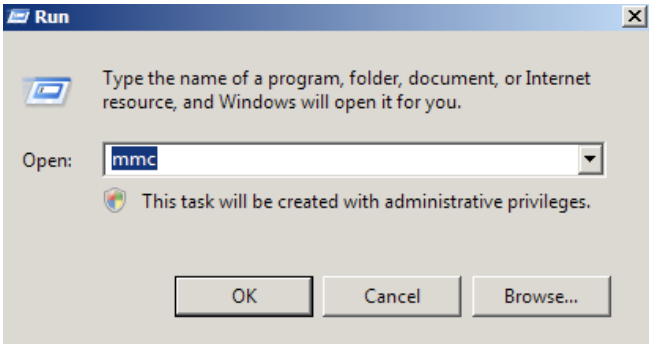
How to generate a proper .PEM file from a Windows CA

Please note that *only* non-password protected certificate files are supported.

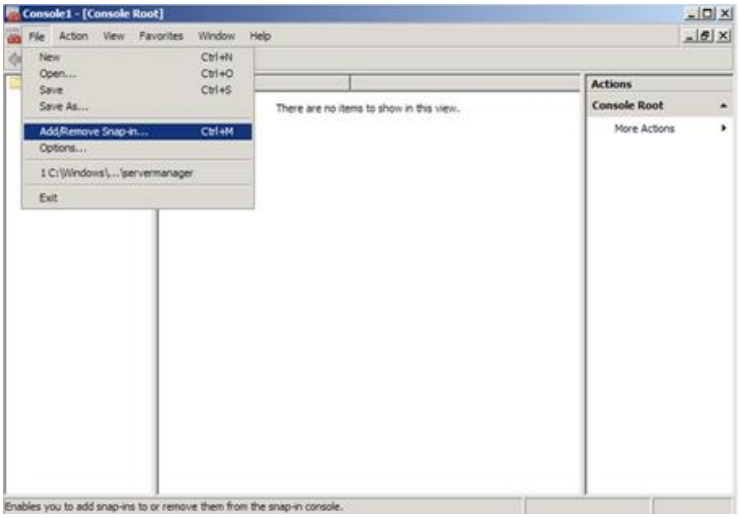
First make the .PFX file export using the steps below:
(taken from https://www.sslsupportdesk.com/export-ssl-certificate-private-key-pfx-using-mmc-windows/)

To backup, export an SSL certificate with its private key and intermediates performing the following steps:
Step 1: Create an MMC Snap-in for Managing Certificates on the first Windows system where the SSL certificate is installed.

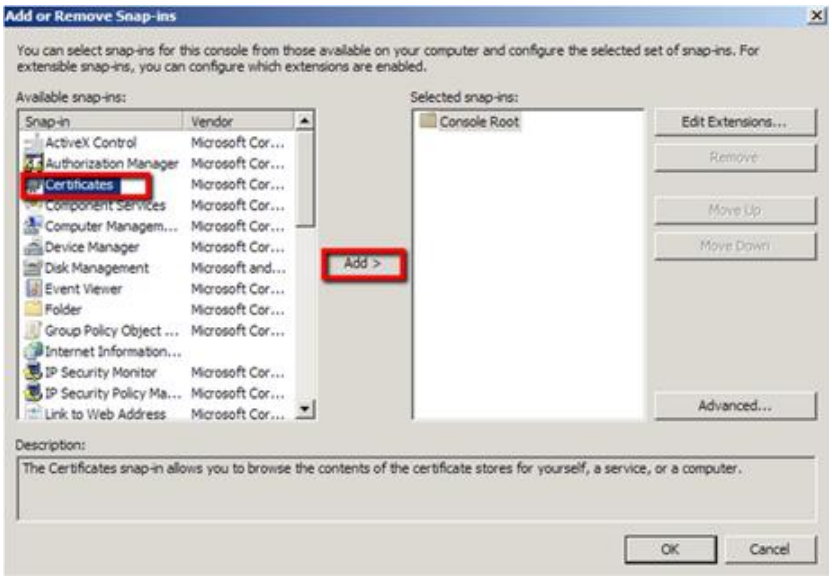
1. **Start** > **run** > **MMC.**



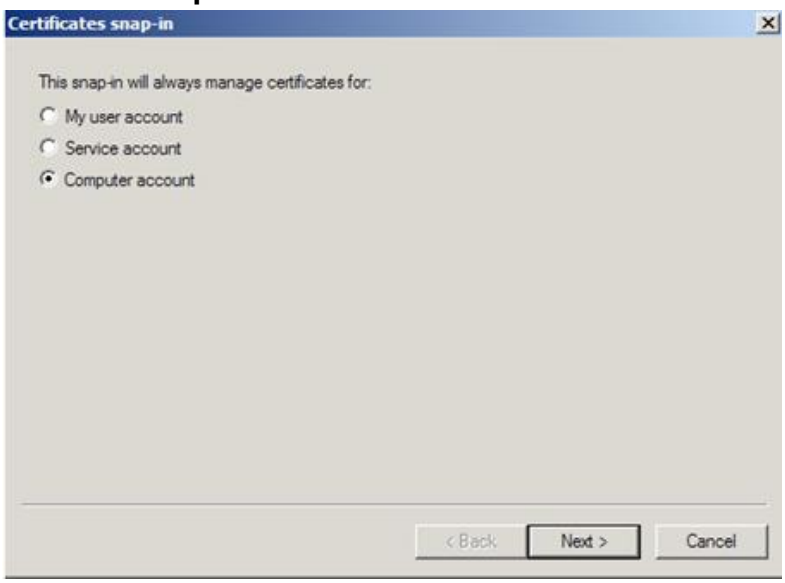
2. Go into the Console Tab > **File** > **Add/Remove Snap-in.**



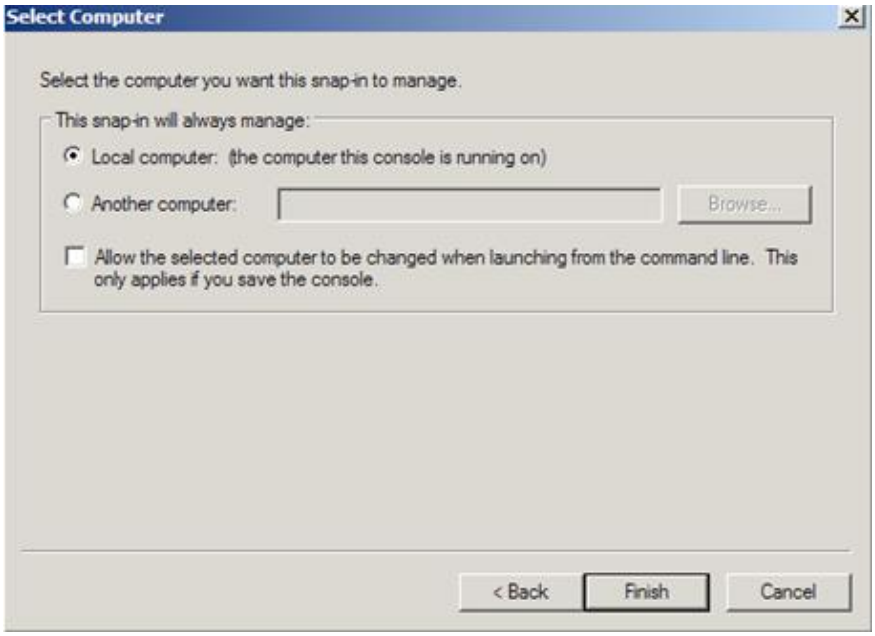
3. Click on **Add** > Click on **Certificates** and click on **Add.**



4. Choose **Computer Account > Next.**



5. Choose **Local Computer > Finish.**



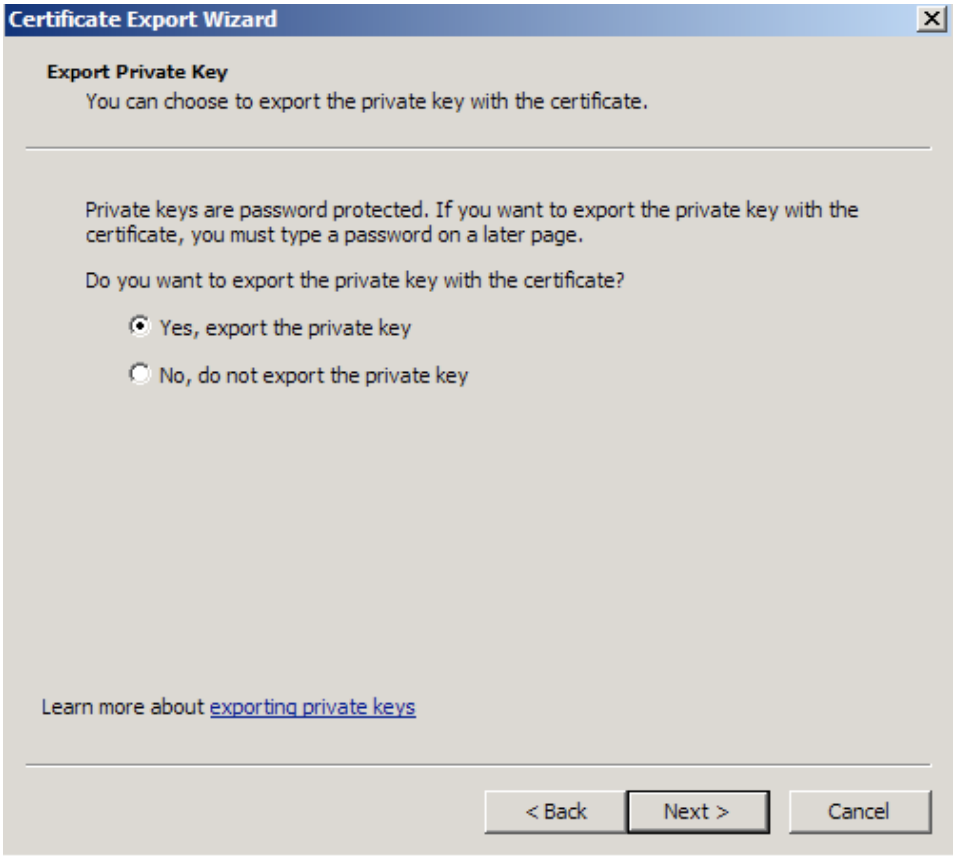
6. Close the **Add Standalone Snap-in** window.
7. Click on **OK** at the **Add/Remove Snap-in** window.

Step 2: Export/Backup certificate to .pfx file:

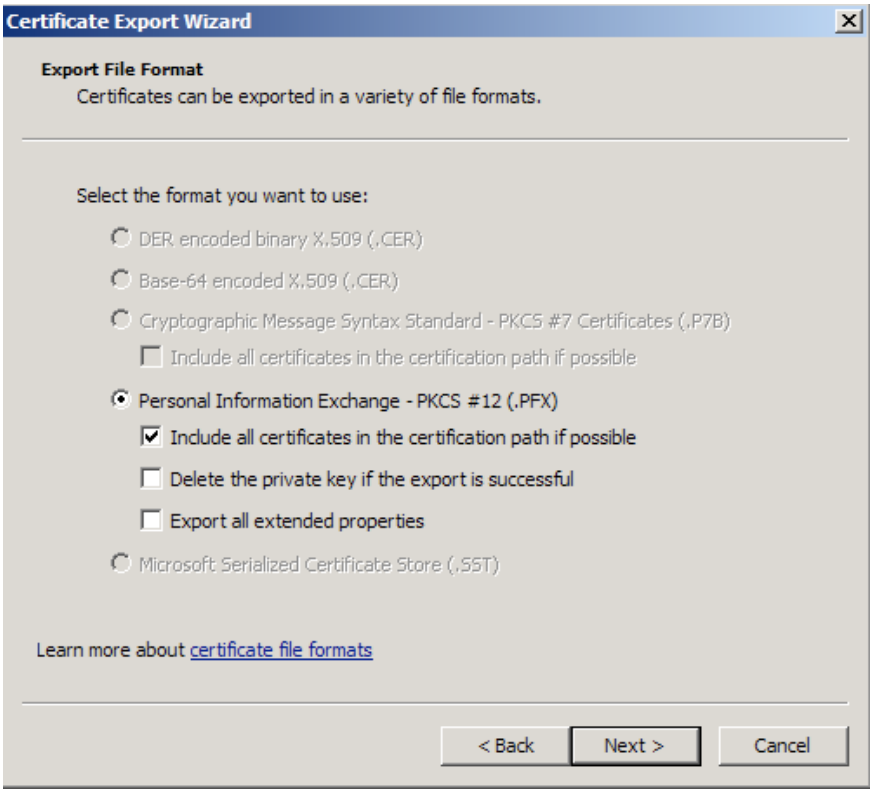
1. In MMC Double click on **Certificates (Local Computer)** in the center window.
2. Double click on the **Personal folder**, and then on **Certificates**.
3. Right Click on the Certificate you would like to backup and choose > **ALL TASKS** > **Export**

4. Follow the Certificate Export Wizard to back up your certificate to a .pfx file.

5. Choose to '**Yes, export the private key**'

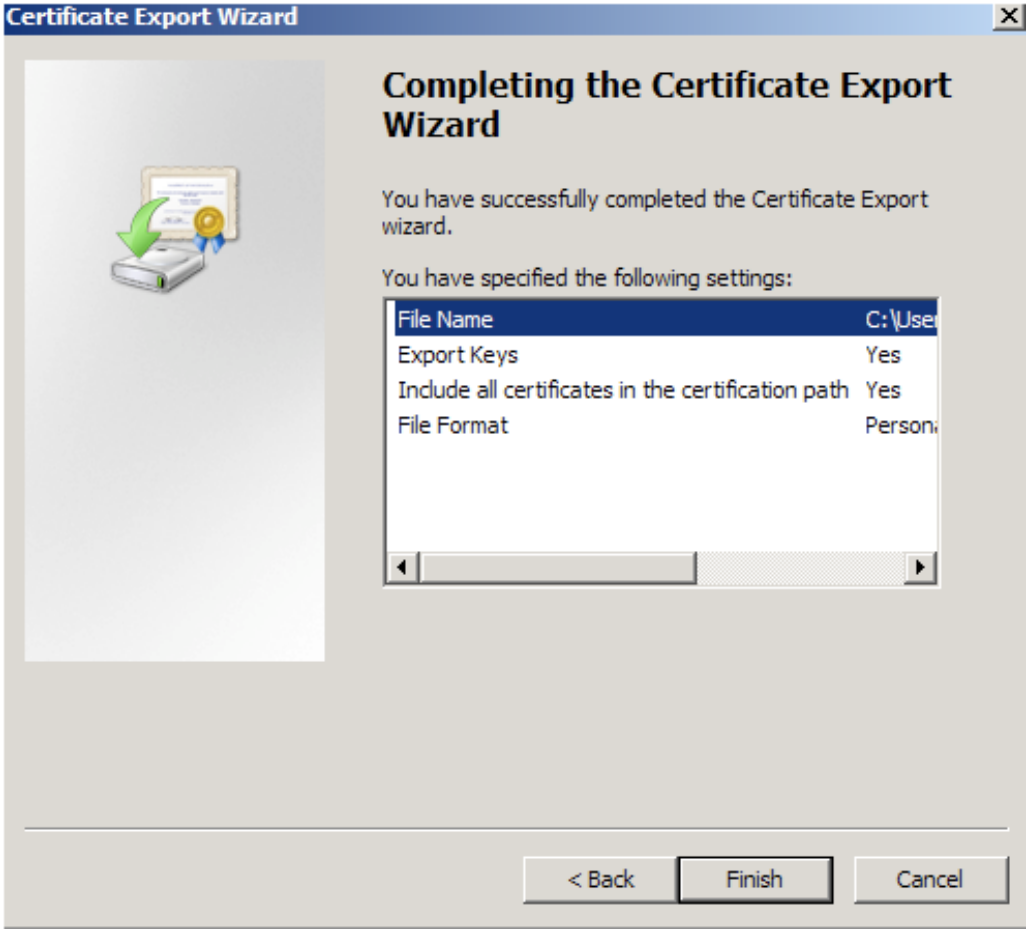


6. Choose to "**Include all certificates in certificate path if possible**." (do NOT select the delete Private Key option)



7. Enter a password you will remember.
8. Choose to save file on a set location.

9. Click **Finish.**



10. You will receive a message > “The export was successful.” > Click **OK.**The .pfx file backup is now saved in the location you selected and is ready to be moved or stored for your safe keeping.

After this you can peform the .PEM conversion in 2 ways, using OpenSSL (recommended) or the DigiCert utility.

1. Use OpenSSL with proper parameters:
http://www.thawte.nl/en/support/manuals/microsoft/all+windows+servers/export+private+key+or+certificate/

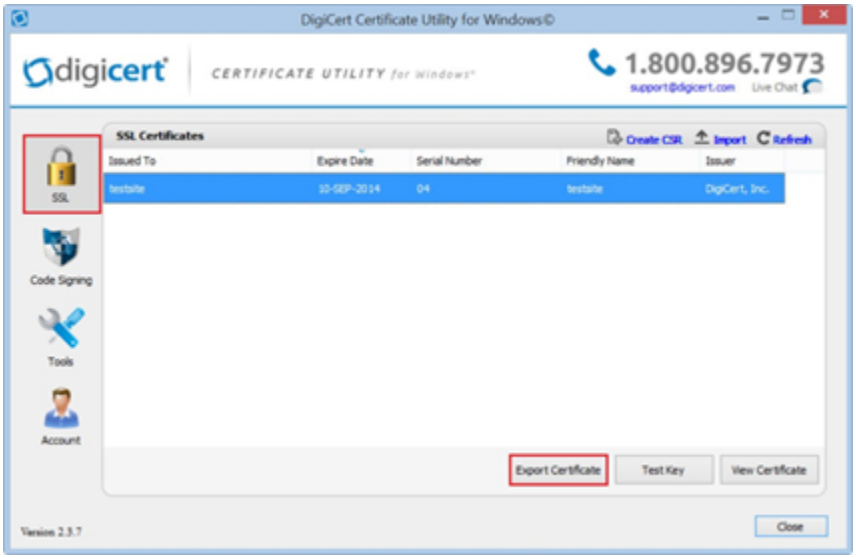
Export the private key file from the pfx file:
openssl pkcs12 -in filename.pfx -nocerts -out key.pem

Export the certificate file from the pfx file:
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.pem

Remove the passphrase from the private key:
openssl rsa -in key.pem -out server.key

When the exports are done, combine the server.key (must be without password!) and cert.pem with Notepad++ and save as USERKEY.PEM

2. Use the DigiCert utility and export it as Apache compatible key:
https://www.digicert.com/util/copy-ssl-from-windows-iis-to-apache-using-digicert-certificate-utility.htm



On this webpage it shows the SSL already in the DigiCert tool, but first you need to import the .PFX that you just exported from the Windows Cert Manager. After that just proceed with the export steps as written on the page.
When the export is done, just combine the Server Cert and Private Key with Notepad++ and save as USERKEY.PEM

The .PEM file is the private key + certificate combined. You can copy them to one file using Notepad++ if you have 2 separate files (it has to be in Unix Line Format and not Windows).

Please contact support@akcp.com if you have any further technical questions or problems.

Thanks for Choosing AKCP!