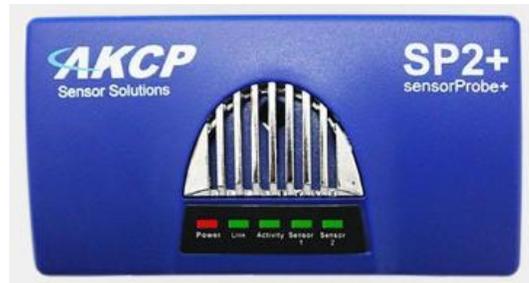




[www.AKCP.com](http://www.AKCP.com)

# SP+ Security Features Manual



Copyright © 2017, AKCP

## Table of Contents

Introduction .....	3
Services.....	4
SSL Certificate.....	5
SNMPv3.....	8
Password Checking and Security .....	9
Password Security options .....	10
Lockdown .....	11
Password Expiration.....	12
Access Control Users and Groups .....	13
Server Integration .....	14
VPN to APS .....	15
Troubleshooting - How to generate a proper .PEM file from a Windows CA.....	16

## Introduction

The security features on the sensorProbe+ units allows users to lock down and secure the unit from exterior threats. Each option will be covered in detail within this manual.

- Services - enable/disable HTTP and HTTPS, and change their ports
- SSL Certificate - ensure the identity of the unit for HTTPS and SNMPv3 communication
- SNMPv3 - secure SNMP traffic
- Password Checking and Security - manage the access to the unit's Web UI, set password expiration and lockdown features
- Server Integration - enable/disable controlling the unit via AKCess Pro Server, and the access control user sync
- VPN to APS - connect the SP+ with an APS VPN server securely

## Services

The screenshot shows the 'Services' configuration page in the AKCP SP2+ web interface. The page is divided into a left sidebar and a main content area. The sidebar contains a menu with 'System' and 'Services' sections. The 'Services' section is currently selected and highlighted in blue. The main content area is titled 'Services' and 'Web Interface'. It contains two main sections: 'Web Interface (HTTP)' and 'Secure Web Interface (HTTPS)'. The 'Web Interface (HTTP)' section has radio buttons for 'Enable' (selected) and 'Disable', and a text input field for 'HTTP Port' with the value '80'. The 'Secure Web Interface (HTTPS)' section has radio buttons for 'Enable' (selected), 'Disable', and 'Use as Default' (unselected), and a text input field for 'HTTPS Port' with the value '443'. Below these sections is an 'Upload Certificate File' section with a 'Choose file' button and 'Save' and 'Cancel' buttons.

You can close or change the ports used to access the unit’s web interface, disable HTTP and enable HTTPS only, which can also be set to be used as default.

On the SP+ family, the HTTPS supports TLS v1.1 and v1.2.  
The HTTPS cypher suites are not customizable.

Using the “Upload Certificate File” option you can upload an SSL certificate that will be used by the unit’s Web UI for HTTPS connection.

## SSL Certificate

SSL certificates are generated for DNS host names and not IP addresses. 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 host name.

*Example:* spplus.mycompany.org

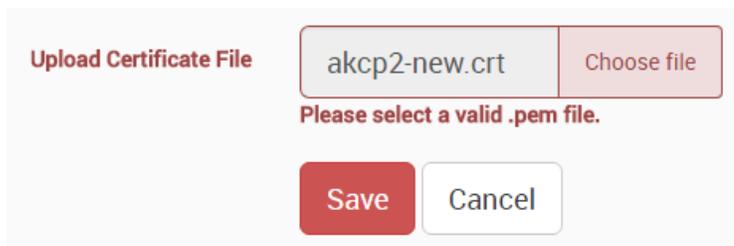
The unit's DNS host name is "spplus". Wildcard SSL certificates should also work, but this hasn't been tested.

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 .PEM format:



Upload Certificate File

akcp2-new.crt Choose file

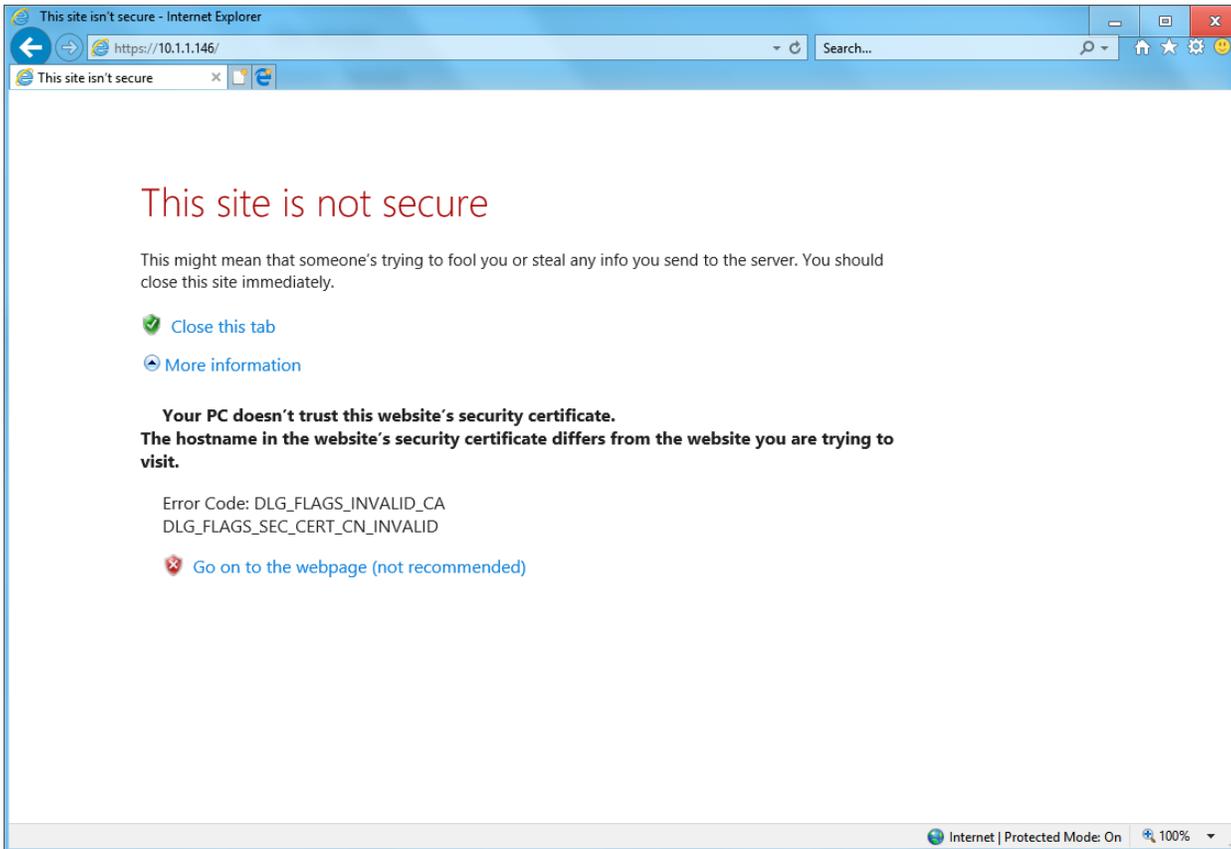
Please select a valid .pem file.

Save Cancel

The .PEM file is the private key + certificate combined. 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):

```
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEowIBAAKCAQE2wkww35S96AYwv9KK3RzABhpVB9S70pPQVmxRrXRc2YhKrBfF
3 IfIV1/mn1IPqFVUJyKwpSIg9D38d0TCfSU5bMT400q61/V4gYQz2AU79qfVUQ19I
4 DhJq7Cmp4HpLq9McrdJ+Rs0Xyy+Z3TITceiAktA6GDxY2mEfVUTPgGubEYw0pQqA
5 LEBNOwCqRgU7nrRipbp5f/EnAuYoLGN3DqwbB7zXmyg9ZRDQSFQKB69Sus11bNGH
6 8Mc5dmFcFXgFUcubQuUpynaR7fr1xfNIw3b9on7EkFM5TCCIT4wDSgzww0dpx1CH
7 Eo3QVA/1+ts0Aqooa+ypuZ4cR4yTexYAdukseQIDAQABaoIBAQCf6t+S1viZC5WY
8 m0c4VFDXfRVg5mnpfbBpTyKqXVurcGXfRAU2FPIAA1b2WtTSyBRcSc5P12Q1x11v
9 md+5jRu6RsLeIhwI3HTFgYwJdQ20rT0gl+/REremunUPFxa071s5d1nXZeuQeo7
10 0MMNUM7TdFYgnTzh/8GNe622Y2QEfZXbcXBolnFS/NVnMQ8Umx8+7prRhPAI4cA
11 v5hmcNjSFox0Wdn1c36wY9pvEkYoHdd35cA8d0J/5kVY3mxSS4HzrLhUwUnid3x5
12 RsVH0IH0YEckmVBkoZrdLMcWl/400z6wjdBX0akW9aJ2BtxUPKzrIFRc/WsUcJTX
13 c+vL1brRAoGBAP6C2M252J0nZB5CKJTMaa4xKm/RazD81wkJhF98fH2uK6Z5fsr
14 /ek0IDot+2xI7tX7jf0ZS5rz18e3ymb2970DnwcMi288yb00kcEwfk1HcL1RrfaG
15 +PZ2lvSytqoTmhj3bMML6e683725usvCvPhL2ByCycfQ+J14TmXR1AoGBANxR
16 N16JsjfppcBDhwQ7HSL9W9YbV0s6VXEP9JYx1aNYwwQAWjJe1ct0eBcm8LbCgq/
17 qwVZ185Id/v85mBP/ww+tv55pnh3aejZGsrFJh0oezVf/+5311oeGN77e+LIcf7AVE
18 NikCNFhwER5hV6y4eU5U54y4bzJ21ZUHQMd1AoGAIrHnqDPbiajDxTpv1KT
19 jBF7wX6I5EapFXRMrU+1EOT7N9SW+2D6ghjPDGx9R8exd04xjv0xx0/J5xok5n2R
20 StF4j1dxcpqQzdAqxnE75oEepsFOIQx0Db+aYQCTrEZYqnoFwsA3A+ThgiRBCKH
21 XdnbNWCXGj/TuwCAvUdCDkCgYAdjYtm1A0i+mVwd94xxrgu1Ft4SeyYu7dsrMl+
22 1selrjuF/x3hr32TASlW+J5aMfWT4Yf4TMfjppgaqN49ThgeJu8/Pd2m1YK10zCHF
23 XzfVwHoEH9Y/fwL69YYdJYy1DVM4CaWaBZNGXmCYMv8Euxx4Ggt8YgjjwRP5W1
24 WRQwbQKBgAlj8pPlz3TCosdgpYlDxo7Cx0+0J1eBF1LrtMFk2H75WIp/QYYNcpJ3
25 PjaGvx0ay09tm1ZCrNACSts0BbhWY404z0DOAIzF0ty4X3k06pSMhb10nBLEZB
26 e6nvTbd2aSlmPhUdhYiaZUk1czEp/P20RBNW0PRdsaoUz2J2JVEB
27 -----END RSA PRIVATE KEY-----
28 -----BEGIN CERTIFICATE-----
29 MIIDTjCCAjYCCQDLi/D8hB/C1DANBgkqhkiG9w0BAQUFAQBpMQswCQYDVQ0GEwJa
30 wjEwMBQGA1UECgAwVXN1c19Mb2NhZG1vb3VlMBMGA1UECgwMVXN1c19Db211wYw5
31 MQ0wCwYDVQ0DDARVc2VYMRwwGgYJKoZIhvcNAQkBFg11c2VyQHVzZXIubmV0MB4X
32 DTE3MDcwNDAA4MzkyM1oXDTI3MDcwMjA4MzkyM1owaTElMAkGA1UEBhMCVloXfjAU
33 BgNVBAGMDVZzZXJfTG9jYXRpb24xFTATBgNVBAoMDFVzZXJfQ29tcGFueTElMAkG
34 A1UEAwwEVXN1c1cjcEcnMB0GCSqGSIb3DQEJARYNdXN1c1c1c2VyLm51dDCCAS1wDQYJ
35 KoZiHvcNAQEBBQADgEPADCCAQoCggEBANsJMMN+UvemML/Sit0cwAYaVQfUu9K
36 T0FZ1610XNmISqwxXShyFdf5p9S06hVVCcisKUIPQ9/HdEwn010wzE+NDqutf1e
37 IGEM9gFO/an1VENfSA4SauwjKeB6S6vTHK3SfkbNF8svmd0yE3HogJLQ0hg8Wnph
38 H1VEz4BnmxGFjqUKGcXATT1nKkYF050YqW6eX/xJwLmKcxdw61mwe815soPlUXQ
39 kEHUcgevUrrItwzYFvDHOXZHXBV4H1Hm0L1Kcp2ke365cXzSMN2/aJ+xJBT0Uwg
40 iE+MA0oM8FtHcadQhXK0FQP5frUtAKqKGVsqbmeHEeM1HsWAHbpLHKCAwEAATAN
41 BgkqhkiG9w0BAQUFAOAQAEAmovxRB7VQaMYTtUI+pmTg1IFLsg8DULXFau7kyMr
42 MPIuYFFLBNyZgeXHSsHuJvgveKhBmAnZiWIEWKK2RRkveBqZeb3XCutohuHTxU17
43 72lmHw1kuyMnQnRsupOwZcxR5c05uhXzvs1xP2HHzG6a7hBm/Zzxaz00j5s8Ced
44 7E1bAKt7E5nrOD8yzESqb4uSBohUuy7/XKdNHcBIBzNYtnTjw0dVLo9srQy4Ka9
45 Axm3yrInytfIF+0mwT+VOiAfwLUX2J1Xmp8VJnM5H1UGh7NZG59qGvGKEx1qcKXxH
46 rr3DPV54XCws4eCE9YsVDBcbngd7Ye8cqTd/WT+Qk1P4A==
47 -----END CERTIFICATE-----
48
```

If you don't upload a certificate but enable HTTPS, a 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:



## SNMPv3

System

AKCP SP2+

System

- General
- Date/Time
- Network
- Modem
- VPN
- SMTP
- SNMP**
- Modbus
- Server Integration
- Services
- Password Checking
- Maintenance
- Heartbeat Messages
- License Management
- About

Get SNMP OID

### SNMPv3

SNMPv3  Enable  Disable

SNMPv3 Mode: Authentication & Privacy

SNMPv3 engineID: AKCP  
engineID parse: 80001F8804414B4350

SNMPv3 Username: admin

Access Privilege: Read Only

Authentication Protocol: SHA

SNMPv3 Pass Phrase: SNMPv3 Pass Phrase

Confirm SNMPv3 Pass Phrase: Confirm SNMPv3 Pass Phra

Privacy Protocol: AES

Privacy Protocol Pass Phrase: Privacy Protocol Pass Phras

Confirm Privacy Protocol Pass Phrase: Confirm Privacy Protocol Pa

Save Cancel

SNMPv3 provides important security features:

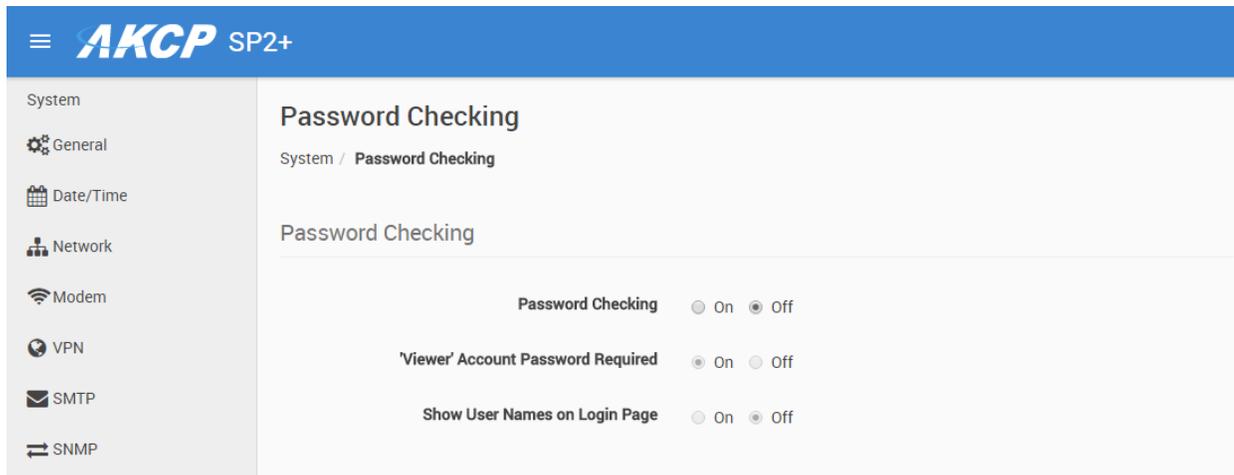
- \* Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.
- \* Integrity - Message integrity to ensure that a packet has not been tampered with in transit.
- \* Authentication - to verify that the message is from a valid source.

The SSL certificate that you can upload to the unit will be also used for signing the SNMPv3 traffic.

Please note that this feature requires a separate license and has to be activated before using.

More details can be found for setting up and using SNMPv3 in the SP+ Introduction Manual.

## Password Checking and Security



You can turn on the password checking for the Web UI to ensure only authenticated users have access to the unit. You can also specify to show all user names on the login page, or keep them confidential.

After you enable the password checking, you'll need to re-login.

If you don't remember the Admin password, you can hold the unit's reset button for 7-12 seconds to be able to log in to the Web UI without a password.

*Note 1:* The passwords can only be set from the unit's Web UI; this option is not available from APS.

*Note 2:* The default password is "public" for all access levels.

### *Web UI user access levels and permissions*

**Admin** - full access to all settings, system and notification configurations

**Viewer** - read-only guest access for every page

**User** - full access to most settings except for those which are the system-related such as network

In detail, the User access level provides these permissions in addition to the Viewer level:

- Allow modifying board/sensor settings
- Allow add/modify/remove notifications
- Allow add/modify/remove heartbeats
- Allow open/close the door on the Handle Lock
- Allow send configuration to Support
- Allow change Graph settings
- Allow change the Web UI language



## Password Security options

System

AKCP SP2+

System

- General
- Date/Time
- Network
- Modem
- VPN
- SMTP
- SNMP
- Server Integration
- Services
- Modbus
- Password Checking**
- Maintenance
- Heartbeat Messages
- License Management

### Password Security

Admin Password	<input type="text" value="Admin Password"/>
Confirm Admin Password	<input type="text" value="Confirm Admin Password"/>
Password Expiration	<input type="text" value="90 Days"/>
Lock-down period after invalid login attempts	<input type="text" value="5 Minutes"/>
User Password	<input type="text" value="User Password"/>
Confirm User Password	<input type="text" value="Confirm User Password"/>
Password Expiration	<input type="text" value="90 Days"/>
Lock-down period after invalid login attempts	<input type="text" value="5 Minutes"/>

[Unlock User Account](#)

All user account types (Admin, User, Viewer) have adjustable password expiration and lockdown periods.

The password can be up to 15 characters (a-z, A-Z, 0-9 and special characters).

The IP address of the remote user's computer will be logged in the syslog so you can trace back each login session to its origin.

## Lockdown

User Password	<input type="text" value="User Password"/>
Confirm User Password	<input type="text" value="Confirm User Password"/>
Password Expiration	<input type="text" value="90 Days"/>
Lock-down period after invalid login attempts	<input type="text" value="5 Minutes"/>
Viewer Password	<input type="text" value="5 Minutes"/>
Confirm Viewer Password	<input type="text" value="5 Minutes"/>
Password Expiration	<input type="text" value="90 Days"/>

**Error!**  
The username or password is incorrect.

**Error!**  
The username or password is incorrect.

**Error!**  
Your account has been locked because you have reached the maximum number of invalid login attempts. Please try again later.

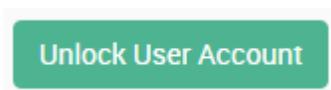
**Error!**  
Your account has been locked because you have reached the maximum number of invalid login attempts. Please try again later.

Username

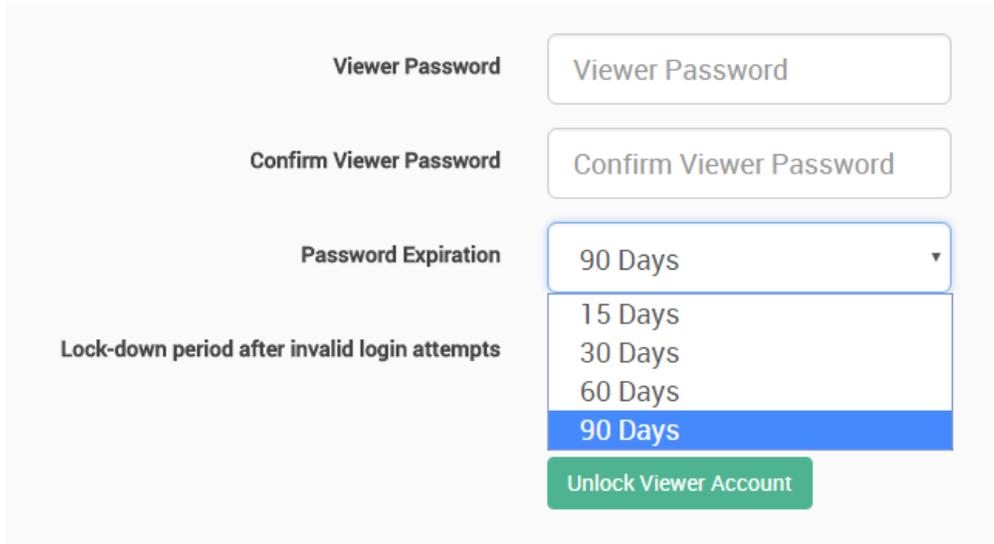
The accounts can be set to lock down the account after 3 invalid login attempts, to prevent brute-force hacking attempts. You can specify how long the account will automatically unlock itself.

Note that for the Admin user, you can't select "indefinitely" as this would prevent you from logging in to the Web UI if it has locked itself.

If an account has been locked, you can unlock it immediately by logging in with the Admin user, and by using the green unlock button:



## Password Expiration



The screenshot shows a configuration interface for password expiration. It includes the following elements:

- Viewer Password:** A text input field containing the placeholder text "Viewer Password".
- Confirm Viewer Password:** A text input field containing the placeholder text "Confirm Viewer Password".
- Password Expiration:** A dropdown menu currently set to "90 Days". The dropdown is open, showing the following options: "15 Days", "30 Days", "60 Days", and "90 Days". The "90 Days" option is highlighted in blue.
- Lock-down period after invalid login attempts:** This label is positioned to the left of the dropdown menu.
- Unlock Viewer Account:** A green button located below the dropdown menu.

You can specify password expiration between every 15 and 90 days for all account types. Note that currently there's no option to set "no expiration".

## Confirmation

Your password has expired. Would you like to change it now?

YES NO

You'll get a notification upon login when the password has expired, and will be asked to change it. It's advised to change it when asked, but you can still proceed without changing.

## Access Control Users and Groups

The Access Control Users and Groups are managed from the AKCess Pro Server and are used for accessing doors with the Swing Handle Lock. You can only view the existing users and groups from the unit's Web UI and modify only a few parameters on them.

↑ First Name	↑ Last Name	Group	Card ID	
Admin	Admin	(None)	-	
Jo	Jo	(None)	-	
mot	mot	(None)	-	

This feature has its own manual, refer to the SP+ Swing Handle Lock Manual for more information.

## Server Integration

System / Server Integration

Server Integration  Enable  Disable

Server Address 0.0.0.0

Server Integration Port 5000

Send Keep Alive Every 1 Minutes

Server Access Control Sync  Enable  Disable

Save Cancel

You can enable/disable controlling the unit via AKCess Pro Server.

If the unit has been added to the APS console, the server's IP address will be also displayed here. You can change the APS port when the server's port changes, and the keep-alive period (heartbeat sync to APS).

Send Keep Alive Every

1 Minutes

30 Seconds

1 Minutes

5 Minutes

10 Minutes

15 Minutes

30 Minutes

1 Hour

2 Hours

5 Hours

12 Hours

24 Hours

You may turn off the access control user sync separately, so that the user database will not be updated together with APS.

## VPN to APS

This feature is used by connecting the SP+ with the APS VPN server securely through a private link. It requires a separate license. After the license has been activated, first you have set up the APS VPN server then you'll need to fill out the same options here to be able to use the VPN connection.

*Note 1:* You can also configure these settings from the APS console for the unit.

*Note 2:* If you use the VPN option, the maximum number of sensors that can be used by the unit will be reduced to 50.

## Troubleshooting - How to generate a proper .PEM file from a Windows CA

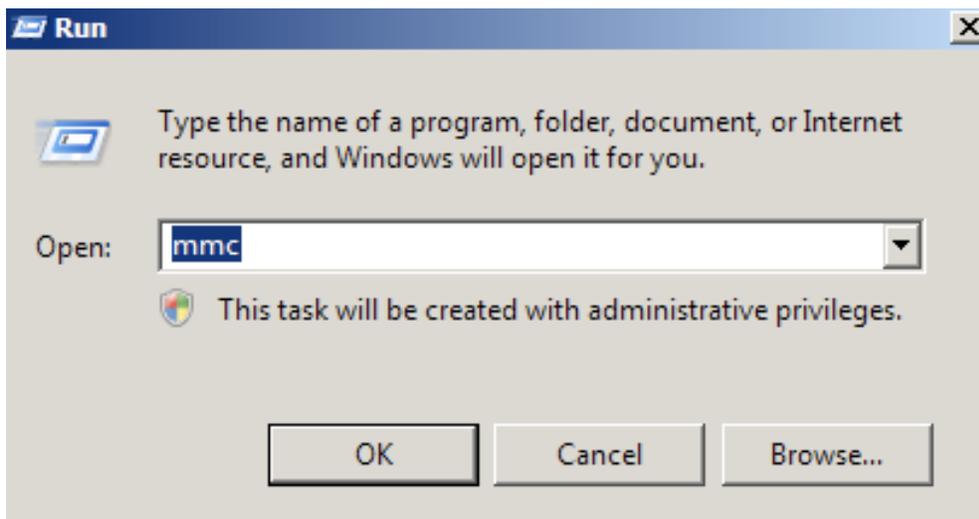
First make the .PFX file export using the steps below:

(taken from <https://www.ssldesk.com/export-ssl-certificate-private-key-pfx-using-mmc-windows/>)

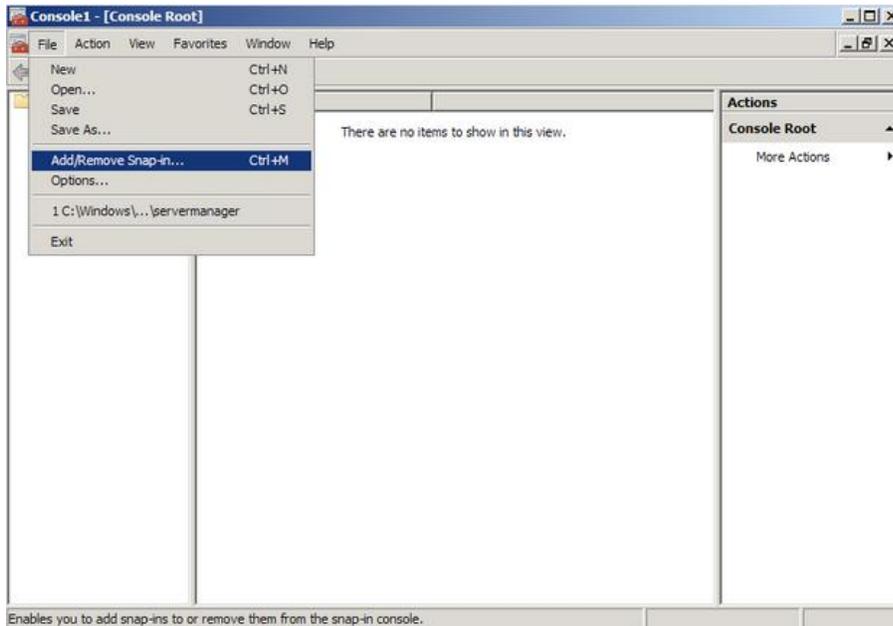
To backup, export an SSL certificate with its private key and intermediates performing the following steps:

**Step 1: Create an MMC Snap-in for Managing Certificates on the first Windows system where the SSL certificate is installed.**

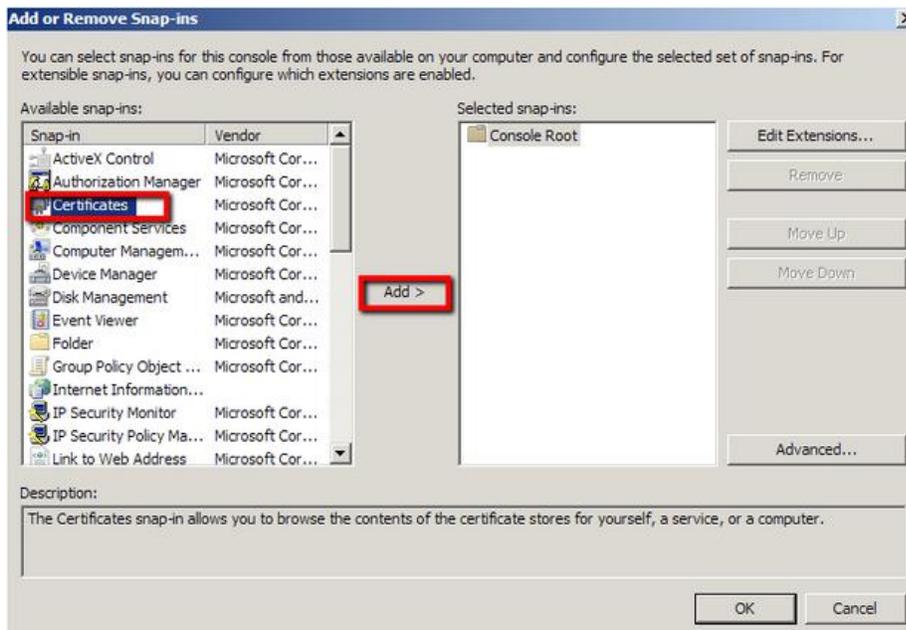
1. **Start > run > MMC.**



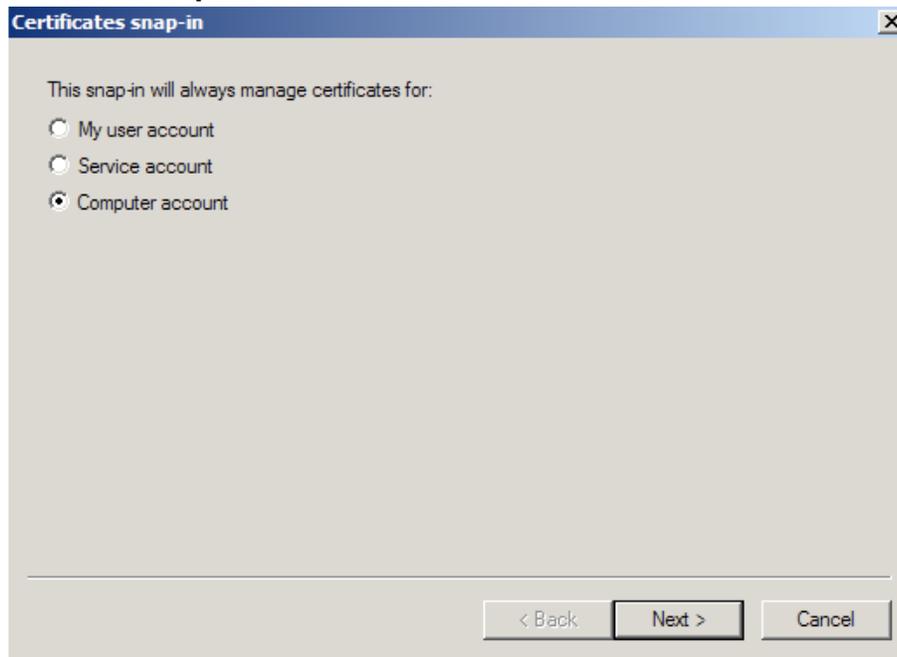
2. Go into the Console Tab > **File** > **Add/Remove Snap-in.**



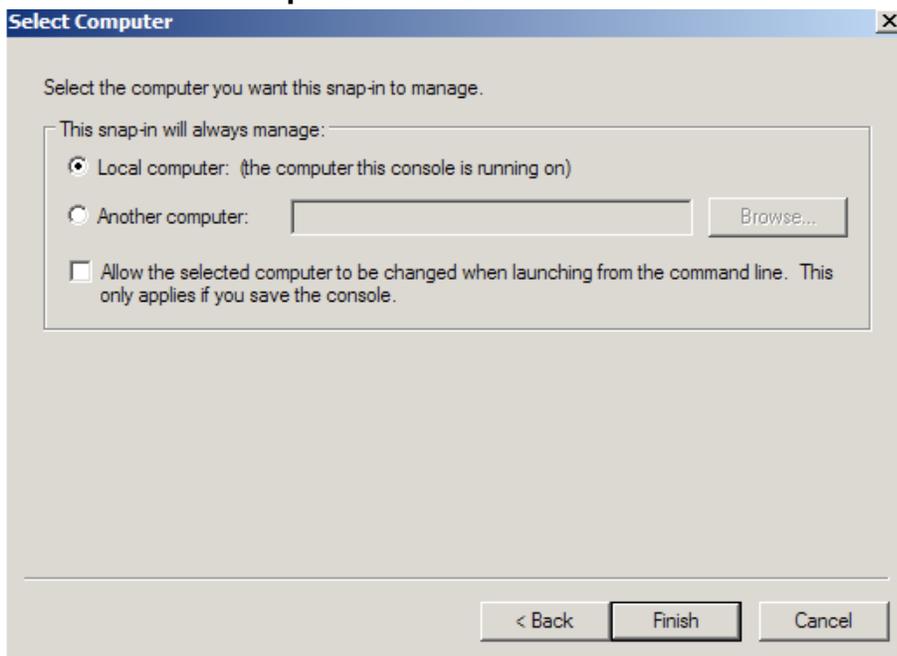
3. Click on **Add** > Click on **Certificates** and click on **Add.**



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



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



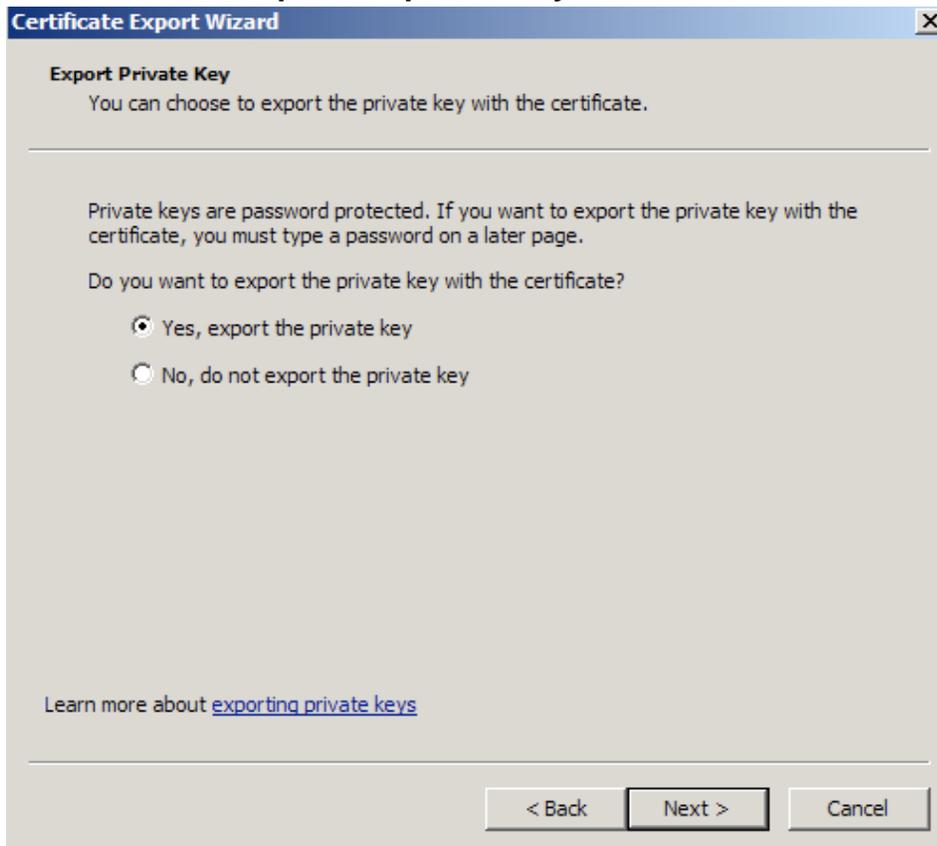
6. Close the **Add Standalone Snap-in** window.
7. Click on **OK** at the **Add/Remove Snap-in** window.

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

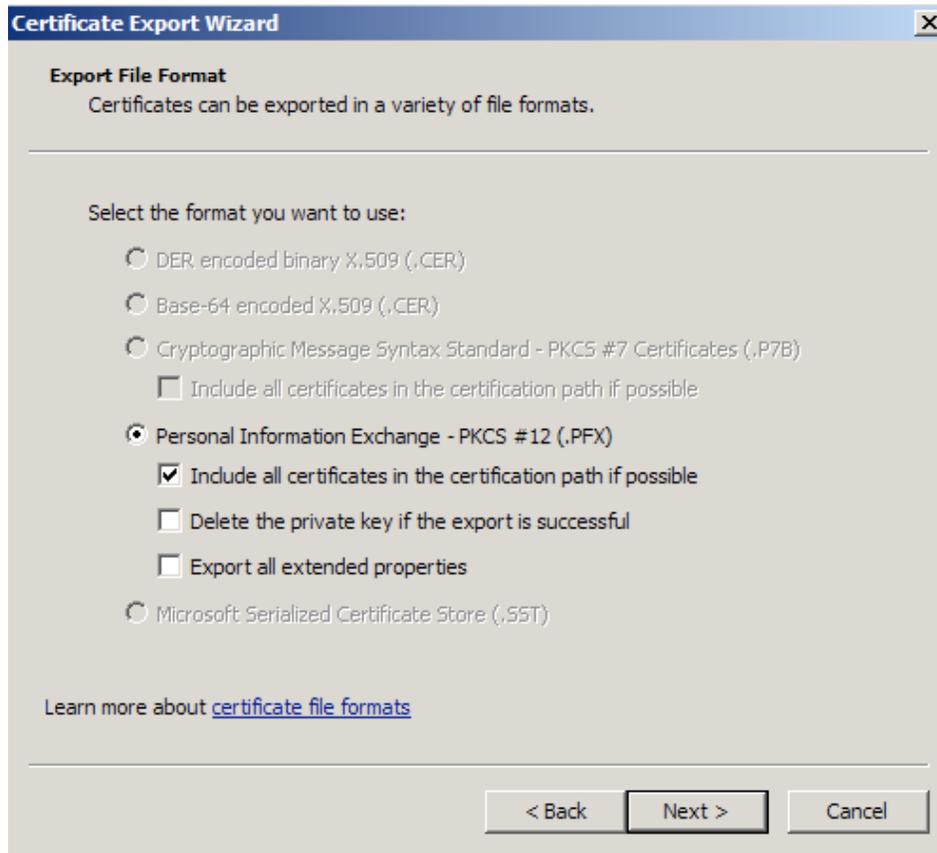
1. In MMC Double click on **Certificates (Local Computer)** in the center window.
2. Double click on the **Personal folder**, and then on **Certificates**.
3. Right Click on the Certificate you would like to backup and choose > **ALL TASKS** > **Export**
4. Follow the Certificate Export Wizard to back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

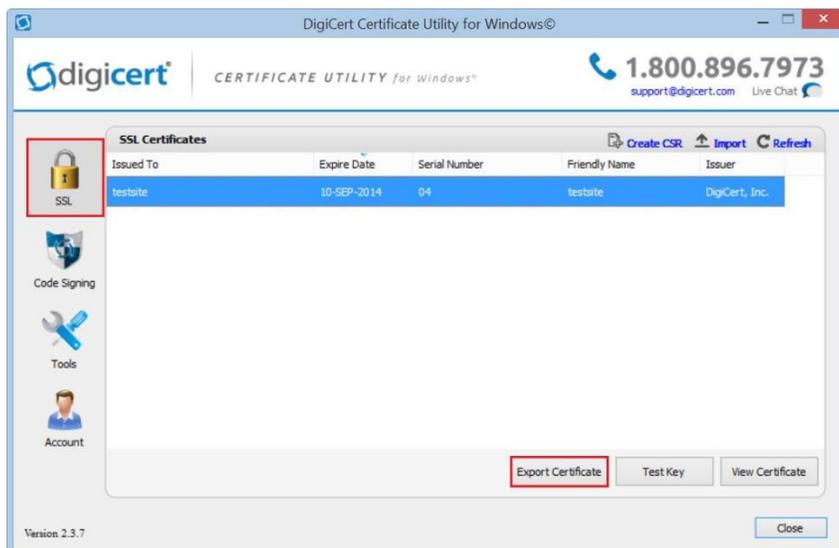
Remove the passphrase from the private key:

```
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



Please contact [support@akcp.com](mailto:support@akcp.com) if you have any further technical questions or problems.

**Thanks for Choosing AKCess Pro!**