www.AKCP.com

SP+ Security Features Manual

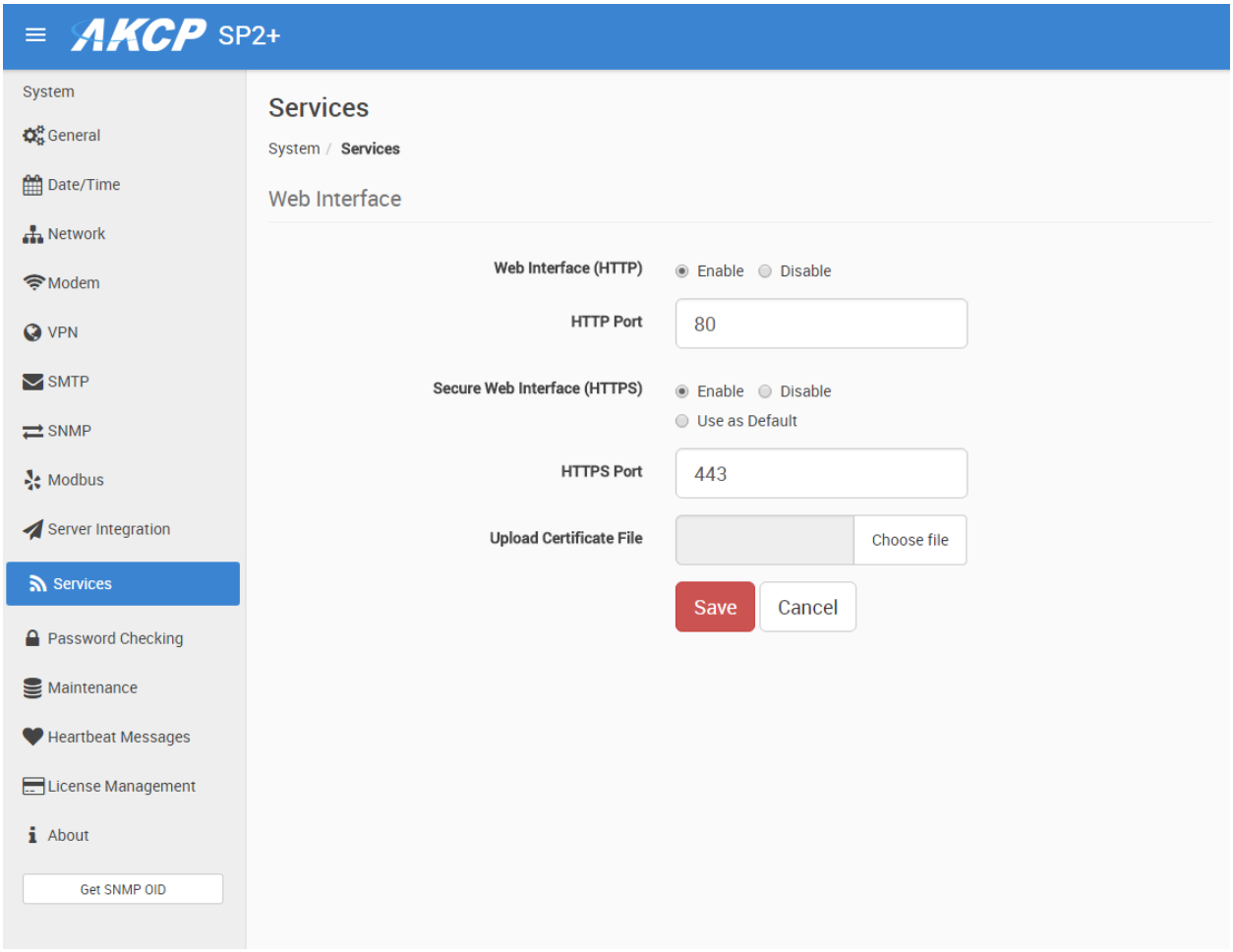
Table of Contents

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



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.

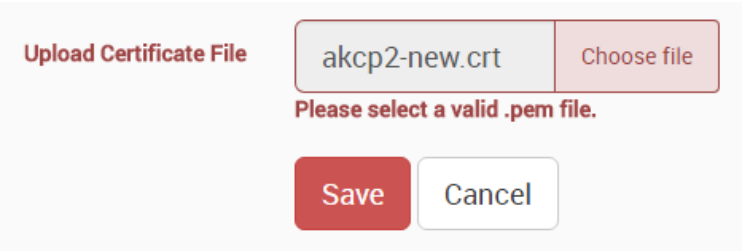
Example: spplus.mycompany.org

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.

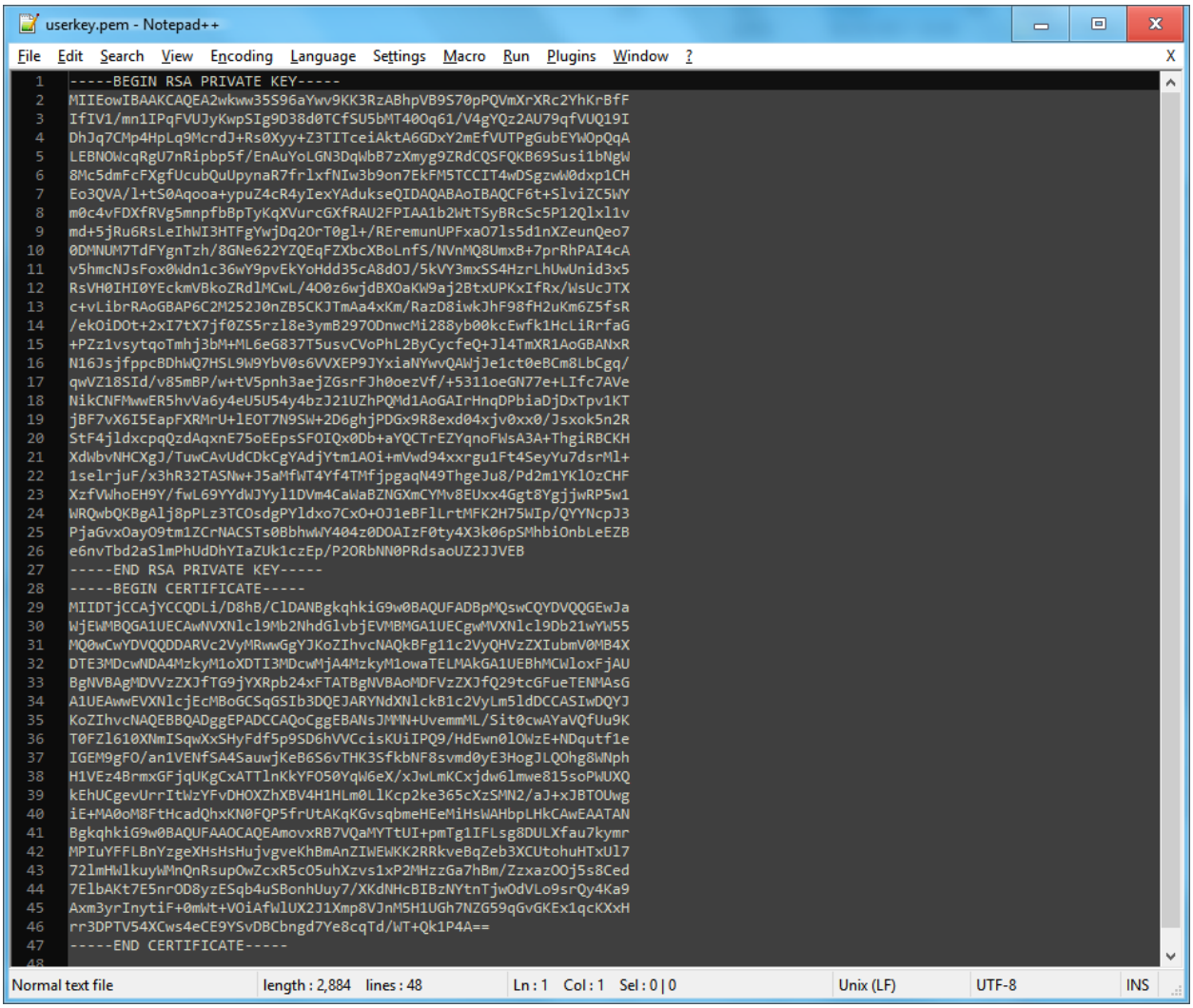
You can purchase a certificate from a trusted, verified Certificate Authority such as GoDaddy or use your company's own CA if you have one.

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

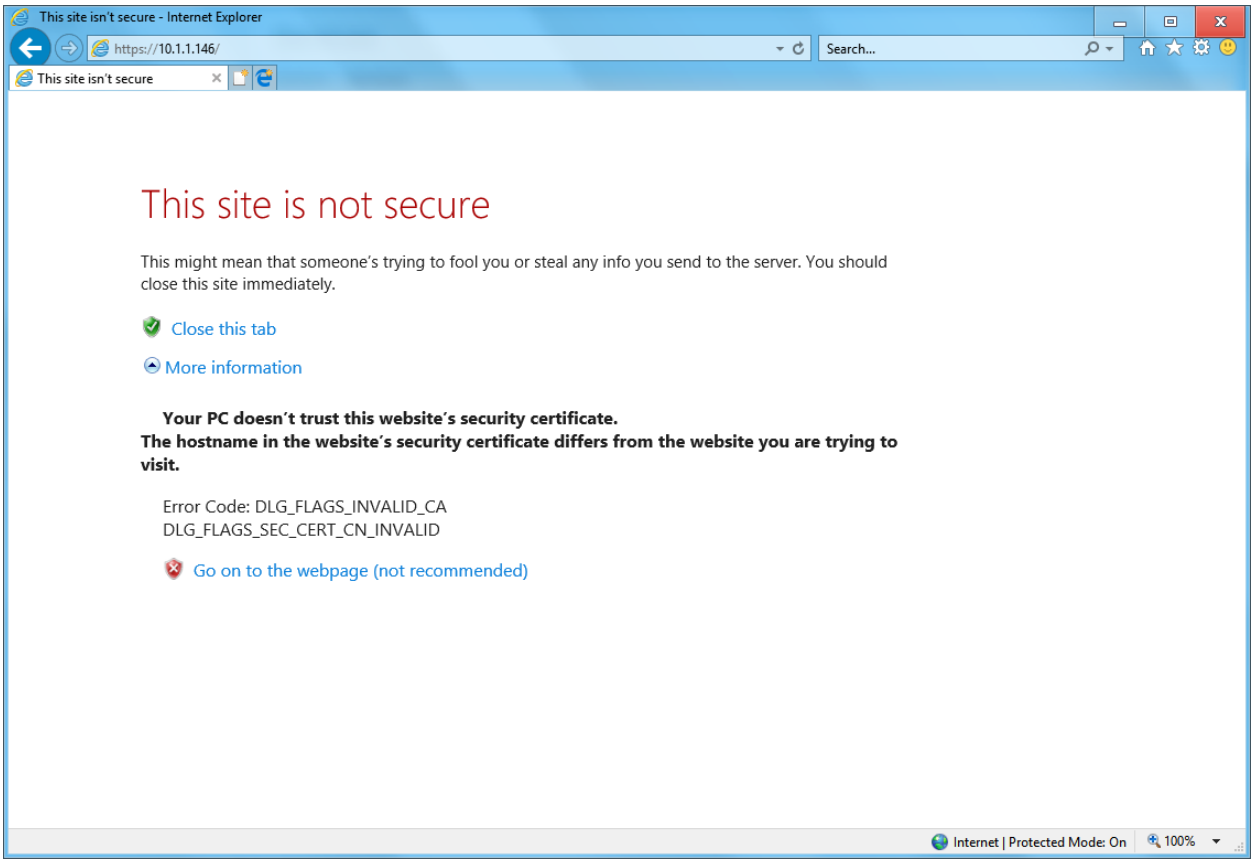
When you select the file for uploading, you'll get a warning if the file is not in .PEM format:



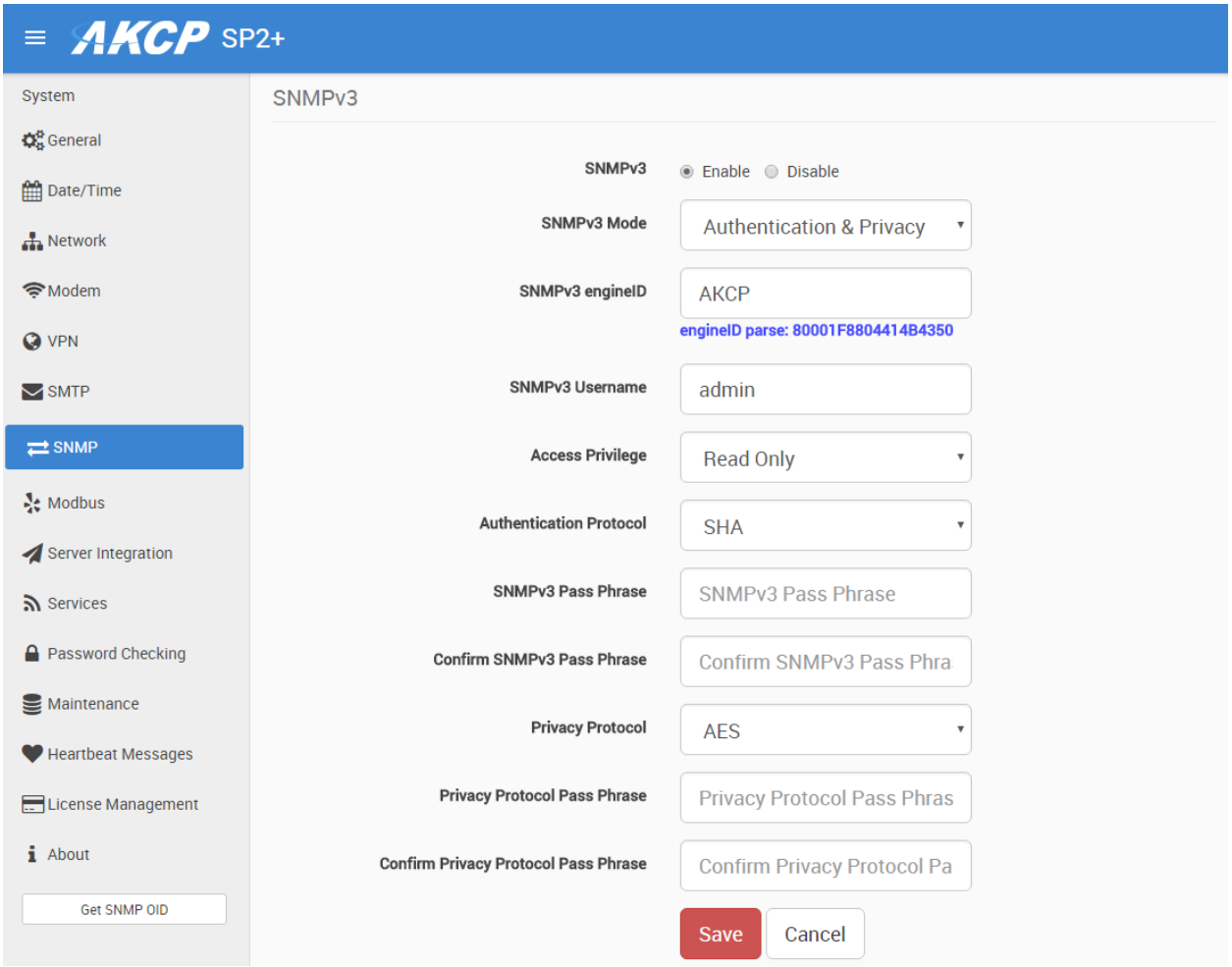
The .PEM file is the private key + certificate combined. You can copy them to one file using Notepad++ if you have 2 separate files, as shown below (it has to be in Unix Line Format and not Windows):



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



SNMPv3 provides important security features:

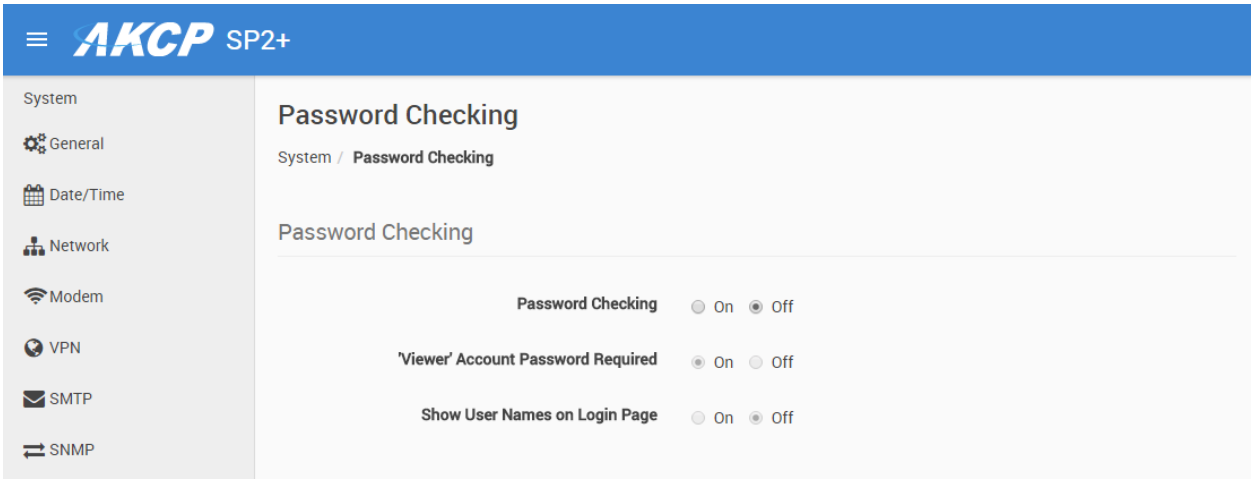
* Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.
* Integrity - Message integrity to ensure that a packet has not been tampered with in transit.
* Authentication - to verify that the message is from a valid source.

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

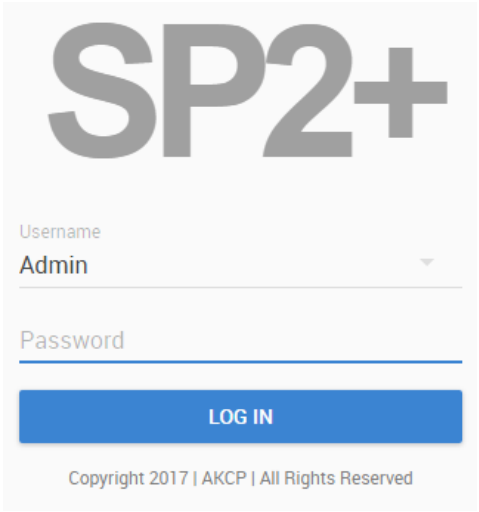


You can turn on the password checking for the Web UI to ensure only authenticated users have access to the unit. You can also specify to show all user names on the login page, or keep them confidential.
After you enable the password checking, you'll need to re-login.
If you don't remember the Admin password, 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

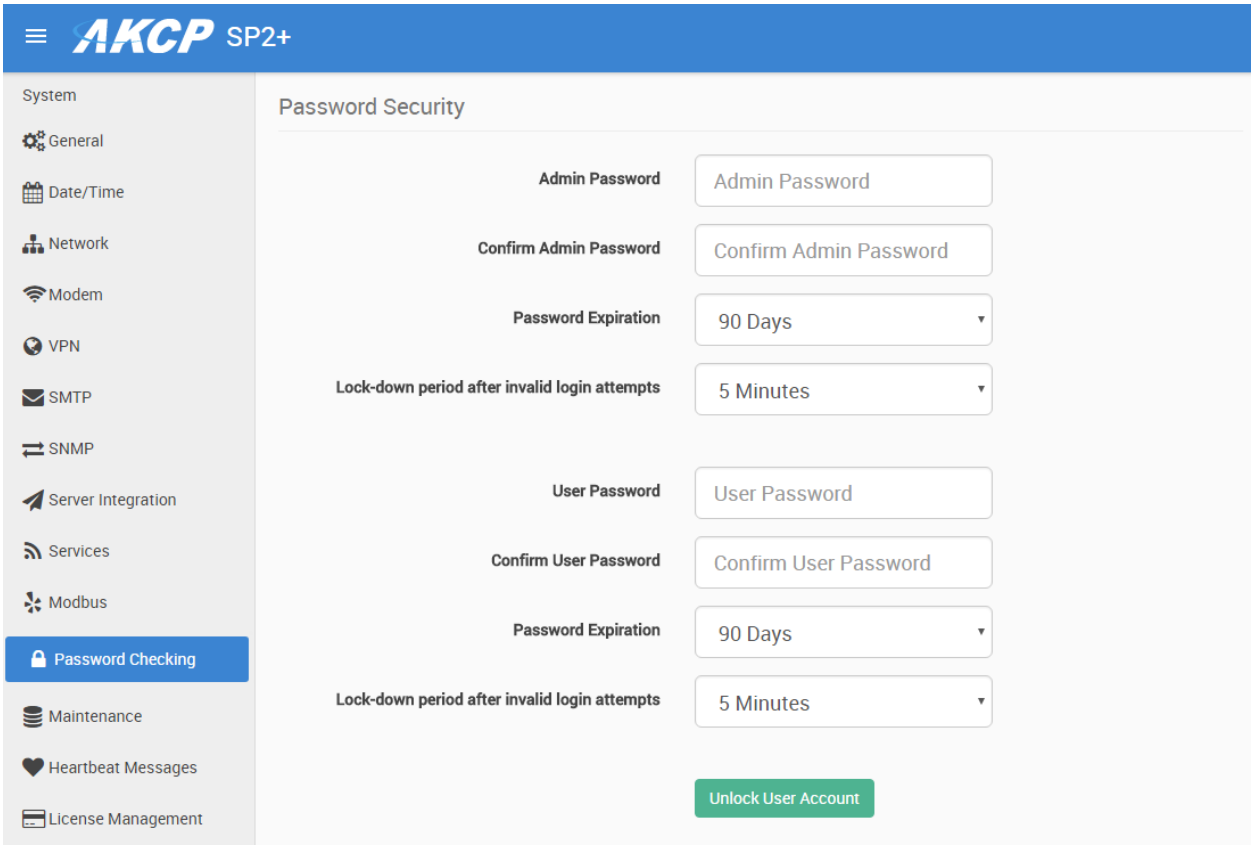
Admin - full access to all settings, system and notification configurations
Viewer - read-only guest access for every page
User - full access to most settings except for those which are the system-related such as network



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

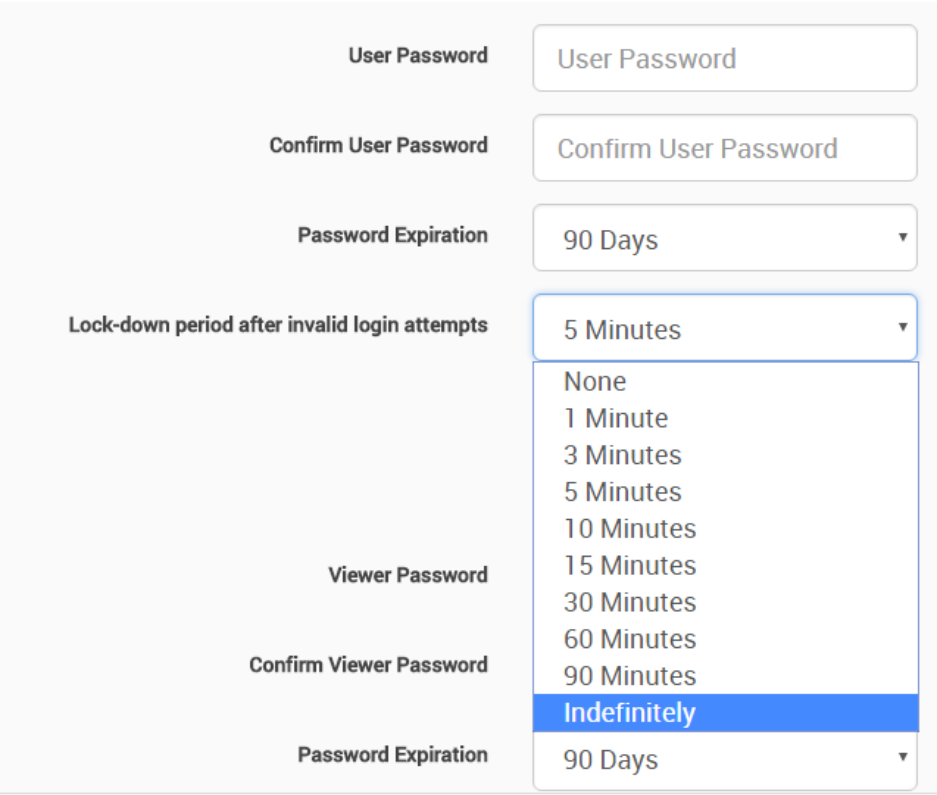


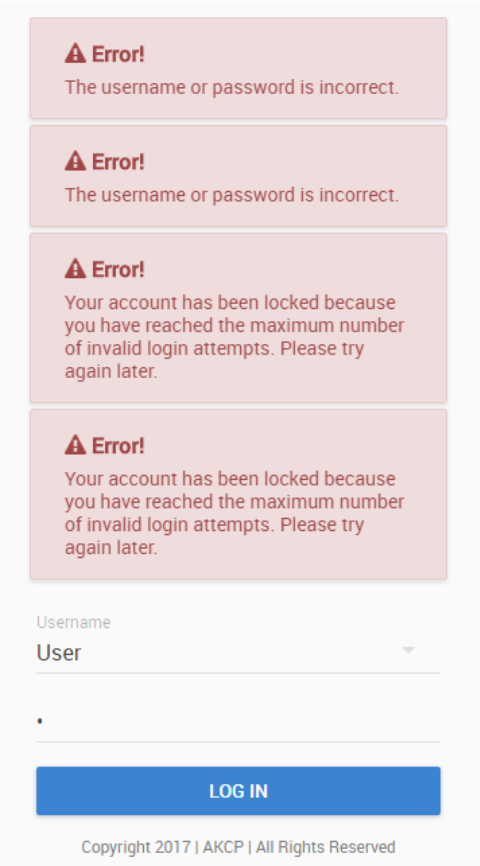
All user account types (Admin, User, Viewer) have adjustable password expiration and lockdown periods.

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

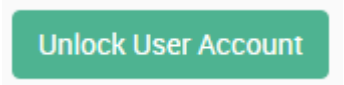




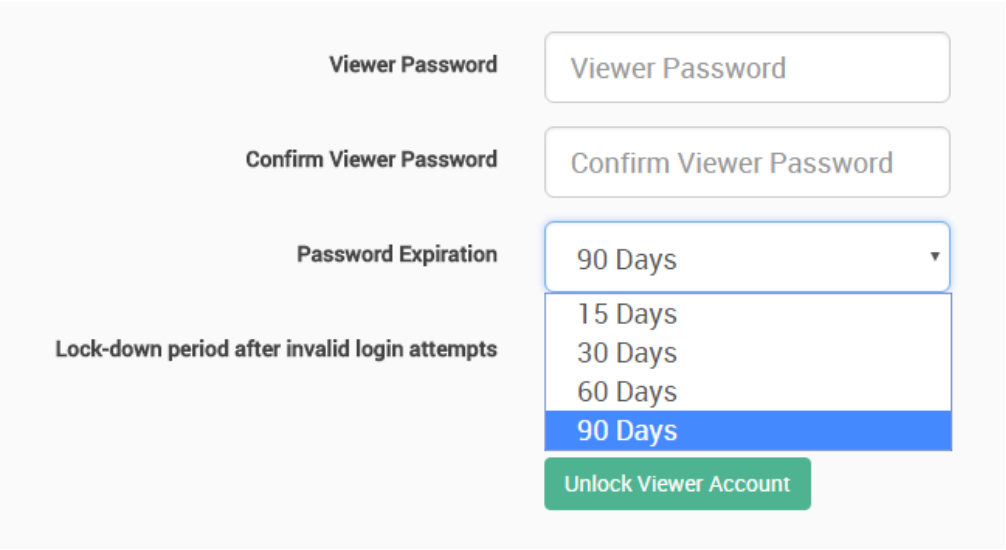
The accounts can be set to lock down the account after 3 invalid login attempts, to prevent brute-force hacking attempts.
You can specify how long the account will automatically unlock itself.

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.

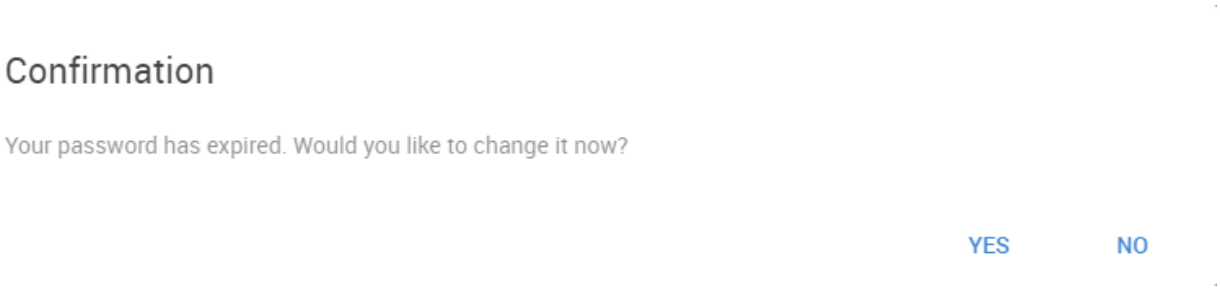
If an account has been locked, you can unlock it immediately by logging in with the Admin user, and by using the green unlock button:



Password Expiration



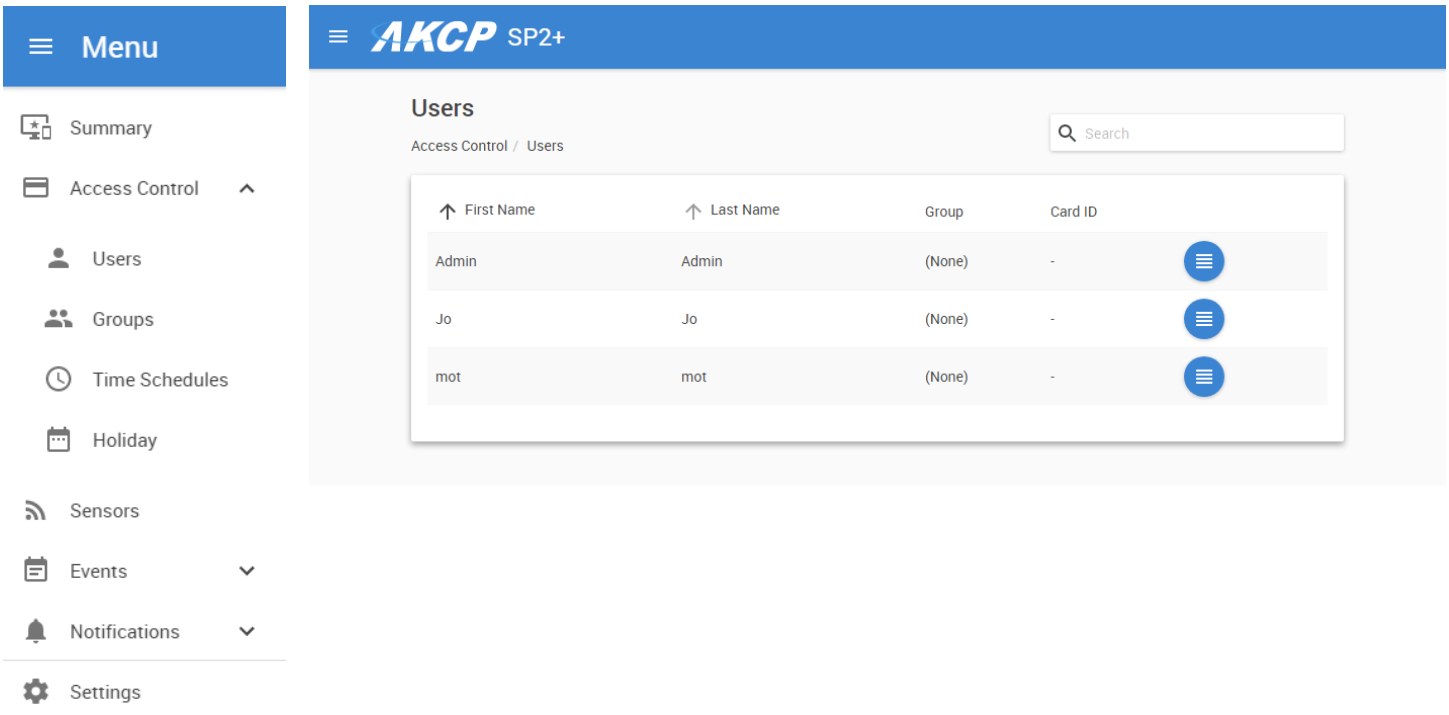
You can specify password expiration between every 15 and 90 days for all account types. Note that currently there's no option to set "no expiration".



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.

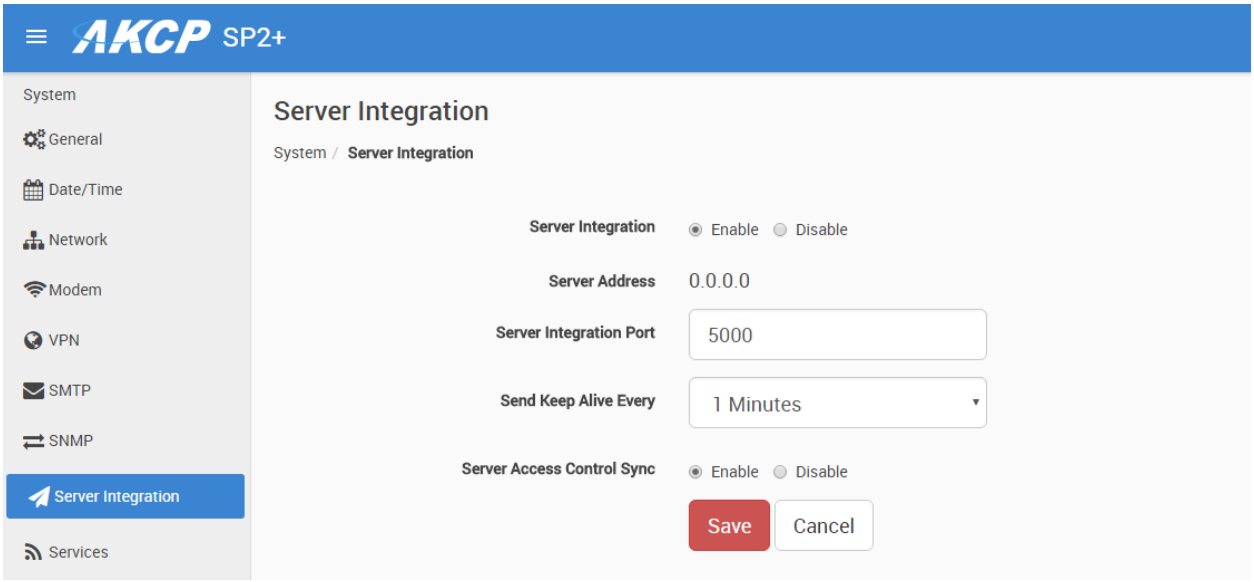
Access Control Users and Groups

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.

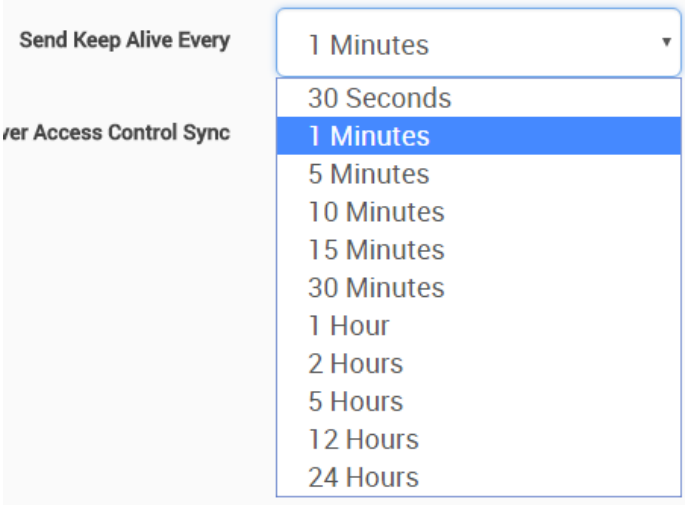


This feature has its own manual, refer to the SP+ Swing Handle Lock Manual for more information.

Server Integration

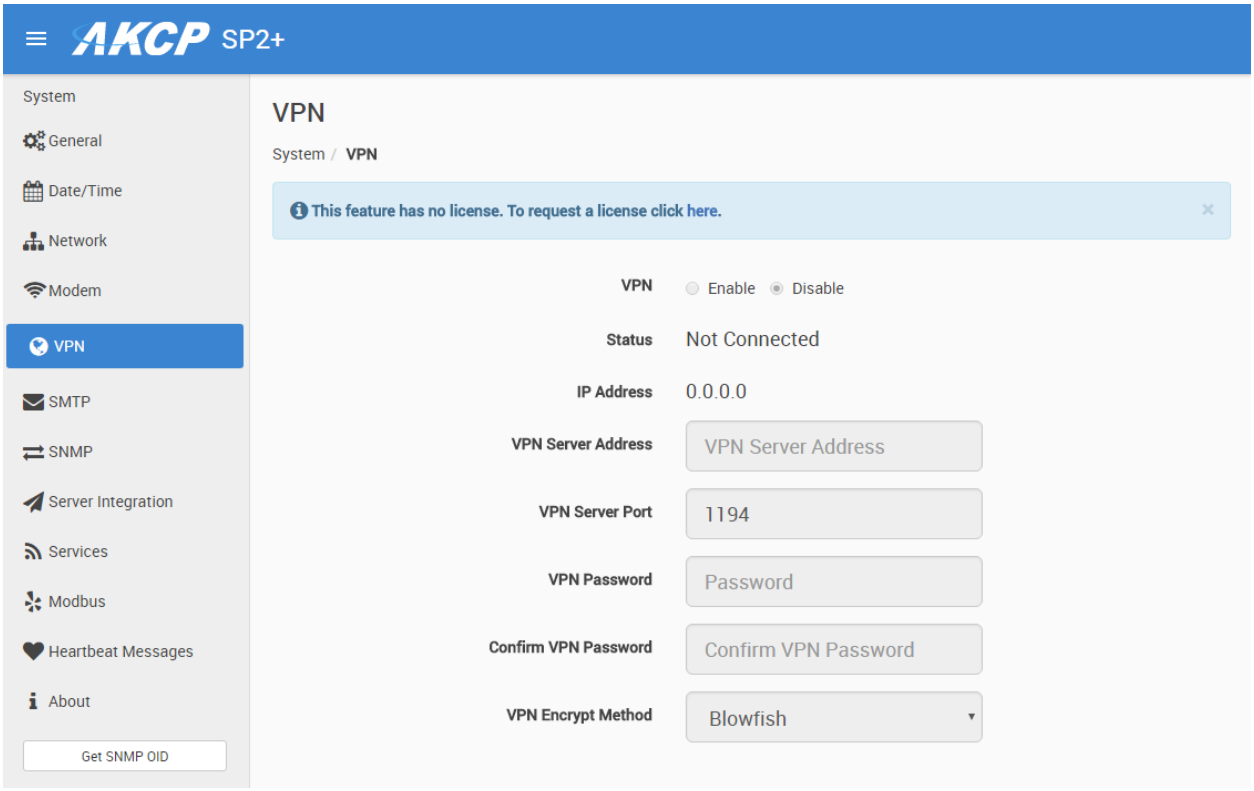


You can enable/disable controlling the unit via AKCess Pro Server.
If the unit has been added to the APS console, the server's IP address will be also displayed here.
You can change the APS port when the server's port changes, and the keep-alive period (heartbeat sync to APS).

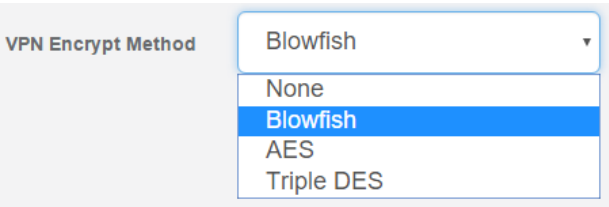


You may turn off the access control user sync separately, so that the user database will not be updated together with APS.

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.

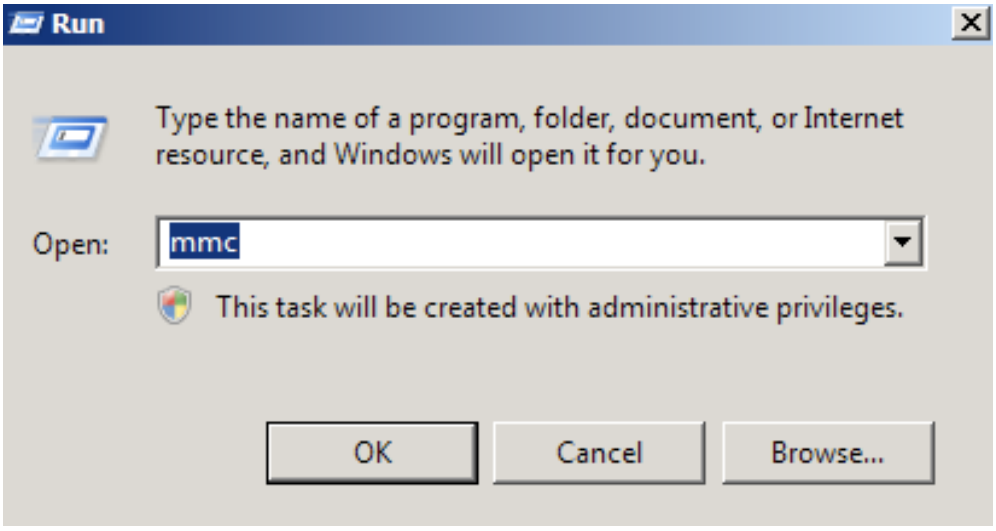
Troubleshooting - How to generate a proper .PEM file from a Windows CA

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

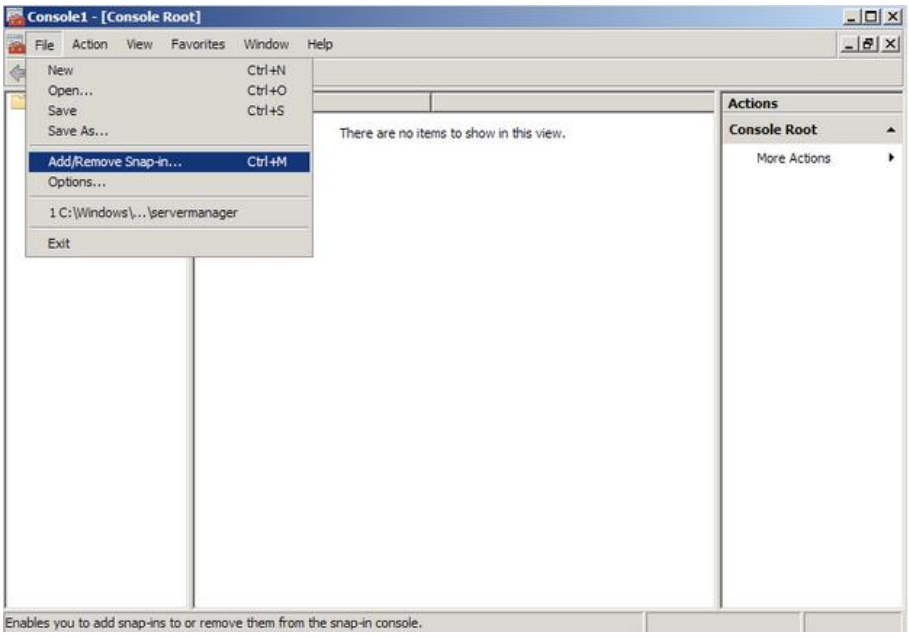
To backup, export an SSL certificate with its private key and intermediates performing the following steps:

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

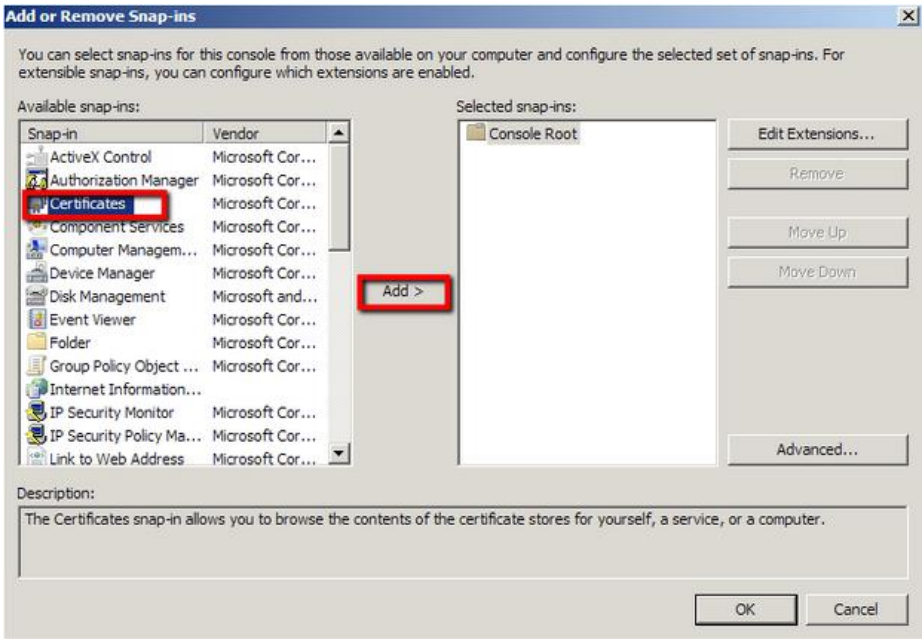
1. **Start** > **run** > **MMC.**



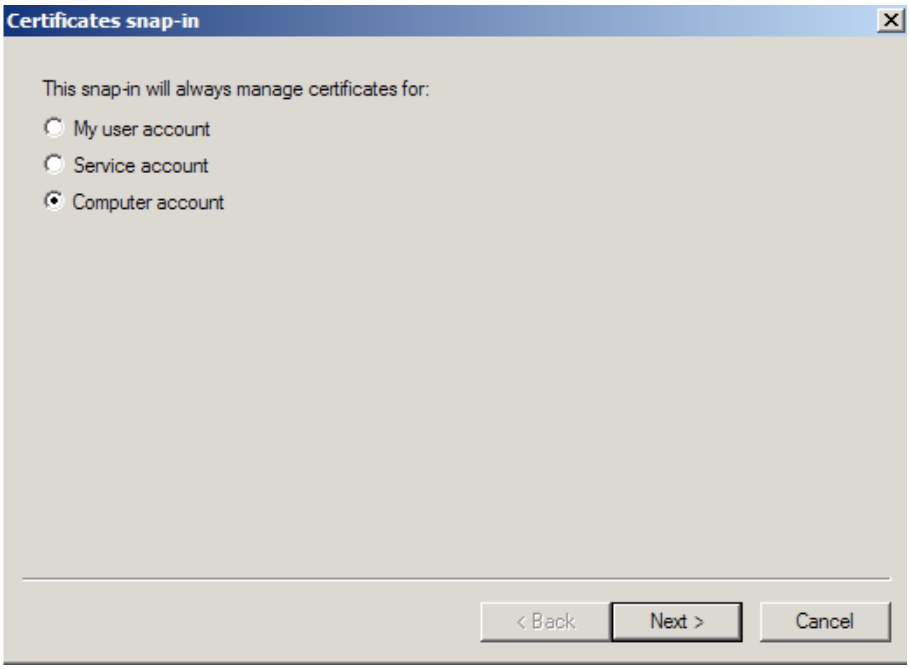
2. Go into the Console Tab > **File** > **Add/Remove Snap-in.**



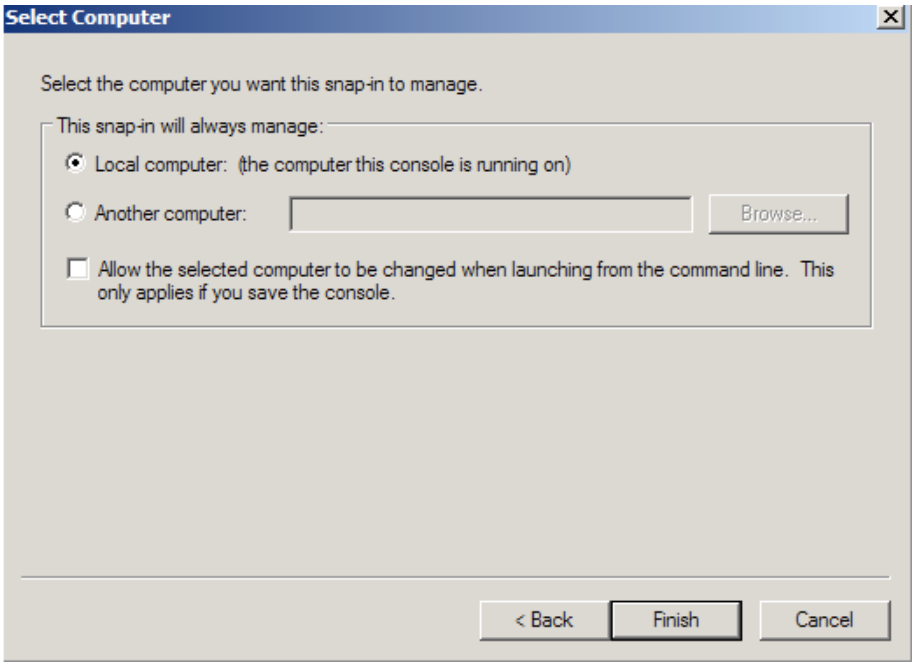
3. Click on **Add** > Click on **Certificates** and click on **Add.**



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



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

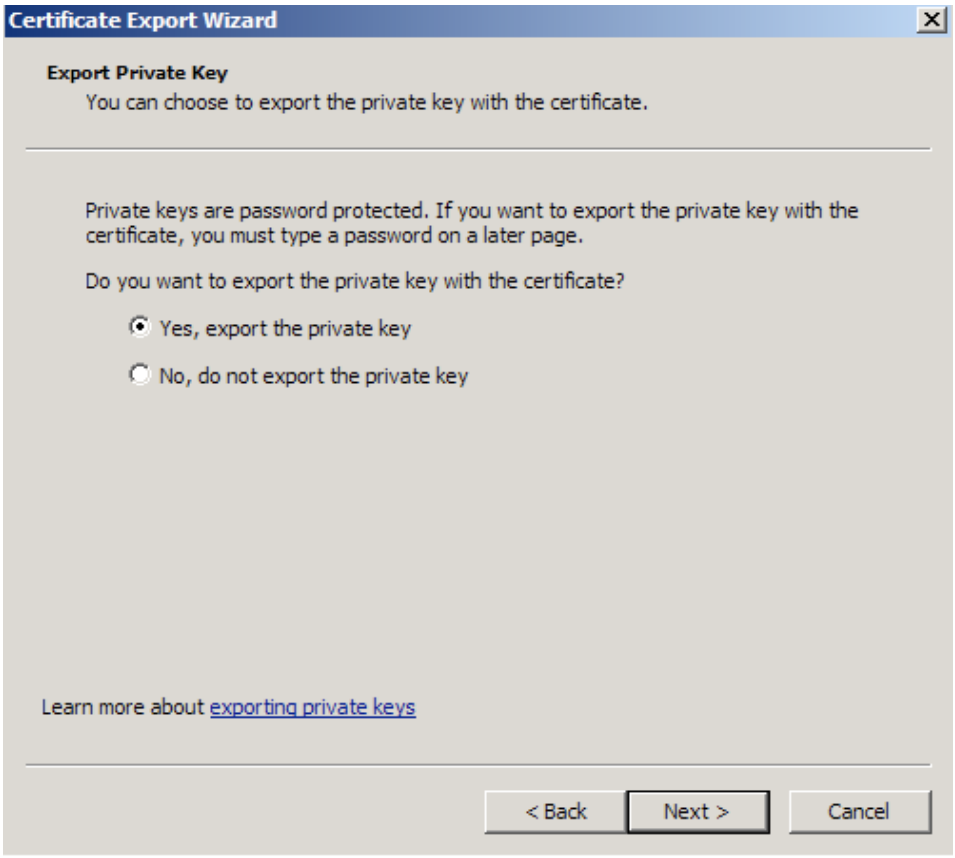


6. Close the **Add Standalone Snap-in** window.
7. Click on **OK** at the **Add/Remove Snap-in** window.

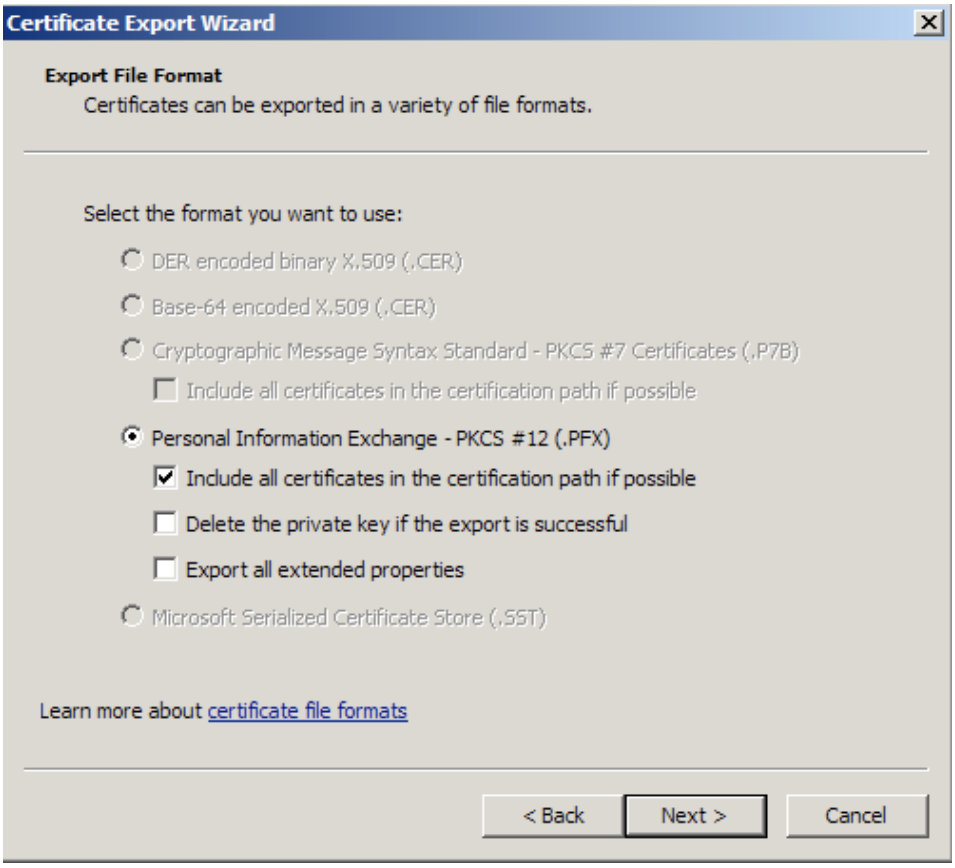
Step 2: Export/Backup certificate to .pfx file:

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**'

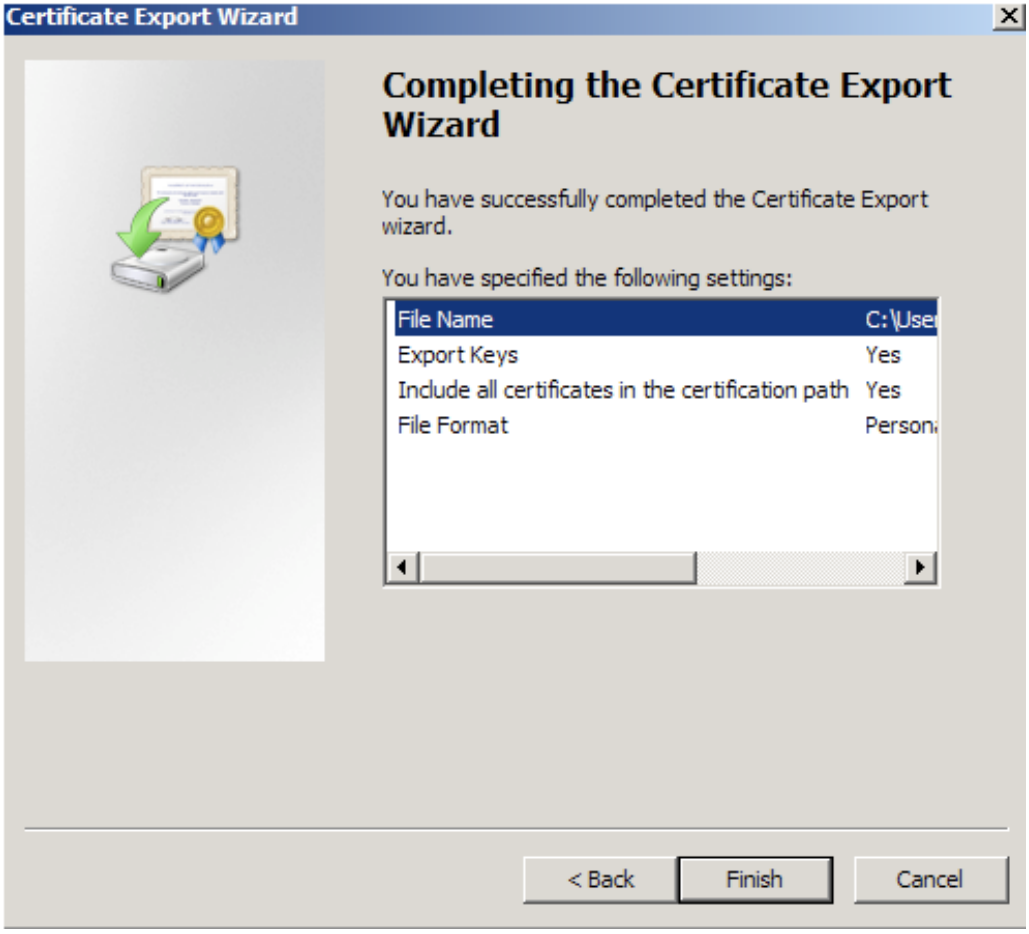


6. Choose to “**Include all certificates in certificate path if possible**.” (do NOT select the delete Private Key option)



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 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/

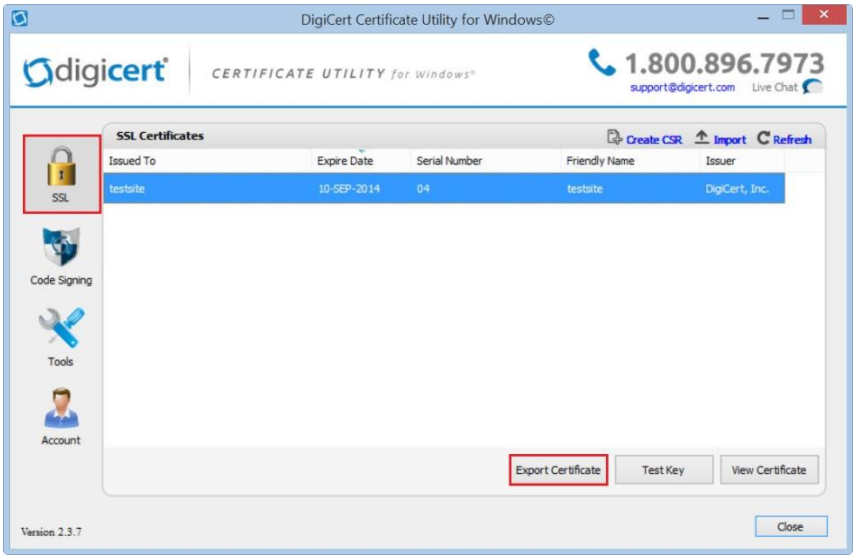
Export the private key file from the pfx file:
```
openssl pkcs12 -in filename.pfx -nocerts -out key.pem
```

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 if you have any further technical questions or problems.

Thanks for Choosing AKCess Pro!