www.AKCP.com

securityProbe

Security Features Manual

Introduction

What are the security features on the securityProbe and securityProbe 5E unit?

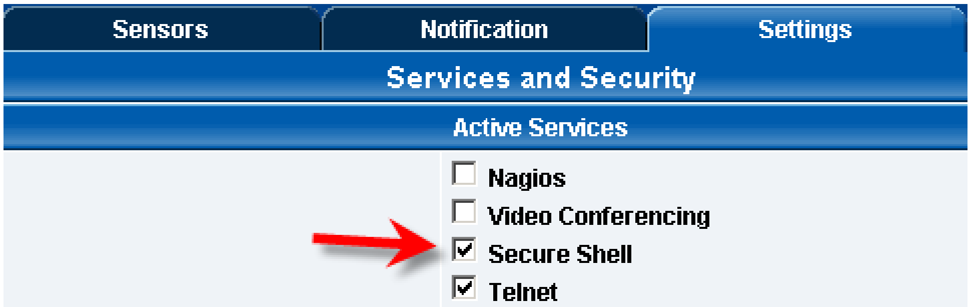
The security services features on the securityProbe are quite extensive and allows users to lock down and secure the unit from exterior threats. Each option will be covered in detail within this manual.

How to use this manual

This manual is meant to provide the user with a step by step guide on how to configure and set up their unit. It utilizes screen shots in an effort to make things simpler for the user to follow. It is split up into sections that form “mini tutorials”. These cover the basic set up and common configurations of the unit, and give an introduction to its most useful features.
If you need any further information or help with using your unit then please contact us on support@akcp.com and one of our technical support staff will be pleased to help you with any information you require.

Services and Security

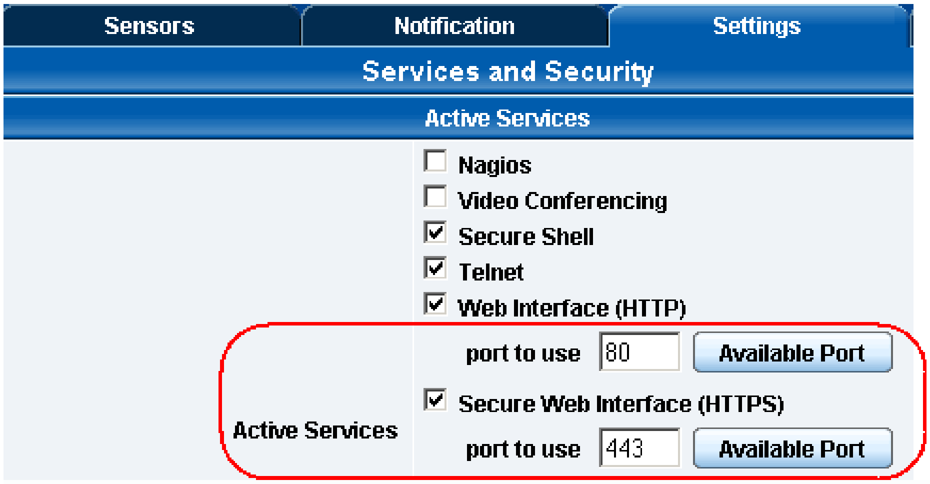
Active Services Application (disabling)



☐ Nagios
☐ Video Conferencing
☑ Secure Shell
☑ Telnet

You can enable or disable the Nagios, Video Conferencing, Secure Shell and Telnet applications running on the unit thus making the unit more secure as shown in the screen capture above.

Closing or changing ports disabling HTTP and enabling HTTPS



☐ Nagios
☐ Video Conferencing
☑ Secure Shell
☑ Telnet
☑ Web Interface (HTTP)

Active Services

port to use 80

☑ Secure Web Interface (HTTPS)

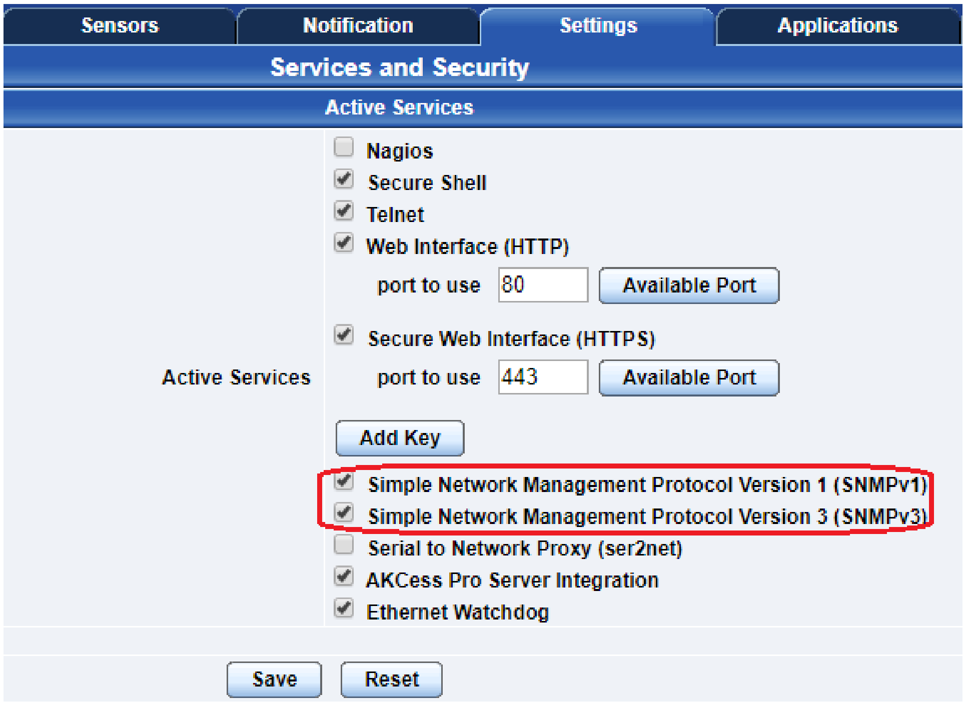
port to use 443

You can also close or change the ports used to access the units web interface, disable HTTP and enable HTTPS only.

The "s" at the conclusion in HTTPS stands for secure. This SSL/TLS connection type is used primarily for high-value sites or ‘pages’, to elevate the potential of being unreadable by anyone but the end-points.
One benefit is the traffic between client and the securityProbe is not cached along the various units as it moves across the ‘Net, and so can’t be accessed by someone after the connection is terminated.

The SSL certificate that is used by the Web UI can be replaced, see below.

The SNMPv3 security feature



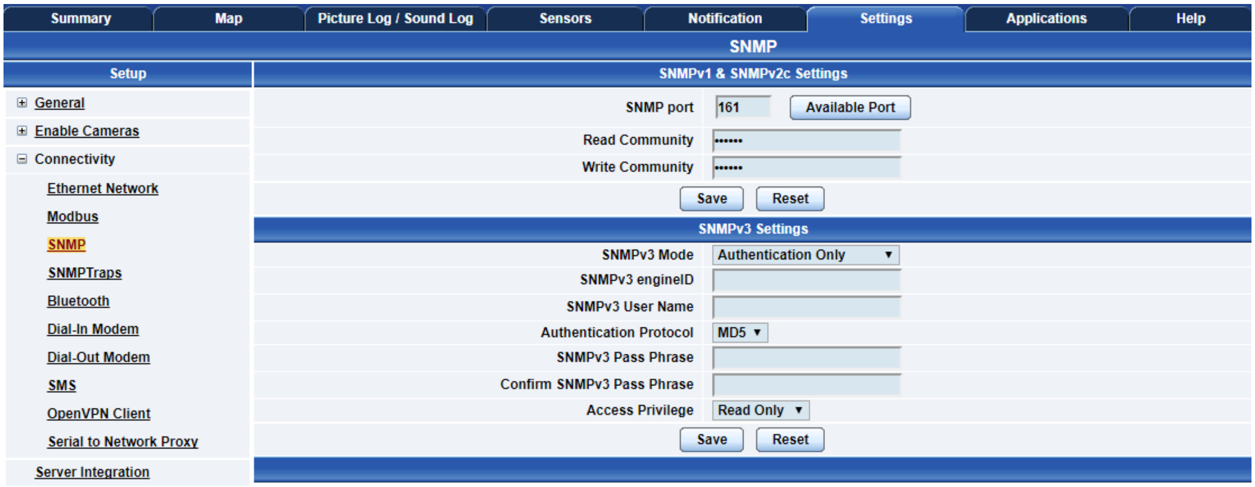
Active Services

□ Nagios
☑ Secure Shell
☑ Telnet
☑ Web Interface (HTTP)
port to use 80
☑ Secure Web Interface (HTTPS)
port to use 443
☑ Simple Network Management Protocol Version 1 (SNMPv1)
☑ Simple Network Management Protocol Version 3 (SNMPv3)
□ Serial to Network Proxy (ser2net)
☑ AKCess Pro Server Integration
☑ Ethernet Watchdog

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.

After you enable SNMPv3, you can configure the settings for it under the Connectivity / SNMP options:



SNMP

SNMPv1 & SNMPv2c Settings

SNMP port 161

Read Community ••••••

Write Community ••••••

SNMPv3 Settings

SNMPv3 Mode Authentication Only ▼

SNMPv3 engineID

SNMPv3 User Name

Authentication Protocol MD5 ▼

SNMPv3 Pass Phrase

Confirm SNMPv3 Pass Phrase

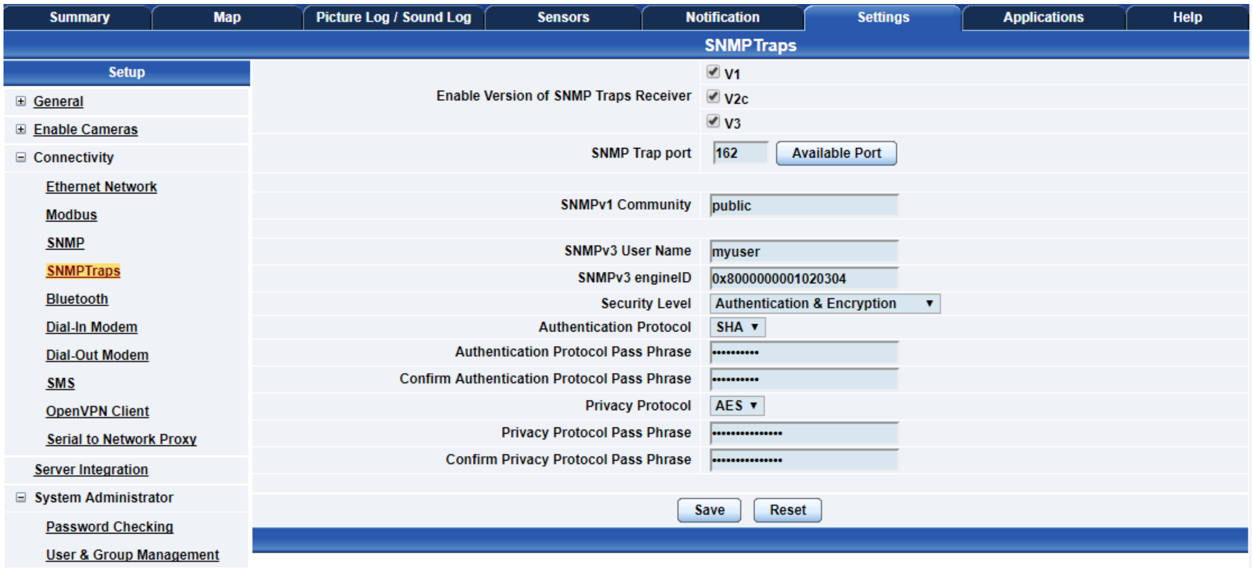
Access Privilege Read Only ▼

Below we'll give a quick description of each setting:

Level	Authentication	Encryption	Description
No Authentication	Username	No	Match Username (same as SNMP v1/v2c)
Authentication Only	MD5 or SHA	No	Auth Based on Algorithms (check password)
Auth&Privacy	MD5 or SHA	Yes - DES	Auth Algorithms and Encryption

Basically if you select **No Authentication** then the setup will be the same as with SNMP v1 and v2c versions: authentication is only checked by unencrypted username.
Authentication Only will provide password protection but no encryption.
Authentication&Privacy provides encrypted username and password protection.

You can also find SNMPv3 settings under the SNMP Trap settings and in the SNMP actions as well:



SNMPTraps

Enable Version of SNMP Traps Receiver: ☑ V1 ☑ V2c ☑ V3

SNMP Trap port: 162

SNMPv1 Community: public

SNMPv3 User Name: myuser

SNMPv3 engineID: 0x8000000001020304

Security Level: Authentication & Encryption

Authentication Protocol: SHA

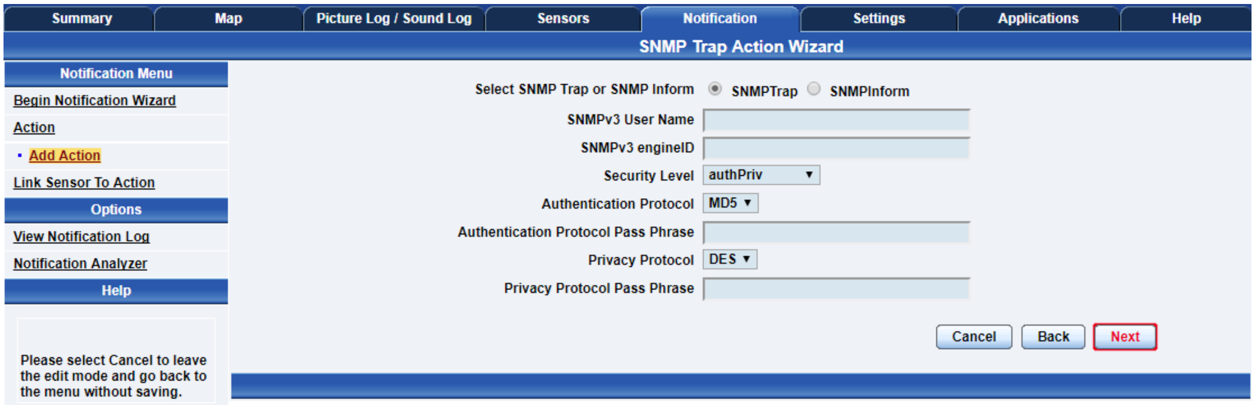
Authentication Protocol Pass Phrase: ••••••••••

Confirm Authentication Protocol Pass Phrase: ••••••••••

Privacy Protocol: AES

Privacy Protocol Pass Phrase: •••••••••••••••

Confirm Privacy Protocol Pass Phrase: •••••••••••••••



SNMP Trap Action Wizard

Select SNMP Trap or SNMP Inform: ● SNMPTrap ○ SNMPInform

SNMPv3 User Name:

SNMPv3 engineID:

Security Level: authPriv

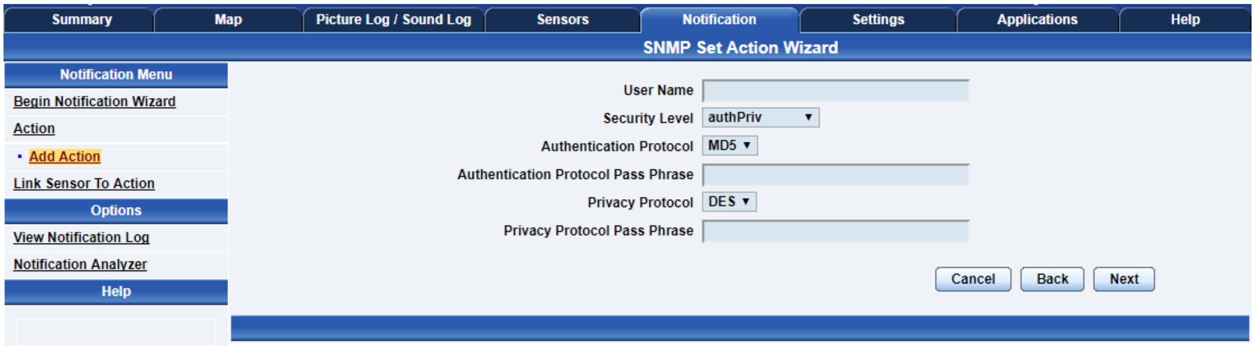
Authentication Protocol: MD5

Authentication Protocol Pass Phrase:

Privacy Protocol: DES

Privacy Protocol Pass Phrase:

Please select Cancel to leave the edit mode and go back to the menu without saving.



SNMP Set Action Wizard

User Name:

Security Level: authPriv

Authentication Protocol: MD5

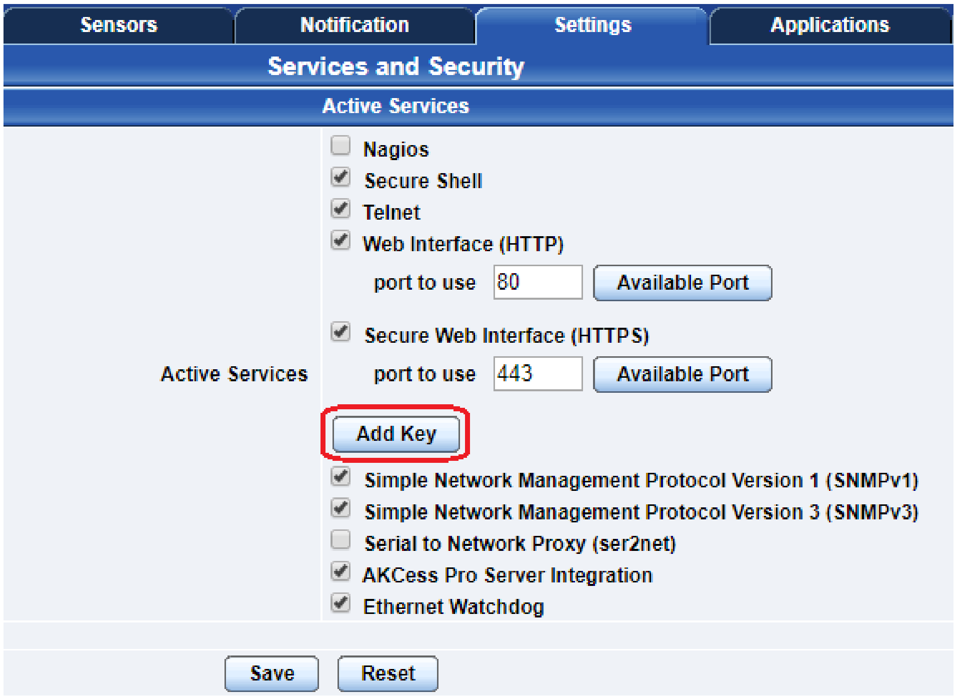
Authentication Protocol Pass Phrase:

Privacy Protocol: DES

Privacy Protocol Pass Phrase:

SSL Certificate for HTTPS and SNMPv3

Use the SSL (Secure Sockets Layer) port for the Web UI, which is the standard security technology for establishing the encrypted link between the securityProbe in our case and the web browser. This link ensures that all data passed between the securityProbe and the browser remains private and integral.



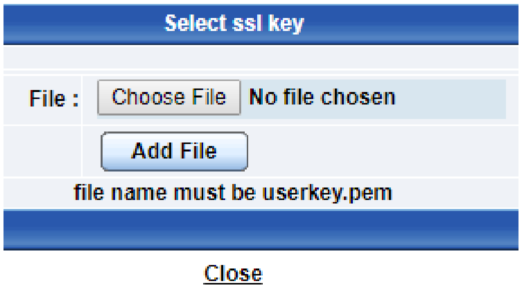
Services and Security

Active Services

Active Services

□ Nagios
☑ Secure Shell
☑ Telnet
☑ Web Interface (HTTP)
port to use 80
☑ Secure Web Interface (HTTPS)
port to use 443
☑ Simple Network Management Protocol Version 1 (SNMPv1)
☑ Simple Network Management Protocol Version 3 (SNMPv3)
□ Serial to Network Proxy (ser2net)
☑ AKCess Pro Server Integration
☑ Ethernet Watchdog

Using the “Add Key” option you can upload an SSL certificate that will be used by the unit’s Web UI for HTTPS connection, and for SNMPv3 to sign the encrypted traffic.



Select ssl key

File : No file chosen

file name must be userkey.pem

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

The file name MUST be userkey.pem, rename the file if necessary.

SSL certificates are generated for DNS host names and not IP addresses. You should set a host name for the SEC unit in your local DNS server or DHCP server, and then generate the SSL certificate for that host name.

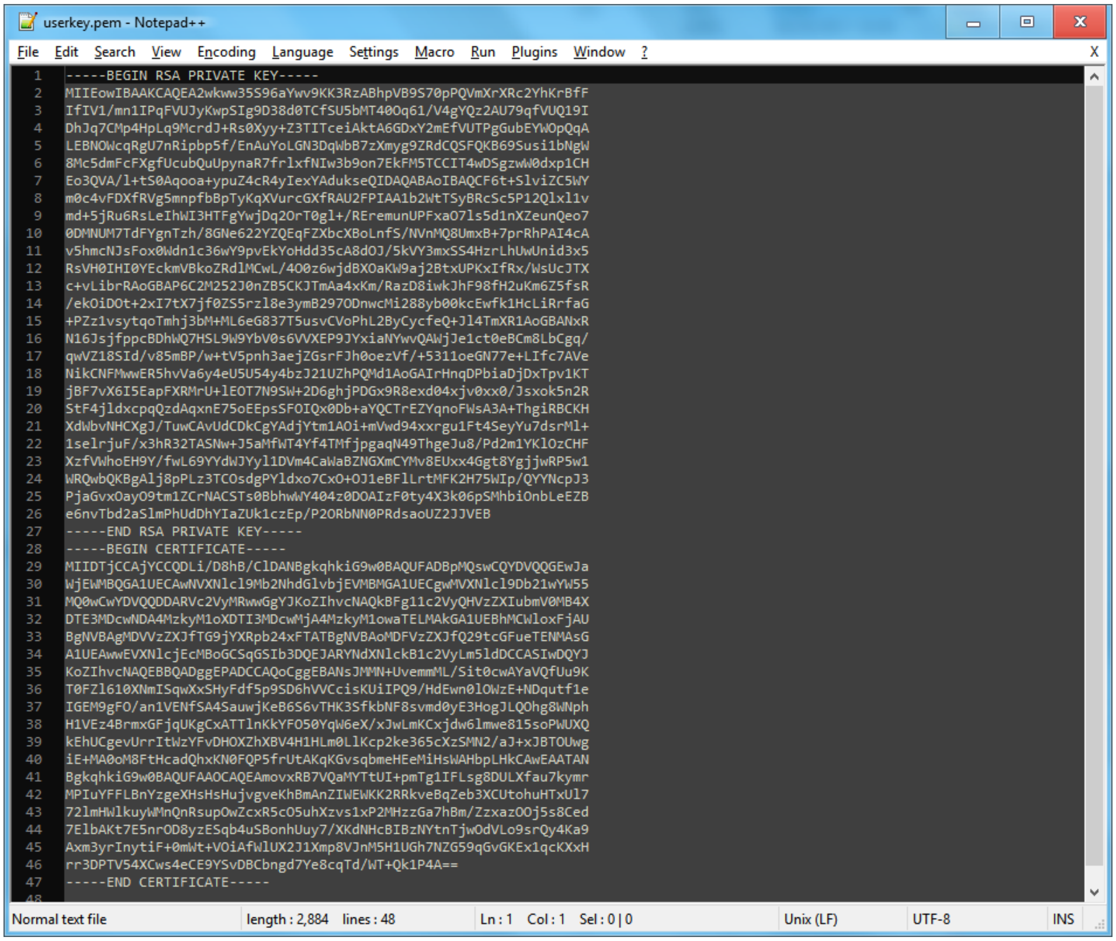
Example: sec.mycompany.org

The unit's DNS host name is "sec". 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.

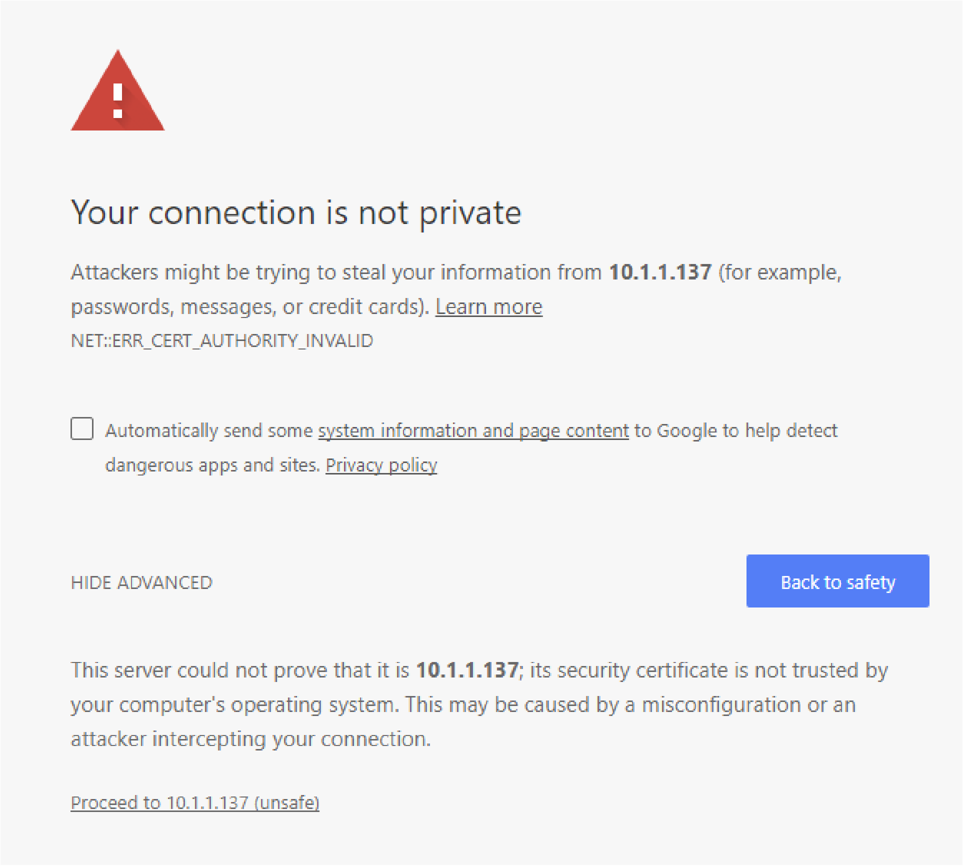
Please note that *only non-password protected certificate files are supported.*

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):



```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2wkww35S96aYwv9KK3RzABhpVB9S70pPQVmXrXRc2YhKrBfF
IfIV1/mn1IPqFVUJyKwpSIg9D38d0TCfSU5bMT40Oq61/V4gYQz2AU79qfVUQ19I
DhJq7CMp4HpLq9McrdJ+Rs0Xyy+Z3TITceiAktA6GDxY2mEfVUTPgGubEYWOpQqA
LEBNOWcqRgU7nRipbp5f/EnAuYoLGN3DqWbB7zXmyg9ZRdCQSFQKB69Susi1bNgW
8Mc5dmFcFXgfUcubQuUpynaR7frlxfNIw3b9on7EkFM5TCCIT4wDSgzwW0dxp1CH
Eo3QVA/l+tS0Aqooa+ypuZ4cR4yIexYAdukseQIDAQABAoIBAQCF6t+SlviZC5WY
m0c4vFDXfRVg5mnpfbBpTyKqXVurcGXfRAU2FPIAA1b2WtTSyBRcSc5P12Qlxl1v
md+5jRu6RsLeIhWI3HTFgYwjDq2OrT0gl+/REremunUPFxaO7ls5d1nXZeunQeo7
0DMNUM7TdFYgnTzh/8GNe622YZQEqFZXbcXBoLnfS/NVnMQ8UmxB+7prRhPAI4cA
v5hmcNJsFox0Wdn1c36wY9pvEkYoHdd35cA8dOJ/5kVY3mxSS4HzrLhUwUnid3x5
RsVH0IHI0YEckmVBkoZRdlMCwL/4O0z6wjdBXOaKW9aj2BtxUPKxIfRx/WsUcJTX
c+vLibrRAoGBAP6C2M252J0nZB5CKJTmAa4xKm/RazD8iwkJhF98fH2uKm6Z5fsR
/ekOiDOt+2xI7tX7jf0ZS5rzl8e3ymB297ODnwcMi288yb00kcEwfk1HcLiRrfaG
+PZz1vsytqoTmhj3bM+ML6eG837T5usvCVoPhL2ByCycfeQ+Jl4TmXR1AoGBANxR
N16JsjfppcBDhWQ7HSL9W9YbV0s6VVXEP9JYxiaNYwvQAWjJe1ct0eBCm8LbCgq/
qwVZ18SId/v85mBP/w+tV5pnh3aejZGsrFJh0oezVf/+5311oeGN77e+LIfc7AVe
NikCNFMwwER5hvVa6y4eU5U54y4bzJ21UZhPQMd1AoGAIrHnqDPbiaDjDxTpv1KT
jBF7vX6I5EapFXRMrU+lEOT7N9SW+2D6ghjPDGx9R8exd04xjv0xx0/Jsxok5n2R
StF4jldxcpqQzdAqxnE75oEEpsSFOIQx0Db+aYQCTrEZYqnoFWsA3A+ThgiRBCKH
XdWbvNHCXgJ/TuwCAvUdCDkCgYAdjYtm1AOi+mVwd94xxrgu1Ft4SeyYu7dsrMl+
1selrjuF/x3hR32TASNw+J5aMfWT4Yf4TMfjpgaqN49ThgeJu8/Pd2m1YKlOzCHF
XzfVWhoEH9Y/fwL69YYdWJYyl1DVm4CaWaBZNGXmCYMv8EUxx4Ggt8YgjjwRP5w1
WRQwbQKBgAlj8pPLz3TCOsdgPYldxo7CxO+OJ1eBFlLrtMFK2H75WIp/QYYNcpJ3
PjaGvxOayO9tm1ZCrNACSTs0BbhwWY404z0DOAIzF0ty4X3k06pSMhbiOnbLeEZB
e6nvTbd2aSlmPhUdDhYIaZUk1czEp/P2ORbNN0PRdsaoUZ2JJVEB
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDTjCCAjYCCQDLi/D8hB/ClDANBgkqhkiG9w0BAQUFADBpMQswCQYDVQQGEwJa
WjEWMBQGA1UECAwNVXNlcl9Mb2NhdGlvbjEVMBMGA1UECgwMVXNlcl9Db21wYW55
MQ0wCwYDVQQDDARVc2VyMRwwGgYJKoZIhvcNAQkBFg11c2VyQHVzZXIubmV0MB4X
DTE3MDcwNDA4MzkyM1oXDTI3MDcwMjA4MzkyM1owaTELMAkGA1UEBhMCWloxFjAU
BgNVBAgMDVVzZXJfTG9jYXRpb24xFTATBgNVBAoMDFVzZXJfQ29tcGFueTENMAsG
A1UEAwwEVXNlcjEcMBoGCSqGSIb3DQEJARYNdXNlckB1c2VyLm5ldDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBANsJMMN+UvemmML/Sit0cwAYaVQfUu9K
T0FZl610XNmISqwXxSHyFdf5p9SD6hVVCcisKUiIPQ9/HdEwn0lOWzE+NDqutf1e
IGEM9gFO/an1VENfSA4SauwjKeB6S6vTHK3SfkbNF8svmd0yE3HogJLQOhg8WNph
H1VEz4BrmxGFjqUKgCxATTlnKkYFO50YqW6eX/xJwLmKCxjdw6lmwe815soPWUXQ
kEhUCgevUrrItWzYFvDHOXZhXBV4H1HLm0LlKcp2ke365cXzSMN2/aJ+xJBTOUwg
iE+MA0oM8FtHcadQhxKN0FQP5frUtAKqKGvsqbmeHEeMiHsWAHbpLHkCAwEAATAN
BgkqhkiG9w0BAQUFAAOCAQEAmovxRB7VQaMYTtUI+pmTg1IFLsg8DULXfau7kymr
MPIuYFFLBnYzgeXHsHsHujvgveKhBmAnZIWEWKK2RRkveBqZeb3XCUtohuHTxUl7
72lmHWlkuyWMnQnRsupOwZcxR5cO5uhXzvs1xP2MHzzGa7hBm/ZzxazOOj5s8Ced
7ElbAKt7E5nrOD8yzESqb4uSBonhUuy7/XKdNHcBIBzNYtnTjwOdVLo9srQy4Ka9
Axm3yrInytiF+0mWt+VOiAfWlUX2J1Xmp8VJnM5H1UGh7NZG59qGvGKEx1qcKXxH
rr3DPTV54XCws4eCE9YSvDBCbngd7Ye8cqTd/WT+Qk1P4A==
-----END CERTIFICATE-----
```

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:



Your connection is not private

Attackers might be trying to steal your information from **10.1.1.137** (for example, passwords, messages, or credit cards). Learn more

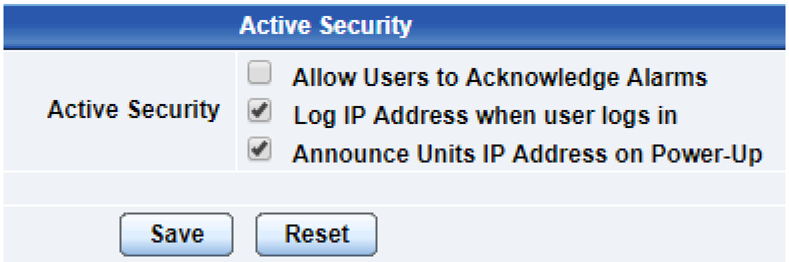
NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

This server could not prove that it is **10.1.1.137**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.1.1.137 (unsafe)

Active Security



Active Security

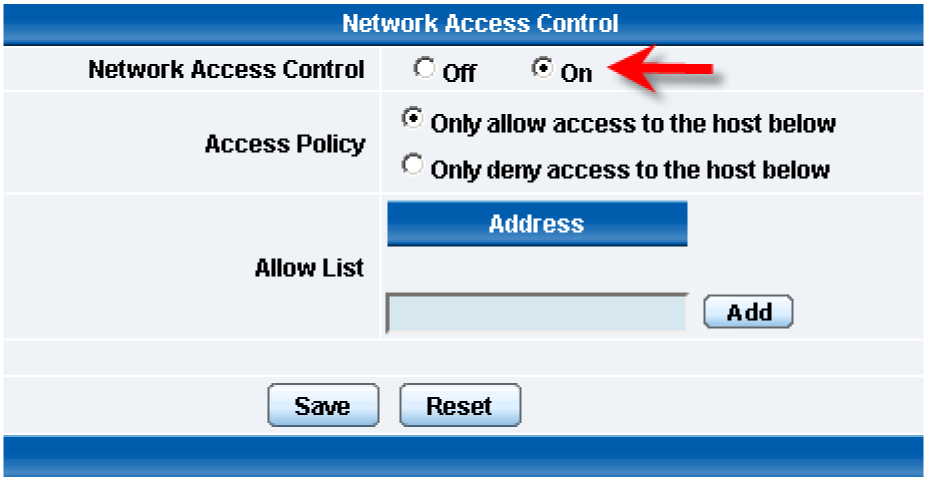
Active Security	☐ Allow Users to Acknowledge Alarms ☑ Log IP Address when user logs in ☑ Announce Units IP Address on Power-Up

In the Active Security section you can allow Users who are logged into the units web interface to “Acknowledge” alarms, which is normally reserved only for the Administrator.

By default, 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.

When the unit boots up, it will announce the IP address that it has been configured with. As an added security feature this announcement can be disabled as in the above screen shot, so that the IP address remains unknown.

The NAC or Network Access Control security feature



Network Access Control

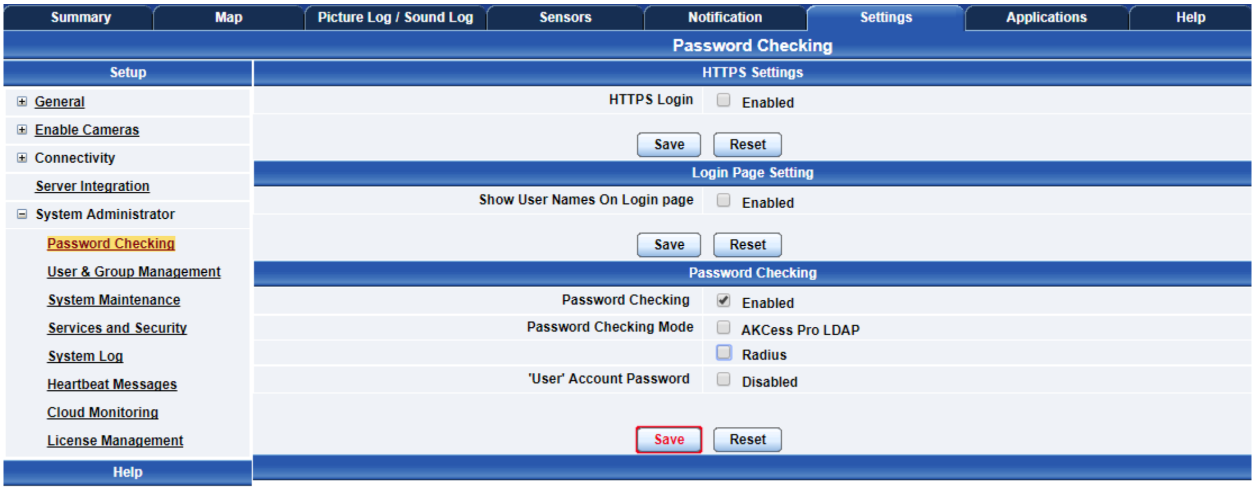
Network Access Control	○ Off ● On
Access Policy	● Only allow access to the host below ○ Only deny access to the host below
Allow List	Address

The NAC or Network Access Control feature allows you to restrict access to the web interface for only certain IP addresses, or deny access to the web interface for only certain IP addresses.
This feature uses the built-in Linux firewall to restrict access.
First select the policy mode between “only allow” or “only deny”, and add the IP addresses or host names to the list one by one, then click Save.

Multi-Users and Groups on the secuirtyProbe 5E

The securityProbe-5E has multi user and group login and access restriction capability built into the web interface.
This allows you to create groups with access to certain features on the securityProbe and securityProbe 5E, or groups of users with only the access you choose those users to have access to within the securityProbe's web interface.
This feature also allows you to create multiple users other than just having a single user and admin web interface login.

To be able to use this feature, first you need to enable **Password Checking** under **Settings / System Administrator**:



Password Checking

HTTPS Settings

HTTPS Login □ Enabled

Login Page Setting

Show User Names On Login page □ Enabled

Password Checking

Password Checking ☑ Enabled

Password Checking Mode □ AKCess Pro LDAP

□ Radius

'User' Account Password □ Disabled

You can also choose to disable the password checking for the built-in "User" account but keep the Admin account password protected.

LDAP and RADIUS password checking methods are also available; these features have their own separate manuals.

It's recommended to enable the HTTPS Login option, so that a secure page will be used for the login processing and by the unit's Web UI. This needs to be enabled separately in addition to the Password Checking option.

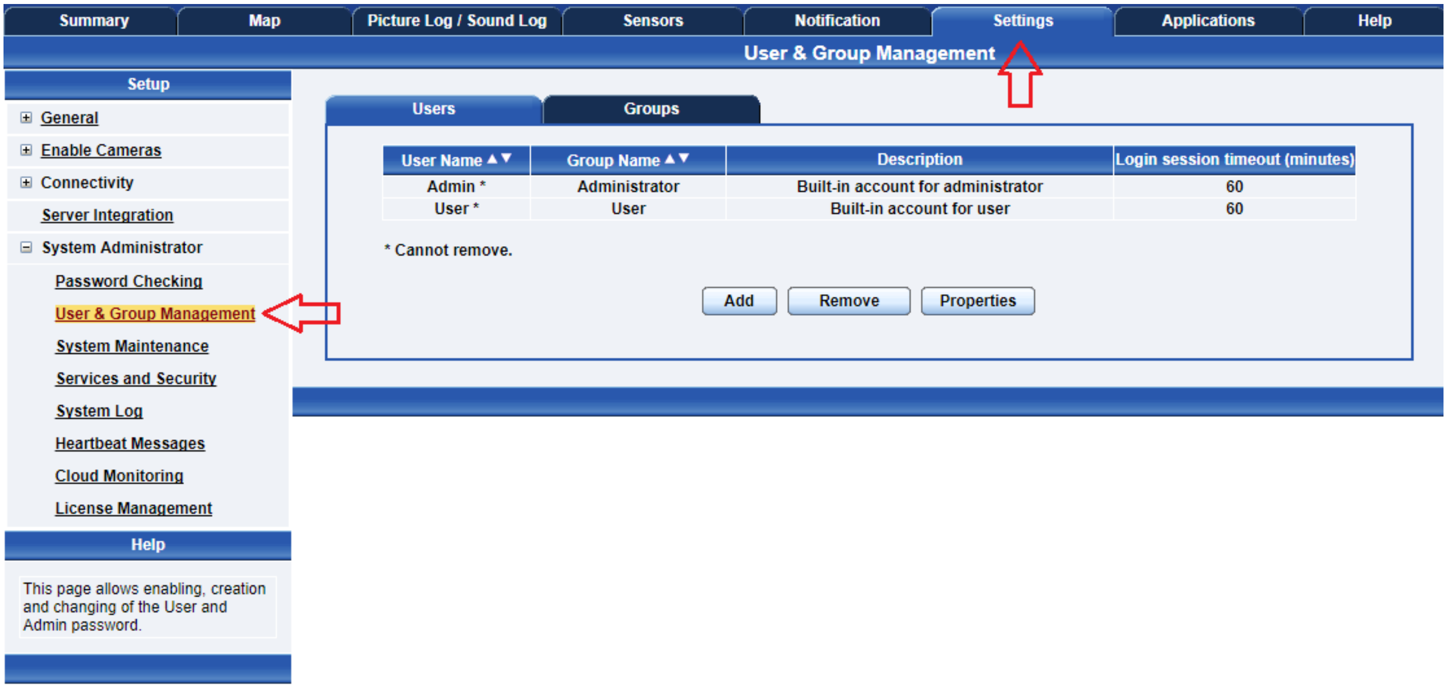
Optionally you can enable to show all user account names on the login page. Without this, the authorized users must know the account names to be able to log in.

Multi-users and groups setup

Log in to the securityProbe or securityProbe 5E with the Admin user and the Administrator password. The default will be “public” if you have not changed this yet (an additional security popup warning will ask you if you want to change it).
Click on the Settings page, then System Administrator then User & Group Management as shown in the screen shot below:

Note: *The following screen shots may appear small and hard to read. Please use the zoom feature in your pdf reader program to increase the size of the page to better view these screen shots.*

1. Group Setup



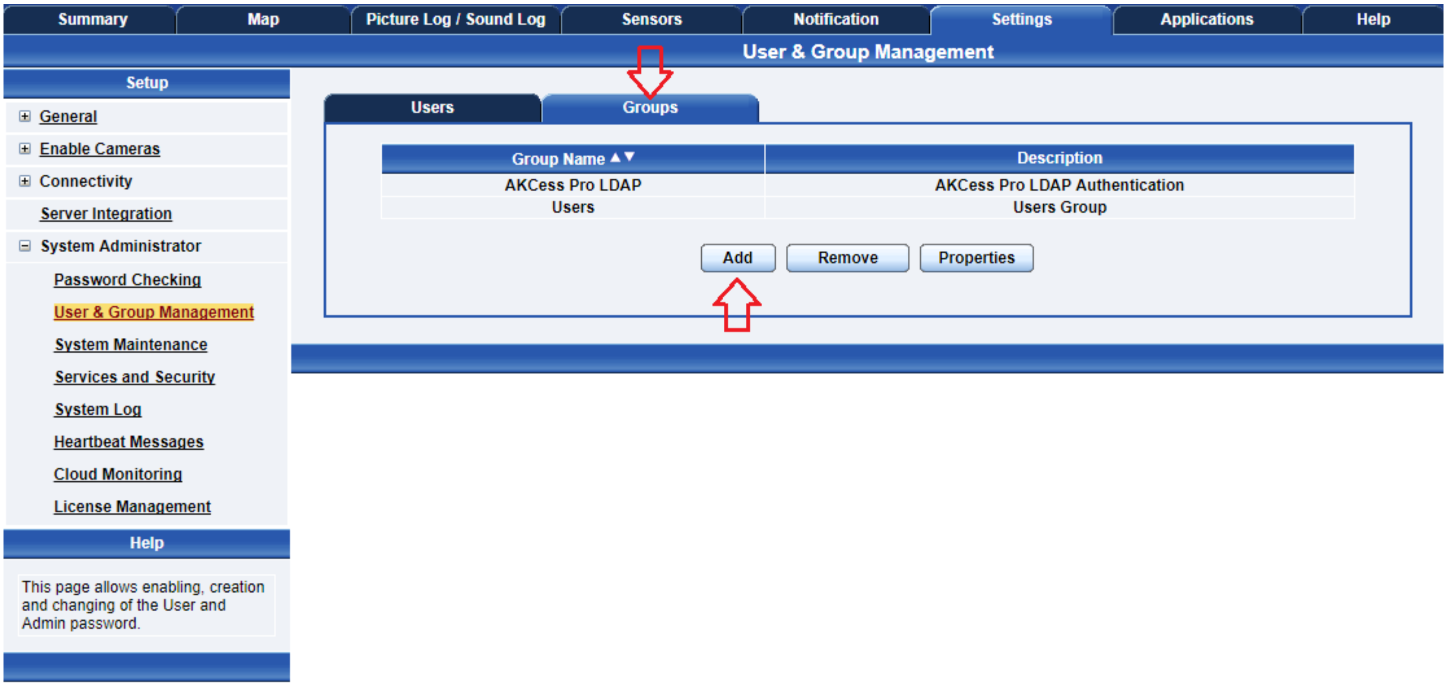
User Name ▲▼	Group Name ▲▼	Description	Login session timeout (minutes)
Admin *	Administrator	Built-in account for administrator	60
User *	User	Built-in account for user	60

* Cannot remove.

This page allows enabling, creation and changing of the User and Admin password.

(continued on next page)

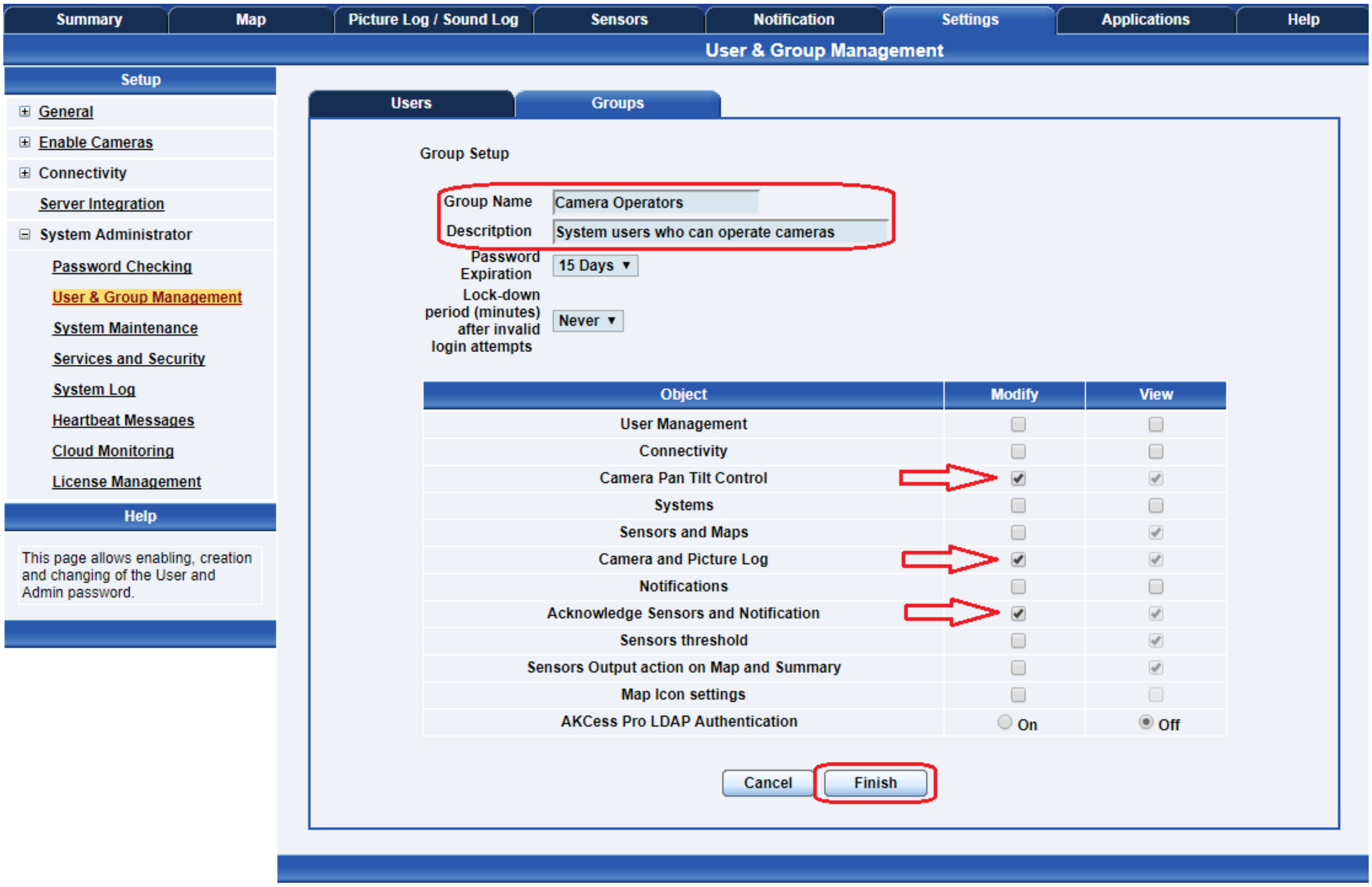
A) Now click on the “Groups” tab that will take you to the Groups page



Group Name ▲▼	Description
AKCess Pro LDAP	AKCess Pro LDAP Authentication
Users	Users Group

This page allows enabling, creation and changing of the User and Admin password.

B) Now click on the “Add” button to add your groups as shown in the screen shot above.



This page allows enabling, creation and changing of the User and Admin password.

Group Setup

Group Name: Camera Operators

Description: System users who can operate cameras

Password Expiration: 15 Days ▼

Lock-down period (minutes) after invalid login attempts: Never ▼

Object	Modify	View
User Management	☐	☐
Connectivity	☐	☐
Camera Pan Tilt Control	☑	☑
Systems	☐	☐
Sensors and Maps	☐	☑
Camera and Picture Log	☑	☑
Notifications	☐	☐
Acknowledge Sensors and Notification	☑	☑
Sensors threshold	☐	☑
Sensors Output action on Map and Summary	☐	☑
Map Icon settings	☐	☐
AKCess Pro LDAP Authentication	○ On	● Off

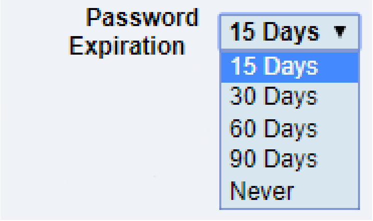
C) Enter your group name for example we have added a group named “Camera Operators” and entered our description.

You may specify the Password Security options for a group (see below).

Now check the objects within the web interface that this group will be able to Modify and View. Then click the “Finish” button to save your group.

Password Security options

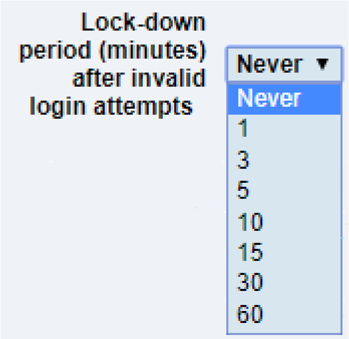
You can specify password expiration and lockdown periods for the user accounts on a per-group basis.



Password Expiration ▼ 15 Days

You can specify password expiration between every 15 and 90 days for all account types.
If you don’t want the password to automatically expire, set it to “never”.

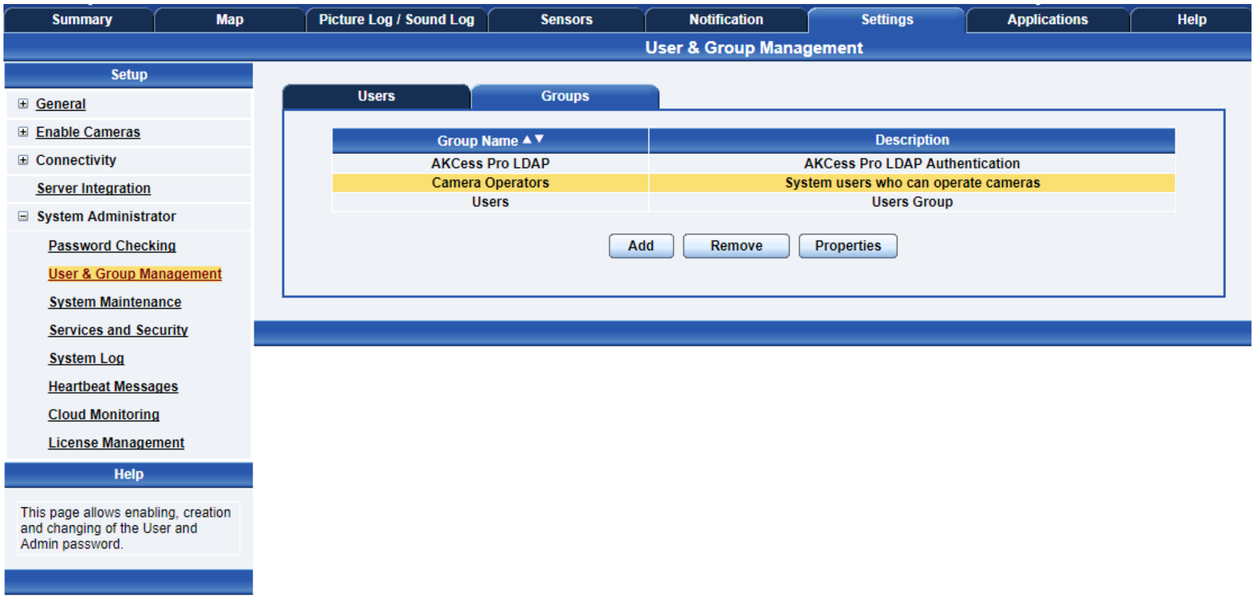
You’ll get a notification upon login when the password has expired, and will be asked to change it.
Another notification will be shown if you’re still using the default Admin password “public”.
It’s advised to change the password when asked, but you can still proceed without changing.



Lock-down period (minutes) after invalid login attempts ▼ Never

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.

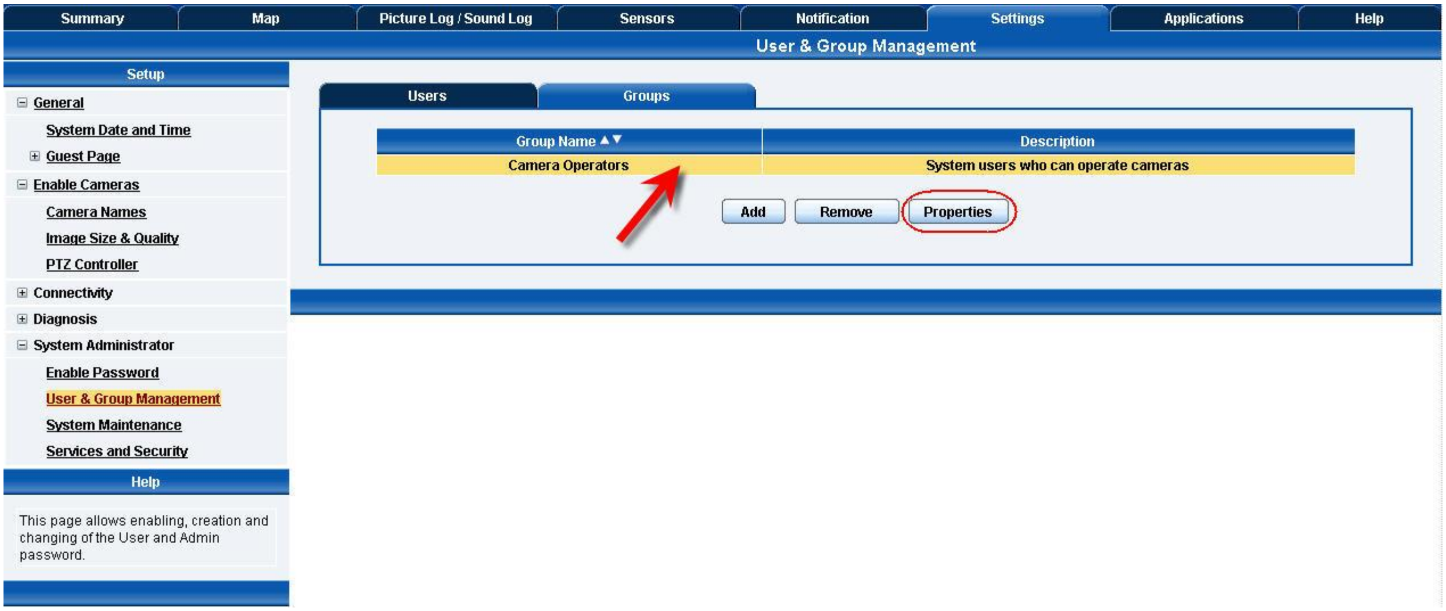
Note that for the Admin user, you can’t select “indefinitely” as this would prevent you from logging in to the Web UI if it has locked itself.



Group Name ▲▼	Description
AKCess Pro LDAP	AKCess Pro LDAP Authentication
Camera Operators	System users who can operate cameras
Users	Users Group

This page allows enabling, creation and changing of the User and Admin password.

D) Now you can see the new group “Camera Operators” has been added to our group list as shown in the screen shot above.

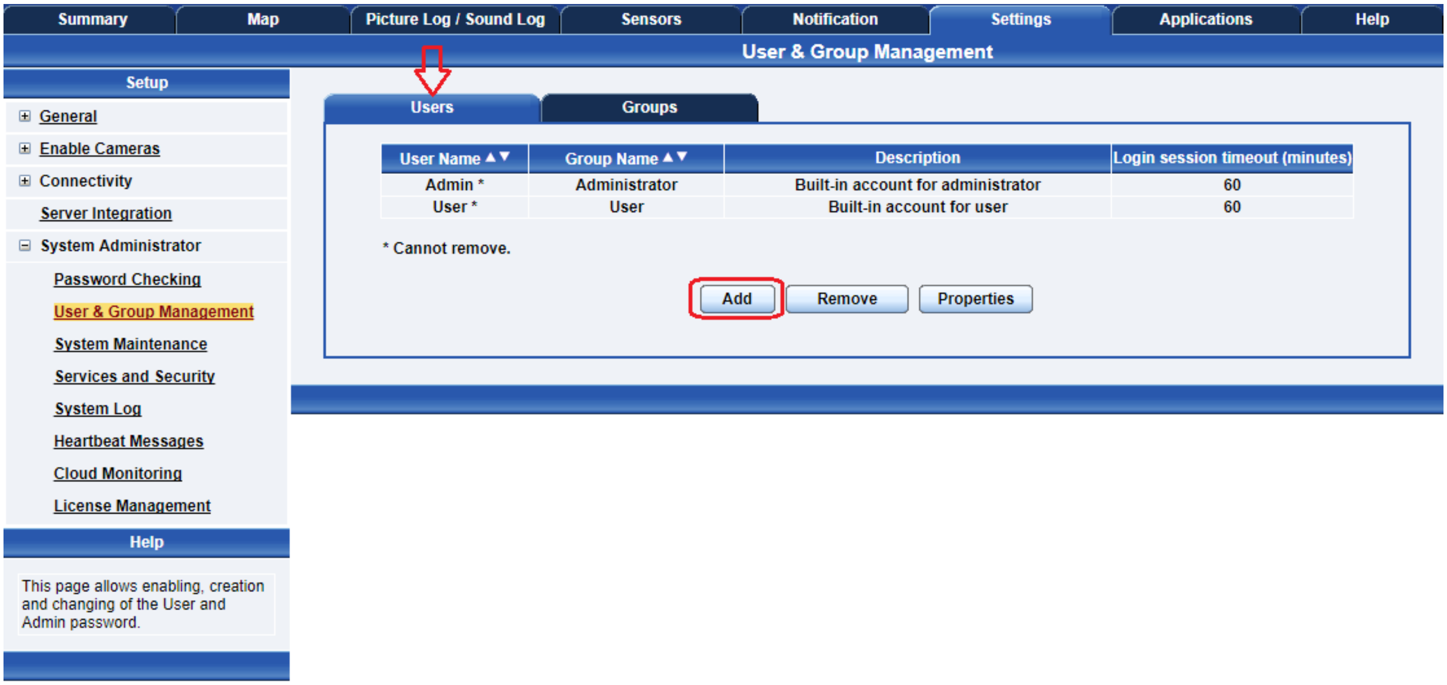


Group Name ▲▼	Description
Camera Operators	System users who can operate cameras

This page allows enabling, creation and changing of the User and Admin password.

E) If you wish to modify your group settings, highlight the group you wish to modify by clicking on it, then click on the “Properties” button as shown in the screen shot above.

2. User Setup

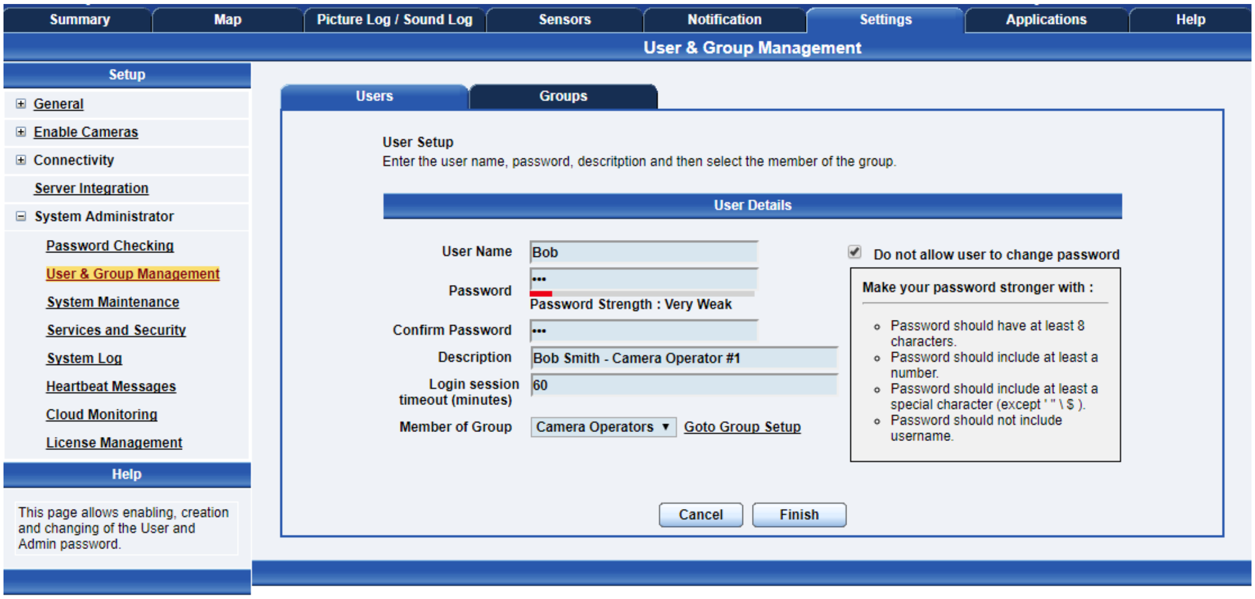


User Name ▲▼	Group Name ▲▼	Description	Login session timeout (minutes)
Admin *	Administrator	Built-in account for administrator	60
User *	User	Built-in account for user	60

* Cannot remove.

This page allows enabling, creation and changing of the User and Admin password.

A) Click on the Users tab then click the “Add” button to add the new Users to your groups as shown above.



User & Group Management

This page allows enabling, creation and changing of the User and Admin password.

User Setup

Enter the user name, password, descritption and then select the member of the group.

User Details

User Name	Bob
Password	••• Password Strength : Very Weak
Confirm Password	•••
Description	Bob Smith - Camera Operator #1
Login session timeout (minutes)	60
Member of Group	Camera Operators ▾

☑ Do not allow user to change password

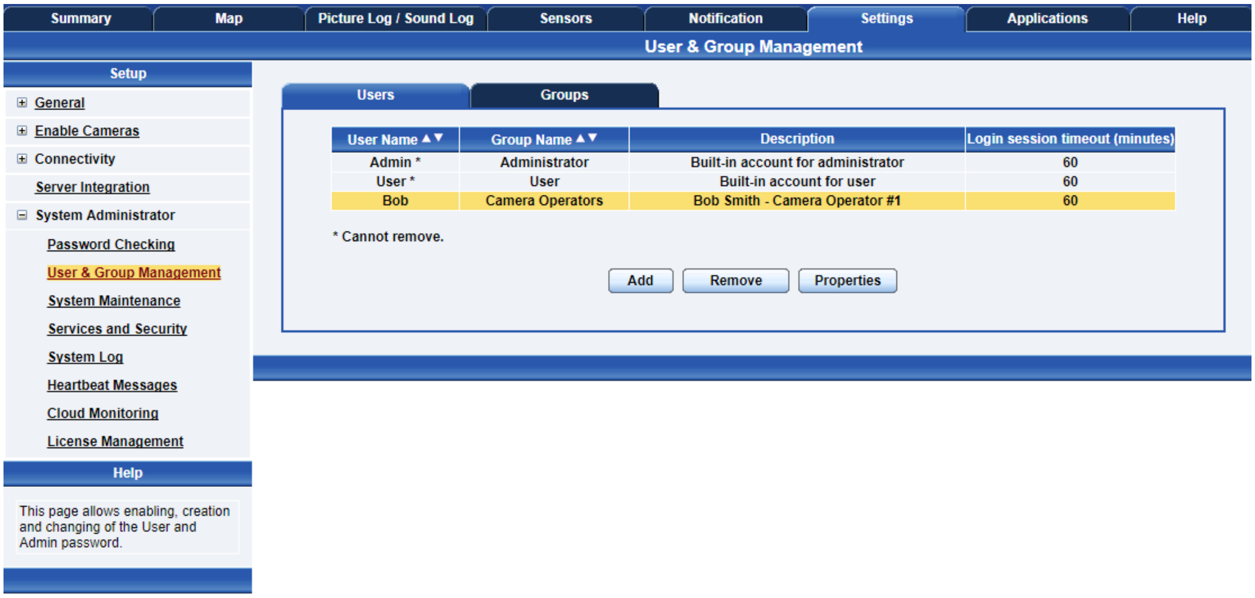
Make your password stronger with :

- Password should have at least 8 characters.
- Password should include at least a number.
- Password should include at least a special character (except ' " \ $).
- Password should not include username.

B) Now enter your User details as shown above. In our example we have entered Bob Smith as our camera operator #1 into our “Camera Operators” group. We have also added the option so that this user cannot change his login password.
You can also specify a custom login session timeout in minutes, after which the user will be automatically logged off when there’s no activity.

A password strength meter is helping you to choose a strong password. You can find additional tips for increasing the strength of your password in the text box on the right.

After addition your users for each group click the “Finish” button to save each user.

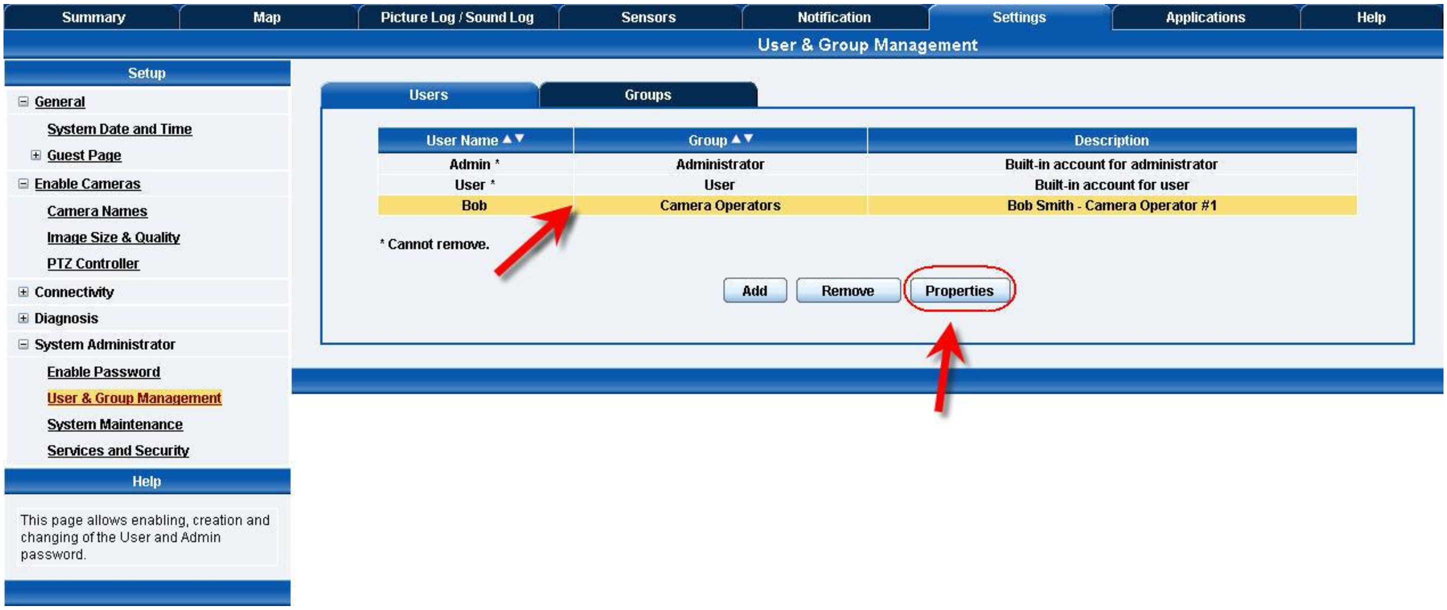


User Name ▲▼	Group Name ▲▼	Description	Login session timeout (minutes)
Admin *	Administrator	Built-in account for administrator	60
User *	User	Built-in account for user	60
Bob	Camera Operators	Bob Smith - Camera Operator #1	60

* Cannot remove.

This page allows enabling, creation and changing of the User and Admin password.

C) Now as you can see the new user has been entered into our list of Users.



User Name ▲▼	Group ▲▼	Description
Admin *	Administrator	Built-in account for administrator
User *	User	Built-in account for user
Bob	Camera Operators	Bob Smith - Camera Operator #1

* Cannot remove.

This page allows enabling, creation and changing of the User and Admin password.

D) To modify a user's setting, first highlight the user by clicking on it, then click the "Properties" button as shown in the screen shoot above.

Troubleshooting

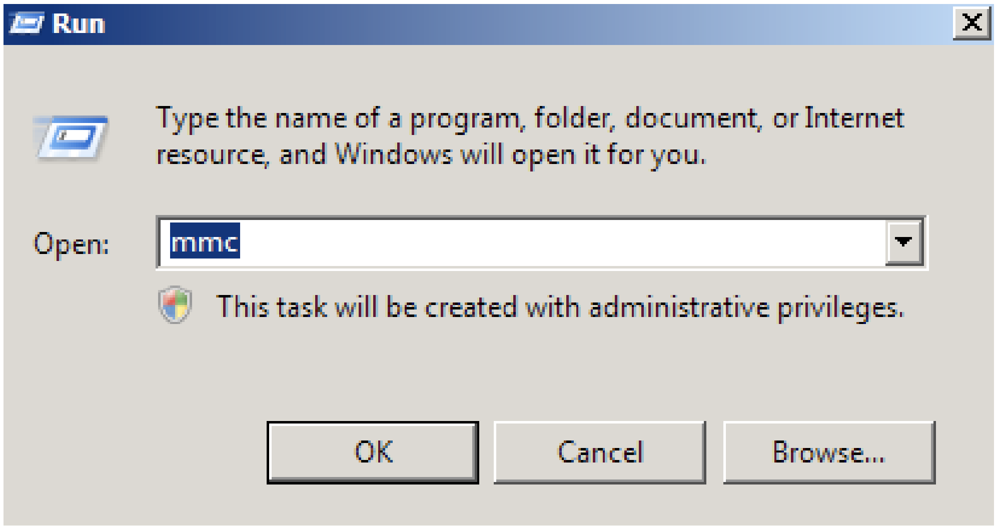
How to generate a proper .PEM file from a Windows CA

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:

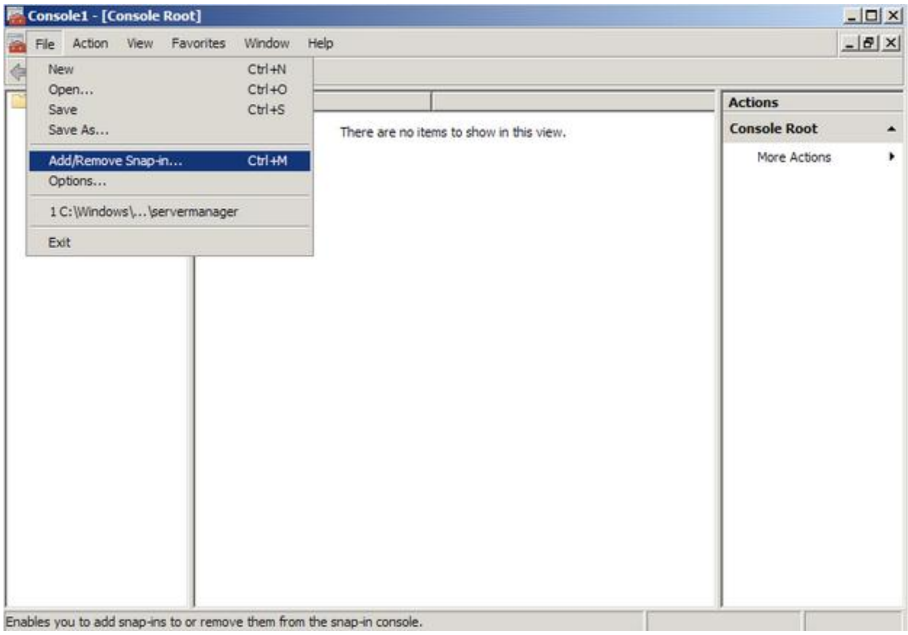
Step 1: Create an MMC Snap-in for Managing Certificates on the first Windows system where the SSL certificate is installed.

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


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
This task will be created with administrative privileges.
OK
Cancel
Browse...

mmc

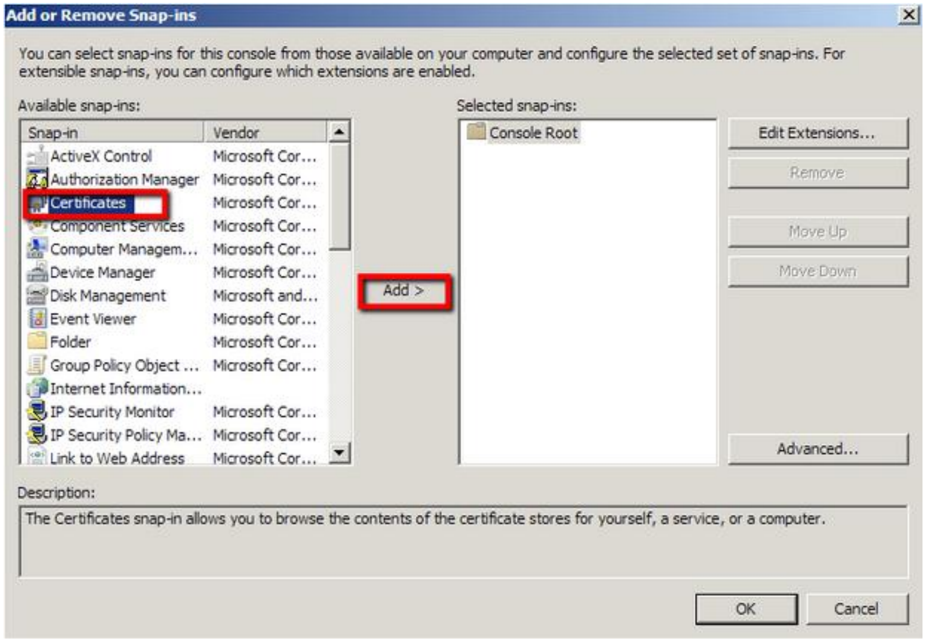
2. Go into the Console Tab > **File** > **Add/Remove Snap-in.**



There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

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



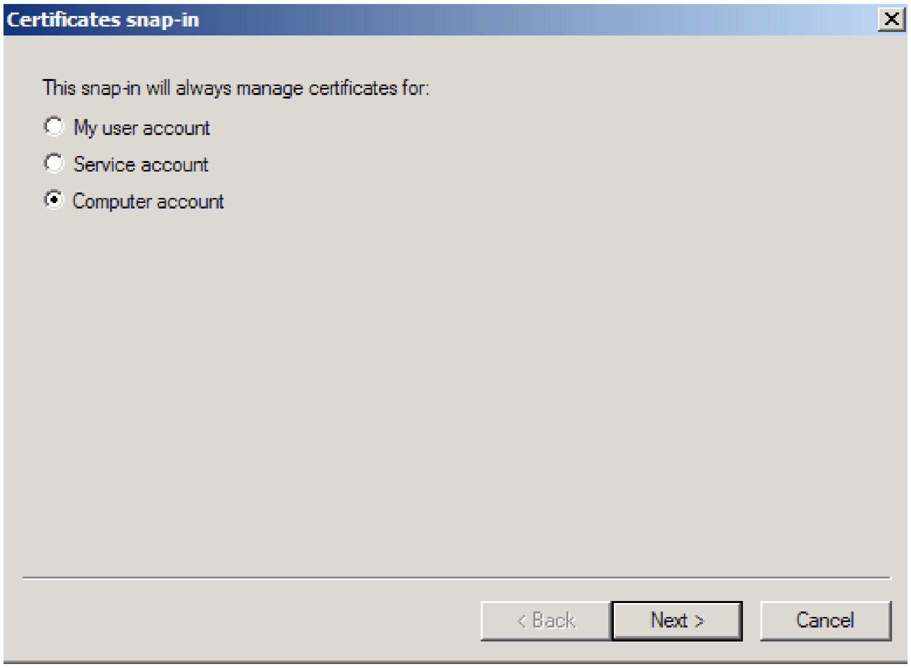
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Information...	
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

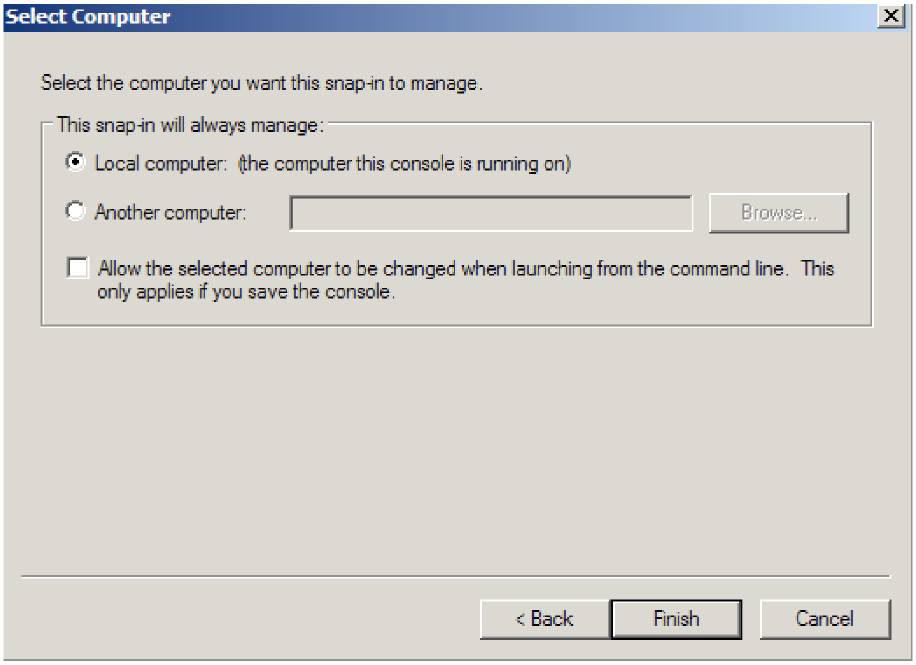
4. Choose **Computer Account > Next.**



This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

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



Select the computer you want this snap-in to manage.

This snap-in will always manage:

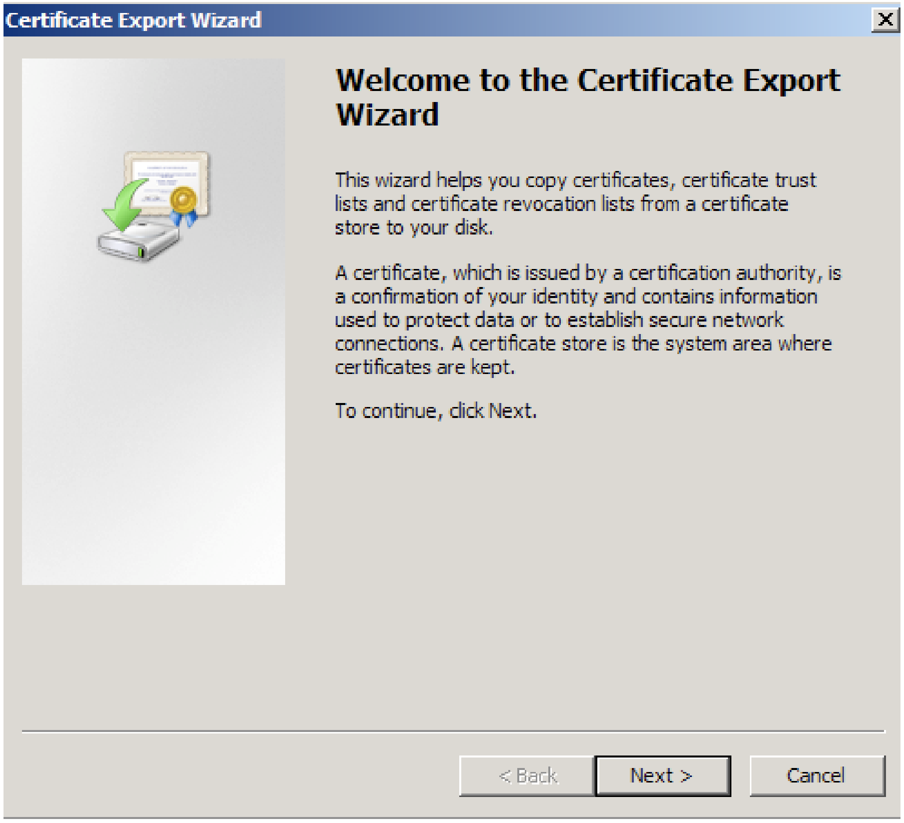
● Local computer: (the computer this console is running on)
○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

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.



Certificate Export Wizard

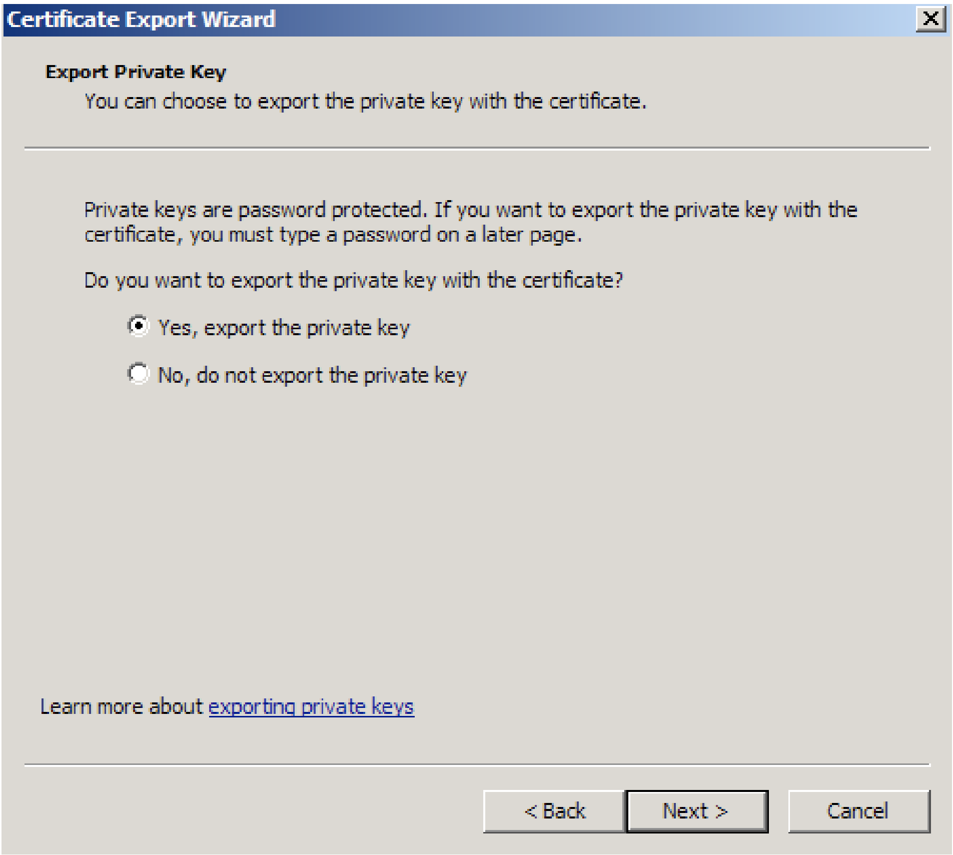
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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



Certificate Export Wizard

Export Private Key

You 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.

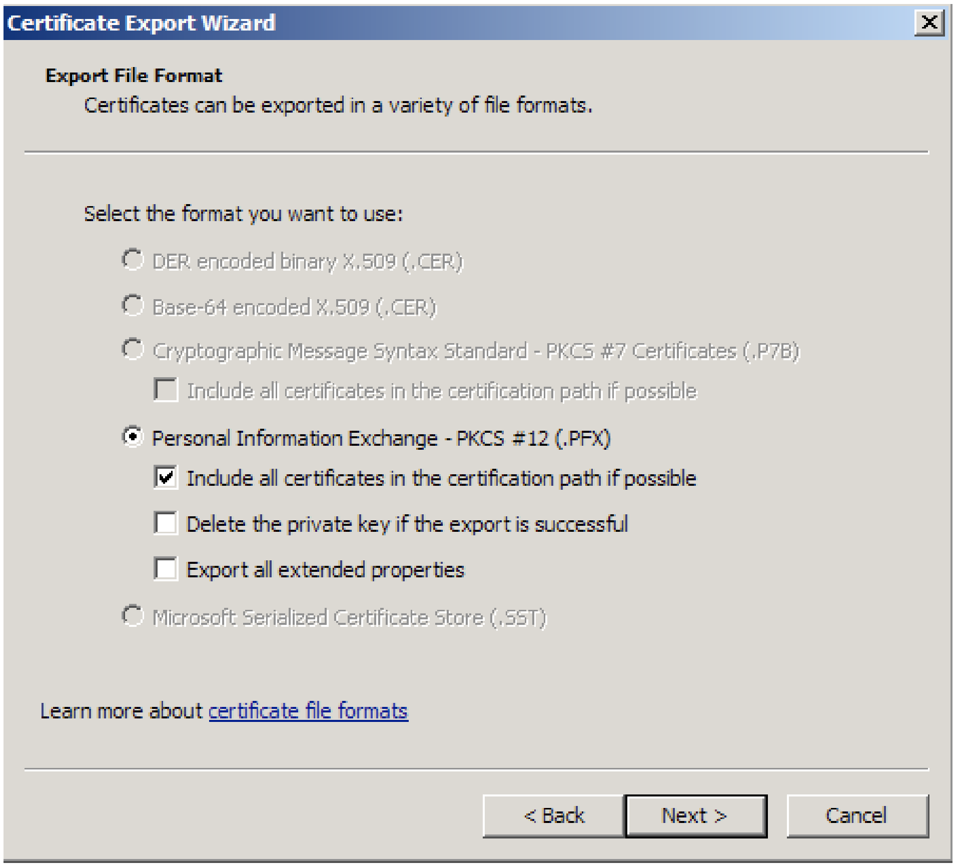
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Learn more about exporting private keys

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



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ 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

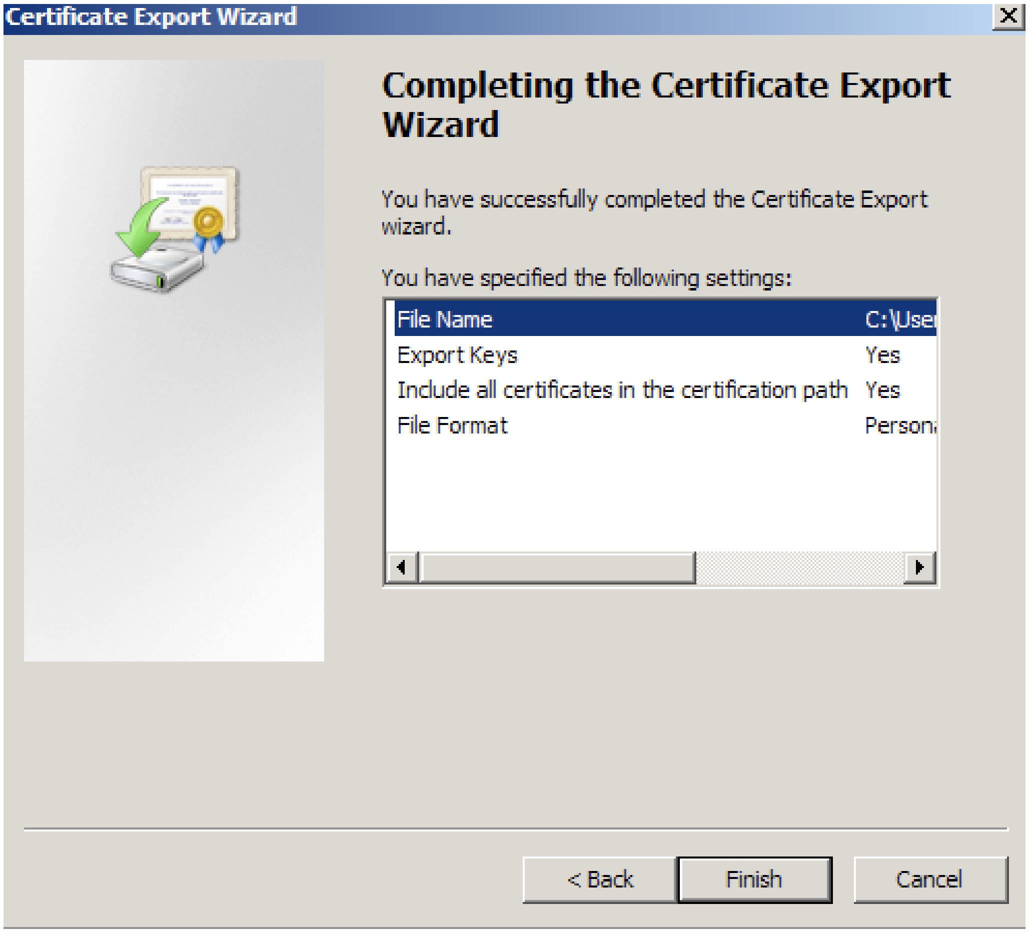
□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

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

9. Click **Finish.**



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\User
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Person

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:

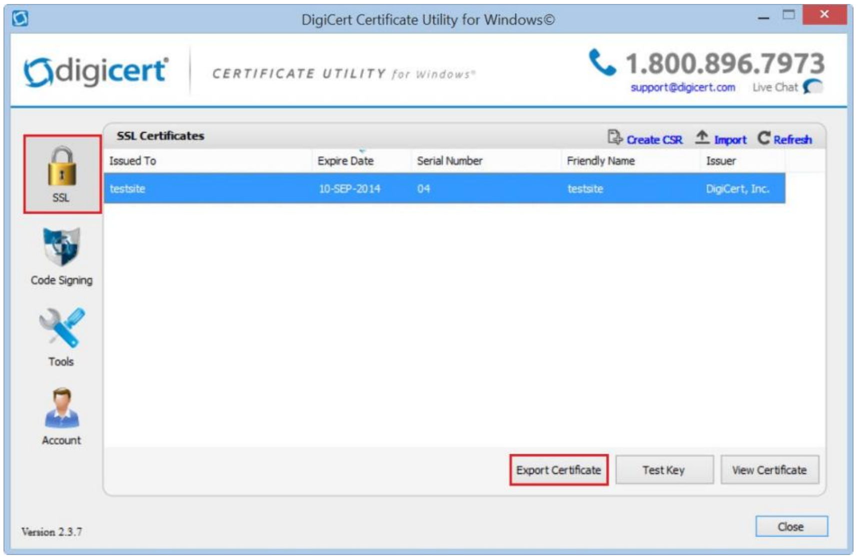
```
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.pem
```

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



Issued To	Expire Date	Serial Number	Friendly Name	Issuer
testsite	10-SEP-2014	04	testsite	DigiCert, Inc.

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

How to troubleshoot a failed Web UI on the SEC

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
```

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

Thanks for Choosing AKCess Pro!