

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

= AKCP SP	2+	
System	Services	
🛱 Date/Time	System / Services	
	Web Interface	
Modem	Web Interface (HTTP)	💿 Enable 🔘 Disable
VPN	HTTP Port	80
SMTP	Secure Web Interface (HTTPS)	Enable Disable
		Use as Default
Nodbus	HTTPS Port	443
A Server Integration	Upload Certificate File	Choose file
Services		Save Cancel
Password Checking		Save
Se Maintenance		
Heartbeat Messages		
E License Management		
i About		
Get SNMP OID		

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-r	new.crt	Choose file
	Please selec	t 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):

📔 use	rkey.pem - Notepad++	_		x
File E	dit Search View Encoding Language Settings Macro Run Plugins Window ?			х
1	REGIN RSA PRIVATE KEV			
2	MTTFnuTBABKCACFA2vksva35596aYvv9KK38z4BhnV/89570nPOVmXrX8c2YhKrBfF			
3	1 TFTV1/ma1TPaFV11vKwpSTg9D38dd7Tf51/5hMT400a61/V4g9V0z2A1/29afV1019T			
4	Dh1a7(Mn4Hn)a9(Mch1)+B50(X)v+73TTTce1AktA6(DxY2)mFfV(ITP6(u)FY)(000a			
5	LEBNOWcgReU7nRipbp5f/EnAuYoLGN3DgWb87zXmvg9ZRdCOSFOKB69Susi1bNeW			
6	8Mc5dmFcFXgfUcub0uUpynaR7fr1xfNIw3b9on7EkFM5TCCIT4wDSgzwW0dxp1CH			
7	Eo3QVA/1+tŠØAgooa+ypuZ4cR4yIexYAdukseQIDAQABAoIBAQCF6t+S1viZC5WY			
8	m0c4vFDXfRVg5mnpfbBpTyKqXVurc6XfRAU2FPIAA1b2WtTSyBRcSc5P12Q1x11v			
9	md+SjRu6RsLeIhWI3HTFgYwjDq20rT0g1+/REremunUPFxa071s5d1nXZeunQeo7			
10	0DMNUM7TdFYgnTzh/8GNe622YZQEqFZXbcXBoLnfS/NVnMQ8UmxB+7prRhPAI4cA			
11	v5hmcNJsFoxØWdn1c36wY9pvEkYoHdd35cA8dOJ/5kVY3mxSS4HzrLhUwUnid3x5			
12	RsVH0IHI0YEckmVBkoZRdlMCwL/400z6wjdBXOaKW9aj2BtxUPKxIfRx/WsUcJTX			
13	c+vLibrRAoGBAP6C2M252J0nZB5CKJTmAa4xKm/RazD8iwkJhF98fH2uKm6Z5fsR			
14	/ekOiDOt+2xI7tX7jf0ZS5rzl8e3ymB297ODnwcMi288yb00kcEwfk1HcLiRrfaG			
15	+PZz1vsytqoTmhj3bM+ML6eG837T5usvCVoPhL2ByCycfeQ+J14TmXR1AoGBANxR			
16	N16JsjfppcBDhWQ7HSL9W9YbV0s6VVXEP9JYxiaNYwvQAWjJe1ct0eBCm8LbCgq/			
17	qwV218SId/v85mBP/w+tV5pnh3aejZGsrFJh0oezVt/+5311oeGN77e+L1tc7AVe			
18	NikCNFMwVERShvVa6y4eUSU54y4bzJ21UZhPQMdIAoGAIrHnqDPb1aDjDxTpv1KT			
19]BF/VX615EapFXRMCU+1E01/N95W+205gn]PUGX9K8eXd04X;V0Xx00/JSX0K5n2K			
20	Str4]IdxCpd(zdAqxne/SocepsSF012x800FarQLiFeZrqnoFwSASAFing2x80KN			
21	Auwownexp3/Tuweavouedexp3fau)Tumavotniwuodexxf801Fed3v9/Vd3r41F			
22	Isel jur/sinszinszinsmissian witerienni jpgawesingesuo/reamitriozenn			
23	AZI WWWWICHIST/ WEDSTRUWSTYILDWWHCAWADZWCAWECHINEROU ZOUGAZUSTEJWA WDDwhoWRAJ13KBJ 37COGADVI dva ZVCALOTIARETI + MEKY2HZSWITA / OVVMcaji			
24	mnownowngmijoprezoicosogritaaancearooiteoitei ein een osanowny ymmegoo Disgwydswijceniacste ABhuwhwarshand i referydskaacsMbhidabi eE78			
26	F Jadvaou jo za			
27				
28	BEGIN CERTIFICATE			
29	MIIDTiCCAiYCCODLi/D8hB/ClDANBgkqhkiG9w0BAQUFADBpMOswCOYDVOOGEwJa			
30	WjEWMBQGAIUECAwNVXNlcl9Mb2NhdGlvbjEVMBMGAIUECgwMVXNlcl9Db21wYW55			
31	MQ0wCwYDVQQDDARVc2VyMRwwGgYJKoZIhvcNAQkBFg11c2VyQHVzZXIubmV0MB4X			
32	DTE3MDcwNDA4MzkyM1oXDTI3MDcwMjA4MzkyM1owaTELMAkGA1UEBhMCWloxFjAU			
33	BgNVBAgMDVVzZXJfTG9jYXRpb24xFTATBgNVBAoMDFVzZXJfQ29tcGFueTENMAsG			
34	A1UEAwwEVXNlcjEcMBoGCSqGSIb3DQEJARYNdXNlckB1c2VyLm5ldDCCASIwDQYJ			
35	KoZIhvcNAQEBBQADggEPADCCAQoCggEBANsJMMN+UvemmML/Sit0cwAYaVQfUu9K			
36	TØFZI610XNmISqwXxSHyFd+5p9SD6hVVCcisKUiIPQ9/HdEwn010WzE+NDqutf1e			
37	IgeN9gF0/an1VENFSA4SauwjKe86S6VTHK3S5HbNF8svmd0yE3HogJLQOhg8NNph			
38	H1VEz4BrmxGFjqUKgCxATTInKkYF050YqW6EX/xJwLmKCxjdw6Imwe815soPWUXQ			
39	KENDCBEVURFILWZFVURFULFULFULFULFULFULFULFULFULFULFULFULFULF			
40	1EthiadoniorthcadQinxkivorQPSTTUTARQkQVSqDmenEeniInswahDpLnkCAwcAATAN			
41	bgrquiktuswobaçor AaccAgcAutovikto/vgani touripini gari tesgobocki du/kyimi MDTuvFeT Bnvzagviktelehui yungekheman 7711FBW/200Pb/geBazeha YC/Ithahuitzvil 7			
43	721mH/Libri Zeckistand yeyekitollaktiziki kwkzkkwycodzeoszcionant asis			
44	ZE IDAKYZENTORWZESODAU SBONDU WZ / XKONIE BTBZNYTNT WODYL OSFOV4Ka9			
45	Axm3vrInvtiF+0mWt+V0iAfW1UX2J1Xmp8VJnM5H1UGh7NZG59aGvGKEx1acKXxH			
46	rr3DPTV54XCws4eCE9YSvDBCbngd7Ye8cgTd/WT+Qk1P4A==			
47	END CERTIFICATE			
48				× 1
Normal	text file length : 2,884 lines : 48 Ln : 1 Col : 1 Sel : 0 0 Unix (LF) UTF-	8	IN	IS 🔡



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:

🦉 This site isn't secure - Internet Explorer	-	• X
← → Ø https://10.1.1.146/	,Q →	ት 🛪 🛱 😃
S This site isn't secure X C C		
This site is not secure		
This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.		
Close this tab		
Your PC doesn't trust this website's security certificate. The hostname in the website's security certificate differs from the website you are trying to visit.		
Error Code: DLG_FLAGS_INVALID_CA DLG_FLAGS_SEC_CERT_CN_INVALID		
🥸 Go on to the webpage (not recommended)		
e In	ternet Protected Mode: On	🔍 100% 🔻



SNMPv3

= AKCP SF	2+	
System	SNMPv3	
😋 General		
🏙 Date/Time	SNMPv3	Enable Disable
👬 Network	SNMPv3 Mode	Authentication & Privacy
奈 Modem	SNMPv3 engineID	АКСР
VPN		engineID parse: 80001F8804414B4350
SMTP	SNMPv3 Username	admin
	Access Privilege	Read Only •
Nodbus 🗧	Authentication Protocol	
Server Integration		ЗПА
a Services	SNMPv3 Pass Phrase	SNMPv3 Pass Phrase
Password Checking	Confirm SNMPv3 Pass Phrase	Confirm SNMPv3 Pass Phra
Se Maintenance	Privacy Protocol	
Heartbeat Messages	, may Protocol	AES
License Management	Privacy Protocol Pass Phrase	Privacy Protocol Pass Phras
i About	Confirm Privacy Protocol Pass Phrase	Confirm Privacy Protocol Pa
Get SNMP OID		
		Save

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

= AKCP SP	2+
System Ø [®] General Date/Time	Password Checking System / Password Checking
👬 Network	Password Checking On Off
VPN	'Viewer' Account Password Required On Off Show User Names on Login Page On Off On

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

SP2+
Username
Admin
Password
LOG IN
Copyright 2017 AKCP All Rights Reserved



Password Security options

= AKCP SP	2+	
System	Password Security	
🔅 General		
🛗 Date/Time	Admin Password	Admin Password
👬 Network	Confirm Admin Password	Confirm Admin Password
奈 Modem	Password Expiration	00 Davia
VPN	rassing Explication	SO Days
SMTP	Lock-down period after invalid login attempts	5 Minutes
₩ SNMP		
Server Integration	User Password	User Password
a Services	Confirm User Password	Confirm User Password
🏃 Modbus		
Password Checking	Password Expiration	90 Days
Se Maintenance	Lock-down period after invalid login attempts	5 Minutes
Heartbeat Messages		
📰 License Management		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	User Password
Confirm User Password	Confirm User Password
Password Expiration	90 Days
Lock-down period after invalid login attempts	5 Minutes 🔹
	None
	1 Minute
	3 Minutes
	5 Minutes
	10 Minutes
Viewer Password	15 Minutes
	30 Minutes
	60 Minutes
Confirm Viewer Password	90 Minutes
	Indefinitely
Password Expiration	90 Days 🔹

A Error!

The username or password is incorrect.

A Error!

The username or password is incorrect.

A Error!

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

A Error!

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

Username User

.
.
LOG IN

Copyright 2017 | AKCP | All Rights Reserved

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:

Unlock User Account



Password Expiration

Viewer Password	Viewer Password
Confirm Viewer Password	Confirm Viewer Password
Password Expiration	90 Days
Lock-down period after invalid login attempts	15 Days 30 Days 60 Days
	90 Days
	Unlock Viewer Account

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.

≡ Menu [≡]	■ <i>AKCP</i> SP2+				
🛓 Summary	Users Access Control / Users			Q Search	
Access Control A	↑ First Name	↑ Last Name	Group	Card ID	
Users	Admin	Admin	(None)	-	
Groups	oL	oL	(None)	-	
S Time Schedules	mot	mot	(None)	-	
📅 Holiday					
a Sensors					
🖻 Events 🗸					
Notifications ¥					
Settings					

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



Server Integration

= AKCP SF	2+		
System © General	Server Integration System / Server Integration		
击 Network	Server Integration	Enable Disable Disable	
奈 Modem	Server Address	0.0.0.0	
VPN	Server Integration Port	5000	
SMTP	Send Keep Alive Every	1 Minutes •	
	Server Access Control Sync	Enable Disable Disable	
Server Integration		Save	
Services		Caller	

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
ver Access Control Sync	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

= AKCP SP	2+		
System Ø g General	VPN System / VPN		
🛗 Date/Time	1 This feature has no license. To request a license cli	ok here.	×
奈 Modem	VPN	Enable Disable	
S VPN	Status	Not Connected	
SMTP SMTP	IP Address	0.0.0.0	
➡ SNMP ✓ Server Integration	VPN Server Port	1194	
Services	VPN Password	Password	
 Modbus Heartbeat Messages 	Confirm VPN Password	Confirm VPN Password	
i About	VPN Encrypt Method	Blowfish	
Get SNMP OID			

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.

VPN Encrypt Method	Blowfish •
	None
	Blowfish
	AES
	Triple DES

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 <u>https://www.sslsupportdesk.com/export-ssl-certificate-private-key-pfx-using-mmc-windows/</u>)

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



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

Console1 - [Console Root]				
File Action View Favorites	Window H	Help		_ 8 ×
Mew Open	CR1+0 CR1+0		Actions	
Save As	CUITS	There are no items to show in this view.	Console Root	-
Add/Remove Snap-in	Ctrl+M		More Actions	,
1 C:\Windows\\servermanage	r			
Exit				
nables you to add enancies to or remov	e them from t	the snan-in console		

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

lap-in	Vendor		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor		The second state states a	
Authorization Manager	Microsoft Cor			Remove
Certificates	Microsoft Cor			
Component Services	Microsoft Cor			Move Up
Computer Managem	Microsoft Cor	_		100000 BB
Device Manager	Microsoft Cor			Move Down
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	•		Advanced
eccletion:				
scriptori.				
IP Security Honiton	Microsoft Cor Microsoft Cor	<u>.</u>		Advanced.



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

Certificates snap-in	X
This snap-in will always manage certificates for:	
O My user account	
C Service account	
Computer account	
Const. Next . Consel	

5. Choose Local Computer > Finish.

Select Computer	×
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)	
C Another computer: Browse	
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

- 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		X
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.	X
	< Back Next > Cancel	



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

ertificate 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	
O No, do not export the private key	
Learn more about <u>exporting private keys</u>	
Z Rady Movt 2 Car	acel
< DALK NEXT > Car	icei



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.

Certificate Export Wizard		×
	Completing the Certificate E Wizard	xport
	You have successfully completed the Certificate wizard.	Export
	You have specified the following settings:	
	File Name	C:\Use
	Export Keys	Yes
	Include all certificates in the certification path	Yes
	File Format	Personi
	< Back Finish	Cancel

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+certif icate/

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

۵			DigiCert Certific	cate Utility for W	lindows©	- 🗆 🗡	
Ødig	icerť	CERTIFICATE UTILITY for Windows®			Supported	Live Chat	
0	SSL Certificat	tes	Fueire Date	Casial Mumber	Create CSR	▲ Import C Refresh	
E C	testsite		10-SEP-2014	04	testsite	DigiCert, Inc.	
Code Signing							
					Export Certificate Test Key	View Certificate	
Version 2.3.7						Close	

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 <u>support@akcp.com</u> if you have any further technical questions or problems.

Thanks for Choosing AKCess Pro!