Securing SpaceLogic C-Bus Automation Controllers

Configuration Guide

Generation of SSL Certificates for secure authenticated access to C-Bus Automation Controllers, for Windows PC, iOS and Android Devices.

Release date 06/2023





Legal Information

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this guide are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

Table of Contents

Safety information	4
Note	5
Safety Precautions	5
Disclosure	5
Introduction	6
Customer value proposition	6
Competencies	7
System Prerequisites	7
Software Installation	8
Preparation for Certificate Creation	8
Root Certificate Generation	9
Applying Certificates to the C-Bus Automation Controller	14
Installing Root Certificate to Windows PC	15
Adding the Trusted root certificate to an iOS device manually	19
Adding Trusted Root Certificate to an Android device Manually	21
Configuring C-Bus Automation Controllers to use HTTPS only for secure	
connection of Devices	23
Defining non-default ports for HTTPS connections	23
Setting HTTPS mode as default connection	24

Safety information

Important information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of either symbol to a "Danger" or "Warning" safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that accompany this symbol to avoid possible injury or death.

A A DANGER

DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.

Failure to follow these instructions will result in death or serious injury.

AWARNING

WARNING indicates a hazardous situation which, if not avoided, **could result** in death or serious injury.

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

Safety Precautions

HAZARD OF INCORRECT INFORMATION

- Do not incorrectly configure the software, as this can lead to incorrect reports and/or data results.
- Do not rely solely on software messages and reports to determine if the system is functioning correctly or meeting all applicable standards and requirements.
- Do not rely solely on the software's messages and information for maintenance or service decisions.
- Consider the implications of unanticipated transmission delays or failures of communications links.

Failure to follow these instructions can result in injury or equipment damage.

Disclosure

This documentation contains general descriptions and/or technical characteristics of the products contained herein. It is not intended to determine whether these products are suitable for specific applications or to determine their reliability. In order to determine whether the products are fit for any particular application or use, users or integrators must conduct the appropriate risk analysis, evaluation, and testing. Any misuse of the information contained herein will not be the responsibility or liability of Schneider Electric or any of its affiliates. If you have suggestions for improvements or amendments or have found errors in this publication, please notify us.

Schneider Electric expressly prohibits the reproduction of any part of this document, electronic or mechanical, including photocopying, without its prior written permission.

The product must be installed and used in accordance with all applicable state, regional, and local safety regulations. In order to ensure safety and compliance with documented system data, only the manufacturer should perform component repairs.

Devices with technical safety requirements must follow the relevant instructions.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage. ©2023 Schneider Electric. All rights reserved

Introduction

This guide explains how to generate SSL certificates for secure and authenticated access. This process offers an alternative to purchasing SSL certificates from a trusted provider, which typically requires an annual fee.

In this guide, we provide step-by-step instructions on how to generate SSL certificates using OpenSSL, a widely used and trusted open-source software for cryptography and SSL/TLS protocols.

This configuration guide describes:

- A process for creating a Root Certificate and sign the server certificate with the root certificate.
- Installing the server certificate on a C-Bus Automation Controller or C-Bus Application Controller.
- Installing the root certificate on a Windows PC.
- · Installing root certificate onto iOS devices such as iPad and iPhones.

This process guides through the installation of a root certificate to provide a seamless connection to the controller on the local and remote networks using HTTPS without the warning notification of certificate/security issues being displayed to the use and ensures all communications are securely encrypted.

The process will conclude with ensuring that the C-Bus Automation Controller or C-Bus Application Controller redirects all HTTP connections to HTTPS.

Customer value proposition

The customer value propositions correspond to real use cases:

On completion, customer devices connection to the C-Bus Automation Controller or C-Bus Application Controller will no longer display a warning or prohibit connection due to an invalid certificate.

•	Warning: Potential Security Risk Ahead				
	Firefox detected a potential security threat and did not continue to 192.168.1.10. If you visit this site, attackers cou try to steal information like your passwords, emails, or credit card details.				
	What can you do about it?				
The issue is most likely with the website, and there is nothing you can do to resolve it.					
	If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assis You can also notify the website's administrator about the problem.				
	Learn more				
	Go Back (Recommended) Advanced				
	Someone could be trying to impersonate the site and you should not continue. Websites prove their identity via certificates. Firefox does not trust 192.168.1.10 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates. Error code: SEC_ERROR_UNKNOWN_ISSUER				
	view Certificate				
	Go Back (Recommended) Accept the Risk and Continue				

Competencies

It is necessary to be familiar with the use of C-Bus Automation Controller or C-Bus Application Controller, use of command line tools on a windows PC environment. An understanding of File extensions and use of Notepad and windows File browser is required.

NOTE: The software used in this guide is not provided by Schneider Electric. The use of OpenSSL Light comes with some legalities, refer OpenSSL.org for more details. The user is strongly adviced to pay close attention to any laws or regulations which applies to the use and distribution of content created through this process. Schneider Electric or any of its subsidiaries are not liable for any violations the user make while applying this configuration guide.

System Prerequisites

Software Version	Version	Download link
5500NAC	1.12.0 or later	5500NAC Firmware
LSS5500NAC	1.12.0 or later	LSS5500NAC Firmware
5500SHAC	1.12.0 or later	5500SHAC Firmware
LSS5500SHAC	1.12.0 or later	LSS5500SHAC Firmware
5500AC2	1.12.0 or later	5500AC2 Firmware
5500NAC2	1.12.0 or later	5500NAC2 Firmware
Win32 Open SSL Light	in32 Open SSL Light Latest Version Win32 Open SSL Light	
Win64 Open SSL Light	Latest Version	Win64 Open SSL Light

Software Installation

Before proceeding, please ensure that you have installed OpenSSL Light for Win32 or Win64 on your machine. You can download OpenSSL Light from the official website (https://slproweb.com/products/Win32OpenSSL.html).

NOTE: Please be aware that the website may change in the future and we cannot guarantee its authenticity. Additionally, please exercise caution while downloading the software from any website, and make sure to verify the source and integrity of the software before installing it on your machine.

Preparation for Certificate Creation

In order to prevent confusion later in selecting the right file, it is recommended to create a folder to store the certificates files. If repeating this process for more than one customer, it is important to create a distinct set of certificates for each one in order to avoid confusion in selecting the right file. Create an easy to remember folder and navigate to e.g: creating a folder called "certificate" within the Documents directory of your PC. Inside the "certificate" folder , consider creating a new folder for the customer "Customer 1" in this example.

Once Folders have been created, Start OpenSLL from the windows command prompt. Open SSL can be found in "C:\Program Files\OpenSSL-Win64\start.bat"



Using the **cd** (change directory) command, navigate to the "customer" folder created during preparation. Example: cd Documents\Certificate\Customer_1

Command Prompt	-		×
Microsoft Windows [Version 10.0.19043.1706] (c) Microsoft Corporation. All rights reserved.			Â
T:\>"C:\Program Files\OpenSSL-Win64\start.bat" Win64 OpenSSL Command Prompt			
OpenSSL 3.0.3 3 May 2022 (Library: OpenSSL 3.0.3 3 May 2022) built on: Wed May 4 02:41:48 2022 UTC platform: VC-WIN64A options: bn(64,64) compiler: cl /Z7 /Fdossi_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V1: OPENSSLDIR: "C:\Program Files\Common Files\SSL" ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3" MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules" Seeding source: os-specific CPUINFO: OPENSSL_ia32cap=0x7ed8320b078bffff:0x400004219c91a9	10_SDK71_	D_WI	NSOCK
C:\Users\UserAccount>CD Documents\Certifcate\Customer_1			
C:\Users\UserAccount\Documents\Certifcate\Customer_1>			
			~

The files will be stored in this folder.

Root Certificate Generation

A root key (also known as a root certificate or private key) is the foundational cryptographic key used to sign and issue SSL certificates. It's necessary to generate a root key because it forms the basis of trust in the SSL certificate system. A root key is used to verify the identity of the SSL certificate holder, which is crucial for providing secure, authenticated access.

It's essential to keep the root key securely stored because if it's compromised, all SSL certificates signed by it could become invalid.

Root Key Generation

Below is the command that can be used to generate a key, you may copy and paste this into the command prompt window and hit enter to execute. The **'root key'** file name in the command below can be changed to match your target product or customer, however this file name will be referred for further commands in the manual (you will need to replace the file name in the commands).

openssl ecparam -name prime256v1 -genkey -out C- Bus_Controller_Root.key

C:\Users\UserAccount\Documents\Certifcate\Customer_1>openssl ecparam -name prime256v1 -genkey -out C-Bus_Controller_Root.key
C:\Users\UserAccount\Documents\Certifcate\Customer_1>

The key file is created and located in the "Customer_1" Folder.

> This PC > Documents > Certifcate > Customer_1				
Name ^	Date modified	Туре	Size	
C-Bus_Controller_Root.key	22/06/2022 9:48 AM	KEY File	1 KB	

Root Certificate Generation

Below is the command that can be used to generate a certificate, you may copy and paste this into the command prompt window and hit enter to execute. The following names and values can be edited to suit your needs, however this file name will be referred for further commands in the manual (you will need to replace the file name in the commands).

"C-Bus_Controller_Root.key" (this file name must be the same name as used in the Root key creations).

"7300" (Validity of the certificate in days. On expiry, a new Certificate has to be created).

"C-Bus_Controller_Root.crt" (File name of the root certificate).

openssl req -x509 -new -nodes -key C-Bus_Controller_Root.key -days 7300 -out C-Bus_Controller_Root.crt -sha256 -reqexts v3_req -extensions v3_ca

The Command Prompt displays a set of information to be included in the certificate, fill the details accordingly. In case if you want to leave them blank, use ".", else the default value will be chosen. This information will be available in the created certificate and is installed into the customer device. If the customer is using an Dynamic name service (DNS) for remote access, then use the customer URL as the FQDN in order to secure remote access. If only Local access is required, then Device Name can be used as local host (Refer to hostname under system menu of the controller).

1 KB

and community routing			-		×
:\Users\UserAccount\Documents\Certifcate\Customer_1>op	penssl req -x509 -new -nodes -key C-l	Bus_Controller_Root.key -days	7300 -ou	t C-Bus	_c î
rou are about to be asked to enter information that will be included to be asked to enter information that will be included and the second s	corporated				
What you are about to enter is what is called a Distinguished N	Jame or a DN				
There are quite a few fields but you can leave some blank	valle of a Div.				
For some fields there will be a default value.					
f you enter '.'. the field will be left blank.					
Country Name (2 letter code) [AU]:.					
State or Province Name (full name) [Some-State]:.					
Locality Name (eg, city) []:.					
Organization Name (eg, company) [Internet Widgits Pty Ltd]:So	chneider Electric				
Organizational Unit Name (eg, section) []:.					
Common Name (e.g. server FQDN or YOUR name) []:5500NAC					
Email Address []:.					
	a				
	Customer_1				
> This PC > Documents > Certifcate >	Customer_1 Date modified	Туре	Size		

Generate the Private Key for the C-Bus Automation Controller

C-Bus_Controller_Root.key

Below is the command that can be used to generate a private key, you may copy and paste this into the command prompt window and hit enter to execute. The following names can be edited to suit your needs, however this file name will be referred for further commands in the manual (you will need to replace the file name in the commands).

22/06/2022 9:48 AM

KEY File

"5500NAC_192.168.1.10.key" (Private Key File name)

openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:2048 -out 5500NAC_192.168.1.10.key



Private Key is Created in Customer folder.

> This PC > Documents > Certifcate > Customer_1					
Name ^	Date modified	Туре	Size		
5500NAC_192.168.1.10.key	22/06/2022 10:36 AM	KEY File	2 KB		
🔄 C-Bus_Controller_Root.crt	22/06/2022 10:26 AM	Security Certificate	1 KB		
C-Bus_Controller_Root.key	22/06/2022 9:48 AM	KEY File	1 KB		

CSR for the C-Bus Automation Controller

Below is the command that can be used to generate a CSR, you may copy and paste this into the command prompt window and hit enter to execute. The following names can be edited to suit your needs, however this file name will be referred for further commands in the manual (you will need to replace the file name in the commands).

"5500NAC_192.168.1.10.key" (Must be the same name as used in Step 3)

"5500NAC_192.168.1.10_CSR.csr" (File name of csr to be created)

openssl req -new -key 5500NAC_192.168.1.10.key -out 5500NAC_192.168.1.10_CSR.csr

The Command Prompt will display information which is to be included in the certificate, fill them accordingly (follow the same procedure as in step 2).



The CSR is created in Customer folder.

This PC > Documents > Certifcate > Customer_1

Name ^	Date modified	Туре	Size
5500NAC_192.168.1.10.key	22/06/2022 10:36 AM	KEY File	2 KB
5500NAC_192.168.1.10_CSR.csr	22/06/2022 10:48 AM	CSR File	1 KB
C-Bus_Controller_Root.crt	22/06/2022 10:26 AM	Security Certificate	1 KB
C-Bus_Controller_Root.key	22/06/2022 9:48 AM	KEY File	1 KB

Generate the Server Certificate, signed by the root certificate.

A configuration file (a text file) must be created and saved to the customer folder, containing the following informations:

- The text file with extension will be used in the script.
- example of the file name: "5500NAC_192.168.1.10_EXT.ext"
- Change the DNS and IP address to fit your device. If you are using FQDN in step 2 and 4, then use the same FQDN for DNS, else use the device hostname.

```
copy and paste the code below to the text file
```

```
basicConstraints=critical,CA:FALSE
keyUsage = digitalSignature, keyEncipherment
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer
subjectAltName = @alt_names
```

```
[alt_names]
DNS=5500NAC
IP=192.168.1.10
```

Create Text file in Customer folder

Name		Date modified	Туре	Size	
5500NAC_192.168.1.10.key		22/06/2022 10:36 AM	KEY File		2 KB
5500NAC_192.168.1.10_CSR.csr		22/06/2022 10:48 AM	CSR File		1 KB
C-Bus_Controller_Root.crt		22/06/2022 10:26 AM	Security Certificate		1 KB
C-Bus_Controller_Root.key		Folder			1 KB
		Shortcut			
AMD Radeon Software	0	Microsoft Access Databas	e		
AMD Link For Windows		Bitmap image			
View	•	Microsoft Word Documen SAPShow Container	t		
Sort by		Microsoft Access Database	e		
Group by	p.	Microsoft PowerPoint Pres	entation		
Refresh		Microsoft Publisher Docur	nent		
Customize this folder	۲	Rich Text Format			
Dacto		SAP GUI Shortcut			
Paste chortcut		Text Document			
Paste shortcut	•	Microsoft Visio Drawing			
Give access to	0	Microsoft Excel Worksheet	t		
New		Compressed (zipped) Fold	ler		

NOTE: The file extension of the text file is .ext .

[Name	Date modified	Туре	Size
	5500NAC_192.168.1.10.key	22/06/2022 10:36 AM	KEY File	2 KB
	5500NAC_192.168.1.10_CSR.csr	22/06/2022 10:48 AM	CSR File	1 KB
	5500NAC_192.168.1.10_EXT.ext	22/06/2022 11:23 AM	EXT File	0 KB
	C-Bus_Controller_Root.crt	22/06/2022 10:26 AM	Security Certificate	1 KB
	C-Bus_Controller_Root.key	22/06/2022 9:48 AM	KEY File	1 KB

Edit the file in notepad and paste to text file.



Generate Service Certificate

Run the following command, to generate the server certificate and perform the following changes.

- "5500NAC_192.168.1.10_CSR.csr" (file name must be named same as used in the CSR creation Step 4).
- "C-Bus_Controller_Root.crt" (file name must be named as used in the Root Certificate creation Step 2)
- "C-Bus_Controller_Root.key" (file name must be named as used in the Root key creation Step 1)
- "5500NAC_192.168.1.10_EXT.ext" (file name must be named as used in the Root key creation Step 5)

You can define the following file names and values according to your requirement.

"-days 825" (Can modify expiry value for days).

NOTE: If used on iOS devices, 825 days is the maximum permissible value.

"5500NAC_192.168.1.10_cert.crt" (file name must be named as used in the Root key creation Step 5).

openssl x509 -req -in 5500NAC_192.168.1.10_CSR.csr -CA C-Bus_Controller_Root.crt -CAkey C-Bus_Controller_Root.key -CAcreateserial -out 5500NAC_192.168.1.10_cert.crt -days 825 -sha256 -extfile 5500NAC_192.168.1.10_EXT.ext

Copy and paste the following command:

> This PC > Documents > Certifcate > Customer_1				
Name ^	Date modified	Туре	Size	
5500NAC_192.168.1.10.key	22/06/2022 10:36 AM	KEY File		2 KB
☑ 🔄 5500NAC_192.168.1.10_cert.crt	22/06/2022 12:50 PM	Security Certificate		1 KB
5500NAC_192.168.1.10_CSR.csr	22/06/2022 10:48 AM	CSR File		1 KB
5500NAC_192.168.1.10_EXT.ext	22/06/2022 11:23 AM	EXT File		0 KB
🔄 C-Bus_Controller_Root.crt	22/06/2022 10:26 AM	Security Certificate		1 KB
C-Bus_Controller_Root.key	22/06/2022 9:48 AM	KEY File		1 KB

Applying Certificates to the C-Bus Automation Controller

- 1. You can apply certificate licenses to C-Bus automation controllers using any web browser by navigating to the **system page**.
- 2. Click Services > HTTP SSL Certificate



The HTTP SSL certificate window is displayed.

HTTP SSL certificate		×
Mode	Upload new private key / certificate	~
Private key (RSA)		
Certificate (SHA256)		
	ОК	Cancel

3. Using a Notepad, open the private key (5500NAC_192.168.1.10.key) and copy-paste the entire content of the file into the **Private key window**.

HTTP SSL certificate		×
Mode	Upload new private key / certificate	۲
Private key (RSA)	NivioDigzmfl95Nv7+TPVPHOx5Lux72kQ99Cv+OXSun95Nvc8 FoxqcKeT2bjn7Gw Gc33GhgIGe5PwTV5lpyX/ax3i6/VTxhpuwvodPvtf4QKBgHO0iP+ F258aPAjV046/ 9xmdRvFT/MbDHL2zqc691z89IP7fHtWJctKqs4ZudR5YA21JW UUyve7KA/ <u>ycDdw</u> Sd7yfkn2w1456/go45bdT7Xjmn6zTWELAcu/18cC7Xz++S12e6fGr bOYp10QjaT7HM vhvstWaB0Kq82mR7ebDQPovti6 END PRIVATE KEY	•
Certificate (SHA256)		

4. Using Notepad, open the service certificate (5500NAC_192.168.1.10_cert. crt) and copy-paste the entire content of the file to the Certificate (SHA256) window.



5. Confirm with OK and Apply changes. The controller will start rebooting.



Installing Root Certificate to Windows PC

÷

To connect securely without displaying warnings, the root certificate created during this process must be installed onto the customer PC.

1. Select **Customer** folder created in the preparation step, right click **Root** certificate > Install Certificate and follow the process as shown in the images below.

Dπ		LE, 00, LOLE 11120 1111	EXTENSE.	0.00
g	C-Rus Controller Root crt	22/06/2022 10:26 AM	Security Certificate	1 KB
]	Open	22/06/2022 9:48 AM	KEY File	1 KB
1	Install Certificate			
8	Classify and protect			

In the Certificate Import window, choose Current User and click Next.

Welcome to the Certificate	e Import Wizard
This wizard helps you copy certificates, co ists from your disk to a certificate store.	ertificate trust lists, and certificate revocation
A certificate, which is issued by a certifica and contains information used to protect connections. A certificate store is the sys	tion authority, is a confirmation of your identity data or to establish secure network tem area where certificates are kept.
Store Location	
Current User	
O Local Machine	
To continue, click Next.	

Next

Cancel

Choose Place all certificates in the following store and click **Browse**.

Cartificat	s Store
Certi	scate stores are system areas where certificates are kept.
Wind the c	ows can automatically select a certificate store, or you can specify a location for ertificate.
0	Automatically select the certificate store based on the type of certificate
0	Place all certificates in the following store
	Certificate store: Browse

Next Cancel

Select the certificate store you want to use and click $\ensuremath{\textbf{OK}}.$

Select Certificate Store	\times
Select the certificate store you want to use.	
Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities	^
Active Directory User Object	~
Show physical stores	
OK Cancel	

Click Next.

•	Certificate Import Wizard
0	ertificate Store
	Certificate stores are system areas where certificates are kept.
	Windows can automatically select a certificate store, or you can specify a location for the certificate.
	○ Automatically select the certificate store based on the type of certificate
	Place all certificates in the following store
	Certificate store:
	Trusted Root Certification Authorities

xt Cancel	<u>N</u> ext Cancel

Confirm Finish

501		
÷	F Certificate Import Wizard	×
	Completing the Certificate Import Wizard	
	The certificate will be imported after you click Finish.	
	You have specified the following settings:	
	Certificate Store Selected by User Content Certification Authorities	

	Cancel	Einish
--	--------	--------

Security	curity Warning	
	You are about to install a certificate from a certification authority (CA) claiming to represent:	
	W4K	
	Windows cannot validate that the certificate is actually from "W4K". You should confirm its origin by contacting "W4K". The following number will assist you in this process:	
	Thumbprint (sha1): FF3FB698 2FA491DE 4747134F 97DC2D19 34447B40	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.	
	Do you want to install this certificate?	
	Yes No	

NOTE: These warnings notifications are meant to protect users from potentially malicious or fraudulent certificates, which could compromise the security of their device. However, if you have created the SSL certificate for a known device and are installing it onto other devices that need to trust this device, then these warning notifications do not apply in this situation (This is because the SSL certificate has been specifically created for this use case and is trusted by the known device).

Click OK.



On installing the certificate successfully, using any web browser navigate to the C-Bus Automation controller using HTTPS.

Example: https://192.168.1.10 , verify that the certificate displays Connection as secure. If an insecure connection is displayed , clear the cache and reconnect to verify.



Adding the Trusted root certificate to an iOS device manually

Devices with iOS software (like iPad and iPhone) to establish a secure network, should have the root certificate installed onto each device. Certificates have a maximum expiration of 825 days (This means that you will need to renew your SSL certificate before it expires to maintain the security and trust of your web services).

- Download or transfer the trusted root certificate to the iOS device (Certificates can be distributed via email or downloaded from a secured site) and install the certificate on the device.
- Once installed, Click Settings > General > Profiles & VPN & Device Management > 5500NAC Profile Install, save the certificate to the device and find the certificate in the Files App.

open the file before going to settings to accept the certificate.

NOTE: On the most recent iOS devices, the menu could appear as **VPN** & **Device Management**.

To manage the certificate, the user must provide their PIN (or authenticate to the device before opening the certificate). As a trusted source of the certificate user is asked to click **install** a second time from the warning page.



NOTE: These warnings notifications are meant to protect users from potentially malicious or fraudulent certificates, which could compromise the security of their device. However, if you have created the SSL certificate for a known device and are installing it onto other devices that need to trust this device, then these warning notifications do not apply in this situation (This is because the SSL certificate has been specifically created for this use case and is trusted by the known device).

Click **Settings > About > Certificate Trust Settings** and enable 5500NAC Certificate.

		About		< About	Certificate Trust Settings	
	Wi-Fi Address					
	Bluetooth			Trust St	tore Version	
	Modern Firmware	9		Trust A	sset Version	
				Some cer	tificate settings are enforced by meet Profile?	
	EID			ENABLE F		
	Service Provider	Lock				
	PHYSICAL SIM					
	Network					
	Service Provider					
	IN ATT					
	IVIEI		-	5500N/	4C	
	ICCID		-			
	MEID					
	AVAILABLE SIM					
	IMEI2					
	Certificate Trust	Settings	>			
<	About Certific	ate Trust Settings		< About	Certificate Trust Settings	
<	About Certific	ate Trust Settings		About	Certificate Trust Settings	
<	About Certific Trust Store Versi	cate Trust Settings		About Trust St	Certificate Trust Settings ore Version	
<	About Certific Trust Store Versi Trust Asset Versi	cate Trust Settings ion		About Trust St Trust As	Certificate Trust Settings ore Version set Version	
<	About Certific Trust Store Vers Trust Asset Vers Some certificate set Management Profile	ion ion togs are enforced by "		About Trust St Trust As Some cert Manager	Certificate Trust Settings ore Version set Version sitcate settings are enforced by each Pointe"	
<	About Certific Trust Store Versi Trust Asset Versi Some certificate set "Management Profile ENABLE FULL TRUS	tere Trust Settings		About Trust St Trust As Some cert Manager ENABLE F	Certificate Trust Settings ore Version set Version shcate settings are enforced by next Profile*	
<	About Certific Trust Store Vers Trust Asset Vers Some certificate set Management Prefile ENABLE FULL TRUS	tion lion high high are enforced by p ¹ t FOR ROOT CERTIFICATES		C About Trust St Trust As Some cert Manager ENABLE F	Certificate Trust Settings ore Version set Version store settings are enforced by end Profile" ULL TRUST FOR ROOT CERTFICATE	55
<	About Certific Trust Store Versi Trust Asset Versi Some certificate set Management Profile ENABLE FULL TRUS	tere Trust Settings		About Trust St Trust As Some cent "Managem ENABLE F	Certificate Trust Settings ore Version set Version set Version set Profile" ULL TRUST FOR ROOT CERTIFICATE	5
<	About Certific Trust Store Vers Some certificate set Management Prote ENABLE FULL TRUS	eate Trust Settings ion togs are enforced by t FOR ROOT CERTFICATES		C About Trust St Trust As Some cent Managen ENABLE F	Certificate Trust Settings ore Version set Version sfate settings are enforced by need Profile* ULL TRUST FOR ROOT CERTIFICATE	5
<	About Certific Trust Store Vers Some certificate set Management Petit ENABLE FULL TRUS Ro Warning - Warning - Warning -	eate Trust Settings ion ion tops are enforced by the BOOT CERTFICATES NOT CERTIficate nabling this certificate for iable thing particulate for		C About Trust St Trust As Some cert "Manager ENABLE F	Certificate Trust Settings ore Version set Version ficate settings are enforced by read Profile*	
<	About Certific Trust Store Versi Trust Asset Versi Some certificate set Microageneet Petiti ENABLE FULL TRUS Ro Warrings e websities will any privat	eate Trust Settings ion ion tigs are enlorced by the enlorced by the enlorced by the enlorced by the enlorced by the enlorced by the enlorced by the enlorced by the enlorced by the enloreed by the enlorced by the enlorced		C About Trust St Trust As Some cert "Managere ENABLE F	Certificate Trust Settings ore Version set Version sideate settings are enforced by event Profile?	
<	About Certific Trust Store Vers Trust Asset Vers Some certificate set Management Profile CNABLE FULL TRUS Warring, e websites will excent	the Trust Settings		About Trust St Trust As Some cert Varage ENABLE F	Certificate Trust Settings ore Version set Version ificate settings are enforced by each Penfer ULL TRUST FOR ROOT CERTIFICATE	
<	About Certific Trust Store Versi Trust Asset Versi Some certificate set Management Profile ENABLE FULL TRUS Warning, e websites with any profile Chance Full TRUS Cance 5500NAC	teste Trust Settings		About Trust St Trust As Some cert Manageri HABLE F	Certificate Trust Settings ore Version set Version effects settings are enforced by effects settings are enforced by effects settings are enforced by entopy of the setting setting setting setting of the setting setting setting setting setting setting of the setting setting setting setting setting setting setting setting setting sett	
<	About Certific Trust Store Versi Trust Asset Versi Some certificate set Maragement Profile ENABLE FULL TRUS Worming: e websites with any profile Cancel 5500NAC Learn more about the	eate Trust Settings ion ion togs are enforced by total Root Certificate nabiling this certificate for label this perificate to rew te data sent to websites. Continue used certificates		About Trust St Trust As Some cert "Managert ENABLE F 5500NA	Certificate Trust Settings ore Version set Version ficate settings are enforced by read Profile ULL TRUST FOR ROOT CERTIFICATE ULL TRUST FOR ROOT CERTIFICATE C e about trusted certificates	
<	About Certific Trust Store Vers Some certificate set Variagement Perio ENABLE FULL TRUS Warning - Warning - Warning - StoonNAC Learn mice about th	eate Trust Settings ion ion togs are enforced by the sector CERTFICATES in the sector CERTFICATES in the sector CERTFICATES in the sector certificate for indiant micro particulate for indiant micro particulate for indiant micro particulate for indiant micro particulate for continue		About Trust St Trust As Some cert "Hanagen ENABLE F 5500NA	Certificate Trust Settings ore Version set Version infcate settings are enforced by read Profile ³ ULL TRUST FOR ROOT CERTIFICATE ULL TRUST FOR ROOT CERTIFICATE e about trusted certificates	
<	About Certific Trust Store Versi Some certificate set Vanagement Petit ENABLE FULL TRUS Re Weitings with any prior Cance 5500NAC Learn more about th	eate Trust Settings ion ion togs are enforced by the BOOT CERTFICATES sot Certificate adding this certificate for ialion thing parties to view the data sent to websites.		About Trust St Trust As Some cert "Variaged ENABLE F 5500NA Learn mar	Certificate Trust Settings ore Version set Version incate estings are enforced by read Profile ⁴ ULL TRUST FOR ROOT CERTIFICATE ULL TRUST FOR ROOT CERTIFICATE C e about trusted certificates	
<	About Certific Trust Store Versi Some certificate set Management Perint ENABLE FULL TRUS Re Wernings Warrings Cancel 5500NAC Learn more about to	eate Trust Settings		About Trust St Trust As Some cert "Hanaged ENABLE F 5500NA Learn mor	Certificate Trust Settings ore Version set Version incate settings are enforced by event Profile* ULL TRUST FOR ROOT CERTIFICATE ULL TRUST FOR ROOT CERTIFICATE C e about trusted certificates	
<	About Certific Trust Store Versi Trust Asset Versi Some certificate set Management Petiti ENABLE FULL TRUS Worring: e websities will any privat Cancel 5500NAC Learn more about to	eate Trust Settings		About Trust St Trust As Some cert "Manageme ENABLE F 5500NAR Learn mor	Certificate Trust Settings ore Version set Version structure settings are enforced by event Profile* ULL TRUST FOR ROOT CERTIFICATE C e about trusted certificates	
	About Certific Trust Store Versi Trust Asset Versi Some certificate set Management belief ENABLE FULL TRUS Warning: e websites with any privat Cance 5500NAC Learn more about to	eate Trust Settings ion ion ings are enlorced by track Root Continue about Certificate in about third parties to view te data sent to websites.		About Trust St Trust As Some cert "Manageme ENABLE F 5500NAR Learns more	Certificate Trust Settings ore Version set Version ificate settings are enforced by enert Profile* ULL TRUST FOR ROOT CERTFFICATE C e about trusted certificates	
	About Certific Trust Store Versi Trust Asset Versi Some certificate set Management Public ENABLE FULL TRUS Warring c websites will any private 5500NAC Learn more about to	eate Trust Settings ion ion ion ings are enlorced by read a corr Correntation about Certificate inabiling this certificate for lation thing parties to view te data sent to websites.		About Trust St Trust As Some cert Taist As Some cert Taistange ENABLE F 5500NA Learn mon	Certificate Trust Settings ore Version set Version ificate settings are enforced by end Profile* ULL TRUST FOR ROOT CERTFFICATE C e about trusted certificates	

Adding Trusted Root Certificate to an Android device Manually

NOTE: The Steps to follow for an Android device are not specific to any particular model or version of Android, and depending on your device these steps may differ. If the process described cannot be followed directly on the target device then, advised to use Google to search up installing trusted certificates on the specific make and model of android device for better instructions.

Follow the below guidance to manually add trusted root certificate to Android.

- Download or transfer the trusted root certificate to the Android device (Certificates can be distributed through email or downloaded from a secured site). Save the certificate once it is on the device. Saving the certificate adds it to the User certificate store on the device.
 - a. To install the certificate on a device, a user must locate install certificates from storage option, the location may change for different android device (example: Biometrics and security > other security settings > Install from Device storage).

< Other security settings
Make passwords visible Show password characters briefly as you type them.
Device admin apps No active apps
Credential storage
View security certificates Display trusted CA certificates.
User certificates View user certificates.
Install from device storage Install certificates from storage.
Clear credentials Remove all certificates.
Certificate management app None
Data protection
Strong protection

b. Select CA Certificate.

< Install from device storage
CA certificate
VPN and app user certificate
Wi-Fi certificate

A Warning message "Your privacy is at risk " is displayed. Select **Install Anyway** to continue.

Your privacy is at risk	
CA certificates are used by websites, apps, and VPNs for encryption. Only install CA certificates from organisations you trust.	
If you install a CA certificate, the certificate owner will be able to access your information, such as passwords, messages, or credit card details, from websites you visit or apps you use, even if that information is encrypted.	
Install anyway Don't install	

NOTE: These warnings notifications are meant to protect users from potentially malicious or fraudulent certificates, which could compromise the security of their device. However, if you have created the SSL certificate for a known device and are installing it onto other devices that need to trust this device, then these warning notifications do not apply in this situation (This is because the SSL certificate has been specifically created for this use case and is trusted by the known device).

The user must provide their PIN (or authenticate to the device before managing the certificate).

 Once the certificate is authenticated, it has to be opened and renamed before saving to the Users certificate store. Make sure the certificate name is same as mentioned in the Trusted Root Certificate profile which will be sent to the device.

Save the certificate after naming to the Users certificate store.

n Q ☴
1∃ Date ↓
C_root.crt unc.10:05 am 824 B

- 3. After being saved, the certificate is ready to use. A user can confirm the certificate is in the correct location on the device.
 - a. Click Settings > Security > Trusted credentials (Use the search bar in settings for "Trusted" or "Certificates" which assist in finding this feature within Android device, else refer to the NAC/SHAC device user manual).
 - b. Find the certificate in the **User** tab.
 - c. If found in the list of User certificates, the certificate is installed correctly.

Configuring C-Bus Automation Controllers to use HTTPS only for secure connection of Devices.

The C-Bus Automation controllers are pre-configured to support HTTP via port 80 and HTTPS via port 443 by default.

Additional Ports for HTTP and HTTPS can be assigned to the unit. However, the default ports will always be enabled. Except for HTTP port 80, which can be disabled only when all HTTP connections are disabled.

The Automation controllers can be accessed remotely from the internet either via the default port 443 or a non-default port.

This document does not cover how to configure remote access through customer devices and assumes that user are familiar with setting up remote access and mapping ports.

Defining non-default ports for HTTPS connections

1. Login to Automation Controller, in the **Configurator** window select **Utilities** tab and click **System**.

HTTP server		×
Additional HTTP port		
Additional HTTPS port		
HTTPS mode	HTTP and HTTPS enabled	~
Default HTTP port: 80,	, default HTTPS port: 443	
CORS origin 1		
CORS origin 2		
CORS origin 3		
CORS origin 4		
	ОК	Cancel

On the System page, Click Menu > Services > HTTP Server

2. Additional ports for HTTPS can be defined in the dialog windows as shown below. Enter a valid port number between 1025 – 65535, and Click Ok.

HTTP server	×
Additional HTTP port	
Additional HTTPS port	4447
HTTPS mode	HTTP and HTTPS enabled
Default HTTP port: 80	, default HTTPS port: 443
CORS origin 1	
CORS origin 2	
CORS origin 3	
CORS origin 4	
	OK Cancel

3. Non default ports must be explicitly defined in the URL for client devices. For example when connecting from any client in the example, the URL would be. https://192.168.1.10:4447, when using an IP range or https://customerurl.com:4447 when using a domain name. The custom port number is defined by the use of (colon) : after the URL or IP Address. In the instance where a link directly to service is required such as a PC desktop view, the Port Address is placed between URL and path. Such as https://192.168.1.10:4447/scada-vis or https://customerurl.com:4447/scada-vis

Setting HTTPS mode as default connection

Once the C-Bus Automation controller and customer devices are configured with certificates, and the connection using HTTPS to the C-Bus Automation Controller has been verified as working it is then advised to configure the C-bus Automation controller to direct all HTTP: communication to HTTPS or accept only HTTPS for connection of devices to the unit.

1. On the Automation Controller, Click System page > Service Menu > HTTP Server

HTTP server		×
Additional HTTP port		
Additional HTTPS port		
HTTPS mode	HTTP and HTTPS enabled	~
Default HTTP port: 80	, default HTTPS port: 443	
CORS origin 1		
CORS origin 2		
CORS origin 3		
CORS origin 4		
	ок	Cancel

 To redirect communications incoming on HTTP to HTTPs, Click HTTPS mode > HTTP only, redirect HTTP to HTTPS Click ok, to apply these settings.

NOTE: HTTP redirect will only redirect the connection made on the default HTTP port to the default HTTPS port. Custom HTTPS ports cannot be redirected with this feature.

HTTP server	1	×
Additional HTTP port		
Additional HTTPS port	4447	
HTTPS mode	HTTPS only, redirect HTTP to HTTPS	•
Default HTTP port: 80,	default HTTPS port: 443	
CORS origin 1		
CORS origin 2		
CORS origin 3		
CORS origin 4		
	OK Cancel	

3. C-Bus automation controllers can also be configured to only accept connections via HTTPS, disabling both the default HTTP port 80 and any custom HTTP ports. In order to use this feature, all devices must connect directly to either the default HTTPS port using HTTPS:// in the url or to custom HTTPS ports (Refer: Step 3 of non-default ports for HTTPs connection, page 23).

Select **HTTPS mode > HTTPS only, HTTP port is disabled** and click **Ok** to enable this mode.

HTTP server	×	
Additional HTTP port		
Additional HTTPS port	4447	
HTTPS mode	HTTPS only, HTTP port is disabled	
Default HTTP port: 80, default HTTPS port: 443		
CORS origin 1		
CORS origin 2		
CORS origin 3		
CORS origin 4		
	OK Cancel	

Schneider Electric Industries SAS If you have technical questions, please contact the Customer Care Centre in your country.

www.se.com/contact

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

© Schneider Electric. All rights reserved.

PKR4296200-00