

# Senstar Symphony Mobile Application 4.0 Security Guide

## Contents

Certificate requirements	3
Obtaining a certificate Use a trusted certificate authority Using your own certificate authority Use a self-signed SSL certificate.	4 5 5
Install the certificate	8
Export the certificate	14
Add an SSL certificate to the Senstar Symphony Server Add an SSL certificate Add an SSL certificate Configure mobile connections Configure mobile connections.	
Add a certificate to an iOS device	20
Add a certificate to an Android device	21



#### Certificate requirements

To secure communication with the Senstar Symphony Server, the Senstar Symphony Mobile Application requires that the Senstar Symphony Server is configured with a valid SSL certificate that can be verified by a trusted root certificate authority installed on the mobile device.

The SSL certificate secures the connection between the server and the application. The application checks this certificate to confirm that it is connecting to the correct server and not a potential impostor trying to intercept your data.

For more information, see What is an SSL certificate.

# Obtaining a certificate

You can obtain a certificate from a trusted certificate authority, from a custom certificate authority, or by generating a self-signed certificate.

Certificate issuer	Device requirements	Domain	Notes
Trusted certificate authority	None	Required	This is the most secure option. This is the recommended option when you want to access your Senstar Symphony Server over the Internet.
Custom certificate authority	Deploy the custom certificate authority on all mobile devices. Add the custom certificate authority to the list of trusted root certificates.	Not required	This option is best for organizations that already use a custom certificate authority and centrally manage mobile devices. This is the recommended option when you want to access your Senstar Symphony Server over a VPN connection.
Self-signed certificate	Deploy the self-signed certificate on all mobile devices. Add the self-signed certificate to the list of trusted root certificates.	Not required	You need to manually create a self-signed certificate that meets the mobile operating system security requirements and then deploy it to the mobile devices that run the application.

#### Use a trusted certificate authority

The recommended option for obtaining a certificate is to get a certificate from a trusted certificate authority.

1. Choose a certificate authority (CA).

You need to select a trusted CA to issue your SSL certificate. Some reputable CAs include DigiCert, GlobalSign, Sectigo, and Let's Encrypt. It is essential that you choose a reputable CA to ensure that your certificate is widely recognized and trusted.

2. Generate a certificate signing request (CSR).

You must generate a CSR to get a certificate. A CSR contains information about the server and the domain that you want to secure. The CA that you select will provide detailed information about how to generate a CSR. We recommend that you use the Microsoft Management Console to generate a CSR. For more information on hot to generate a CSR, see CSR Generation - using Windows Certificate Snap-in.

3. Submit the CSR to the CA.

Once you have generated a CSR, you submit the CSR to the CA. The CA that you select will provide detailed information about how to submit a CSR (usually using the website of the CA). The CA uses your CSR to generate the certificate.

4. Validate your domain ownership.

The CA might require that you validate your domain ownership. This typically involves responding to a confirmation email that the CA sends to a domain-specific email address (e.g., admin@yourdomain.com) or adding a specific DNS record to your domain's DNS configuration. The validation requirements can vary depending on the CA and the type of certificate.

5. Issue the certificate.

After your domain ownership is validated, the CA issues your SSL certificate. The certificate contains a public key and information about your server and your domain.

After you obtain a certificate, install the certificate.

#### Using your own certificate authority

If you choose not to get a certificate from a trusted certificate authority, you can use your own custom certificate authority to generate SSL certificates that will work with the Senstar Symphony Mobile Application and the Senstar Symphony Server.

This solution is recommended in cases where your organization manages all of the mobile devices that run the Senstar Symphony Mobile Application. Your IT department needs to deploy and install the custom certificate authority that signs the SSL certificate. The custom certificate authority needs to be added to the trusted root certificate list.

To use your own certificate authority:

- 1. Generate the certificate signing request (CSR).
- 2. Have your IT department generate the certificate.
- 3. Install the certificate.
- 4. Export the certificate.
- 5. Add the certificate to the Senstar Symphony Server and configure the certificate for mobile connections.
- 6. Add the certificate to mobile devices.

#### Use a self-signed SSL certificate

If you choose not to get a certificate from a trusted certificate authority, you can create your own selfsigned certificate that will work with the Senstar Symphony Mobile Application and the Senstar Symphony Server.

- 1. To open the Windows PowerShell, complete the following tasks:
  - a) Press the Windows key.
  - b) In the prompt, type PowerShell.

c) Click Run as Administrator.



2. Modify the following text and paste it into the Windows PowerShell prompt:

```
$params = @{
   Subject = 'CN=domain_name, O=organization, OU=division, L=locality, S=state, C=country'
   TextExtension = @(
        '2.5.29.37={text}1.3.6.1.5.5.7.3.1', #ServerAuthentication
        '2.5.29.17={text}DNS=domain_name&IPAddress=ip_address')
        CertStoreLocation = "cert:\LocalMachine\My"
        KeyUsage=@('DigitalSignature', 'KeyEncipherment')
        NotAfter = (Get-Date).AddDays(365)
        KeyAlgorithm = 'RSA'
        KeyLength = 2048
        HashAlgorithm = 'SHA256'
}
```

Where:

- domain\_name is the name of your domain or computer.
- organization is the name of your organization.
- division is the name of your organizational unit.
- · locality is the city in which your organization is located.
- state is the state or province in which your organization is located.
- country is the county in which your organization is located.
- ip\_address is the IP address of the Senstar Symphony Server. Use only if you do not access the Senstar Symphony Server through a domain name. If you access the Senstar Symphony Server through a domain name, you can remove the entire substring (&IPAddress=ip address

3. Run the following command in the Windows PowerShell prompt:

New-SelfSignedCertificate @params

After you run this command, you receive a confirmation message that the self-signed certificate was generated and added to the certificate store on the computer.

After you generate a self-signed certificate, export the certificate.



## Install the certificate

Install the certificate on the computer that hosts the Senstar Symphony Server.

- 1. Open the Microsoft Management Console by pressing Windows + R, typing MMC, and pressing Enter.
- 2. Click File > Add/Remove Snap-In > .



3. In the Available snap-ins list, select Certificates and click Add.

Sonsole1 - [Console Root]			$\times$
🚟 File Action View Favorites Window He	p	-	8 ×
🗢 🔶 📰 🗟 🖬			
Console Root	Name	Actions	
	There are no items to show in this view	Console Root	•
	mere are no items to show in this view.	More Actions	•
	Add or Remove Snap-ins X		
	You can select enap-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.		
	Available snap-ins: Selected snap-ins:		
	Snap-in Vendor ^ Console Root Edit Extensions		
	ActiveX Control Microsoft Cor Remove		
	Certificates Microsoft Cor		
	Component Services Microsoft Cor Move Up		
	Device Manager Microsoft Cor Add >		
	Disk Management Microsoft and		
	Folder Microsoft Cor		
	Group Policy Object Microsoft Cor		
	I Piccarly Policy M 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.		
	UK Cancel		

4. Select **Computer account** and click **Next**.

-		
Sonsole1 - [Console Root]		- 🗆 ×
🚟 File Action View Favorites Window He	,	_ 8 ×
← →   □   ➡		
Console Root	Name	Actions
		Console Root
	There are no items to show in this view.	More Actions
	Add as Barray Care in	
	Certificates snap-in X	
	of snap-ins. For	
	This snap-in will always manage certificates for:	
	O My user account	
	O Service account	
	Computer account	
	Move Lip	
	Maria Davia	
	Plove Down	
	Advanced	
	< Back Next > Cancel r a computer.	
	OK Cancel	

#### 5. Select Local computer and click Finish.

Console1 - [Console Root]		- 🗆 X
File Action View Favorites Window He	elp	- 6 X
Conrole Poot		A stress
Console Noor	Name	Console Root
	There are no items to show in this view.	Concole Root  More Actions
	Advanced	
	Cancel r a computer.	

6. Click OK.

There are no items to show in this view.	Name				Actions	
Add or Remove Snap-ins       X         You can select snap-ins, you can configure which extensions are enabled.       Selected snap-ins. For extensions are enabled.         Available snap-ins:       Vendor         Solected snap-ins:       Control of Solected snap-ins:         Computer Management Microsoft Com.       Control Microsoft Com.         Open Network Management Microsoft Com.       Microsoft Com.         Open Network Management Microsoft Com.       Microsoft Com.         Otok Management Microsoft Com.       Microsoft Com.         Otok Management Microsoft Com.       Microsoft Com.         Address Nickink With Microsoft Com.       Microsoft Com.         Decorption:       Advanced         Decorption:       Control Microsoft Com.         The Control Microsoft Com.       Microsoft Com.         Wink by Weak Address Microsoft Com.       Microsoft Com.         Decorption:       Microsoft Com.         The Control Microsoft Com.       Microsoft Com.         Wink by Weak Address Microsoft Com.       Microsoft Com.         Decorption:       Microsoft Com.         The Control Microsoft Com.       Microsoft Com.         Microsoft Com.       Microsoft Com.         Microsoft Com.       Microsoft Com.         Microsoft Com.       Microsoft Com.		There are no item	s to show in this view.		Console Root More Actions	•
You can select map-ins of the consider with decisions at enabled.         Available map-ins:         Selected map-ins:	Add or Remove Snap-ins			×		
Drug-in       Verdor         Authorization Manage       Morosoft Corr         Authorization Manage       Morosoft Corr         Computer Bangement       Morosoft Corr         Color, Namage       Morosoft Corr         Computer Management       Morosoft Corr         Color, Namagement       Morosoft Corr         P Security Neutry       Morosoft Corr         P Security Neutry       Morosoft Corr         Decorption:       Advanced         Decorption:       Decorption:         Decorption:       Decorption:         Decorption:       Decorption:         Decorption:       Decorption:         Decorption:       Decorption:	You can select snap-ins for thi extensible snap-ins, you can c Available snap-ins:	is console from those available on ya configure which extensions are enab	our computer and configure the selected : led. Selected snap-ins:	set of snap-ins. For		
Component Services Worsch Com Wo	Snap-in V ActiveX Control V Cal Authorization Manager V Certificates V	Vendor ^ Microsoft Cor Microsoft Cor Microsoft Cor	Certificates (Local Computer)	Edit Extensions Remove		
Herer Werer Microsoft Corr     Group Policy Object Microsoft Corr     Description:     The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.     OK Cancel	<ul> <li>Component Services</li> <li>Computer Managem</li> <li>Disk Management</li> </ul>	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft and		Move Up Move Down		
Becorption:      The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.      OK Cancel	Event Viewer     Folder     Group Policy Object      P P Security Monitor	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor				
Decorption: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer. OK Cancel	Unk to Web Address	Microsoft Cor		Advanced		
OK Cannot	Description: The Certificates snap-in allow	ws you to browse the contents of th	e certificate stores for yourself, a service	e, or a computer.		
				OK Cancel		

7. In the Microsoft Management Console, click **Console Root** > **Certificates (Local Computer** > **Personal** > **Certificates** 

Console1 - [Console Root\Certificates (Local Com	puter)\Personal\Certificates]							-	• ×
	ih								
	Issued To	Issued By Senstar Symphony	Expiration Date 10/31/2123	Intended Purposes <all></all>	Friendly Name ga-sn/2019	Status	≻	Actions Certificates More Actions	, , , , , , , , , , , , , , , , , , ,
Personal store contains 1 certificate.									

- Console1 [Console Root\Certificates (Local Computer)\Personal\Certificates] × 
   File
   Action
   View
   Favorites
   Window
   Help

   ◆
   ◆
   ★
   ★
   ▲
   ■
   - 6 × A The second secon Issued To Friendly Name Status Certi Actions Issued By Expiration Date Intended Purposes 10/31/2123 <All> Senstar Symphony qa-srv2019 Certificates More Actions All Tasks > Request New Certificate... Import... Refresh Advanced Operations > Export List... View Arrange Icons Line up Icons Help Add a certificate to a store
- 8. To open the Certificate Import Wizard, right click in the Details pane and click All Tests > Import.

9. In the Certificate Import Wizard, click Next.

🕶 🔿 🙍 📰 🗈 🛛 🖻 🖬 🖬									
Console Root Certificates Console Root Certificates Console Root Certificates Console Root Certificates Cert	Issued To ^	Issued By Senstar Symphony E Certificate Import Wizard Welcome to the Certif Ints wizard helps you copy certificate Ists from your dark to a certificate	Expiration Date 10/31/2123 Ficate Import Wi ates, certificate trust list store.	Intended Purposes <all> zard</all>	Friendly Name qa-srv2019 X	Status	Certi	Actions Certificates More Actions	,
<ul> <li>Smart Card Trusted Roots</li> <li>Trusted Porices</li> <li>Windows Live ID Token Issuer</li> </ul>		A certificate, which is issued by a and contain information used to a connections. A certificate store is Store Location Current User (D Local Machine To continue, dick Next.	certification authority are voiced data or the stability line system area where o	confination of your left in source retroids, this case is kept.	Cancel				

10. Browse to and select the certificate from the certificate authority and click Next.



11. Select **Place all certificates in the following store**, browse to and select the Personal certificate store, and click **Next**.

🖀 Console1 - [Console Root\Certificates (Local Com	iputer)\Personal\Certificates]						-	
🔚 File Action View Favorites Window He	lp							- 8 ×
🗢 🔿 🙍 🖬 🗎 🖓 🕞 🛛 🖬								
Console Root  Console Root  Console Root  Personal  Certificates  Certi	Issued To	Issued By Senstar Symphony	Expiration Date 10/31/2123	Intended Purposes <all></all>	Friendly Name qa-srv2019 X	Status Cer	ti Actions Certificates More Actions	•
Dirtruste Certification Authonities     Trusted People     Crieff Authonitication Issuers     Preview Build Roots     Renote Desktop     Certificate Enrollment Requests     Smart Card Trusted Roots     Trusted Devices     Windows Live ID Token Issuer		Certificate Store Certificate stores are system areas o Windows can automatically select a c the certificate. Automatically select the certifi @ Place all certificates in the fold Certificate store: Personal	where certificates are ertificate store, or yr cate store based on t wing store	kept.	or			
	4			Next	Cancel			

12. Click Finish.



After you install the certificate, export the certificate.

## Export the certificate

You can export a certificate to add it to the Senstar Symphony Server, iOS devices, or Android devices.

To use the certificate on the Senstar Symphony Server, you must export it in the . PFX format. To use the certificate on iOS devices or Android devices, you must export it the .CER format.

- 1. Open the Microsoft Management Console by pressing Windows + R, typing MMC, and pressing Enter.
- In the Microsoft Management Console, click Console Root > Certificates (Local Computer > Personal > Certificates
- 3. Right click the certificate and click **All Tasks > Export**.

Console1 - [Console Root\Certificates (Local Com	puter)\Personal\Certi	ficates]								- 1	- X
🔚 File Action View Favorites Window He	lp										- 6 ×
🔶 🙍 📷 🔏 🗞 🔀 🛃 🖬											
Console Root	Issued To		Issued	Ву	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
✓ Gertificates (Local Computer)	Subm.test		Sensta	MobileAppCA	10/30/2024	<all></all>	<none></none>			Certificates	
Personal     Contificator	💱 qa-srv2019		Sensta	Symphony	10/31/2123	<all></all>	qa-srv2019			More Actions	•
Trusted Root Certification Authorities	🙀 test.senstar.com	0	5000 B	MobileAppCA	11/2/2024	<all></all>	test_senstar_com				
Certificates		open	_							test.senstar.com	•
> 🧾 Enterprise Trust		All Tasks	>	Open						More Actions	•
Intermediate Certification Authorities		Cut		Request Certificate with	New Key						
> Untrusted Certificates		Сору		Renew Certificate with I	lew Key						
> Arrow Third-Party Root Certification Authorities		Delete		Manage Private Keys							
> iii Trusted People		Properties		Advanced Operations	>						
Client Authentication Issuers     Preview Build Roots		Mala	_	-							
> Test Roots		нөр		Export							
> 🛅 Remote Desktop											
Certificate Enrollment Requests											
Smart Card Trusted Roots     Trusted Devices											
> 🔛 Windows Live ID Token Issuer											
	<								>		
Export a certificate											

4. Click Next.

Console1 - [Console Root\Certificates (Local Com	puter)\Personal\Certificates]							- 🗆 X
File Action View Favorites Window Hel	lp							- 8
🗢 🔿 🙍 🛅 📋 🙆 📑 🔟								
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions
Certificates (Local Computer)	💱 qa-srv2019	Senstar Symphony	10/31/2123	<all></all>	qa-srv2019			Certificates
Personal     Certificates								More Actions
> Trusted Root Certification Authorities					~			
> iii Enterprise Trust					^			
> Intermediate Certification Authorities	÷	🐉 Certificate Import Wizard						
> Untrusted Certificates								
> Initial Third-Party Root Certification Authorities								
> Trusted People		Welcome to the Certif	icate Import Wi	zard				
Client Authentication issuers								
> 📫 Test Roots		This wizard helps you copy certifica	tes, certificate trust lists	and certificate revocatio	n			
> Remote Desktop		lists from your disk to a certificate s	itore.					
Smart Card Trusted Roots		A certificate, which is issued by a cr	ertification authority, is a	confirmation of your iden	tity			
> Trusted Devices		and contains information used to pr	otect data or to establish	i secure network				
> Windows Live ID Token Issuer			in opposition of commerce co	interes or chepti				
		Store Location						
		<ul> <li>Current User</li> </ul>						
		Icocal Machine						
		To continue, click Next.						
				Next	Cancel			
	4							
						_	-	

- 5. On the **Export Private Key** screen, complete one of the following tasks:
  - To export the certificate for use on the Senstar Symphony Server, select **Yes, export the private key** and then click **Next**.

• To export the certificate for use on mobile devices, select **No**, **do not export the private key** and then click **Next**.

	1 A								
.onsole Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
Personal	bm.test	SenstarMobileAppCA	10/30/2024	<all></all>	<none></none>			Certificates	
Certificates	Sal qa-srv2019	Senstar Symphony	10/31/2123	<all></all>	qa-srv2019			More Actions	
Trusted Root Certification Authorities	Tige test.senstar.com	SenstarMobile2nn( 2	11/2/2024	< 411>	tect censtar_com			test constar com	
Certificates					~			Marchatlana	
<sup>(2)</sup> Enterprise Trust <sup>(2)</sup> Enterprise Trust <sup>(2)</sup> Intermediate Certification Authorities <sup>(2)</sup> Trusted Publishers <sup>(2)</sup> Untrusted Certificates		← 🐉 Certificate Export Wizard						More Actions	
Comparison of the second		Export Private Key You can choose to export t	he private key with the certific	ate.					
Preview outline hoods     Test Roots     Preview Desktop     Certificate Enrollment Requests		Private keys are password certificate, you must type a Do you want to export the	protected. If you want to exp password on a later page. private key with the certificate	ort the private key with the?	e				
Smart Card Trusted Roots		Yes, export the priv	ate key						
<ul> <li>Trusted Devices</li> <li>Windows Live ID Token Issuer</li> </ul>		○ No, do not export t	he private key						
				Net	Cancel				
				Hex	current				

- 6. On the **Export File Format** page, complete one of the following tasks:
  - To export the certificate for use on the Senstar Symphony Server, select **Personal Information Exchange - PKCS #12 (.PFX), Include all certificates in the certification path if possible**, and **Enable certificate privacy**; and then click **Next**.

Image: Second Secon	puter)\Personal\Certificates]								×
Cenciel Real Concole Concole Concole Concole Concole Concole Concole	Issued To Submitted Supervision Supervisi	Issued By SentatAMbilicAppCA SentatAMbilicAppCA SentatAMbilicAppCA SentatAMbilicAppCA CentralAbilicAppCA Cen	Expiration Date 103/30224 103/32233 110/2014 artety of file formats.	Intended Purposes <ab <ab <ab <ab <ab <ab <ab <ab< td=""><td>Friendly Name + None&gt; @esv2019 test sambg.com X Cancel</td><td>Status</td><td>Certi</td><td>Actions Certificates More Actions test-sensitir .com More Actions</td><td>- - - - </td></ab<></ab </ab </ab </ab </ab </ab </ab 	Friendly Name + None> @esv2019 test sambg.com X Cancel	Status	Certi	Actions Certificates More Actions test-sensitir .com More Actions	- - - - 

 To export the certificate for use on mobile devices, select Base-64 encoded X.509 (.CER) and then click Next.

Console 1 - (Console Root)Certificates (Local Com	nputer)\Personal\Certificates] elp								×
Concus Res (Load Computer)     Control Res (Load Computer)     Control Res (Load Computer)     Control Res (Load Computer)     Control Res (Load Computer)     Thutsel Paul Root Entitlation Authonties     Thutsel Paul Root Entitlation Ruthonties     Thutsel Paul Root Res     Thutsel Paul Root Root Res     Thutsel Paul Root Root Root Res     Thutsel Paul Root Root Root Root Res     Thutsel Root Root Root Root Res     Thutsel Root Root Root Res     Thutsel Root Root Root Root Root Root Root Roo	Kuned 10 Spanhout Spanhout Pletisenstancom	Insued By Isoahort Sender Symphony ←	Expiration Date 11/2/023 10/31/2123 10/31/2123 Interve of file formats. (LCR) EXR) EXRS EXRS Solveded - PVCS # 7 How events associated to the certification path of the cert	Intended Purposes Client Authenticatio. AI> Certificates (P78) possible possible	Friendly Nume chorps) g.e.an2019 X er_com Cancel	Status	Certi	Actions Certificates More Actions Interactions	• • •

7. This step only applies to certificates that you export for use on the Senstar Symphony Server. On the **Security** page, select **Password**, type and confirm a password for the PFX file, and then click **Next**.

Console1 - [Console Root\Certificates (Local Cor Elle Action View Favorites Window H-	nputer)\Personal\Certificates] elp							×
Console Root     Console Root     Console Root     Console Root     Confidence Root     Confidence Root     Confidence Root     Confidence     Thread Root Confidence Authorities     Thread Root Confidence     Thread Root Confidence	Issued To ^ ^ Second Second	I Issued By SentarMobileCopCA Sentar Symphony Central Symphony Central Symphony Central Control Control Umage Descent A Confinetion security, you must pro- um a passend. Confine Descent A Confine Descent A Confine Descent A Confine Descent A Confine Descent A Descent A Descent A Confine Descent A Descent	Expiration Date U0392024 U0392024 U0392024 U0392023 U1272002 U127200 U127200 U127200 U127200 U127200 U12720 U12720 U127200 U127200 U12720	Intended Purposes cAID- cAID- cAID- cAID- security principal or by <u>AAA</u> <u>Benove</u>	Friendly Name (None) (a)-502019 tet usergr_com ×	Status Certi	Actions Certificates More Actions tetLanslat.com More Actions	

8. Select where to save the certificate file and click **Save**.



#### 9. Click **Finish**.

After you export the certificate, add the certificate to the Senstar Symphony Server, iOS devices, or Android devices.

# Add an SSL certificate to the Senstar Symphony Server

After you have installed the certificate on the computer that hosts the Senstar Symphony Server, you must add the certificate to the Senstar Symphony Server and select the certificate for mobile connections using the Senstar Symphony Server configuration interface.

The procedure for adding and selecting SSL certificates changed in Senstar Symphony Server 8.6. Be sure that you are following the procedure for your version of the Senstar Symphony Server.

#### Add an SSL certificate

You can add an SSL certificate to the Senstar Symphony Server in the Senstar Symphony Server configuration interface. This topic applies to Senstar Symphony Server 8.6 and later.

The Senstar Symphony Server uses the SSL certificate to secure connections from browsers and the Senstar Symphony Mobile Application. The Senstar Symphony Server supports PFX certificate files.

- 1. In the Senstar Symphony Server configuration interface, click Settings > Servers.
- 2. Select the Senstar Symphony Server and click Edit.
- 3. Navigate to the SSL Certificate section.
- 4. In the **Password** field, type the password for the certificate.
- 5. Drag the certificate file into the field or browse for the certificate file.
- 6. Click Save.

#### Add an SSL certificate

You can add an SSL certificate to the Senstar Symphony Server in the Senstar Symphony Server configuration interface. This topics applies to Senstar Symphony Server 8.5 and earlier.

The Senstar Symphony Server uses the SSL certificate to secure connections from browsers and the Senstar Symphony Mobile Application.

- 1. In the Senstar Symphony Server configuration interface, click **Settings** > **General Settings**.
- 2. Navigate to the SSL Certificate section.
- 3. In the **Password** field, type the password for the certificate.
- 4. Drag the certificate file into the field or browse for the certificate file.
- 5. Click Save.

#### Configure mobile connections

You can configure the Senstar Symphony Server to support connections with the Senstar Symphony Mobile Application on mobile devices. This topic applies to Senstar Symphony Server 8.6 and later.

- 1. In the Senstar Symphony Server configuration interface, click Settings > Servers.
- 2. Select the Senstar Symphony Server and click Edit.
- 3. Navigate to the Mobile Connections section.
- 4. To select the SSL certificate, click **Change**, select the certificate, and click **OK**.
- 5. To select the network adapter for mobile connections, click **Change**, select the network adapter, and click **OK**.
- 6. In the **Mobile Port** field, set the port that the Senstar Symphony Server uses to listen for requests from mobile devices.
- 7. In the **Video Proxy Port** field, set the port that the Senstar Symphony Server uses to stream video to and receive video from mobile devices.
- 8. Click Save.

#### Configure mobile connections

You can configure the Senstar Symphony Server to support connections with the Senstar Symphony Mobile Application on mobile devices. This topics applies to Senstar Symphony Server 8.5 and earlier.

- 1. In the Senstar Symphony Server configuration interface, click **Settings** > **General Settings**.
- 2. Navigate to the Mobile Connections section.
- 3. To select the SSL certificate, click **Change**, select the certificate, and click **OK**.
- 4. In the **Mobile Port** field, set the port that the Senstar Symphony Server uses to listen for requests from mobile devices.
- 5. In the **Video Proxy Port** field, set the port that the Senstar Symphony Server uses to stream video to and receive video from mobile devices.
- 6. To allow the Senstar Symphony Server to send push notifications to iOS devices, select **Enable iOS Notifications**.
- 7. Click Save.

## Add a certificate to an iOS device

- 1. Send the certificate files to the iOS device.
- 2. Tap the certificate in the email.
- 3. Choose your device to install the profile.
- 4. Tap Settings > General > VPN and Device Management.
- 5. Tap the certificate and follow the on-screen instructions to install the certificate.
- 6. After the certificate is installed, tap **Settings** > **General** > **About** > **Certificate Trust Settings**.
- 7. Enable full trust for the installed certificate.

### Add a certificate to an Android device

- 1. Tap Settings > Security & Privacy > More security & privacy > Encryption & credentials.
- 2. Tap Install a certificate.
- 3. Tap CA certificate.
- 4. Tap Install anyway.
- 5. Browse to the crt file.

You can view or uninstall the certificate in Settings > Security & Privacy > More security & privacy > Encryption & credentials > Trusted credentials > User.