

Senstar Symphony Mobile Application 4.0 Security Guide

Contents

Certificate requirements Obtaining a certificate	3 3
Use the Senstar Symphony Server as a certificate authority Configure the certificate authority Export the certificate authority certificate	5 5 5
Use a trusted certificate authority SSL certificates with the Senstar Symphony Server 8.6.1 Select a certificate authority Configure mobile connections SSL certificates with the Senstar Symphony Server 8.6.0 Add an SSL certificate Configure mobile connections SSL certificates with the Senstar Symphony Server 8.5.x Add an SSL certificate Configure mobile connections	7 7 8 8 8 8 9 9 9
Use a custom certificate authority Install the certificate SSL certificates with the Senstar Symphony Server 8.6.1 Select a certificate authority Configure mobile connections SSL certificates with the Senstar Symphony Server 8.6.0 Add an SSL certificate Configure mobile connections SSL certificates with the Senstar Symphony Server 8.5.x Add an SSL certificate Configure mobile connections	.10 .13 .14 .14 .14 .14 .15 .15 .15 .15
Add a certificate to an iOS device	. 17
Add a certificate to an Android device	.18

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.

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.

Requirements for the certificate authority certificate:

- · Must be within the Not Before and Not After dates
- The RSA key size must be 2048 bits or longer
- · The hash algorithm must be in the SHA-2 family
- · The basic constraints must contain certificate authority usage

Requirements for the SSL certificate on the server

- · Must be within the Not Before and Not After dates
- The RSA key size must be 2048 bits or longer
- · The hash algorithm must be in the SHA-2 family
- The Subject Alternative Name must contain at least one DNS entry
- · The enhanced key usage must contain the server authentication usage
- · The validity period must be 825 days or less

Obtaining a certificate

You can obtain a certificate from the Senstar Symphony Server, a trusted certificate authority, or from a custom certificate authority that you create for your organization.

Certificate issuer	Requirements	Domain ownership	Notes
Senstar Symphony Server	Senstar Symphony Server 8.6.1 or later	Required (or static IP)	With the Senstar Symphony Server 8.6.1 and later, you can configure the Senstar Symphony Server to act as a certificate authority.
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.

Certificate issuer	Requirements	Domain ownership	Notes
Custom certificate authority	Deploy the custom certificate authority certificate to 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.

Use the Senstar Symphony Server as a certificate authority

You can use the Senstar Symphony Server as a certificate authority to secure communication between the Senstar Symphony Server and the Senstar Symphony Mobile Application.



Important: The functionality to act as a certificate authority is available in the Senstar Symphony Server 8.6.1 and later.

- 1. Configure the Senstar Symphony Server to act as a certificate authority.
- 2. Export the Senstar Symphony Server certificate authority certificate.
- 3. (Optional) Install the certificate authority certificate on the other Senstar Symphony Server instances in the server farm and use the Senstar Symphony setup wizard to select the Senstar Symphony Server as the certificate authority.
- 4. Install the Senstar Symphony Server certificate authority certificate on the mobile device.
- 5. Configure mobile connections on the Senstar Symphony Server.
- 6. Add the Senstar Symphony Server as a site in the Senstar Symphony Mobile Application to connect the mobile device to the Senstar Symphony Server.

Configure the certificate authority

You can configure the Senstar Symphony Server 8.6.1 or later to act as a certificate authority in the Senstar Symphony setup wizard. See the Senstar Symphony Installation Guide for more information.

You can configure the Senstar Symphony Server to act as a certificate authority when you install the Senstar Symphony Server or after installation by using the setup wizard.

- 1. Run the Senstar Symphony setup wizard.
- 2. In the **Networking** pane on the **Server Configuration** tab, select **Have the setup wizard generate SSL certificates** and type your domain in the **Domain name** field.

Vetworking		
Allow modification of the Windows dynamic port	range settings 🔽	
Port 443 -		
Select an SSL certificate:	Select item	~
Select an SSL certificate authority:	Select item	~
Have the setup wizard generate SSL certific	ates.	
Domain name:	example.com	
		Verify

- 3. Click **Verify**.
- 4. Click Apply.

The Senstar Symphony Server generates a certificate authority certificate and installs it on the computer that hosts the Senstar Symphony Server. You can export the certificate authority certificate to install it on other Senstar Symphony Server instances in a server farm or on mobile devices so that the Senstar Symphony Mobile Application can use the Senstar Symphony Server as a certificate authority.

Export the certificate authority certificate

You can export the certificate authority certificate to add it to mobile devices

- 1. Open the Microsoft Management Console by pressing Windows + R, typing MMC, and pressing Enter.
- 2. To add the Certificates snap-in to the Microsoft Management Console, complete the following steps:
 - a) In the Microsoft Management Console, click **File > Add/Remove Snap-in**.

b) In the Add or Remove Snap-ins window, click Certificates and click Add.

valiable snap-ins:			1	Selected snap-ins:	
Snap-in	Vendor			Console R	Edit Extensions.
📩 ActiveX Control	Microsoft Co				Remove
Authorization Man	Microsoft Co				
Certificates	Microsoft Co				Mayalla
Component Services	Microsoft Co	Т			wove op
F Computer Manage	Microsoft Co	1			Move Down
🖣 Device Manager	Microsoft Co		Add >		
Ŧ Disk Management	Microsoft an				
🛃 Event Viewer	Microsoft Co				
📔 Folder	Microsoft Co				
Group Policy Obje	Microsoft Co				
Hyper-V Manager	Microsoft Co				
🛃 IP Security Monitor	Microsoft Co				Advanced

- c) In the Certificates snap-in window, select Computer account and click Next.
- d) In the Select Computer window, select Local computer and click Finish.
- e) In the Add or Remove Snap-ins window, click OK.
- 3. In the Microsoft Management Console, click Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates

Console Root	based To	based By	Expiration Date	Intended Purposes	Friendly Name	Status C	Actions	
Cetificates (Local Computer)	AAA Cetificate Services	AAA Cetificate Services	12/31/2028	Client Authenticati	Section (AAA)		Certificates	
Personal	Add hust External CA Root	AddTrust External CA Root	5/30/2020	Client Authenticati	Section (AddTrust)		14	
Trusted Root Certification Authorities	Baltimore CyberTrust Root	Baltimore Cyber Trust Root	5/12/2025	Client Authenticati	DisiCet Baltimore		More Actions	
Cetholes	Bitdefender Personal CA.000000.	Ekdefender Personal CA.00000000.	10/11/2013	<ad></ad>	(None)			
Enterproc Inut	Certurn CA	Certare CA	6/11/2027	Client Authenticati	Certarn			
Intermediate Centrication Authorities	Cetum Trutted Network CA	Certurn Trutted Network CA	12/31/2029	Client Authenticati	Certurn Trated Net			
C University of Cashillandary	Cless 3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/1/2028	Cient Authenticati	VeriSign Class 3 Pp.,			
Dist. Party Bost Cartification Authorities	COMODO RSA Certification Au-	COMODO RSA Cetification Auth.	1/18/2098	Client Authenticati	Section Bormerly C			
Tructed People	Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta			
Client Authentication Issuers	DigiCert Assured ID Root CA	DisiCet Assured ID Root CA	11/9/2031	Clent Authenticati	DisiCet			
Preview Build Roots	DigiCent CS RSA4096 Root G5	DigiCett CS RSA4096 Root GS	1/14/2046	Code Signing, Time	DigiCett CS RSA409_			
Test Roots	DigiCert Global Root CA	DisiCert Global Root CA	11/9/2031	Client Authenticati	DisKet			
AAD Token bouer	DigiCert Global Root G2	DigiCert Global Root G2	1/15/2008	Client Authenticati	DigiCet Global Roo			
eSM Certification Authorities	DigiCert Global Root G3	DisiCert Global Root G3	1/15/2038	Ciert Authenticati	DipiCert Global Roo			
Homegroup Machine Certificates	DigiCert High Assurance EV Ro	DigiCet High Assurance EV Root	11/9/2031	Client Authenticati	DigiCet			
Cocal NonRemovable Certificates	DigiCert Trusted Root 64	DigiCert Trusted Root G4	1/15/2038	Client Authenticeti	DigiCert Trasted Ro			
CEM eSIM Certification Authorities	DST Reet CA X3	DSTRoot CA X3	9/30/2021	Client Authenticati	DST Root CA X3			
Passpoint Trusted Roots	Entrust Root Certification Auth	Entrust Root Certification Authority	11/27/2026	Client Authenticati	Entrust			
Smart Card Trusted Roots	Entrust Root Certification Auth	Entrust Root Certification Authori	12/18/2037	Client Authenticati	Entrust Root Certifi-			
Trusted Packaged App Installation Authorit	Entrust Root Certification Auth	Intrust Root Certification Authoriu.	12/7/2000	Client Authenticati	Entruct.net			
Inusted Devices	Entrust net Certification Author	Entrust net Certification Authority	7/24/2029	Client Authenticati	Entrust (2048)			
Windows Live ID loken Issuer	GlobalSign	GlobalSign	3/10/2029	Client Authenticati	GlebalSign Root CA.			
windowserverupdateservices	GlobalSign	GlobelSign	12/9/2034	Ciert Authenticati	GlobalSign Root CA.			
	GlobalSign Code Signing Root	GlobalSign Code Signing Root R45	3/17/2045	Code Signing	GlobalSign Code Si			
	GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticeti	Globalbign Root CA			
	Go Daddy Class 2 Certification	Go Daddy Class 2 Certification Au.	6/29/2034	Client Authenticati	Go Daddy Class 2 C			
	Go Daddy Root Certificate Auth-	Go Daddy Root Certificate Author	12/31/2037	Client Authenticati	Go Daddy Reet Car			
	GTS Reet R4	GTS Root R4	6/21/2096	Client Authenticati	GTS Root R4			
	Hotspot 2.0 Trust Reet CA - 03	Hetspot 2.0 Trust Root CA - 03	12/8/2043	Client Authenticati	Hotspot 2.0 Trust R.,			
	G ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticati	ISRG Root X1			
	Microsoft Authenticodeltm) Ro-	Microsoft Authenticode/tml Root	12/31/1999	Secure Imail: Code	Microsoft Authenti			

- 4. Right click the certificate and click **All Tasks > Export**.
- 5. Click Next.
- 6. On the Export File Format page, select DER encoded binary X.509 (.CER) and click Next.



- 7. Type a file name and click **Next**.
- 8. Click Finish.

After you export the certificate authority certificate, add the certificate authority certificate to mobile devices.

Use a trusted certificate authority

You can use a trusted certificate authority to secure communication between the Senstar Symphony Server and the Senstar Symphony Mobile Application.

1. Choose a certificate authority.

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

2. Generate a certificate signing request.

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

3. Submit the certificate signing request to the certificate authority.

Once you have generated a certificate signing request, you submit the certificate signing request to the certificate authority. The certificate authority that you select provides detailed information about how to submit a certificate signing request (usually using the website of the certificate authority). The certificate authority uses your certificate signing request to generate the certificate.

4. Validate your domain ownership.

The certificate authority might require that you validate your domain ownership. This typically involves responding to a confirmation email that the certificate authority 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 certificate authority and the type of certificate.

5. Issue the certificate.

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

After you obtain a certificate, follow the instructions from your chosen certificate authority to install the certificate.

SSL certificates with the Senstar Symphony Server 8.6.1

After you have installed the certificate authority certificate on the computer that hosts the Senstar Symphony Server, you must select the certificate authority certificate for mobile connections.

In the Senstar Symphony Server 8.6.1 and later, you add certificates in the Senstar Symphony setup wizard and you configure mobile connections on the **Settings** > **Servers** page in the Senstar Symphony Server configuration interface. For more information, see the Senstar Symphony Installation Guide.

Select a certificate authority

For the Senstar Symphony Server 8.6.1 or later, you can select a certificate authority in the Senstar Symphony setup wizard.

- 1. Run the Senstar Symphony setup wizard.
- 2. In the **Networking** pane on the **Server Configuration** tab, select **Select an SSL certificate authority** and select the certificate authority in the list.

- 3. Click Verify.
- 4. Click Apply.

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 8.6.1 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 network adapter for mobile connections, click **Change**, select the network adapter, and click **OK**.
- 5. In the **Mobile Port** field, set the port that the Senstar Symphony Server uses to listen for requests from mobile devices.
- 6. 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.
- Click Save.

SSL certificates with the Senstar Symphony Server 8.6.0

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.

In the Senstar Symphony Server 8.6.0, you add certificates and configure mobile connections on the **Settings > Servers** page in the Senstar Symphony Server configuration interface.

Add an SSL certificate

You can add an SSL certificate to the Senstar Symphony Server in the Senstar Symphony Server configuration interface. This topic only applies to Senstar Symphony Server 8.6.0. In the Senstar Symphony Server 8.6.1, the SSL certificate settings moved to the setup wizard. See the Senstar Symphony Installation Guide for more information.

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.

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 8.6.0.

You configure the SSL certificate that the Senstar Symphony Server uses for mobile connections in the Senstar Symphony setup wizard.

- 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.

SSL certificates with the Senstar Symphony Server 8.5.x

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.

In the Senstar Symphony Server 8.5.x, you add certificates and configure mobile connections on the **Settings** > **General Settings** page in the Senstar Symphony Server configuration interface.

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 topics applies to Senstar Symphony Server 8.5.x 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.

Use a custom certificate authority

You can use a custom certificate authority to secure communication between the Senstar Symphony Server and the Senstar Symphony Mobile Application.

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 .

- 1. Generate the certificate signing request.
- 2. Have your IT department generate the certificate.
- 3. Install the certificate authority certificate on the computer that hosts the Senstar Symphony Server.
- 4. Add the certificate to the Senstar Symphony Server and configure the certificate for mobile connections.
- 5. Export the Add the certificate to mobile devices.

Install the certificate

Install the certificate authority 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.

Paragua
Parates
Kentove
Move Up
Move Down
Advanced

4. Select Computer account and click Next.



5. Select Local computer and click Finish.



- 6. Click OK.
- 7. In the Microsoft Management Console, click **Console Root** > **Certificates (Local Computer** > **Trusted Root Certification Authorities** > **Certificates**

	r -							- 0 /
	<u>^</u>							
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status C	Actions	
Berronal	AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati	Sectigo (AAA)		Certificates	-
7 Tourted Post Certification Authorities	🔄 AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Client Authenticati	Sectigo (AddTrust)		More Actions	•
Certificates	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati	DigiCert Baltimore			
Enterprise Trust	Bitdefender Personal CA.000000	Bitdefender Personal CA.00000000	10/13/2033	<all></all>	<none></none>			
> Intermediate Certification Authorities	Certum CA	Certum CA	6/11/2027	Client Authenticati	Certum			
> i Trusted Publishers	Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Client Authenticati	Certurn Trusted Net			
> iii Untrusted Certificates	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/1/2028	Client Authenticati	VeriSign Class 3 Pu			
> iii Third-Party Root Certification Authorities	COMODO RSA Certification Au	COMODO RSA Certification Auth	1/18/2038	Client Authenticati	Sectigo (formerly C			
> 🧾 Trusted People	Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta			
> 🧾 Client Authentication Issuers	DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authenticati	DigiCert			
> Preview Build Roots	DigiCert CS RSA4096 Root G5	DigiCert CS RSA4096 Root G5	1/14/2046	Code Signing, Time	DigiCert CS RSA409			
> 📫 Test Roots	🔄 DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati	DigiCert			
> 📫 AAD Token Issuer	🖙 DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati	DigiCert Global Roo			
> In eSIM Certification Authorities	🕞 DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authenticati	DigiCert Global Roo			
> Homegroup Machine Certificates	DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root	11/9/2031	Client Authenticati	DigiCert			
> Local NonRemovable Certificates	DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati	DigiCert Trusted Ro			
> OEM eSIM Certification Authorities	DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati	DST Root CA X3			
Passpoint Irusted Roots	Entrust Root Certification Auth	Entrust Root Certification Authority	11/27/2026	Client Authenticati	Entrust			
> Smart Card Irusted Roots	Entrust Root Certification Auth	Entrust Root Certification Authori	12/18/2037	Client Authenticati	Entrust Root Certifi			
Trusted Packaged App Installation Addition	Entrust Root Certification Auth	Entrust Root Certification Authori	12/7/2030	Client Authenticati	Entrust.net			
Windows Live ID Token Issuer	Entrust.net Certification Author	Entrust.net Certification Authority	7/24/2029	Client Authenticati	Entrust (2048)			
WindowsServerUndateServices	🕎 GlobalSign	GlobalSign	3/18/2029	Client Authenticati	GlobalSign Root CA			
/	🖙 GlobalSign Code Signing Root	GlobalSign Code Signing Root R45	3/17/2045	Code Signing	GlobalSign Code Si			
	🕞 GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticati	GlobalSign Root CA			
	Go Daddy Class 2 Certification	Go Daddy Class 2 Certification Au	6/29/2034	Client Authenticati	Go Daddy Class 2 C			
	Go Daddy Root Certificate Auth	Go Daddy Root Certificate Author	12/31/2037	Client Authenticati	Go Daddy Root Cer			
	GTS Root R4	GTS Root R4	6/21/2036	Client Authenticati	GTS Root R4			
	Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Client Authenticati	Hotspot 2.0 Trust R			
	ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticati	ISRG Root X1			
	Given State Authenticode (tm) Ro	Microsoft Authenticode(tm) Root	12/31/1999	Secure Email, Code	Microsoft Authenti			
	Microsoft FCC Product Root Ce	Microsoft ECC Product Root Certi-	2/27/2043	< 411>	Microsoft ECC Prod			

8. To open the Certificate Import Wizard, click right click in the Details pane and click Action > All Tasks > Import.

9. In the Certificate Import Wizard, click Next.



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

File to Im	ort			
Speci	y the file you want to in	nport.		
File n	ame:			
C:\(artificates\Senstar.cer			Browse
Note	More than one certifica	ate can be stored in a	single file in the fo	llowing formats:
Pe	rsonal Information Exch	ange- PKCS #12 (.PF)	(,.P12)	
C	yptographic Message Sy	ntax Standard- PKCS	#7 Certificates (.	P 7 B)
M	rosoft Serialized Certific	ate Store (.SST)		

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

r	×
🔶 😼 Certificate Import Wizard	
Certificate 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 Browse	
Next Cance	e)

12. Click Finish.

🤶 🍃 Certifi	icate Import Wizard			×
Con	npleting the Certific	ate Import Wizard		
The ce	ertificate will be imported after	you dick Finish.		
You hi	ave specified the following sett	ings:		
Cert	tificate Store Selected by User tent	Trusted Root Certification Authoritie Certificate	s	
File I	Name	C:\certificates\Senstar.cer		
L]	
		Fini	sh Cance	el 🛛

After you install the certificate authority certificate, you can select the certificate for use with the Senstar Symphony Server and export the certificate authority certificate to install and use on mobile devices.

SSL certificates with the Senstar Symphony Server 8.6.1

After you have installed the certificate authority certificate on the computer that hosts the Senstar Symphony Server, you must select the certificate authority certificate for mobile connections.

In the Senstar Symphony Server 8.6.1 and later, you add certificates in the Senstar Symphony setup wizard and you configure mobile connections on the **Settings** > **Servers** page in the Senstar Symphony Server configuration interface. For more information, see the Senstar Symphony Installation Guide.

Select a certificate authority

For the Senstar Symphony Server 8.6.1 or later, you can select a certificate authority in the Senstar Symphony setup wizard.

- 1. Run the Senstar Symphony setup wizard.
- 2. In the **Networking** pane on the **Server Configuration** tab, select **Select an SSL certificate authority** and select the certificate authority in the list.
- 3. Click Verify.
- 4. Click **Apply**.

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 8.6.1 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 network adapter for mobile connections, click **Change**, select the network adapter, and click **OK**.
- 5. In the **Mobile Port** field, set the port that the Senstar Symphony Server uses to listen for requests from mobile devices.
- 6. 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.
- 7. Click Save.

SSL certificates with the Senstar Symphony Server 8.6.0

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.

In the Senstar Symphony Server 8.6.0, you add certificates and configure mobile connections on the **Settings > Servers** page in the Senstar Symphony Server configuration interface.

Add an SSL certificate

You can add an SSL certificate to the Senstar Symphony Server in the Senstar Symphony Server configuration interface. This topic only applies to Senstar Symphony Server 8.6.0. In the Senstar Symphony Server 8.6.1, the SSL certificate settings moved to the setup wizard. See the Senstar Symphony Installation Guide for more information.

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.

SENSTAR_{...}

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 8.6.0.

You configure the SSL certificate that the Senstar Symphony Server uses for mobile connections in the Senstar Symphony setup wizard.

- 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.

SSL certificates with the Senstar Symphony Server 8.5.x

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.

In the Senstar Symphony Server 8.5.x, you add certificates and configure mobile connections on the **Settings** > **General Settings** page in the Senstar Symphony Server configuration interface.

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 topics applies to Senstar Symphony Server 8.5.x 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

To connect the Senstar Symphony Mobile Application on an iOS device to the Senstar Symphony Server, you must install the certificate authority certificate.



Important: The location of the certificate settings can vary in different versions of iOS.

- Send the certificate files to the iOS device.
 You can send the certificate to the iOS device by email or by using cloud storage.
- 2. Tap the certificate in the email or iCloud.
- 3. Choose your device to download the profile.
- 4. Tap Settings > General > VPN and Device Management.
- 5. Tap the downloaded profile.
- 6. Tap Install.
- 7. Tap Install.
- 8. If prompted, type your passcode.
- 9. Tap Install.
- 10. Tap **Done**.
- 11. After the certificate is installed, tap Settings > General > About > Certificate Trust Settings.
- 12. Enable full trust for the installed certificate.

Add a certificate to an Android device

To connect the Senstar Symphony Mobile Application on an Android device to the Senstar Symphony Server, you must install the certificate authority certificate.



Important: The location of the certificate settings can vary in different versions of Android.

- 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 certificate file and tap the file to install it.

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