Senstar Symphony Mobile Application

4.0

Security Guide

Contents

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.

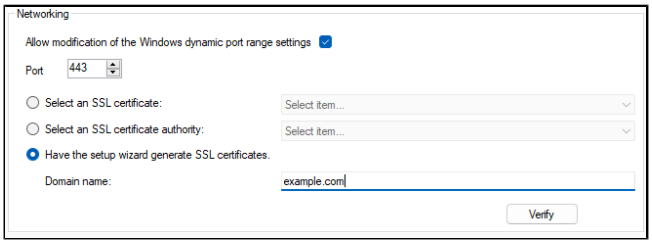
1. Configure the Senstar Symphony Server to act as a certificate authority.
2. Export the Senstar Symphony Server certificate authority certificate.
3. (Optional) Install the certificate authority certificate on the other Senstar Symphony Server instances in the server farm and use the Senstar Symphony 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.



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

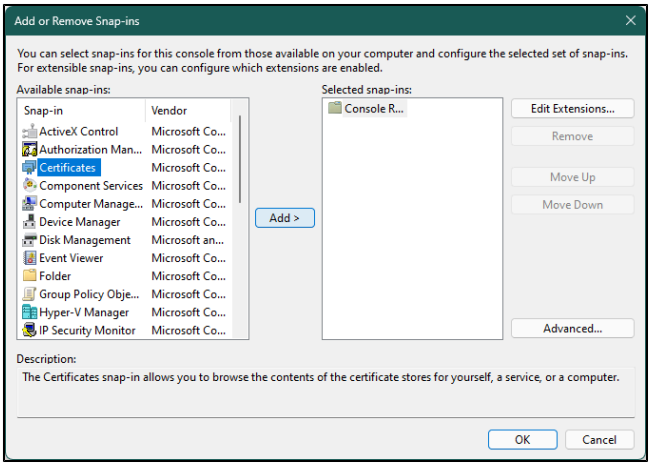
The Senstar Symphony Server generates a certificate authority certificate and installs it on the computer that hosts the Senstar Symphony Server. You can export the certificate authority certificate to install it on other Senstar Symphony Server instances in a server farm or on mobile devices so that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

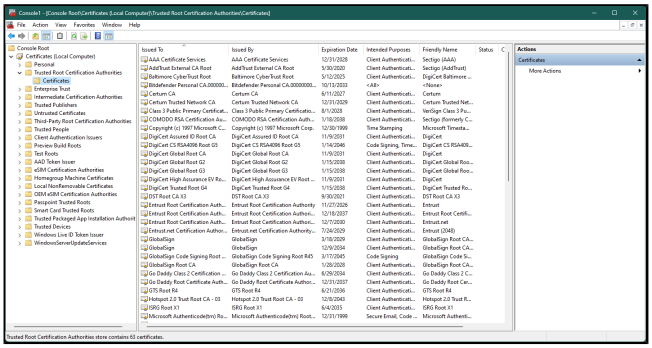


c) In the **Certificates snap-in** window, select **Computer account** and click **Next**.

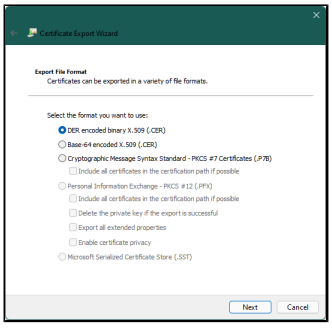
d) In the **Select Computer** window, select **Local computer** and click **Finish**.

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**



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.
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**.

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.

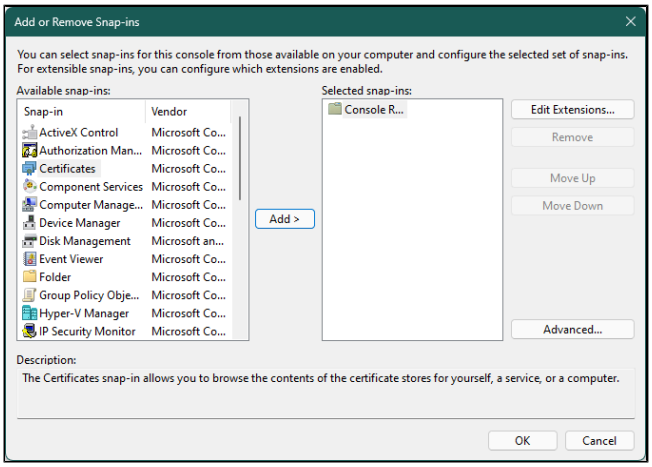
This solution is recommended in cases where your organization manages all of the mobile devices that run the Senstar Symphony Mobile Application. Your IT department needs to deploy and install the custom certificate authority that signs the SSL certificate. The custom certificate authority needs to be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

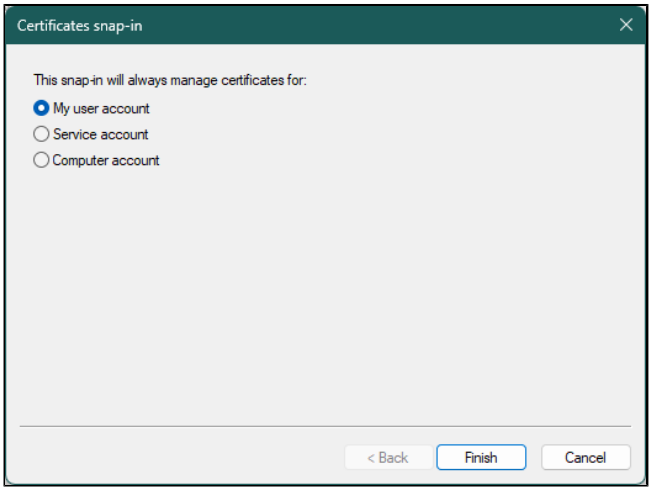
Install the certificate

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

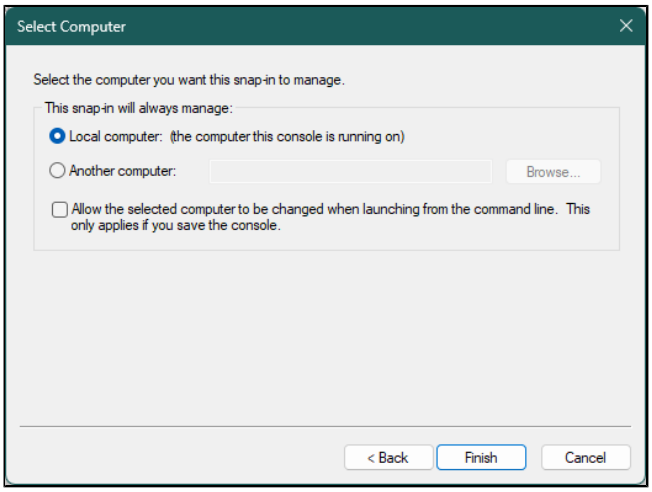
1. Open the Microsoft Management Console by pressing `Windows + R`, typing `MMC`, and pressing **Enter**.
2. Click **File** > **Add/Remove Snap-In**.
3. In the **Available snap-ins** list, select **Certificates** and click **Add**.



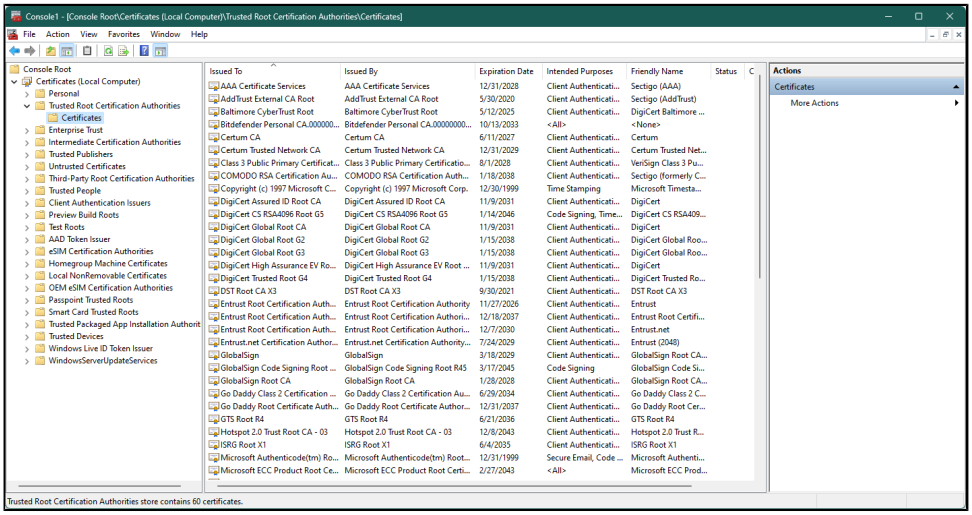
4. Select **Computer account** and click **Next**.



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

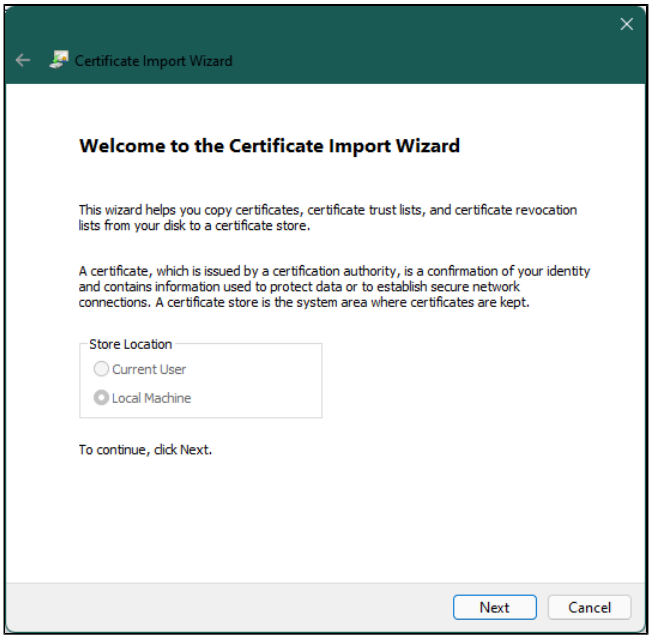


6. Click **OK**.
7. In the Microsoft Management Console, click **Console Root** > **Certificates (Local Computer** > **Trusted Root Certification Authorities** > **Certificates**

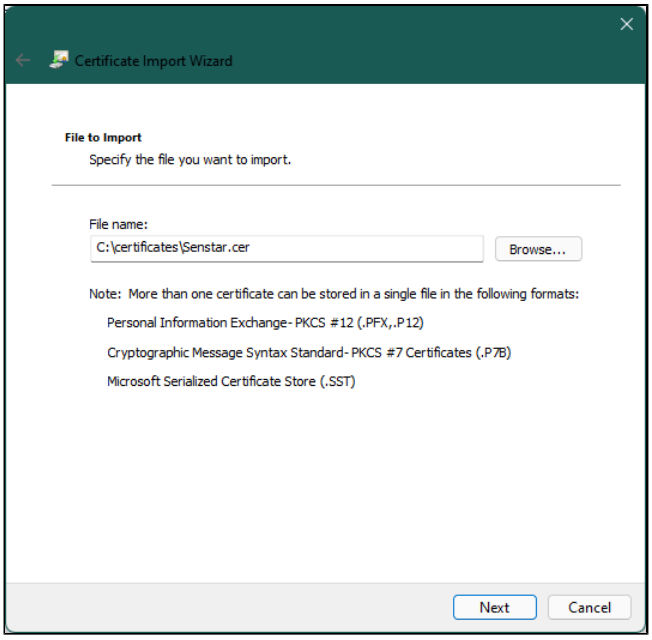


8. To open the Certificate Import Wizard, click right click in the Details pane and click **Action** > **All Tasks** > **Import**.

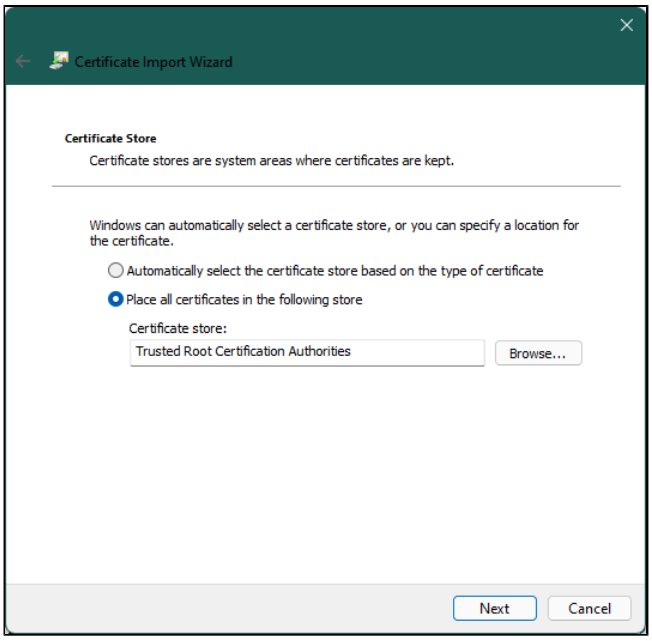
9. In the Certificate Import Wizard, click **Next**.



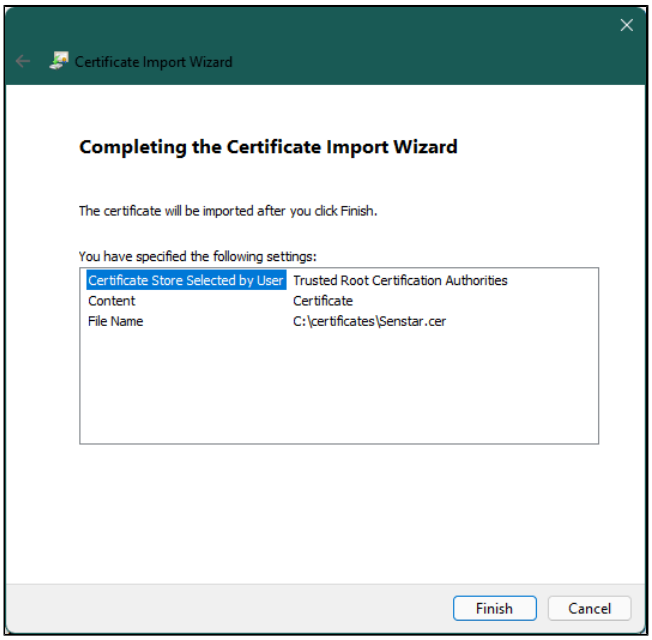
10. Browse to and select the certificate from the certificate authority and click **Next**.



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



12. Click **Finish**.



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**.

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.

1. 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**.