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 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:

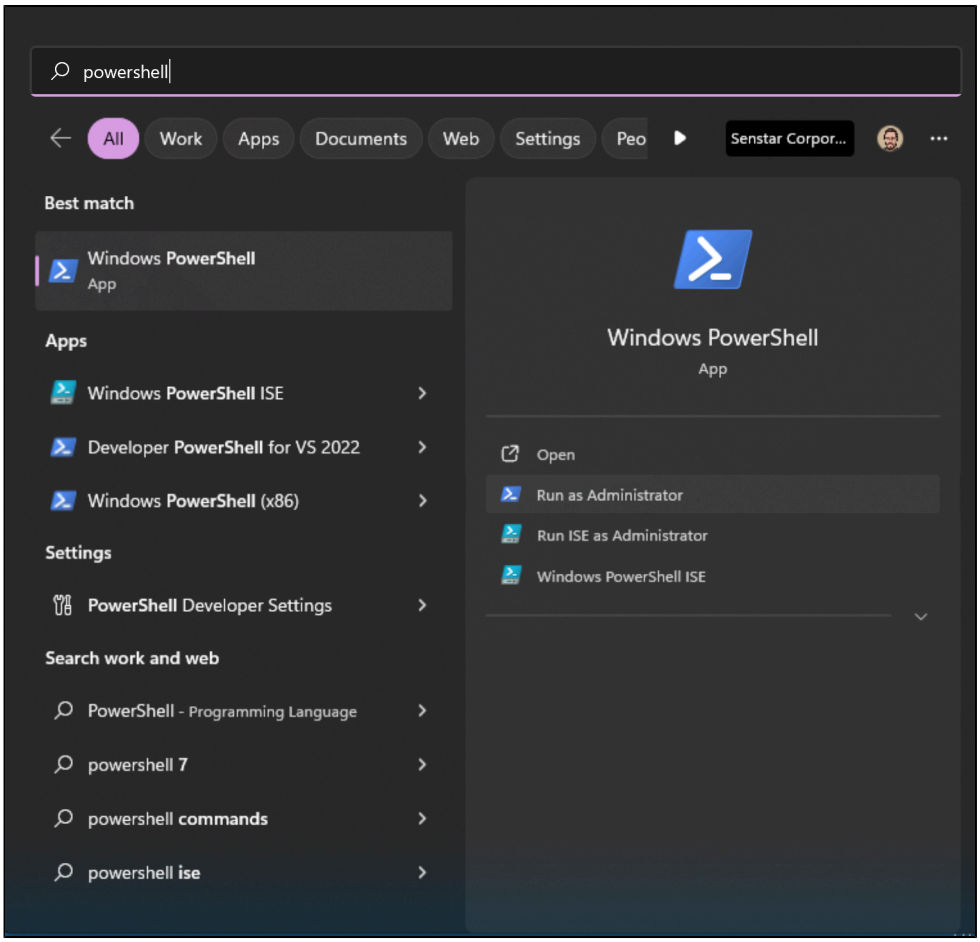
1. Generate the certificate signing request (CSR).
2. Have your IT department generate the certificate.
3. Install the certificate.
4. Export the certificate.
5. Add the certificate to the Senstar Symphony Server and configure the certificate for mobile connections.
6. Add the certificate to mobile devices.

Use a self-signed SSL certificate

If you choose not to get a certificate from a trusted certificate authority, you can create your own self-signed 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
        '2.5.29.19={critical}{text}ca=true&pathlength=0', #Certificate Authority
        '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
   ```

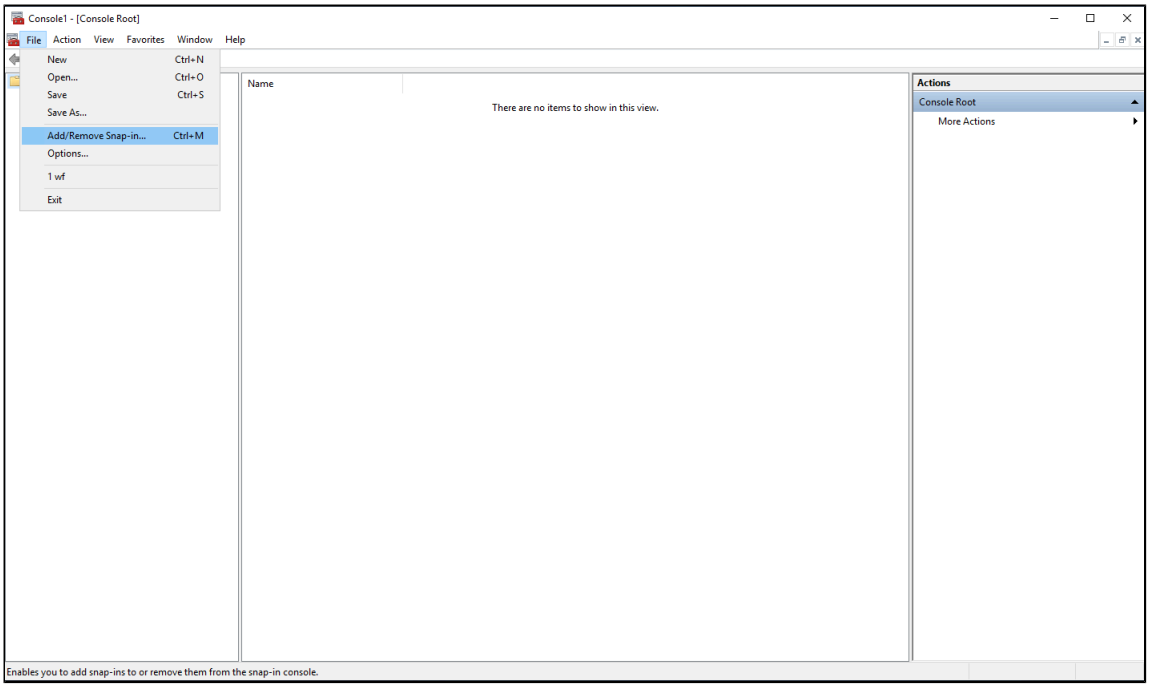
   After you run this command, you receive a confirmation message that the self-signed certificate was generated and added to the certificate store on the computer.

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

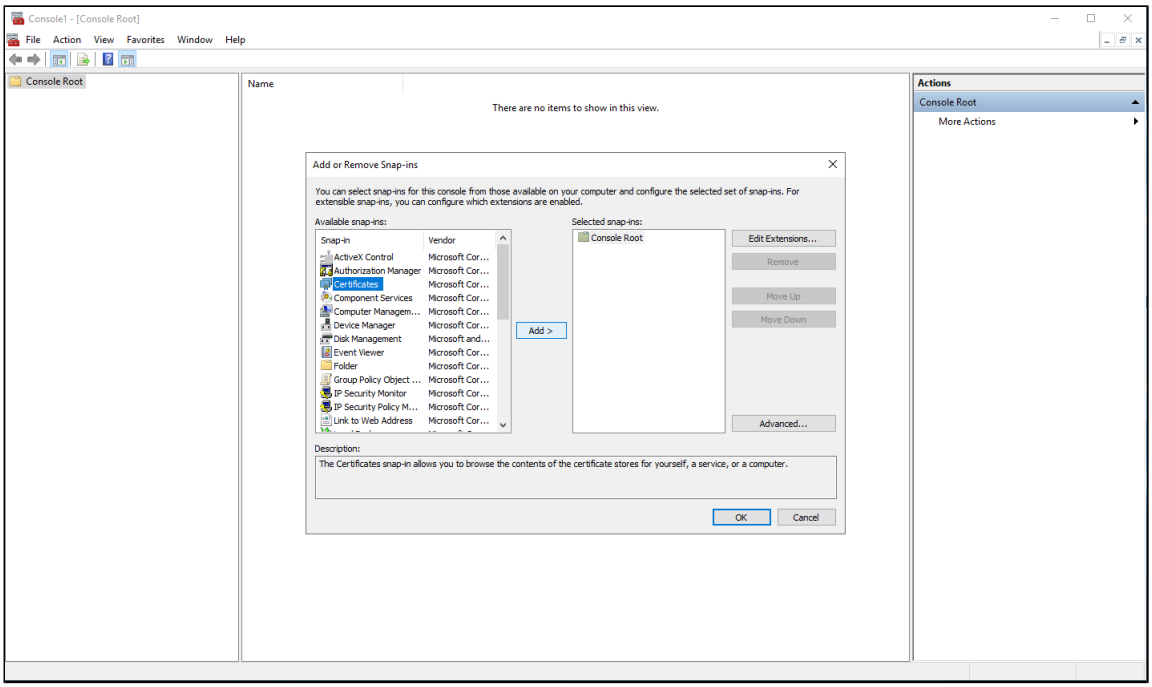
Install the certificate

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

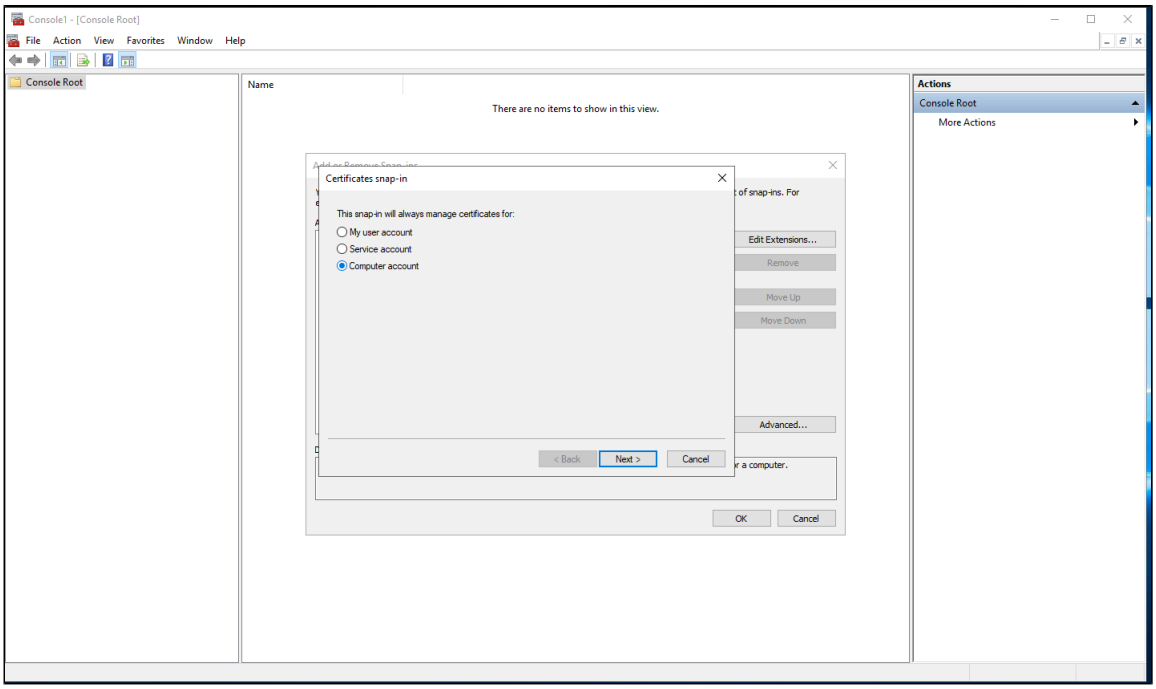
1. Open the Microsoft Management Console by pressing `Windows + R`, typing `MMC`, and pressing **Enter**.
2. Click **File** > **Add/Remove Snap-In** > **.**



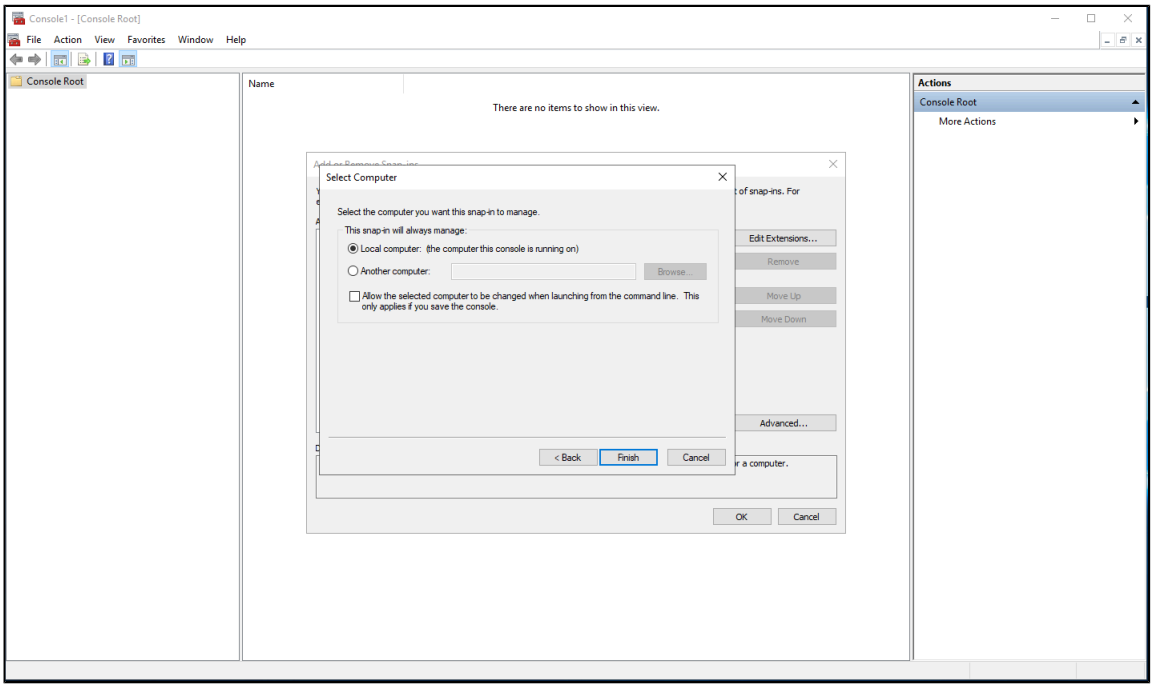
3. In the **Available snap-ins** list, select **Certificates** and click **Add**.



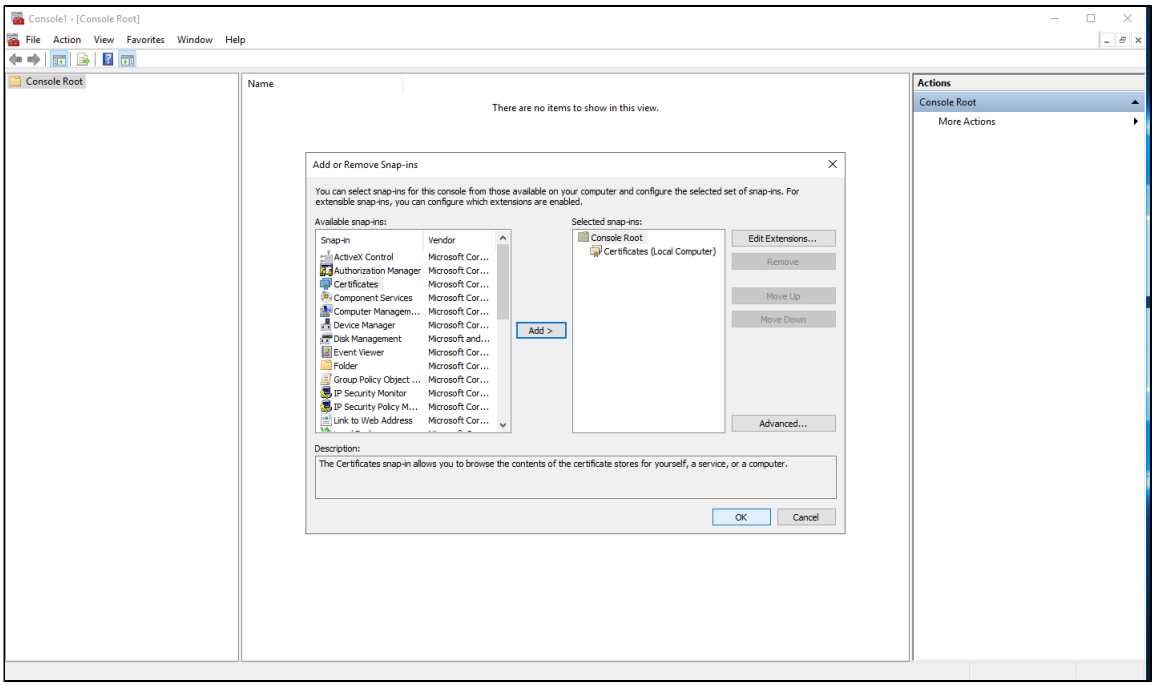
4. Select **Computer account** and click **Next**.



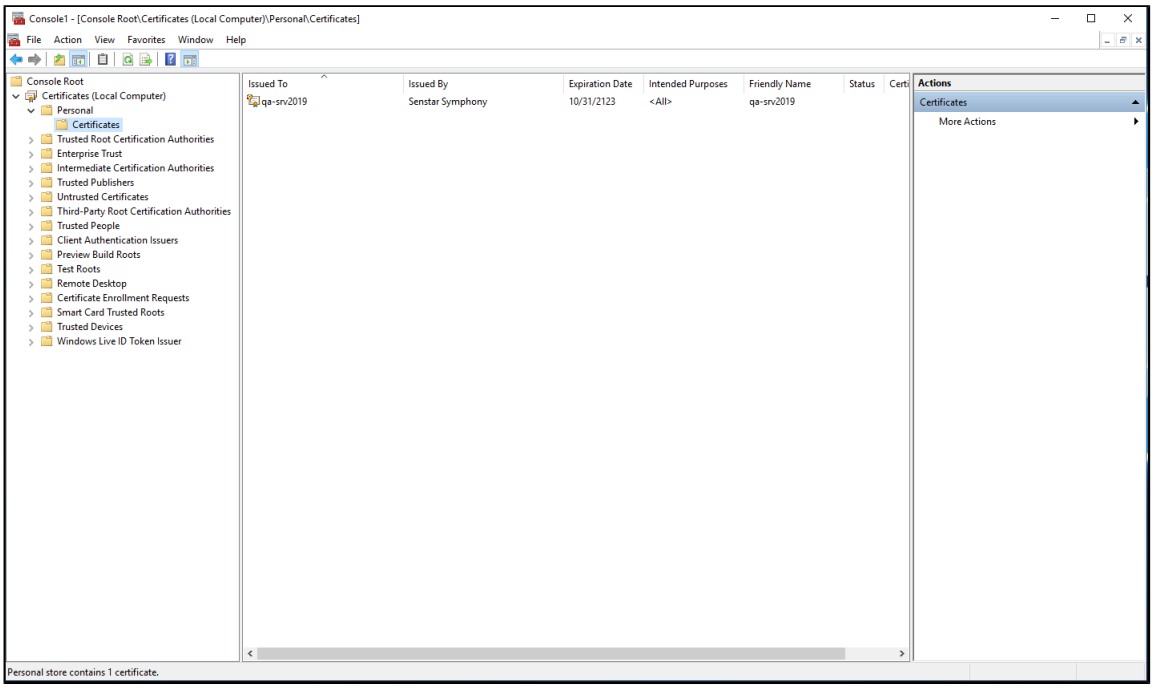
5. Select **Local computer** and click **Finish**.



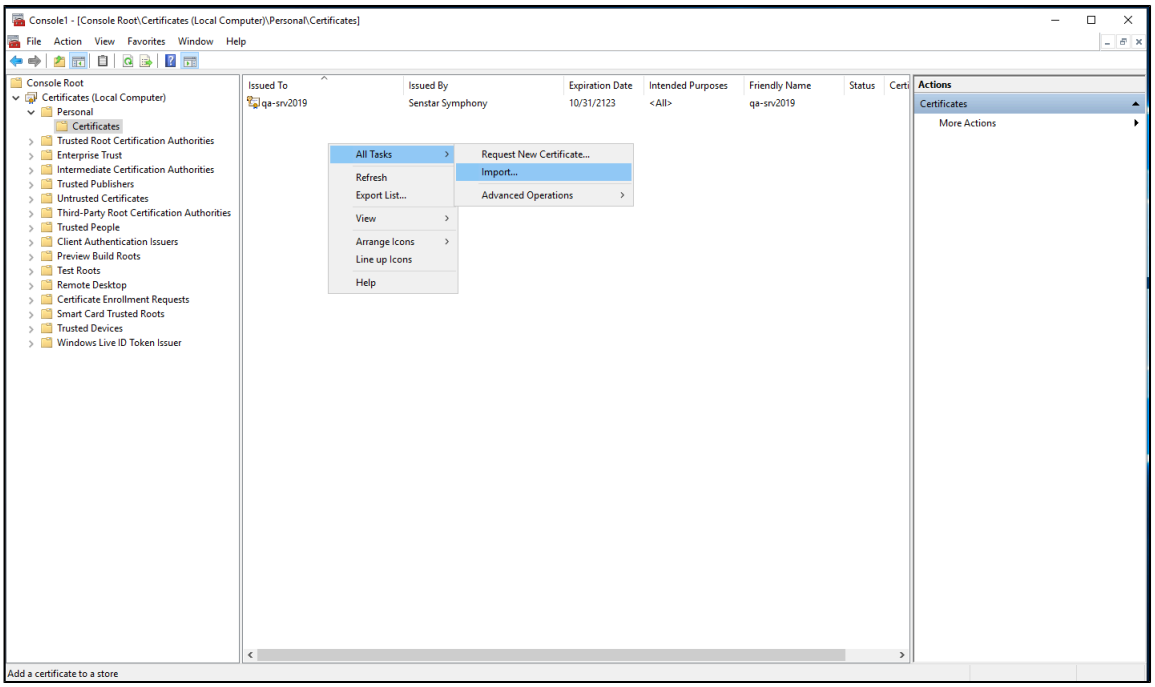
6. Click **OK**.



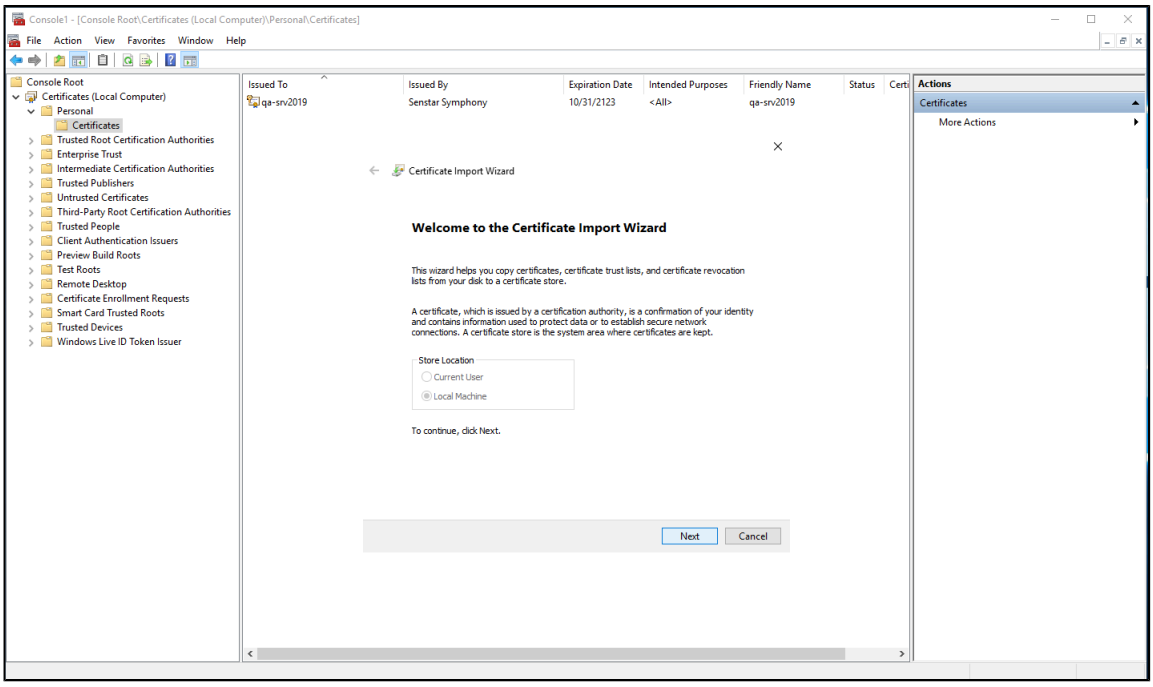
7. In the Microsoft Management Console, click **Console Root** > **Certificates (Local Computer** > **Personal** > **Certificates**



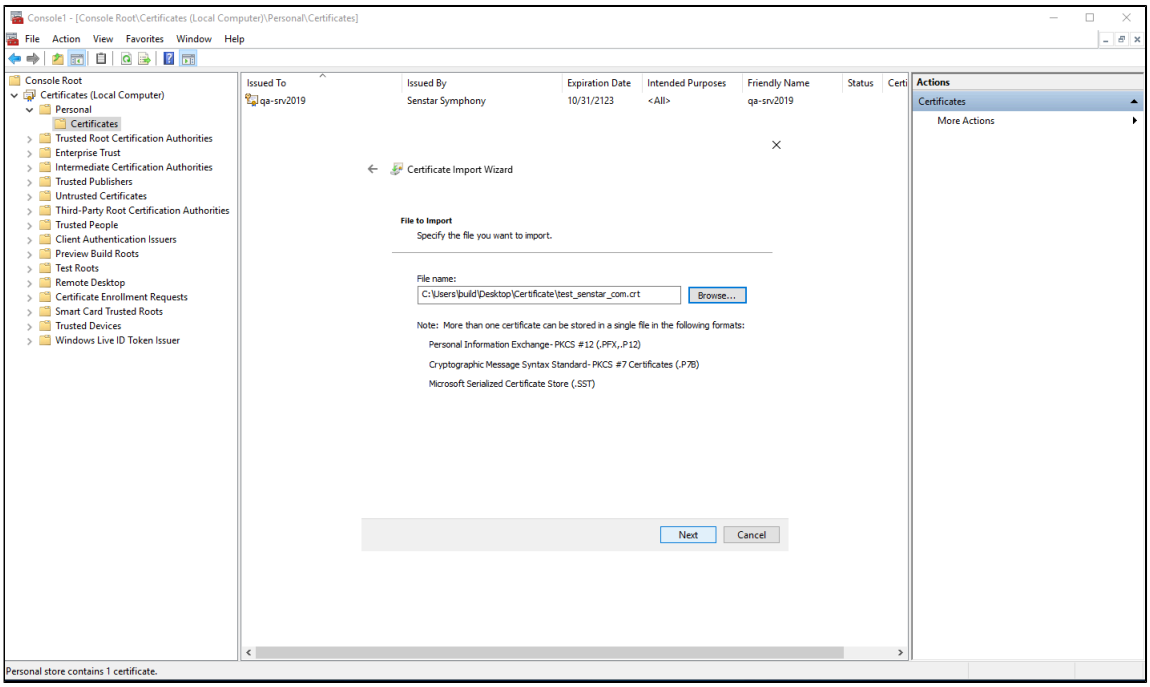
8. To open the Certificate Import Wizard, right click in the Details pane and click **All Tests** > **Import**.



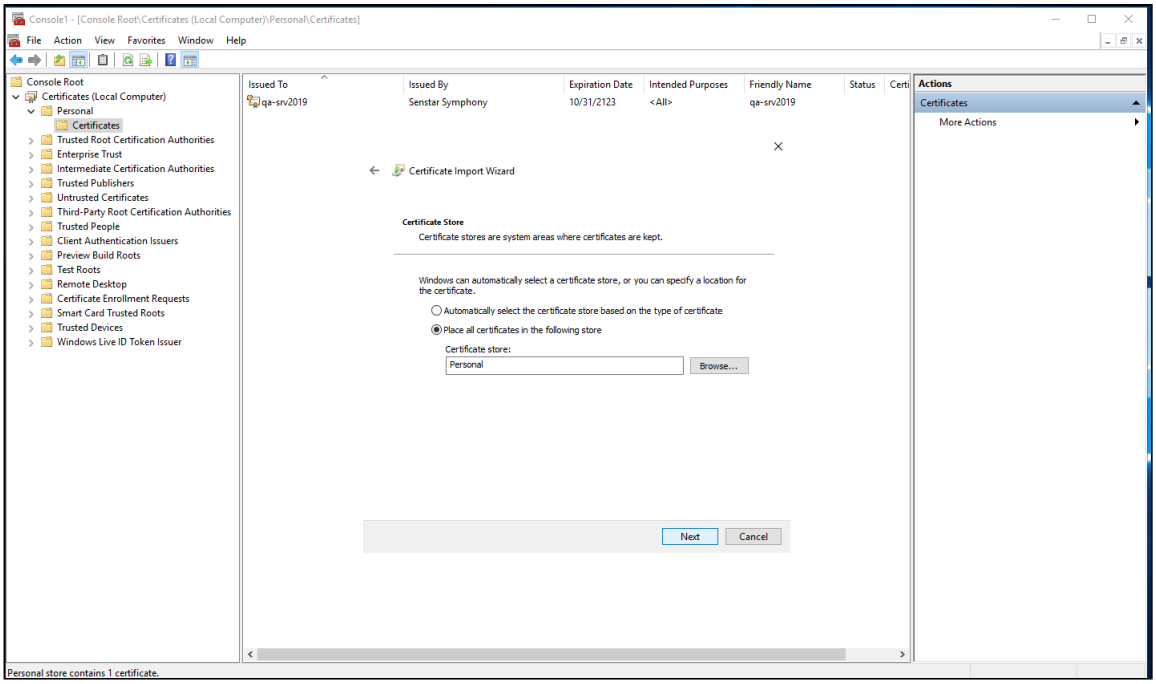
9. In the Certificate Import Wizard, click **Next**.



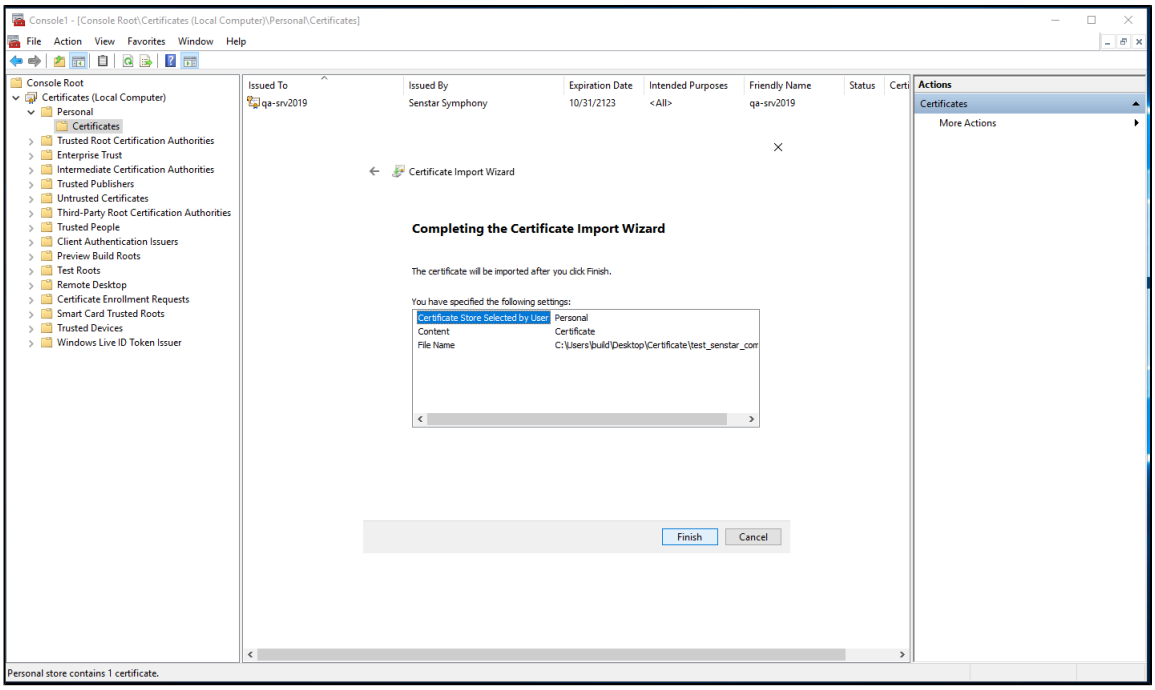
10. Browse to and select the certificate from the certificate authority and click **Next**.



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



12. Click **Finish**.



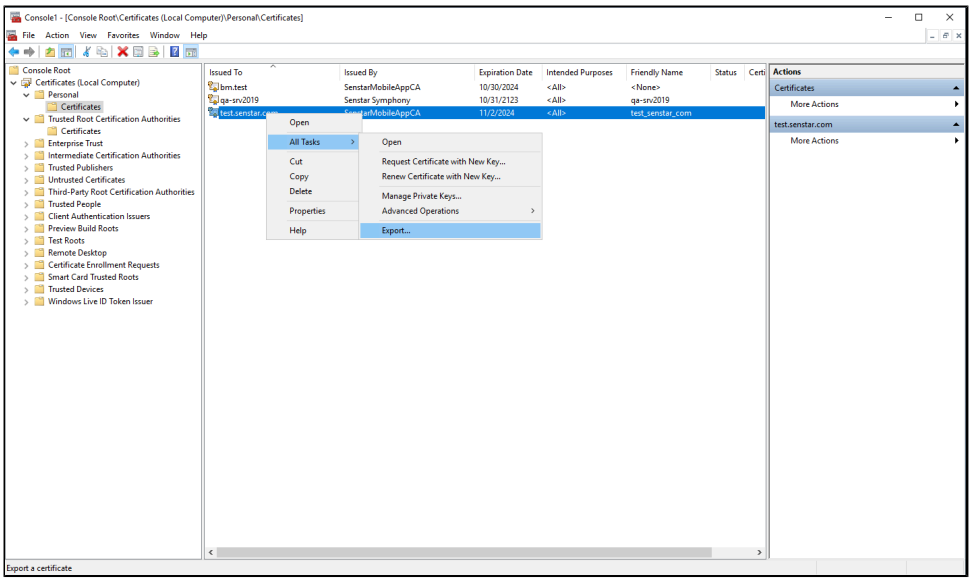
After you install the certificate, export the certificate.

Export the certificate

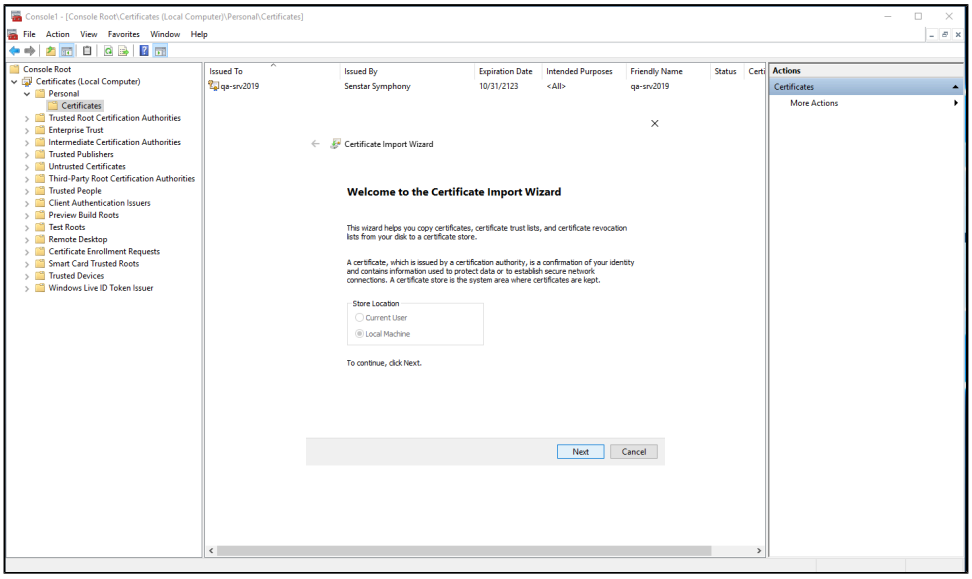
You can export a certificate to add it to the Senstar Symphony Server, iOS devices, or Android devices.

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**.
2. In the Microsoft Management Console, click **Console Root** > **Certificates (Local Computer** > **Personal** > **Certificates**
3. Right click the certificate and click **All Tasks** > **Export**.

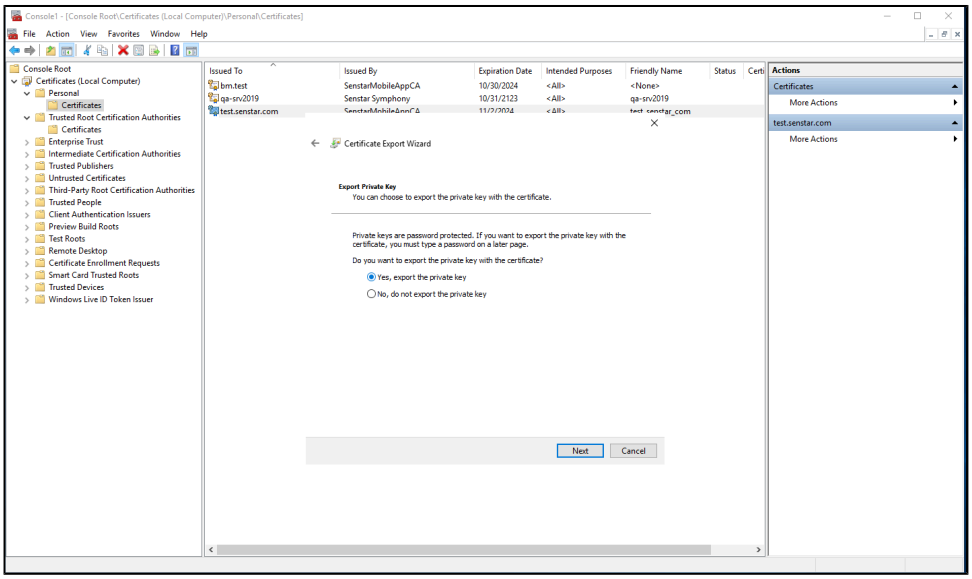


4. Click **Next**.



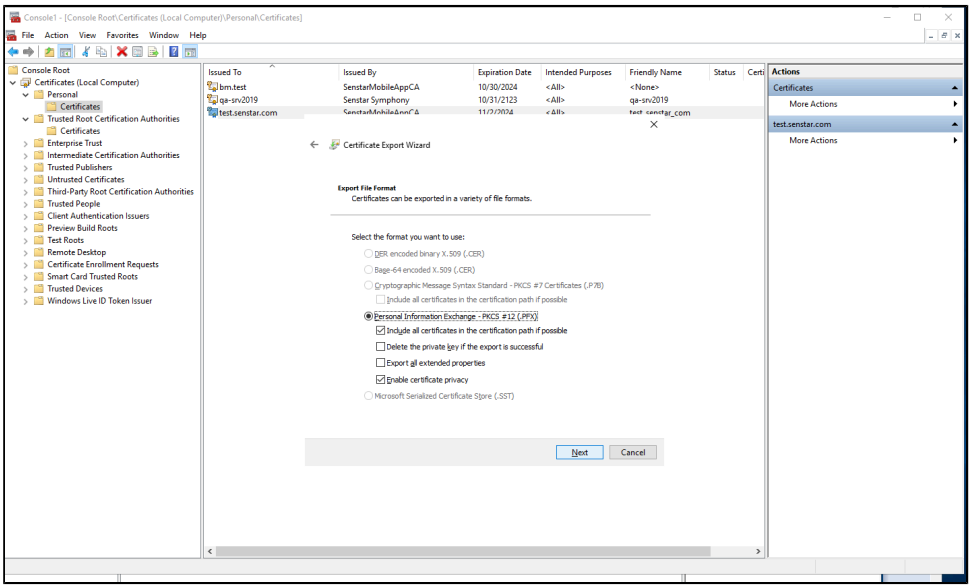
5. On the **Export Private Key** screen, complete one of the following tasks:
   - To export the certificate for use on the Senstar Symphony Server, select **Yes, export the private key** and then click **Next**.

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

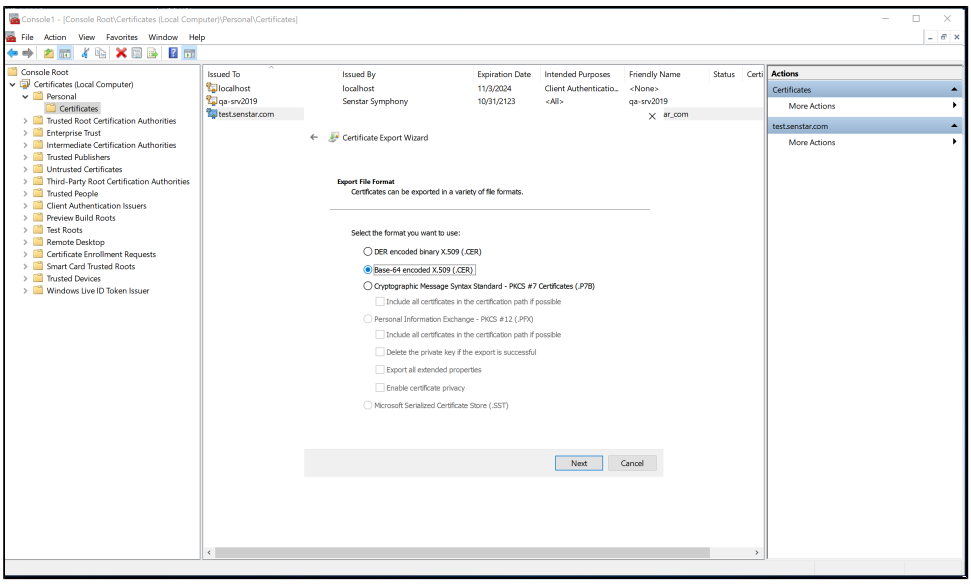


6. On the **Export File Format** page, complete one of the following tasks:

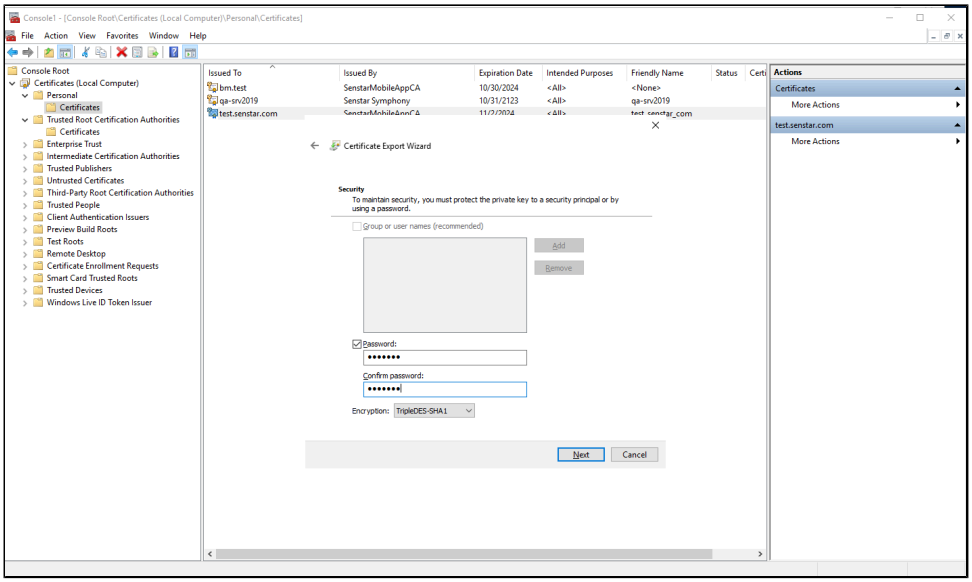
- To export the certificate for use on the Senstar Symphony Server, select **Personal Information Exchange - PKCS #12 (.PFX)**, **Include all certificates in the certification path if possible**, and **Enable certificate privacy**; and then click **Next**.



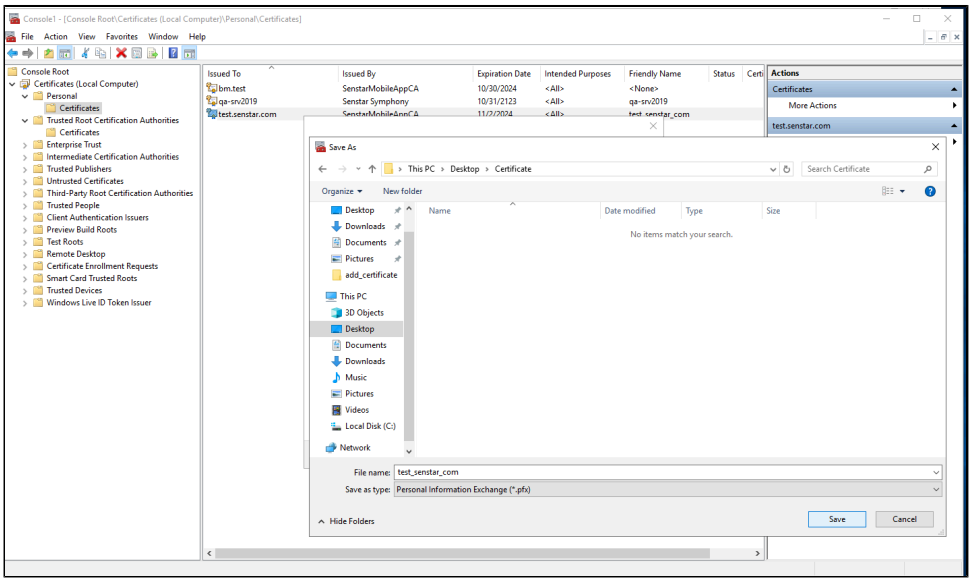
- To export the certificate for use on mobile devices, select **Base-64 encoded X.509 (.CER)** and then click **Next**.



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.**



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**.