Senstar Symphony Mobile Anwendung

4.0

Sicherheitsleitfaden

Inhalt

Anforderungen an das Zertifikat

Um die Kommunikation mit dem Senstar Symphony Server zu sichern, muss der Senstar Symphony Server mit einem gültigen SSL-Zertifikat konfiguriert sein, das von einer vertrauenswürdigen Stammzertifizierungsstelle auf dem mobilen Gerät überprüft werden kann.

Das SSL-Zertifikat sichert die Verbindung zwischen dem Server und der Anwendung. Die Anwendung überprüft dieses Zertifikat, um sicherzustellen, dass sie sich mit dem richtigen Server verbindet und nicht mit einem potenziellen Betrüger, der versucht, Ihre Daten abzufangen.

Weitere Informationen finden Sie unter Was ist ein SSL-Zertifikat?

Verwendung eines Zertifikats

Sie können ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle, von einer benutzerdefinierten Zertifizierungsstelle oder durch die Erstellung eines selbstsignierten Zertifikats erhalten.

Aussteller des Zertifikats	Anforderungen an das Gerät	Domain	Anmerkungen
Vertrauenswürdige Zertifizierungsstelle	Keine	Erforderlich	Dies ist die sicherste Option. Dies ist die empfohlene Option, wenn Sie über das Internet auf Ihren Senstar Symphony Server zugreifen möchten.
Benutzerdefinierte Zertifizierungsstelle	Stellen Sie die benutzerdefinierte Zertifizierungsstelle auf allen mobilen Geräten bereit. Fügen Sie die benutzerdefinierte Zertifizierungsstelle zur Liste der vertrauenswürdigen Stammzertifikate hinzu.	Nicht erforderlich	Diese Option eignet sich am besten für Organisationen, die bereits eine benutzerdefinierte Zertifizierungsstelle verwenden und mobile Geräte zentral verwalten. Dies ist die empfohlene Option, wenn Sie über eine VPN-Verbindung auf Ihren Senstar Symphony Server zugreifen möchten.
Selbstsigniertes Zertifikat	Stellen Sie das selbstsignierte Zertifikat auf allen mobilen Geräten bereit. Fügen Sie das selbstsignierte Zertifikat zur Liste der vertrauenswürdigen Stammzertifikate hinzu.	Nicht erforderlich	Sie müssen manuell ein selbstsigniertes Zertifikat erstellen, das die Sicherheitsanforderungen des mobilen Betriebssystems erfüllt, und es dann auf die mobilen Geräte verteilen, auf denen die Anwendung ausgeführt wird.

Verwendung einer vertrauenswürdigen Zertifizierungsstelle

Die empfohlene Option für den Erhalt eines Zertifikats ist ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle.

1. Wählen Sie eine Zertifizierungsstelle (CA).

   Sie müssen eine vertrauenswürdige CA auswählen, die Ihr SSL-Zertifikat ausstellt. Zu den seriösen CAs gehören DigiCert, GlobalSign, Sectigo und Let's Encrypt. Es ist wichtig, dass Sie eine seriöse CA wählen, um sicherzustellen, dass Ihr Zertifikat allgemein anerkannt und vertrauenswürdig ist.

2. Erzeugen Sie eine Zertifikatsignierungsanforderung (CSR).

   Sie müssen eine CSR erstellen, um ein Zertifikat zu erhalten. Eine CSR enthält Informationen über den Server und die Domäne, die Sie sichern möchten. Die von Ihnen gewählte Zertifizierungsstelle stellt detaillierte Informationen über die Erstellung einer CSR zur Verfügung. Wir empfehlen, dass Sie die Microsoft Management Console verwenden, um eine CSR zu erstellen. Weitere Informationen zur Erstellung einer CSR finden Sie unter CSR-Erstellung - mit dem Windows Certificate Snap-in.

3. Reichen Sie den CSR bei der CA ein.

   Sobald Sie einen CSR erstellt haben, reichen Sie ihn bei der zuständigen Zertifizierungsstelle ein. Die von Ihnen gewählte Zertifizierungsstelle stellt ausführliche Informationen darüber zur Verfügung, wie Sie eine CSR einreichen können (in der Regel über die Website der Zertifizierungsstelle). Die Zertifizierungsstelle verwendet Ihre CSR, um das Zertifikat zu erstellen.

4. Bestätigen Sie Ihre Domaineigentümerschaft.

   Die Zertifizierungsstelle kann verlangen, dass Sie die Inhaberschaft Ihrer Domäne bestätigen. Dies beinhaltet in der Regel die Beantwortung einer Bestätigungs-E-Mail, die die CA an eine domänenspezifische E-Mail-Adresse sendet (z. B., admin@yourdomain.com) oder das Hinzufügen eines bestimmten DNS-Eintrags zur DNS-Konfiguration Ihrer Domäne. Die Validierungsanforderungen können je nach CA und Zertifikatstyp variieren.

5. Stellen Sie das Zertifikat aus.

   Nachdem Ihr Domänenbesitz bestätigt wurde, stellt die CA Ihr SSL-Zertifikat aus. Das Zertifikat enthält einen öffentlichen Schlüssel und Informationen über Ihren Server und Ihre Domain.

Nachdem Sie ein Zertifikat erhalten haben, installieren Sie das Zertifikat.

Verwendung Ihrer eigenen Zertifizierungsstelle

Wenn Sie sich dafür entscheiden, kein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle zu erhalten, können Sie Ihre eigene benutzerdefinierte Zertifizierungsstelle verwenden, um SSL-Zertifikate zu generieren, die mit der Senstar Symphony Mobile Application und dem Senstar Symphony Server funktionieren.

Diese Lösung wird empfohlen, wenn Ihr Unternehmen alle mobilen Geräte verwaltet, auf denen die Senstar Symphony Mobile Application läuft. Ihre IT-Abteilung muss die benutzerdefinierte Zertifizierungsstelle, die das SSL-Zertifikat signiert, bereitstellen und installieren. Die benutzerdefinierte Zertifizierungsstelle muss zur Liste der vertrauenswürdigen Stammzertifikate hinzugefügt werden.

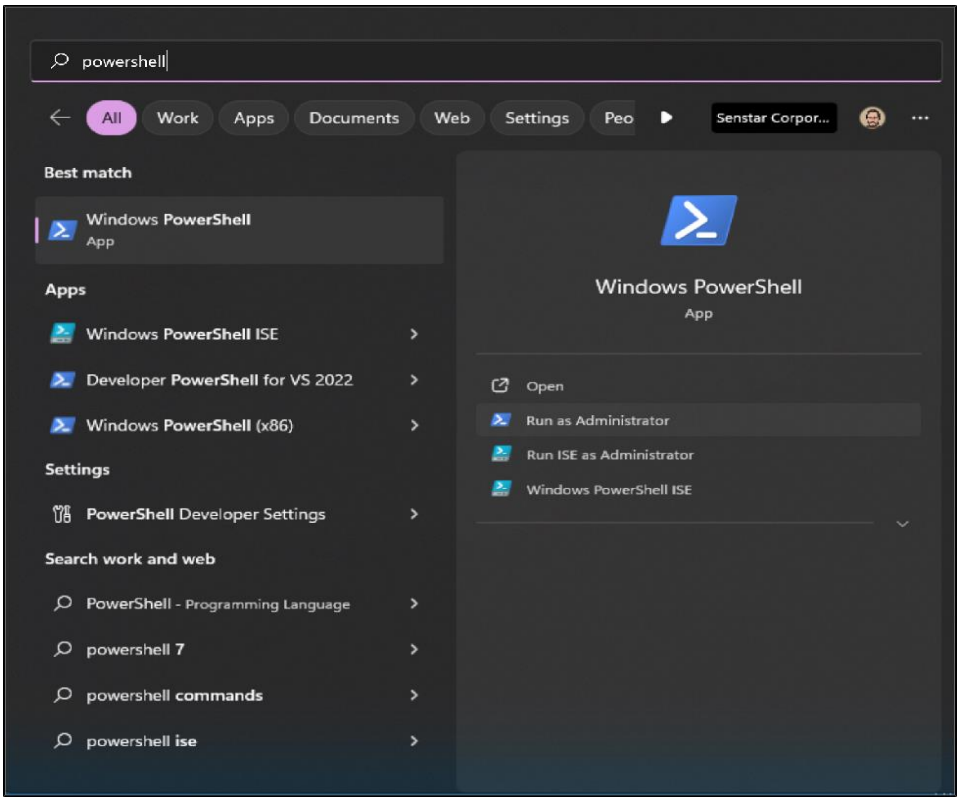
Um Ihre eigene Zertifizierungsstelle zu verwenden:

1. Erzeugen Sie die Zertifikatsignierungsanforderung (CSR).
2. Lassen Sie das Zertifikat von Ihrer IT-Abteilung erstellen.
3. Installieren Sie das Zertifikat.
4. Exportieren Sie das Zertifikat.
5. Fügen Sie das Zertifikat zum Senstar Symphony Server hinzu und konfigurieren Sie das Zertifikat für mobile Verbindungen.
6. Fügen Sie das Zertifikat zu mobilen Geräten hinzu.

Verwendung eines selbstsignierten SSL-Zertifikats

Wenn Sie sich dafür entscheiden, kein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle zu erhalten, können Sie ein eigenes selbstsigniertes Zertifikat erstellen, das mit der Senstar Symphony Mobile Application und dem Senstar Symphony Server funktioniert.

1. Um die Windows PowerShell zu öffnen, führen Sie die folgenden Aufgaben aus:
   a) Drücken Sie die Windows-Taste.
   b) Geben Sie in der Eingabeaufforderung `PowerShell` ein.
   c) Klicken Sie auf **Als Administrator ausführen**.



2. Ändern Sie den folgenden Text und fügen Sie ihn in die Windows PowerShell-Eingabeaufforderung ein:

```
$params = @{
    Subject = 'CN=domain_name, O=Organisation, OU=Abteilung, L=Ort, S=Staat, C=Land'
    TextExtension = @(
        '2.5.29.37={text}1.3.6.1.5.5.7.3.1', #ServerAuthentifizierung
        '2.5.29.19={critical}{text}ca=true&pathlength=0', #Zertifizierungsstelle
        '2.5.29.17={text}DNS=domain_name&IPAddress=ip_address')
    CertStoreLocation = "cert:\LocalMachine\My"
    KeyUsage=@('DigitalSignature', 'KeyEncipherment')
    NotAfter = (Get-Date).AddDays(365)
    SchlüsselAlgorithmus = 'RSA'
    Schlüssellänge = 2048
    HashAlgorithmus = 'SHA256'
}
```

   Ersetzen Sie die Platzhalter:

   - *domain_name* ist der Name Ihrer Domain oder Ihres Computers.
   - *Organisation* ist der Name Ihrer Organisation.
   - *Abteilung* ist der Name Ihrer Organisationseinheit.
   - *Ort* ist die Stadt, in der sich Ihre Organisation befindet.
   - *Staat* ist der Staat oder die Provinz, in der Ihre Organisation ansässig ist.
   - *Land* ist der Bezirk, in dem sich Ihre Organisation befindet.
   - *ip_address* ist die IP-Adresse des Senstar Symphony Servers. Nur verwenden, wenn Sie nicht über einen Domänennamen auf den Senstar Symphony Server zugreifen. Wenn Sie über einen Domänennamen auf den Senstar Symphony Server zugreifen, können Sie die gesamte Teilzeichenkette entfernen (*&IPAddress=ip_address)*.

3. Führen Sie den folgenden Befehl in der Windows PowerShell-Eingabeaufforderung aus:

   ```
   New-SelfSignedCertificate @params
   ```

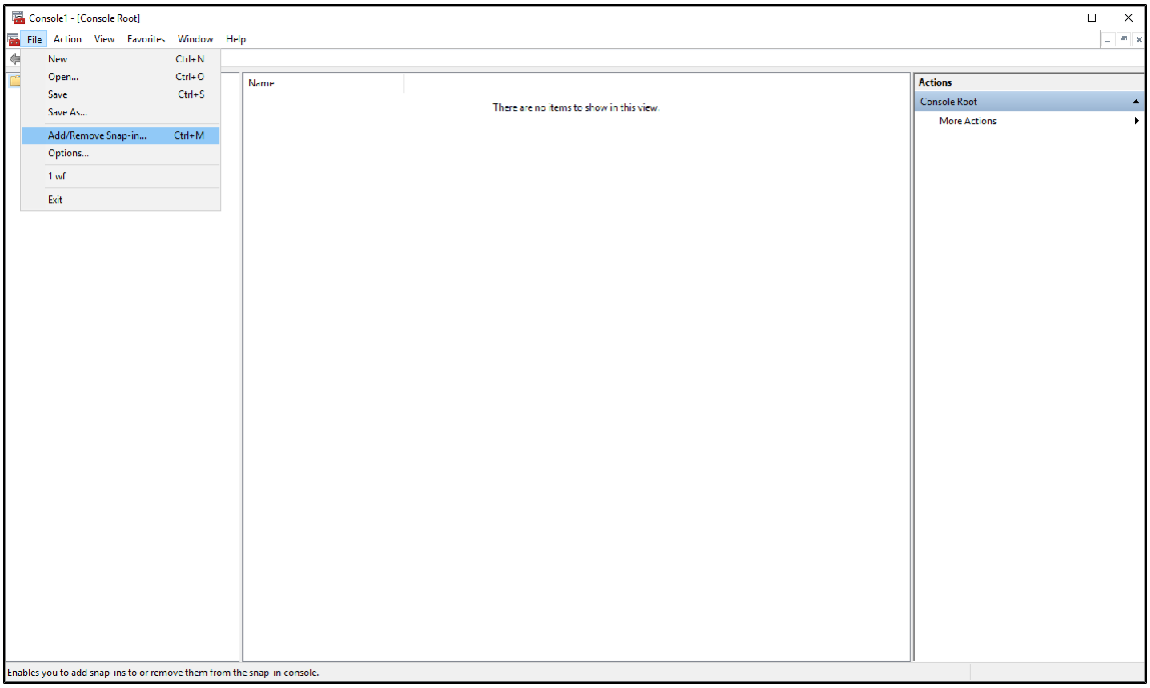
   Nachdem Sie diesen Befehl ausgeführt haben, erhalten Sie eine Bestätigungsmeldung, dass das selbstsignierte Zertifikat generiert und dem Zertifikatspeicher auf dem Computer hinzugefügt wurde.

Nachdem Sie ein selbstsigniertes Zertifikat erstellt haben, exportieren Sie das Zertifikat.

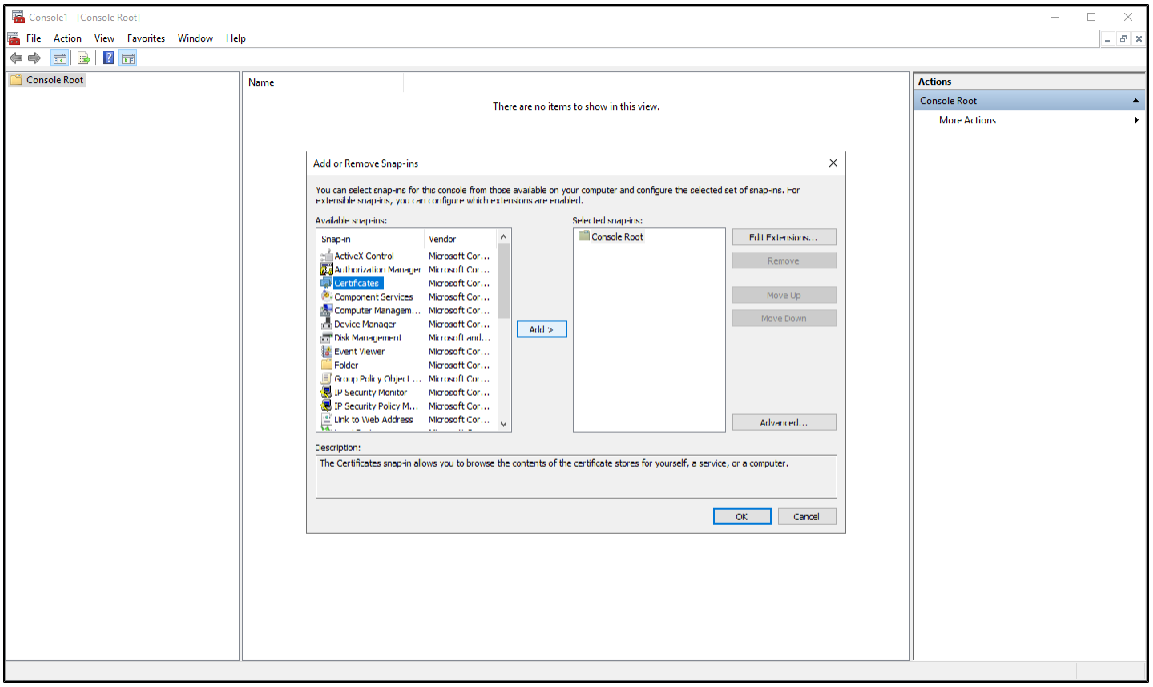
Installation des Zertifikats

Installieren Sie das Zertifikat auf dem Computer, auf dem der Senstar Symphony Server läuft.

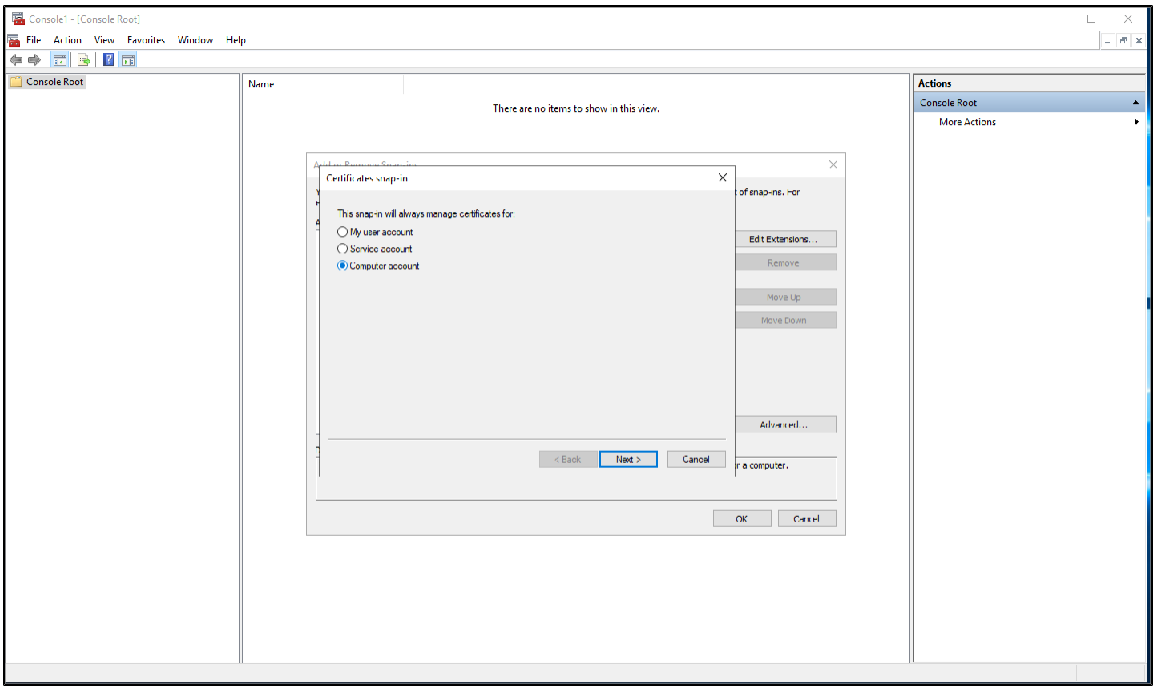
1. Öffnen Sie die Microsoft Management Console, indem Sie die Tastenkombination `Windows + R` drücken, `MMC` eingeben und mit Enter bestätigen.
2. Klicken Sie auf **Datei** > **Snap-In hinzufügen/entfernen** > **.**



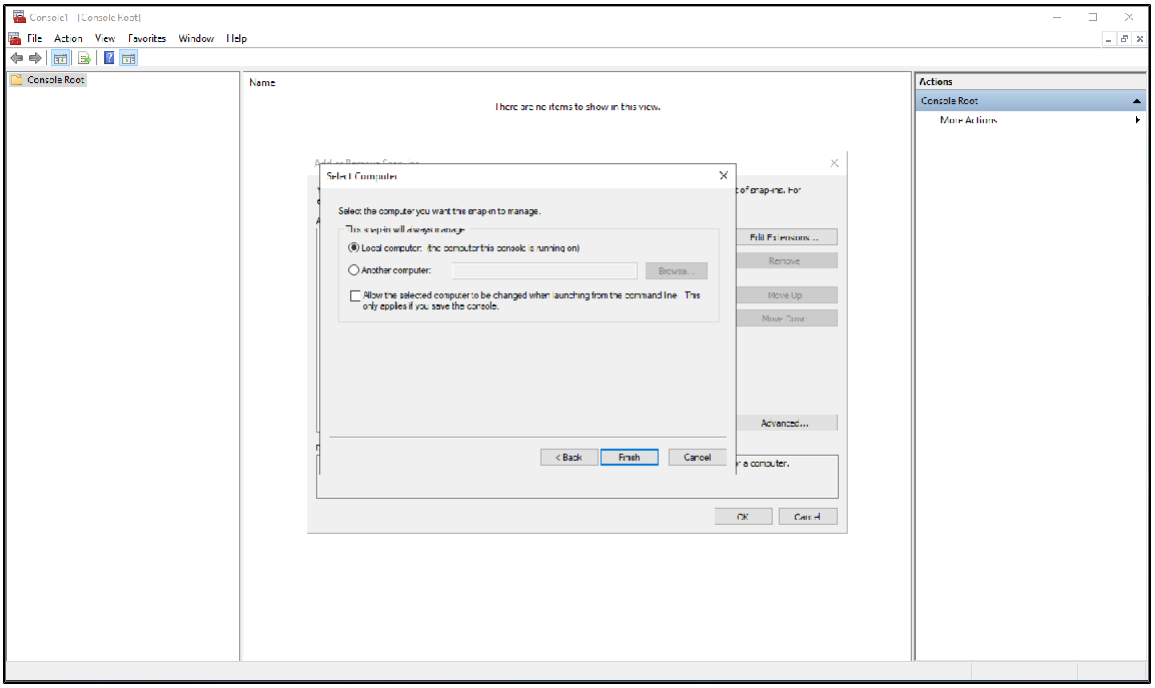
3. Wählen Sie in der Liste **Verfügbare Snap-Ins** die Option **Zertifikate** und klicken Sie auf **Hinzufügen**.



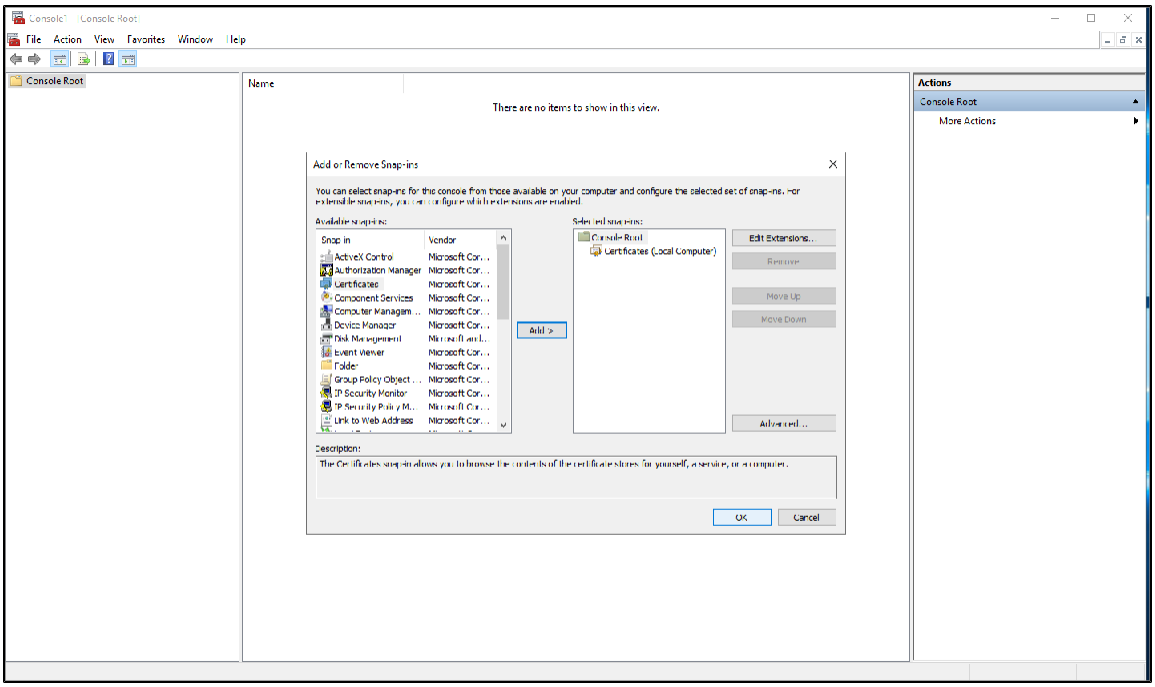
4. Wählen Sie **Computerkonto** und klicken Sie auf **Weiter**.



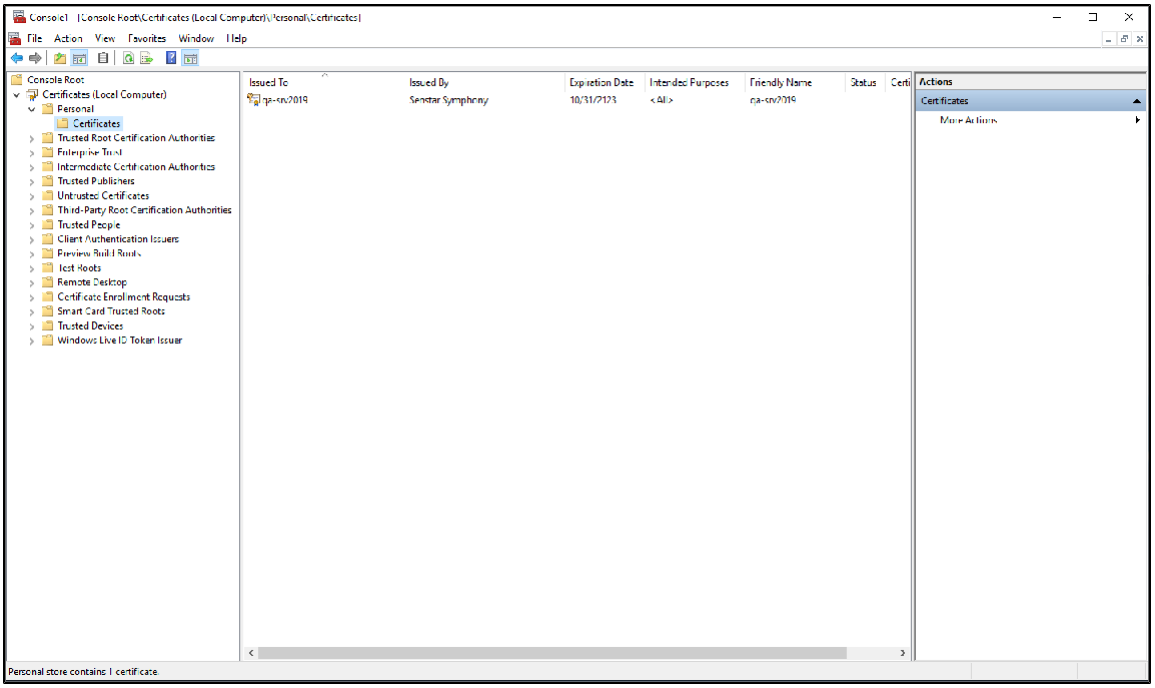
5. Wählen Sie **Lokaler Computer** und klicken Sie auf **Fertig stellen**.



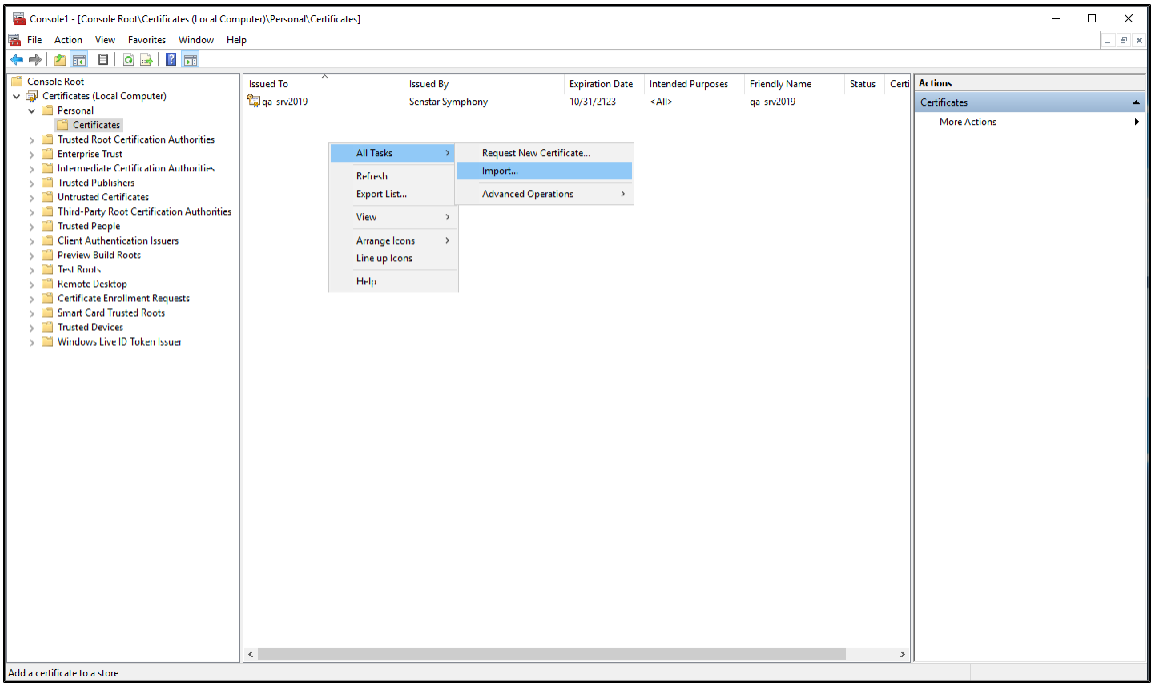
6. Klicken Sie auf **OK**.



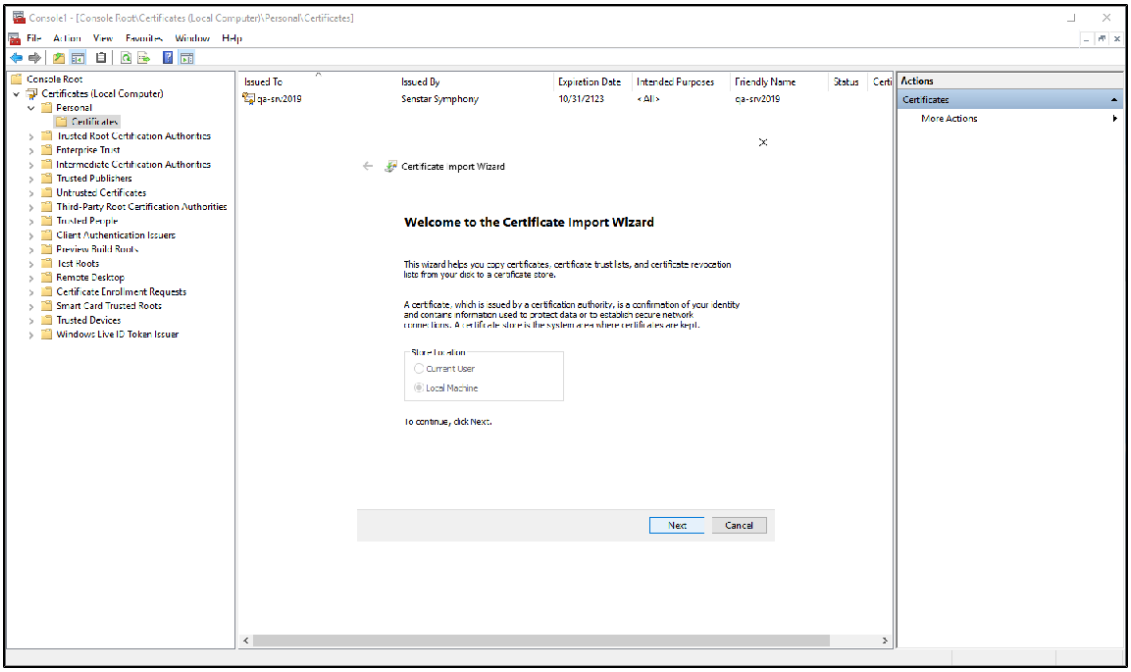
7. Klicken Sie in der Microsoft Management Console auf **Konsolenstamm > Zertifikate (Lokaler Computer** > **Eigene Zertifikate** > **Zertifkate)**



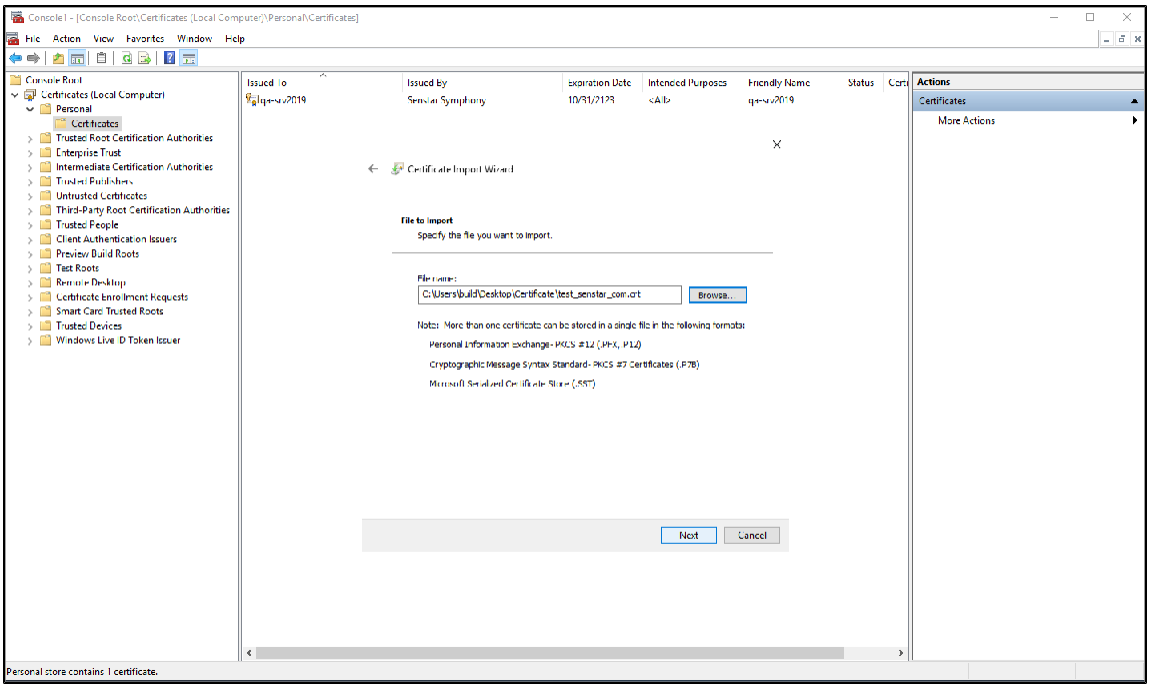
8. Um den Assistenten für den Zertifikatsimport zu öffnen, klicken Sie mit der rechten Maustaste auf den Detailbereich und dann auf **Alle Aufgaben** > **Importieren**.



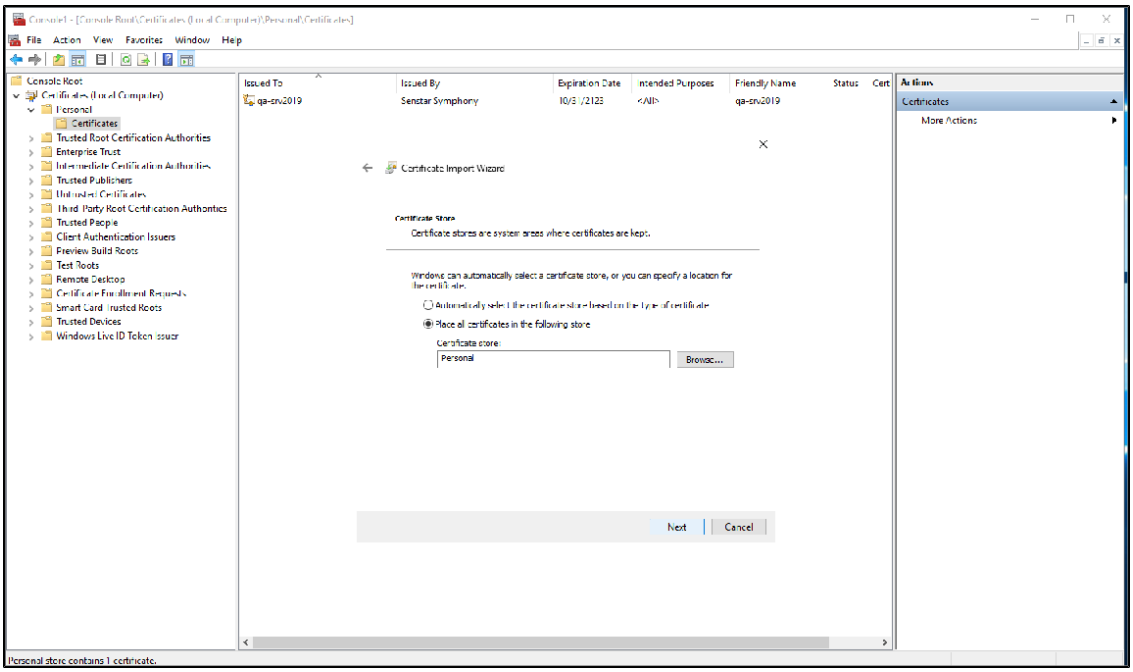
9. Klicken Sie im Assistenten für den Zertifikatsimport auf **Weiter**.



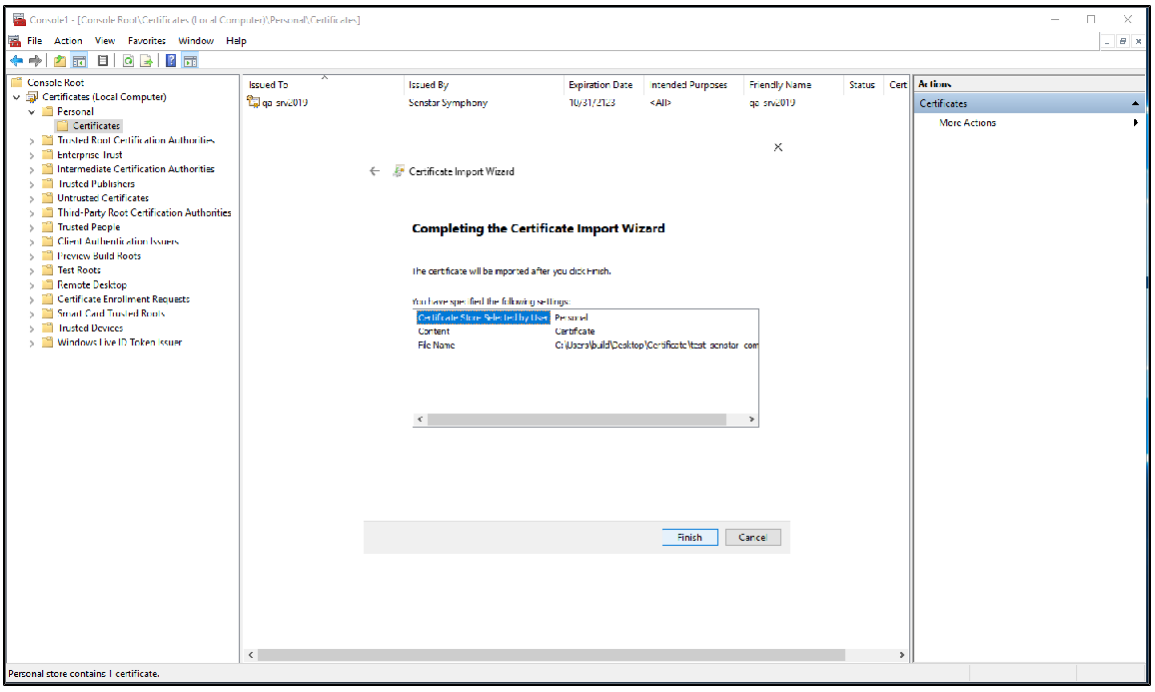
10. Suchen Sie das Zertifikat der Zertifizierungsstelle, wählen Sie es aus und klicken Sie auf **Weiter**.



11. Wählen Sie **Alle Zertifikate im folgenden Speicher ablegen**, suchen und wählen Sie „Eigene Zertifikate“, und klicken Sie auf **Weiter**.



12. Klicken Sie auf **Fertigstellen**.



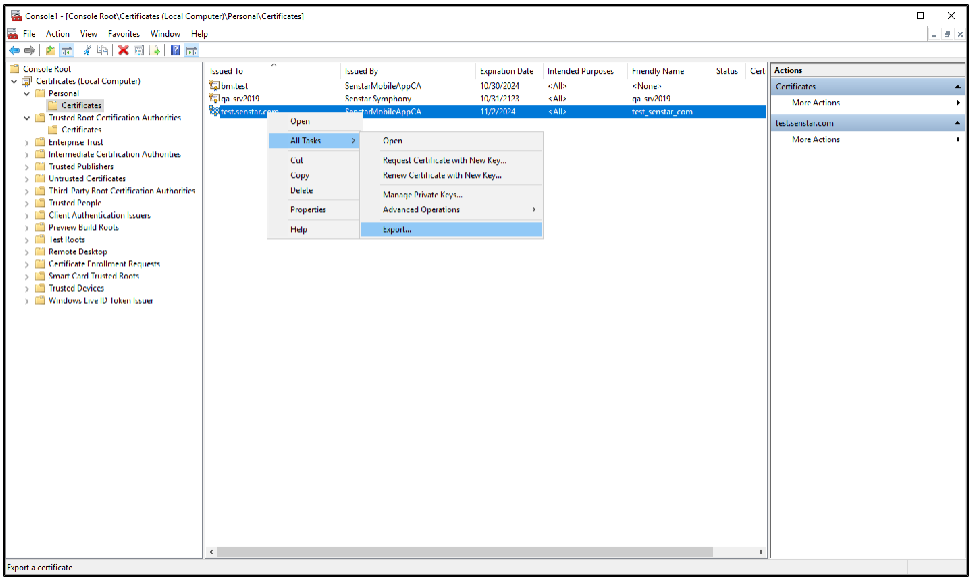
Nachdem Sie das Zertifikat installiert haben, exportieren Sie das Zertifikat.

Exportieren des Zertifikats

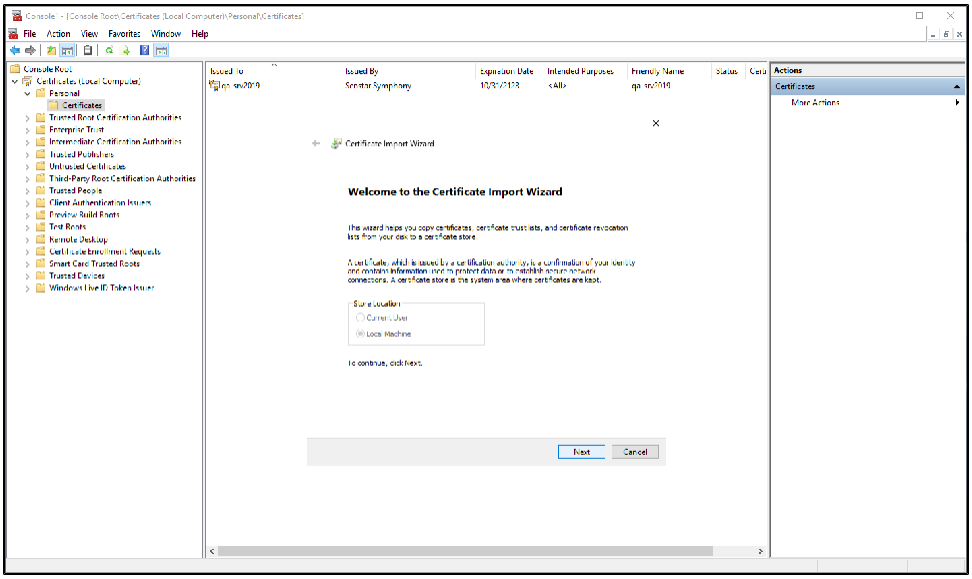
Sie können ein Zertifikat exportieren, um es dem Senstar Symphony Server, iOS- oder Android-Geräten hinzuzufügen.

Um das Zertifikat auf dem Senstar Symphony Server zu verwenden, müssen Sie es im `.PFX`-Format exportieren. Um das Zertifikat auf iOS- oder Android-Geräten zu verwenden, müssen Sie es im `.CER`-Format exportieren.

1. Öffnen Sie die Microsoft Management Console, indem Sie die Tastenkombination `Windows + R` drücken, `MMC` eingeben und bestätigen Sie mit Enter.
2. Klicken Sie in der Microsoft Management Console auf **Konsolenstamm > Zertifikate (Lokaler Computer > Eigene Zertifikate > Zertifikate**
3. Klicken Sie mit der rechten Maustaste auf das Zertifikat und dann auf **Alle Aufgaben** > **Exportieren**.

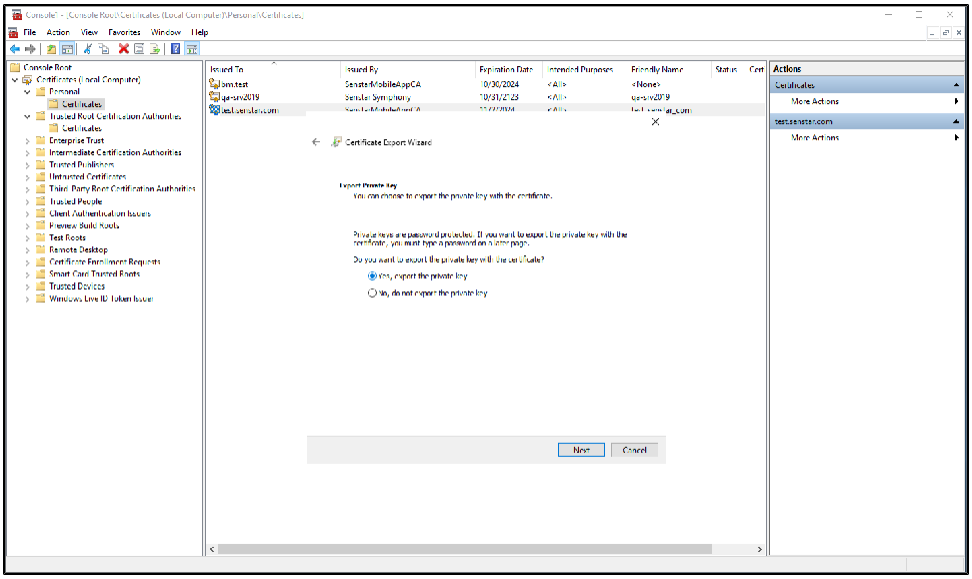


4. Klicken Sie auf **Weiter**.



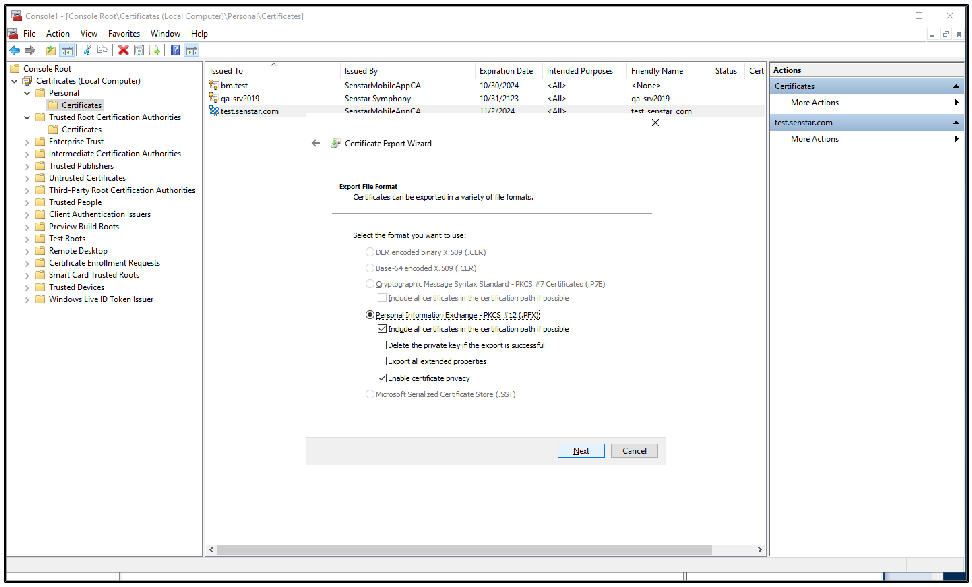
5. Führen Sie auf dem Bildschirm **Privaten Schlüssel exportieren** eine der folgenden Aufgaben aus:
   - Um das Zertifikat zur Verwendung auf dem Senstar Symphony Server zu exportieren, wählen Sie **Ja, privaten Schlüssel exportieren** und klicken Sie dann auf **Weiter**.

- Um das Zertifikat zur Verwendung auf mobilen Geräten zu exportieren, wählen Sie **Nein, privaten Schlüssel nicht exportieren** und klicken Sie auf **Weiter**.

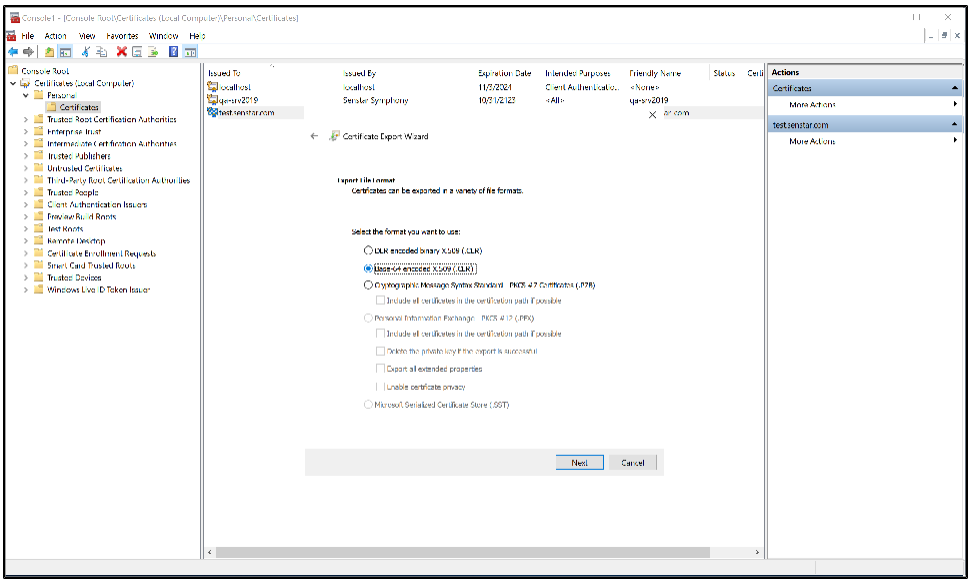


6. Führen Sie auf der Seite **Format der zu exportierenden Datei** eine der folgenden Aufgaben aus:

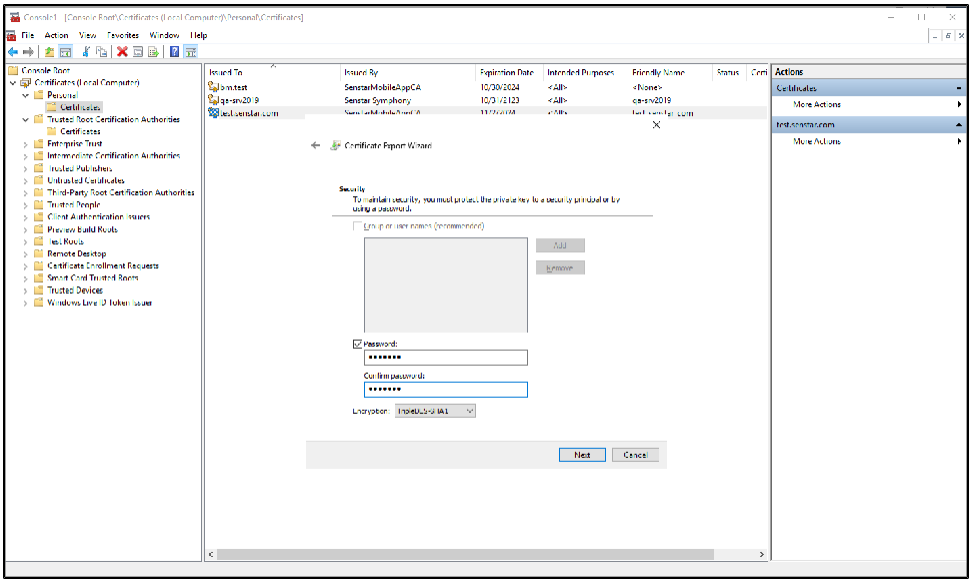
- Um das Zertifikat zur Verwendung auf dem Senstar Symphony Server zu exportieren, wählen Sie **Privater Informationsaustausch - PKCS #12 (.PFX)**, **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** und **Zeritifikatsschutz aktivieren**; und klicken Sie dann auf ne**xt**.



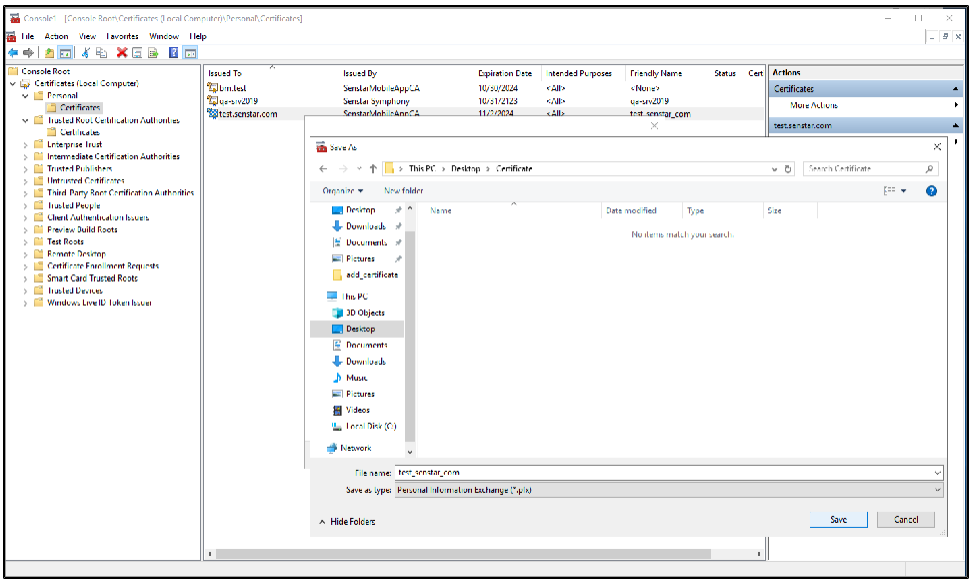
- Um das Zertifikat zur Verwendung auf mobilen Geräten zu exportieren, wählen Sie **Base-64-codiert X.509 (.CER)** und klicken Sie auf **Weiter**.



7. Dieser Schritt gilt nur für Zertifikate, die Sie zur Verwendung auf dem Senstar Symphony Server exportieren. Auf dem Wählen Sie auf der Seite **Sicherheit** die Option **Kennwort**, geben Sie ein Kennwort für die PFX-Datei ein und bestätigen Sie es, und klicken Sie dann auf **Weiter.**



8. Wählen Sie aus, wo die Zertifikatsdatei gespeichert werden soll, und klicken Sie auf **Speichern**.



9. Klicken Sie auf **Fertigstellen**.

Nachdem Sie das Zertifikat exportiert haben, fügen Sie das Zertifikat zum Senstar Symphony Server, zu iOS- oder Android-Geräten hinzu.

Hinzufügen eines SSL-Zertifikats zum Senstar Symphony Server

Nachdem Sie das Zertifikat auf dem Computer installiert haben, auf dem der Senstar Symphony Server läuft, müssen Sie das Zertifikat zum Senstar Symphony Server hinzufügen und das Zertifikat für mobile Verbindungen über die Konfigurationsoberfläche des Senstar Symphony Servers auswählen.

Das Verfahren zum Hinzufügen und Auswählen von SSL-Zertifikaten wurde in Senstar Symphony Server 8.6 geändert. Stellen Sie sicher, dass Sie das Verfahren für Ihre Version von Senstar Symphony Server befolgen.

Ein SSL-Zertifikat hinzufügen (8.6 und neuer)

Sie können dem Senstar Symphony Server ein SSL-Zertifikat in der Konfigurationsoberfläche des Senstar Symphony Servers hinzufügen.

Der Senstar Symphony Server verwendet das SSL-Zertifikat, um Verbindungen von Browsern und der Senstar Symphony Mobile Application zu sichern. Der Senstar Symphony Server unterstützt PFX-Zertifikatsdateien.

1. Klicken Sie in der Konfigurationsoberfläche von Senstar Symphony Server auf **Einstellungen** > **Server**.
2. Wählen Sie den Senstar Symphony Server aus und klicken Sie auf **Bearbeiten**.
3. Navigieren Sie zum Abschnitt **SSL-Zertifikat**.
4. Geben Sie in das Feld **Passwort** das Passwort für das Zertifikat ein.
5. Ziehen Sie die Zertifikatsdatei in das Feld oder suchen Sie die Zertifikatsdatei.
6. Klicken Sie auf **Speichern**.

Ein SSL-Zertifikat hinzufügen (8.5 und älter)

Sie können dem Senstar Symphony Server ein SSL-Zertifikat in der Konfigurationsoberfläche des Senstar Symphony Servers hinzufügen.

Der Senstar Symphony Server verwendet das SSL-Zertifikat, um Verbindungen von Browsern und der Senstar Symphony Mobile Application zu sichern.

1. Klicken Sie in der Konfigurationsoberfläche von Senstar Symphony Server auf **Einstellungen** > **Allgemeine Einstellungen**.
2. Navigieren Sie zum Abschnitt **SSL-Zertifikat**.
3. Geben Sie in das Feld **Passwort** das Passwort für das Zertifikat ein.
4. Ziehen Sie die Zertifikatsdatei in das Feld oder suchen Sie die Zertifikatsdatei.
5. Klicken Sie auf **Speichern**.

Konfigurieren der mobilen Verbindungen (8.6 und neuer)

Sie können den Senstar Symphony Server so konfigurieren, dass er Verbindungen mit der Senstar Symphony Mobile App auf mobilen Geräten unterstützt. Dieses Thema gilt für Senstar Symphony Server 8.6 und höher.

1. Klicken Sie in der Konfigurationsoberfläche von Senstar Symphony Server auf **Einstellungen** > **Server**.
2. Wählen Sie den Senstar Symphony Server aus und klicken Sie auf **Bearbeiten**.
3. Navigieren Sie zum Abschnitt **Mobile Verbindungen**.
4. Um das SSL-Zertifikat auszuwählen, klicken Sie auf **Ändern**, wählen das Zertifikat aus und klicken auf **OK**.
5. Um den Netzwerkadapter für mobile Verbindungen auszuwählen, klicken Sie auf **Ändern**, wählen Sie den Netzwerkadapter aus, und klicken Sie auf **OK**.
6. Legen Sie im Feld **Mobiler Port** den Port fest, den der Senstar Symphony Server verwendet, um auf Anfragen von mobilen Geräten zu warten.

7. Legen Sie im Feld **Video-Proxy-Port** den Port fest, den der Senstar Symphony Server zum Streamen von Videos an mobile Geräte und zum Empfang von Videos von mobilen Geräten verwendet.
8. Klicken Sie auf **Speichern**.

Konfigurieren der mobilen Verbindungen (8.5 und älter)

Sie können den Senstar Symphony Server so konfigurieren, dass er Verbindungen mit der Senstar Symphony Mobile App auf mobilen Geräten unterstützt. Dieses Thema gilt für Senstar Symphony Server 8.5 und früher.

1. Klicken Sie in der Konfigurationsoberfläche von Senstar Symphony Server auf **Einstellungen** > **Allgemeine Einstellungen**.
2. Navigieren Sie zum Abschnitt **Mobile Verbindungen**.
3. Um das SSL-Zertifikat auszuwählen, klicken Sie auf **Ändern**, wählen das Zertifikat aus und klicken auf **OK**.
4. Legen Sie im Feld **Mobiler Port** den Port fest, den der Senstar Symphony Server verwendet, um auf Anfragen von mobilen Geräten zu warten.
5. Legen Sie im Feld **Video-Proxy-Port** den Port fest, den der Senstar Symphony Server zum Streamen von Videos an mobile Geräte und zum Empfang von Videos von mobilen Geräten verwendet.
6. Damit der Senstar Symphony Server Push-Benachrichtigungen an iOS-Geräte senden kann, wählen Sie **iOS-Benachrichtigungen aktivieren**.
7. Klicken Sie auf **Speichern**.

Hinzufügen eines Zertifikats zu einem iOS-Gerät

1. Senden Sie die Zertifikatsdateien an das iOS-Gerät.
2. Tippen Sie auf das Zertifikat in der E-Mail.
3. Wählen Sie Ihr Gerät aus, um das Profil zu installieren.
4. Tippen Sie auf **Einstellungen** > **Allgemein** > **VPN und Geräteverwaltung**.
5. Tippen Sie auf das Zertifikat und folgen Sie den Anweisungen auf dem Bildschirm, um das Zertifikat zu installieren.
6. Tippen Sie nach der Installation des Zertifikats auf **Einstellungen** > **Allgemein** > **Info** > **Zertifikatsvertrauenseinstellungen**.
7. Aktivieren Sie das volle Vertrauen für das installierte Zertifikat.

Hinzufügen eines Zertifikats zu einem Android-Gerät

1. Tippen Sie auf **Einstellungen** > **Sicherheit und Datenschutz** > **Mehr Sicherheit und Datenschutz** > **Verschlüsselung und Zugangsdaten**.
2. Tippen Sie auf **Zertifikat installieren**.
3. Tippen Sie auf **CA-Zertifikat**.
4. Tippen Sie **trotzdem** auf **Installieren**.
5. Suchen Sie nach der crt-Datei.

Sie können das Zertifikat unter **Einstellungen** > **Sicherheit und Datenschutz** > **Mehr Sicherheit und Datenschutz** anzeigen oder deinstallieren.
Verschlüsselung & Anmeldedaten > **Vertrauenswürdige Anmeldedaten** > **Nutzer**.