

Installieren Sie den ExtraHOP Session Key Forwarder auf einem Windows-Server

Veröffentlicht: 2025-02-12

Perfect Forward Secrecy (PFS) ist eine Eigenschaft sicherer Kommunikationsprotokolle, die den kurzfristigen, vollständig privaten Austausch von Sitzungsschlüsseln zwischen Clients und Servern ermöglichen. ExtraHop bietet eine Software zur Weiterleitung von Sitzungsschlüsseln an, die Sitzungsschlüssel zur TLS-Entschlüsselung an das ExtraHop-System senden kann. Kommunikation zwischen dem Key Spediteur und dem Sensor ist mit TLS 1.2 oder TLS 1.3 verschlüsselt, und die Anzahl der Sitzungsschlüssel, die das ExtraHop-System empfangen kann, ist unbegrenzt.



Hinweis: Weitere Informationen darüber, wie sich der Traffic-Feed oder Änderungen an der Konfiguration auf Sensoren auswirken könnten, finden Sie in den Metriken für Desynchronisierung und Erfassung der Drop-Rate in der [Systemstatus-Dashboard](#).

Sie müssen das ExtraHop-System für die Weiterleitung von Sitzungsschlüsseln konfigurieren und dann die Forwarder-Software auf dem [Windows](#) und [Linux](#) Server mit dem TLS-Verkehr, den Sie entschlüsseln möchten.

Bevor du anfängst

- Lesen Sie über [TLS-Entschlüsselung](#) und überprüfen Sie die Liste von [unterstützte Cipher Suites](#).
- Stellen Sie sicher, dass das ExtraHop-System für TLS Decryption und TLS Shared Secrets lizenziert ist.
- Stellen Sie sicher, dass Ihre Serverumgebung von der ExtraHop Session Key Forwarder-Software unterstützt wird:
 - Microsoft Secure Channel (Schannel) -Sicherheitspaket
 - Java TLS (Java-Versionen 8 bis 17). Führen Sie kein Upgrade auf diese Version des Session Key Forwarders durch, wenn Sie derzeit Java 6- oder Java 7-Umgebungen überwachen. Version 7.9 des Session Key Forwarders unterstützt Java 6 und Java 7 und ist mit der neuesten ExtraHop-Firmware kompatibel.
 - Dynamisch verknüpfte OpenSSL-Bibliotheken (1.0.x und 1.1.x). OpenSSL wird nur auf Linux-Systemen mit den Kernelversionen 4.4 und höher sowie RHEL 7.6 und höher unterstützt.
- Stellen Sie sicher, dass der Server, auf dem Sie den Session Key Forwarder installieren, dem TLS-Zertifikat des ExtraHop vertraut Sensor.
- Stellen Sie sicher, dass Ihre Firewallregeln zulassen, dass vom überwachten Server Verbindungen zum TCP-Port 4873 auf dem Sensor initiiert werden.



Wichtig: Das ExtraHop-System kann den TLS-verschlüsselten TDS-Verkehr nicht durch Weiterleitung von Sitzungsschlüsseln entschlüsseln. Stattdessen können Sie ein RSA hochladen [privater Schlüssel](#).

- Installieren Sie den Session Key Forwarder auf einem oder mehreren Windows 2016- oder Windows 2019-Servern, auf denen TLS-basierte Dienste mit dem nativen Windows TLS-Framework ausgeführt werden. OpenSSL unter Windows wird derzeit nicht unterstützt.



Wichtig: Nach der Installation der Sitzungsschlüsselweiterleitungssoftware funktionieren Anwendungen, die TLS-fähige Funktionen enthalten, wie EDR-Agenten und Windows Store-Anwendungen, möglicherweise nicht richtig.

Überprüfen Sie die Kompatibilität des Session Key Forwarders in Ihrer Windows-Testumgebung, bevor Sie ihn in Ihrer Produktionsumgebung bereitstellen.

Entschlüsselung des Windows-Anwendungsverkehrs

Der folgende Microsoft-Anwendungsdatenverkehr kann mit der Sitzungsschlüsselweiterleitung entschlüsselt werden.

- Microsoft IIS
- Microsoft PowerShell
- Microsoft SQL Server

Installieren Sie die Software mit dem Installationsassistenten

1. Loggen Sie sich auf dem Windows-Server ein.
2. [Herunterladen](#)  die neueste Version der Sitzungsschlüsselweiterleitungssoftware.
3. Doppelklicken Sie auf `ExtraHopSessionKeyForwarder.exe` ablegen und klicken **Weiter**.
4. Wenn das System Sie auffordert, das Installationsprogramm für die Ausführung mit Administratorrechten zu autorisieren, klicken Sie auf **OK**.
5. Wählen Sie das Kästchen aus, um die Bedingungen der Lizenzvereinbarung zu akzeptieren, und klicken Sie dann auf **Weiter**.
6. Geben Sie den Hostnamen oder die IP-Adresse des Sensor wohin Sie Sitzungsschlüssel weiterleiten möchten.



Hinweis Sie können Sitzungsschlüssel an mehr als einen Sensor weiterleiten, indem Sie kommagetrennte Hostnamen eingeben. Zum Beispiel:

```
packet-sensor.example.com,ids-sensor.example.com
```

7. Optional: Wählen Sie den **Erweiterte Optionen** Checkbox. Akzeptieren Sie den standardmäßigen TCP-Listenportwert 598 (empfohlen), oder geben Sie einen benutzerdefinierten Portwert ein.
8. Klicken **Installieren**.
9. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**.

Installationsoption über die Befehlszeile

Die folgenden Schritte zeigen Ihnen, wie Sie die Sitzungsschlüsselweiterleitung über eine Windows-Eingabeaufforderung oder Windows PowerShell installieren.

1. Loggen Sie sich auf dem Windows-Server ein.
2. [Herunterladen](#)  die neueste Version der Sitzungsschlüsselweiterleitungssoftware.
3. Führen Sie den folgenden Befehl aus:

```
ExtraHopSessionKeyForwarderSetup.exe -q EDA_HOSTNAME="<hostname or IP address of sensor>"
```



Hinweis Das `-q` Die Option installiert den Forwarder im nicht interaktiven Modus, der nicht zur Bestätigung auffordert. Sie können das weglassen `-q` Option, um den Forwarder im interaktiven Modus zu installieren.



Hinweis Sie können mehrere Sensoren in einer kommagetrennten Liste angeben. Der folgende Befehl spezifiziert beispielsweise zwei Sensoren:

```
ExtraHopSessionKeyForwarderSetup.exe EDA_HOSTNAME="packet-sensor.example.com,ids-sensor.example.com"
```

Weitere Hinweise zu den Installationsoptionen finden Sie unter [Installationsparameter](#).

Aktivieren Sie den TLS-Sitzungsschlüsselempfängerdienst

Sie müssen den Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktivieren, bevor das System Sitzungsschlüssel vom Sitzungsschlüssel-Forwarder empfangen und entschlüsseln kann. Standardmäßig ist dieser Dienst deaktiviert.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Dienstleistungen**.
3. Wählen Sie die **Empfänger für SSL-Sitzungsschlüssel** Ankreuzfeld.
4. Klicken Sie **Speichern**.

Einen globalen Port zur Protokollzuordnung hinzufügen

Fügen Sie jedes Protokoll für den Datenverkehr hinzu, den Sie mit Ihren Sitzungsschlüsselweiterleitungen entschlüsseln möchten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **SSL-Entschlüsselung**.
4. In der Entschlüsselung des privaten Schlüssels Abschnitt, löschen Sie das Private Schlüssel erforderlich Ankreuzfeld.
5. In der Zuordnung von globalem Protokoll zu Port Abschnitt, klicken Sie **Globales Protokoll hinzufügen**.
6. Aus dem **Protokoll** Wählen Sie im Dropdownmenü das Protokoll für den Verkehr aus, den Sie entschlüsseln möchten.
7. In der Hafen Feld, geben Sie die Nummer des Ports ein.
Typ 0 um alle Ports hinzuzufügen.
8. Klicken Sie **Hinzufügen**.

Schlüsselweiterleitungen verbundener Sitzungen anzeigen

Sie können kürzlich verbundene Sitzungsschlüsselweiterleitungen anzeigen, nachdem Sie die Sitzungsschlüsselweiterleitung auf Ihrem Server installiert und den TLS-Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktiviert haben. Beachten Sie, dass auf dieser Seite nur Sitzungsschlüsselweiterleitungen angezeigt werden, die in den letzten Minuten eine Verbindung hergestellt haben, nicht alle Sitzungsschlüsselweiterleitungen, die derzeit verbunden sind.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. klicken **Geteilte SSL-Geheimnisse**.

Weiterleitung des Sitzungsschlüssels validieren

Gehen Sie wie folgt vor, um sicherzustellen, dass die Installation erfolgreich war und der Session Key Forwarder die Schlüssel an das ExtraHop-System weiterleitet.

1. Melden Sie sich beim Windows-Server an.
2. Öffnen Sie das MMC-Snap-In Services. Stellen Sie sicher, dass der Dienst „ExtraHop Session Key Forwarder“ den Status „Wird ausgeführt“ anzeigt.
3. Wenn einer der Dienste nicht ausgeführt wird, beheben Sie das Problem, indem Sie die folgenden Schritte ausführen.
 - a) Öffnen Sie das MMC-Snap-In der Ereignisanzeige und navigieren Sie zu Windows-Protokolle > Anwendung.

- b) Suchen Sie die neuesten Einträge für die ExtraHopAgent-Quelle. Häufige Fehlerursachen und die zugehörigen Fehlermeldungen sind in der **Beheben Sie häufig auftretende Fehlermeldungen** Abschnitt unten.
4. Wenn das Snap-In „Dienste“ und die Ereignisanzeige keine Probleme anzeigen, wenden Sie eine Arbeitslast auf die überwachten Dienste an und überprüfen Sie im ExtraHop-System, ob die geheime Entschlüsselung funktioniert.

Wenn das ExtraHop-System Sitzungsschlüssel empfängt und sie auf entschlüsselte Sitzungen anwendet, wird der Shared Secret-Metrikzähler (unter Anwendungen > Alle Aktivitäten > SSL-Sitzungen entschlüsselt) erhöht. Erstellen Sie ein Dashboard-Diagramm mit dieser Metrik, um zu sehen, ob der Sensor erfolgreich Sitzungsschlüssel von den überwachten Servern empfängt.

The screenshot shows a dashboard interface with a 'Region' dropdown at the top. Below it is a section titled 'All Activity SSL Sessions Decrypted with Shared Secret' with a dropdown arrow. Under this section is a table with two columns: 'Application' and 'Sessions Decrypted with Shared Secret'. The 'Application' column has a link 'All Activity'. The 'Sessions Decrypted with Shared Secret' column shows the value '14176'.

Application	Sessions Decrypted with Shared Secret
All Activity	14176

Überprüfen Sie die Konfiguration über die Kommandozeile

In Fällen, in denen Sie möglicherweise Probleme mit der Konfiguration haben, enthält die Binärdatei für die Sitzungsschlüsselweiterleitung einen Testmodus, auf den Sie über die Kommandozeile zugreifen können, um Ihre Konfiguration zu testen.

1. Loggen Sie sich auf Ihrem Windows-Server ein.
2. Öffnen Sie die Windows PowerShell-Anwendung.
3. Führen Sie einen Verifizierungstest durch, indem Sie den folgenden Befehl ausführen:

```
& 'C:\Program Files\ExtraHop\extrahop-agent.exe' -t -server <eda
hostname>
```

Wo <eda hostname> ist der vollqualifizierte Domainname des Sensor, an den Sie Secrets weiterleiten.

Die folgende Ausgabe sollte erscheinen:

```
<timestamp> Performing connectivity test
<timestamp> No connectivity issues detected
```

Wenn ein Konfigurationsproblem auftritt, werden in der Ausgabe Tipps zur Fehlerbehebung angezeigt, die Ihnen bei der Behebung des Problems helfen. Folgen Sie den Vorschlägen, um das Problem zu lösen, und führen Sie den Test dann erneut aus.

4. Sie können optional die Überschreibung des Zertifikatspfads und des Servernamens testen, indem Sie dem obigen Befehl die folgenden Optionen hinzufügen.

- Geben Sie diese Option an, um das Zertifikat zu testen, ohne es dem Zertifikatsspeicher hinzuzufügen.

```
-cert <file path to certificate>
```

- Geben Sie diese Option an, um die Verbindung zu testen, falls eine Diskrepanz zwischen dem Hostnamen des ExtraHop-Systems, den der Forwarder kennt (SERVER), und dem allgemeinen Namen (CN), der im TLS-Zertifikat des ExtraHop-Systems enthalten ist, besteht.

```
-server-name-override <common name>
```

Wichtige Kennzahlen zum Zustand des Empfängersystems

Das ExtraHop-System bietet wichtige Empfängermetriken, die Sie zu einem Dashboard-Diagramm hinzufügen können, um den Zustand und die Funktionalität der wichtigsten Empfänger zu überwachen.

Um eine Liste der verfügbaren Messwerte anzuzeigen, klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Metrischer Katalog**. Typ **Schlüsselempfänger** im Filterfeld, um alle verfügbaren wichtigen Empfängermetriken anzuzeigen.

Metric Catalog	
key receiver	
System	Key Receiver System Health - Attempted Connections <i>The number of TCP connections that were initiated to the session key receiver port</i>
System	Key Receiver System Health - Disconnections <i>The number of connections that clients ended intentionally. This number does not</i>
System	Key Receiver System Health - Failed SSL Handshakes <i>The number of connections to the session key receiver port that did not proceed</i>
System	Key Receiver System Health - Failed Certificate Authority <i>The number of connections to the session key receiver port that did not proceed</i>



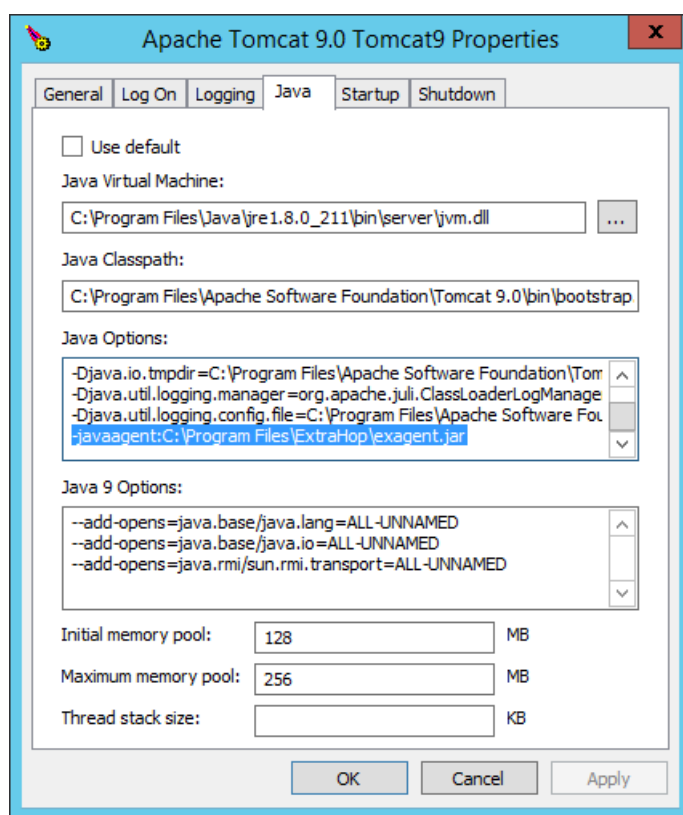
Hinweis: Informationen zum Erstellen eines neuen Dashboard-Diagramms finden Sie unter [Ein Diagramm mit dem Metric Explorer bearbeiten](#).

Integrieren Sie den Forwarder in die Java-basierte TLS-Anwendung

Der ExtraHop Session Key Forwarder integriert sich in Java-Anwendungen über den `-javaagent` Option. Lesen Sie die spezifischen Anweisungen Ihrer Anwendung zum Ändern der Java-Laufzeitumgebung, um Folgendes einzubeziehen `-javaagent` Option.

Beispielsweise unterstützt Apache Tomcat die Anpassung von Java-Optionen in den Eigenschaften des Tomcat Service Managers. Im folgenden Beispiel fügen Sie `-javaagent` Die Option für den Abschnitt Java-Optionen bewirkt, dass die Java-Laufzeitumgebung die Geheimnisse der TLS-Sitzung mit dem Key-Forwarder-Prozess teilt, der die Geheimnisse dann an das ExtraHop-System weiterleitet, damit die Geheimnisse entschlüsselt werden können.

```
-javaagent:C:\Program Files\ExtraHop\exagent.jar
```



Hinweis: Wenn auf Ihrem Server Java 17 oder höher ausgeführt wird, müssen Sie dem `sun.security.ssl`-Modul auch den Zugriff auf alle unbenannten Module mit dem `--add-opens` Option, wie im folgenden Beispiel gezeigt:

```
--add-opens java.base/sun.security.ssl=ALL-UNNAMED
```

Anlage

Beheben Sie häufig auftretende Fehlermeldungen

Fehlermeldungen werden in Protokolldateien an den folgenden Speicherorten gespeichert, wobei TMP der Wert Ihrer TMP-Umgebungsvariablen ist:

- TMP\ExtraHopSessionKeyForwarderSetup.log
- TMP\ExtraHopSessionKeyForwarderMsi.log

Die folgende Tabelle enthält häufig auftretende Fehlermeldungen, die Sie beheben können. Wenn Sie einen anderen Fehler sehen oder die vorgeschlagene Lösung Ihr Problem nicht löst, wenden Sie sich an den ExtraHop Support.

Nachricht	Ursache	Lösung
connect: dial tcp <IP address>:4873: connectex: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond	Der überwachte Server kann keinen Datenverkehr an den weiterleiten Sensor.	Stellen Sie sicher, dass die Firewallregeln das Initiieren von Verbindungen durch den überwachten Server zum TCP-Port 4873 auf dem Sensor.
connect: dial tcp <IP address>:4873: connectex: No connection could be made because the target machine actively refused it	Der überwachte Server kann den Verkehr an den weiterleiten Sensor, aber der Empfangsvorgang hört nicht zu.	Stellen Sie sicher, dass Sensor ist sowohl für die Funktionen TLS Decryption als auch TLS Shared Secrets lizenziert.
connect: x509: certificate signed by unknown authority	Der überwachte Server ist nicht in der Lage, die zu verketteten Sensor Zertifikat für eine vertrauenswürdige Zertifizierungsstelle (CA).	Stellen Sie sicher, dass der Windows-Zertifikatspeicher für das Computerkonto über vertrauenswürdige Stammzertifizierungsstellen verfügt, die eine Vertrauenskette für das Sensor.
connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANS	Eine IP-Adresse wurde als angegeben EDA_HOSTNAME Parameter bei der Installation des Forwarders, aber das vom Sensor vorgelegte TLS-Zertifikat enthält keine IP-Adresse als Subject Alternate Name (SAN).	Wählen Sie aus den folgenden drei Lösungen. • Wenn es einen Hostnamen gibt, mit dem der Server eine Verbindung herstellen kann Sensor mit, und dieser Hostname entspricht dem Betreffnamen in der Sensor Zertifikat, deinstalliere und installiere den Forwarder neu, wobei du diesen Hostnamen als Wert von gibst EDA_HOSTNAME. • Wenn der Server eine Verbindung zum herstellen muss Sensor nach IP-Adresse, deinstallieren Sie den Forwarder und installieren Sie ihn erneut, wobei Sie den Betreffnamen aus dem Sensorzertifikat

Nachricht	Ursache	Lösung
		als Wert von angeben SERVERNAMEOVERRIDE.
		Neuaufgabe der Sensor Zertifikat, das einen IP Subject Alternative Name (SAN) für die angegebene IP-Adresse enthält.

Deinstalliere die Software

Wenn Sie nicht mehr möchten, dass die ExtraHop-Sitzungsschlüsselweiterleitungssoftware installiert wird, oder wenn sich einer der ursprünglichen Installationsparameter geändert hat (Sensor-Hostname oder Zertifikat) und Sie die Software mit neuen Parametern neu installieren müssen, gehen Sie wie folgt vor:

 **Wichtig:** Sie müssen den Server neu starten, damit die Konfigurationsänderungen wirksam werden.

1. Loggen Sie sich auf dem Windows-Server ein.
2. Optional: Wenn Sie den Sitzungsschlüssel-Forwarder in Apache Tomcat integriert haben, entfernen Sie den `-javaagent:C:\Program Files\ExtraHop\exagent.jar` Eintrag von Tomcat, um zu verhindern, dass der Webservice gestoppt wird.
3. Wählen Sie eine der folgenden Optionen, um die Software zu entfernen:
 - Öffnen Sie das Control Panel und klicken Sie auf **Deinstalliere ein Programm**. Wählen **ExtraHop-Sitzungsschlüsselweiterleitung** aus der Liste und klicken Sie dann auf **Deinstallation**.
 - Öffnen Sie eine PowerShell-Eingabeaufforderung und führen Sie die folgenden Befehle aus, um die Software und die zugehörigen Registrierungseinträge zu entfernen:

```
1. $app=Get-WMIObject -class win32_product | where-object {$_.name -eq "ExtraHop Session Key Forwarder"}
```

```
2. $app.Uninstall()
```

4. Klicken **Ja** zur Bestätigung.
5. Nachdem die Software entfernt wurde, klicken Sie auf **Ja** um das System neu zu starten

Installationsparameter

Sie können die folgenden MSI-Parameter angeben:

MSI-Installationsparameter	EDA_HOSTNAME
Eintrag in die Registrierung	HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\EDAHost
Beschreibung	Das Sensor Hostname oder IP-Adresse, an die TLS-Sitzungsschlüssel gesendet werden. Dieser Parameter ist erforderlich.
MSI-Installationsparameter	EDA_CERTIFICATEPATH
Eintrag in die Registrierung	N/A

Beschreibung	Der überwachte Server muss dem Aussteller des vertrauen Sensor TLS-Zertifikat über den Zertifikatsspeicher des Servers. In einigen Umgebungen ist der Sensor arbeitet mit dem selbstsignierten Zertifikat , das die ExtraHop-Firmware bei der Installation generiert. In diesem Fall muss das Zertifikat zum Zertifikatsspeicher hinzugefügt werden. Das EDA_CERTIFICATEPATH Mit diesem Parameter kann ein dateibasiertes PEM-kodiertes Zertifikat bei der Installation in den Windows-Zertifikatsspeicher importiert werden. Wenn der Parameter bei der Installation nicht angegeben wird und ein selbstsigniertes oder anderes CA-Zertifikat manuell im Zertifikatsspeicher abgelegt werden muss, muss der Administrator das Zertifikat auf dem überwachten System unter Zertifikate (Computerkonto) > Vertrauenswürdige Stammzertifizierungsstellen importieren. Dieser Parameter ist optional, wenn der überwachte Server zuvor so konfiguriert wurde, dass er dem TLS-Zertifikat des Sensor über den Windows-Zertifikatsspeicher.
MSI-Installationsparameter	SERVERNAMEOVERRIDE
Eintrag in die Registrierung	HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\ServerNameOverride
Beschreibung	Wenn es eine Diskrepanz zwischen dem Sensor Hostname, den der Forwarder kennt (EDA_HOSTNAME) und der allgemeine Name (CN), der im TLS-Zertifikat des Sensor, dann muss der Forwarder mit dem richtigen CN konfiguriert werden. Dieser Parameter ist optional. Wir empfehlen, dass Sie das selbstsignierte TLS-Zertifikat auf der Grundlage des Hostnamens aus dem TLS-Zertifikat Abschnitt der Administrationseinstellungen, anstatt diesen Parameter anzugeben.
MSI-Installationsparameter	TCPLISTENPORT
Eintrag in die Registrierung	HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\TCPListenPort
Beschreibung	Der Key Forwarder empfängt Sitzungsschlüssel lokal aus der Java-Umgebung über einen TCP-Listener auf localhost (127.0.0.1) und den in der TCPListenPort Eintrag. Wir empfehlen, für diesen Port die Standardeinstellung 598 beizubehalten.

Dieser Parameter ist optional.

Unterstützte TLS-Verschlüsselungssammlungen

Das ExtraHop-System kann TLS-Verkehr entschlüsseln, der mit PFS- oder RSA-Cipher-Suites verschlüsselt wurde. Alle unterstützten Cipher-Suites können entschlüsselt werden, indem der Session Key Forwarder auf einem Server installiert und das ExtraHop-System konfiguriert wird.

Cipher Suites für RSA können den Datenverkehr auch mit einem Zertifikat und einem privaten Schlüssel entschlüsseln – mit oder ohne Sitzungsschlüsselweiterleitung.

Entschlüsselungsmethoden

Die folgende Tabelle enthält eine Liste von Cipher-Suites, die das ExtraHop-System kann [entschlüsseln](#) zusammen mit den unterstützten Entschlüsselungsoptionen.

- **PFS + GPP:** das ExtraHop-System kann diese Verschlüsselungssammlungen mit Sitzungsschlüsselweiterleitung entschlüsseln und [Zuordnung von globalem Protokoll zu Port](#)
- **PFS + Zertifikat:** Das ExtraHop-System kann diese Cipher-Suites mit Sitzungsschlüsselweiterleitung entschlüsseln und [Zertifikat und privater Schlüssel](#)
- **RSA + Zertifikat:** das ExtraHop-System kann diese Cipher-Suites ohne Weiterleitung des Sitzungsschlüssels entschlüsseln, solange Sie die Datei hochgeladen haben [Zertifikat und privater Schlüssel](#)

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0 x 04	TLS_RSA_MIT_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 05	TLS_RSA_MIT_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 0A	TLS_RSA_MIT_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 16	TLS_DHE_RSA_MIT_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0x2F	TLS_RSA_MIT_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 33	TLS_DHE_RSA_MIT_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0x35	TLS_RSA_MIT_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x39	TLS_DHE_RSA_MIT_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0x3C	TLS_RSA_MIT_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0x3D	TLS_RSA_MIT_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x67	TLS_DHE_RSA_MIT_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0x6 B	TLS_DHE_RSA_MIT_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Zertifikat
0x9C	TLS_RSA_MIT_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9D	TLS_RSA_MIT_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9E	TLS_DHE_RSA_MIT_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0x9F	TLS_DHE_RSA_MIT_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0 x 1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	PFS + GPP PFS + Zertifikat
0 x 1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Zertifikat
0 x 1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Zertifikat
0xC007	TLS_ECDHE_ECDSA_MIT_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS + GPP
0xC008	TLS_ECDHE_ECDSA_MIT_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS + GPP
0xC009	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0xC011	TLS_ECDHE_RSA_MIT_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Zertifikat
0xC012	TLS_ECDHE_RSA_MIT_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0xC013	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0xC014	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0xC023	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0xC024	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0xC027	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0xC028	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Zertifikat
0xC02B	TLS_ECDHE_ECDSA_MIT_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_MIT_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP
0xC02F	TLS_ECDHE_RSA_MIT_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0xC030	TLS_ECDHE_RSA_MIT_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0xCCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat
0xCCA9	TLS_ECDHE_ECDSA_MIT_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP
0xCCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat

Exportieren Sie die MSI-Datei aus der ausführbare Datei

Sie können die MSI-Datei aus der ausführbare Datei exportieren, um einen benutzerdefinierten Installationsablauf zu unterstützen.

Öffnen Sie eine PowerShell-Eingabeaufforderung und führen Sie den folgenden Befehl aus:

```
ExtraHopSessionKeyForwarderSetup.exe -e
```



Hinweis Sie können anhängen <directory> zum -e Parameter zum Speichern des .msi Datei in ein anderes Verzeichnis als das aktuelle Arbeitsverzeichnis. Mit dem folgenden Befehl wird die Datei beispielsweise im install_dir Verzeichnis:

```
ExtraHopSessionKeyForwarderSetup.exe -e install_dir
```