Install the ExtraHop session key forwarder on a Windows server

Published: 2021-09-04

Perfect Forward Secrecy (PFS) is a property of secure communication protocols that enables short-term, completely private session key exchanges between clients and servers. ExtraHop offers session key forwarding software that can send session keys to the ExtraHop system for SSL/TLS decryption. There is no limit to the number of session keys that the ExtraHop system can receive.

You must configure the ExtraHop system for session key forwarding and then install the forwarder software on the Windows and Linux servers that have the SSL/TLS traffic that you want to decrypt.

Before you begin

- Read about SSL/TLS decryption and review the list of supported cipher suites.
- Make sure that the ExtraHop system is licensed for SSL Decryption and SSL Shared Secrets.
- Make sure that your server environment is supported by the ExtraHop session key forwarder software:
  - Microsoft Secure Channel (Schannel) security package
  - Java SSL/TLS (Java versions 8 through 13). Do not upgrade to this version of the session key forwarder if you are currently monitoring Java 6 or Java 7 environments. Version 7.9 of the session key forwarder supports Java 6 and Java 7, and is compatible with the latest ExtraHop firmware.
  - Dynamically linked OpenSSL (1.0.x and 1.1.x) libraries. OpenSSL is only supported on Linux systems with kernel versions 4.4 and later and RHEL 7.6 and later.

  Important: The ExtraHop system cannot decrypt TLS-encrypted TDS traffic through session key forwarding. Instead, you can upload an RSA private key.
- Install the session key forwarder on one or more Windows 2008 R2, Windows 2012 R2, or Windows 2016 servers running SSL-based services with the native Windows SSL framework. OpenSSL on Windows is not currently supported.

  Important: After you install the session key forwarder software on Windows 2012 R2 or Windows 2016 systems, applications that include SSL-enabled features, such as Microsoft Edge and Windows Store applications that incorporate sandboxing features, might fail to function correctly.

  Validate the compatibility of the session key forwarder in your Windows test environment before deploying in your production environment.

Windows application traffic decryption

The following Microsoft application traffic can be decrypted with the session key forwarder.

- Microsoft IIS
- Microsoft PowerShell
- Microsoft SQL Server

Install the software with the installation wizard

Warning: The installation requires a restart of the server. Do not start the installation unless you are able to restart the server after the installation completes.

1. Log in to the Windows server.
2. Download the latest version of the session key forwarder software.
3. Double-click the `ExtraHopSessionKeyForwarder.msi` file and click **Next**.

4. Select the box to accept the terms of the license agreement and then click **Next**.
5. Type the name of the Discover appliance where you want to forward session keys.
6. Accept the default TCP listen port value of 598 (recommended), or type a custom port value and then click **Next**.
7. Click **Install**.
8. When the installation completes, click **Finish**, and then click **Yes** to reboot the server.

Command-line installation option

The following steps show you how to install the session key forwarder from a Windows command prompt or Windows PowerShell.

> **Warning:** The installation requires a restart of the server. Do not start the installation unless you are able to restart the server after the installation completes.

1. Log in to the Windows server.
2. Download the latest version of the session key forwarder software.
3. Run the following command:

```
msiexec /i C:\ExtraHopSessionKeyForwarder.msi EDA_HOSTNAME=<hostname or
 IP address of Discover appliance>
```

Where `C:\ExtraHopSessionKeyForwarder.msi` is the path to the installer file.

If required for your configuration, you can add optional parameters to the command:

```
msiexec /i C:\ExtraHopSessionKeyForwarder.msi EDA_HOSTNAME=<hostname or
 IP address of Discover appliance>
EDACERTIFICATEPATH=<path to .pem file> SERVERNAMEOVERRIDE=<Common Name>
 TCPLISTENPORT=<Port Number>
```

For more information, see Installation parameters in the Appendix.

4. When the installation completes, click **Yes** to reboot the server.

Enable the SSL session key receiver service

You must enable the session key receiver service on the ExtraHop system before the system can receive and decrypt session keys from the session key forwarder. By default, this service is disabled.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **Services**.
3. Select the **SSL Session Key Receiver** checkbox.
4. Click **Save**.

Add a global port to protocol mapping

Add each protocol for the traffic that you want to decrypt with your session key forwarders.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **SSL Decryption**.
4. In the Private Key Decryption section, clear the Require Private Keys checkbox.
5. In the Global Protocol to Port Mapping section, click **Add Global Protocol**.

6. From the Protocol drop-down list, select the protocol for the traffic that you want to decrypt.
7. In the Port field, type the number of the port. Type `0` to add all ports.
8. Click **Add**.

View connected session key forwarders

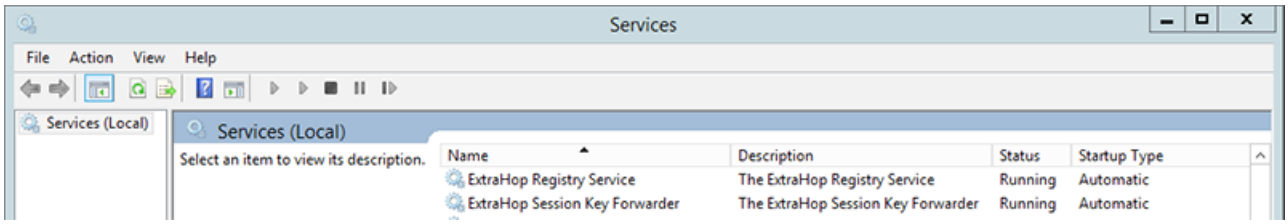
You can view recently connected session key forwarders after you install the session key forwarder on your server and enable the SSL session key receiver service on the ExtraHop system. Note that this page only displays session key forwarders that have connected over the last few minutes, not all session key forwarders that are currently connected.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **SSL Shared Secrets**.

Validate session key forwarding

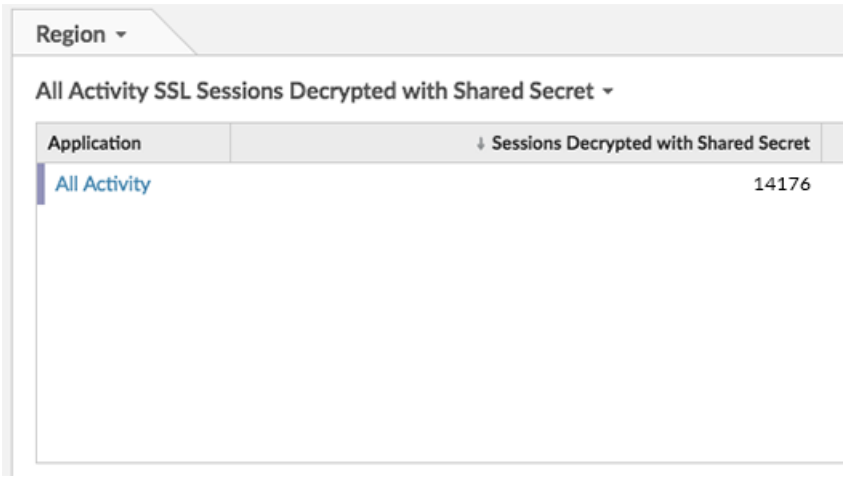
Perform these steps to make sure that the installation was successful and the session key forwarder is forwarding the keys to the ExtraHop system.

1. Log in to the Windows server.
2. Open the Services MMC snap-in. Ensure both services, “ExtraHop Session Key Forwarder” and ExtraHop Registry Service” show the status as “Running”.



3. If either service is not running, troubleshoot the issue by completing the following steps.
   a) Open the Event Viewer MMC snap-in and navigate to Windows Logs > Application.
   b) Locate the most recent entries for the ExtraHopAgent source. Common reasons for failure and their associated error messages are listed in the Troubleshoot common error messages section below.
4. If the Services and Event Viewer snap-in do not indicate any issues, apply a workload to the monitored services and go to the ExtraHop system to verify that secret-based decryption is working.

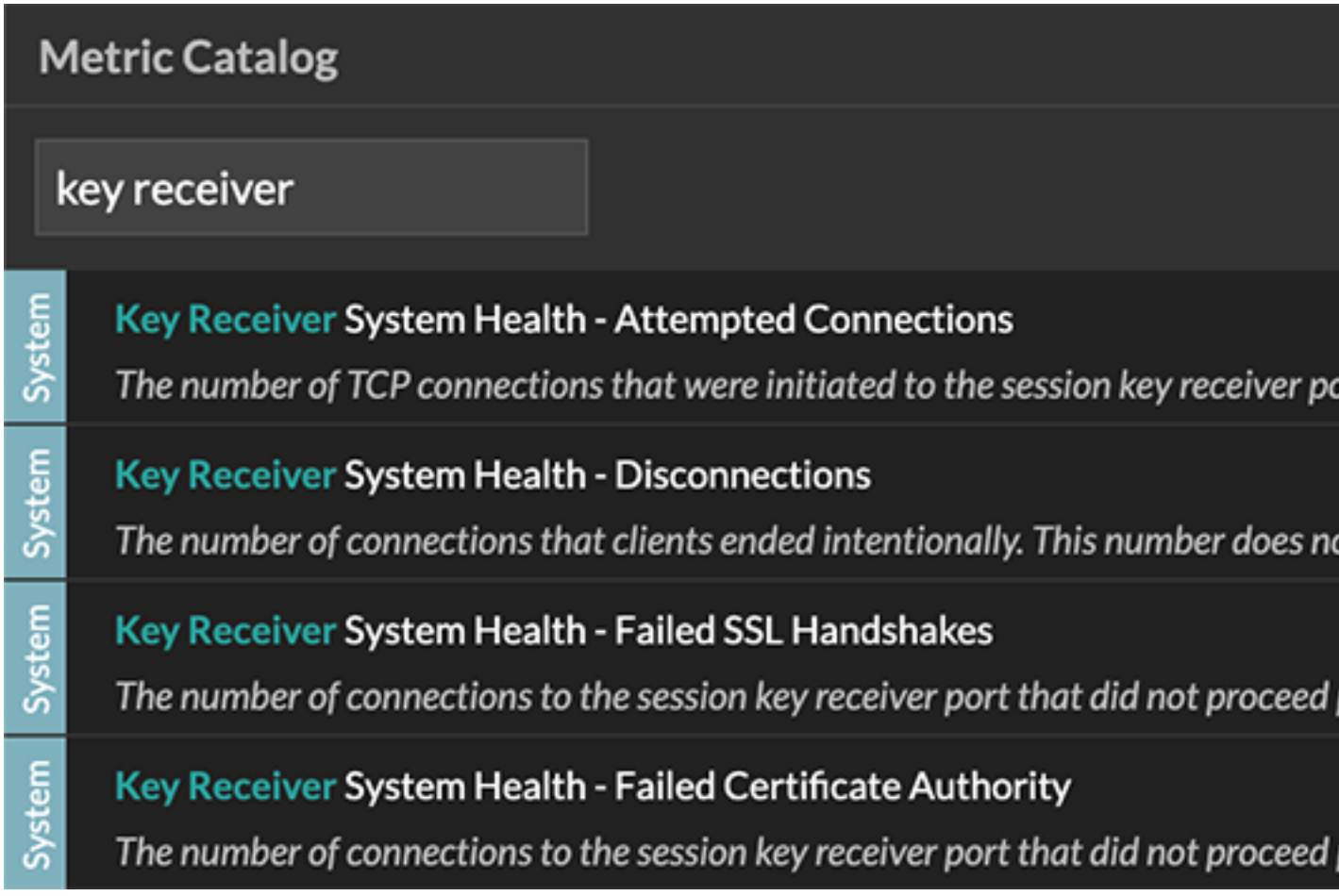
When the ExtraHop system receives session keys and applies them to decrypted sessions, the Shared Secret metric counter (in Applications > All Activity > SSL Sessions Decrypted) is incremented. Create a dashboard chart with this metric to see if the Discover appliance is successfully receiving session keys from the monitored servers.



Key receiver system health metrics

The ExtraHop system provides key receiver metrics that you can add to a dashboard chart to monitor key receiver health and functionality.

To view a list of available metrics, click the System Settings icon and then click **Metric Catalog**. Type `key receiver` in the filter field to display all available key receiver metrics.



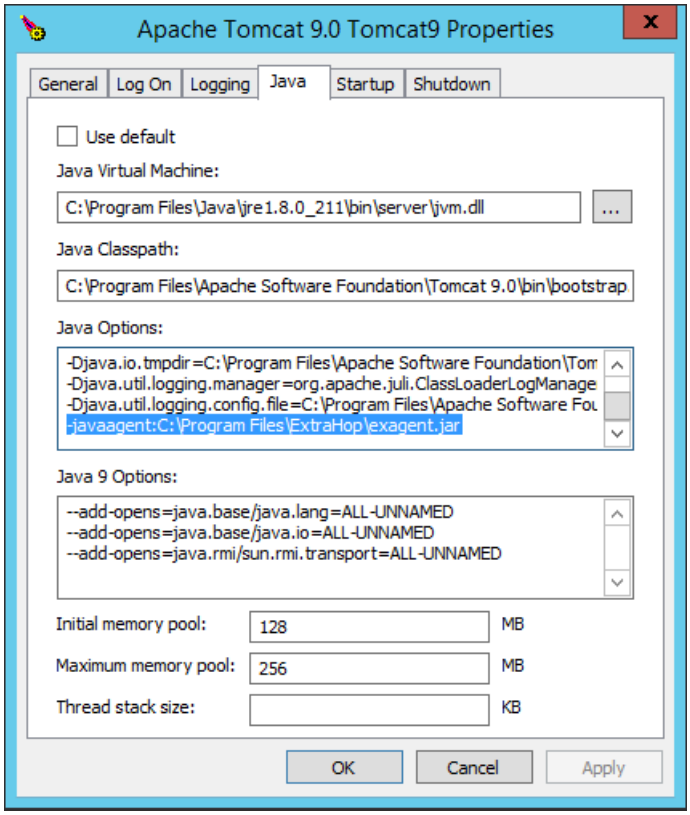
Tip: To learn how to create a new dashboard chart, see Edit a chart with the Metric Explorer.

Integrate the forwarder with the Java-based SSL application

The ExtraHop session key forwarder integrates with Java applications through the `-javaagent` option. Consult your application's specific instructions for modifying the Java runtime environment to include the `-javaagent` option.

As an example, Apache Tomcat supports customization of Java options in the Tomcat service manager properties. In the following example, adding the `-javaagent` option to the Java Options section causes the Java runtime to share SSL session secrets with the key forwarder process, which then relays the secrets to the ExtraHop system so that the secrets can be decrypted.

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



Troubleshoot common error messages

The following table shows common error messages that you can troubleshoot. If you see a different error or the proposed solution does not resolve your issue, contact ExtraHop Support.

Message	Cause	Solution
`connect: dial tcp <IP address>:4873: connectex: A connection attempt failed because the`	The monitored server cannot route any traffic to the Discover appliance.	Ensure firewall rules allow connections to be initiated by the monitored server to TCP port 4873 on the Discover appliance.

Message	Cause	Solution
`connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond`		
`connect: dial tcp <IP address>:4873: connectex: No connection could be made because the target machine actively refused it`	The monitored server can route traffic to the Discover appliance, but the receiving process is not listening.	Ensure that the Discover appliance is licensed for both the SSL Decryption and SSL Shared Secrets features.
`connect: x509: certificate signed by unknown authority`	The monitored server is not able to chain up the Discover appliance certificate to a trusted Certificate Authority (CA).	Ensure that the Windows certificate store for the computer account has trusted root certificate authorities that establish a chain of trust for the Discover appliance.
`connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANs`	An IP address was supplied as the `EDA_HOSTNAME` parameter when installing the forwarder, but the SSL certificate presented by the Discover appliance does not include an IP address as a Subject Alternate Name (SAN).	Select from the following three solutions. • If there is a hostname that the server can connect to the Discover appliance with, and that hostname matches the subject name in the Discover appliance certificate, uninstall and reinstall the forwarder, specifying that hostname as the value of `EDA_HOSTNAME`. • If the server is required to connect to the Discover appliance by IP address, uninstall and reinstall the forwarder, specifying the subject name from the Discover appliance certificate as the value of `SERVERNAMEOVERRIDE`. • Re-issue the Discover appliance certificate to include an IP Subject Alternative Name (SAN) for the given IP address.

Uninstall the software

If you no longer want the ExtraHop session key forwarder software installed, or if any of the original installation parameters have changed (Discover appliance hostname or certificate) and you need to reinstall the software with new parameters, do the following:

Important: You must restart the server for the configuration changes to take effect.

1. Log in to the Windows server.
2. Optional: If you integrated the session key forwarder with Apache Tomcat, remove the `-javaagent:C:\Program Files\ExtraHop\exagent.jar` entry from Tomcat to prevent the web service from stopping.
3. Choose one of the following options to remove the software:
   - Open the Control Panel and click **Uninstall a program**. Select **ExtraHop Session Key Forwarder** from the list and then click **Uninstall**.
   - Run the following command to remove the software and associated registry entries:

     ```
     msiexec /x C:\ExtraHopSessionKeyForwarder.msi
     ```

     Where `C:\ExtraHopSessionKeyForwarder.msi` is the path to the installer file.
4. Click **Yes** to confirm.
5. After the software is removed, click **Yes** to restart the system

Installation parameters

The session key forwarder software is provided as an MSI package. A complete installation of the forwarder requires specifying the `EDA_HOSTNAME` parameter. Three additional parameters, `EDA_CERTIFICATEPATH`, `SERVERNAMEOVERRIDE`, or `TCPLISTENPORT` might be required and are described in the tables below.

MSI Installation Parameter	`EDA_HOSTNAME`
Registry Entry	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\EDAHost`
Description	The Discover appliance hostname or IP address where SSL session keys will be sent. This parameter is required.

MSI Installation Parameter	`EDA_CERTIFICATEPATH`
Registry Entry	N/A
Description	The monitored server must trust the issuer of the Discover appliance SSL certificate through the server's certificate store. In some environments, the Discover appliance works with the self-signed certificate that the ExtraHop firmware generates upon installation. In this case, the certificate must be added to the certificate store. The `EDA_CERTIFICATEPATH` parameter enables a file-based PEM-encoded certificate to be imported into the Windows certificate store at installation.

	If the parameter is not specified at installation and a self-signed or other CA certificate must be placed into the certificate store manually, the administrator must import the certificate to Certificates (Computer Account) > Trusted Root Certification Authorities on the monitored system. This parameter is optional if the monitored server was previously configured to trust the SSL certificate of the Discover appliance through the Windows certificate store.

MSI Installation Parameter	`SERVERNAMEOVERRIDE`
Registry Entry	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\ServerNameOverride`
Description	If there is a mismatch between the Discover appliance hostname that the forwarder knows (EDA_HOSTNAME) and the common name (CN) that is presented in the SSL certificate of the Discover appliance, then the forwarder must be configured with the correct CN. This parameter is optional. We recommend that you regenerate the SSL self-signed certificate based on the hostname from the SSL Certificate section of the Administration settings instead of specifying this parameter.

MSI Installation Parameter	`SET_REBOOT_PENDING="0"`
Registry Entry	`N/A`
Description	A system restart is required for the install to complete. If you specify this parameter you will not be prompted to restart the system. This parameter is not recommended.

MSI Installation Parameter	`TCPLISTENPORT`
Registry Entry	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\TCPListenPort`
Description	The key forwarder receives session keys locally from the Java environment through a TCP listener on localhost (127.0.0.1) and the port specified in the `TCPListenPort` entry. We recommended that this port remain set to the default of 598. This parameter is optional.

Supported SSL/TLS cipher suites

The ExtraHop system can decrypt SSL/TLS traffic that has been encrypted with PFS or RSA cipher suites. All supported cipher suites can be decrypted by installing the session key forwarder on a server and configuring the ExtraHop system.

Cipher suites for RSA can also decrypt the traffic with a certificate and private key—with or without session key forwarding.

Decryption methods

The table below provides a list of cipher suites that the ExtraHop system can decrypt along with the supported decryption options.

- **PFS + GPP**: the ExtraHop system can decrypt these cipher suites with session key forwarding and global protocol to port mapping
- **PFS + Cert**: the ExtraHop system can decrypt these cipher suites with the session key forwarding and the certificate and private key
- **RSA + Cert**: the ExtraHop system can decrypt these cipher suites without session key forwarding as long as you have uploaded the certificate and private key.

Hex Value	Name (IANA)	Name (OpenSSL)	Supported Decryption
0x04	TLS_RSA_WITH_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Cert RSA + Cert
0x05	TLS_RSA_WITH_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Cert RSA + Cert
0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Cert RSA + Cert
0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Cert
0x2F	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Cert RSA + Cert
0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Cert
0x35	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Cert RSA + Cert
0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Cert
0x3C	TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Cert RSA + Cert
0x3D	TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Cert RSA + Cert
0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Cert
0x6B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Cert
0x9C	TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Cert RSA + Cert

Hex Value	Name (IANA)	Name (OpenSSL)	Supported Decryption
0x9D	TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Cert RSA + Cert
0x9E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Cert
0x9F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Cert
0x1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	PFS + GPP PFS + Cert
0x1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Cert
0x1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Cert
0xC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS + GPP
0xC008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS + GPP
0xC009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0xC011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Cert
0xC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Cert
0xC013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Cert
0xC014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Cert
0xC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP
0xC024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0xC027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Cert
0xC028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Cert
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP

Hex Value	Name (IANA)	Name (OpenSSL)	Supported Decryption
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Cert
0xC030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Cert
0xCCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Cert
0xCCA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP
0xCCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Cert