Install the ExtraHop session key forwarder on a Windows server

Published: 2020-02-22

Perfect Forward Secrecy (PFS) is a property of secure communication protocols that enables short-term, completely private session key exchanges between clients and servers. When the session keys are only shared between the client and server, the Discover appliance is unable to decrypt this traffic, even when the Discover appliance has a copy of the server private key. The only way for the Discover appliance to decrypt this traffic is to get a copy of the session key from the server.

ExtraHop offers session key forwarding software for Windows and Linux that you can install on your servers that are sending SSL-encrypted traffic. The forwarder sends the SSL sessions keys to your ExtraHop Discover appliance. The session keys then enable the Discover appliance to decrypt those SSL/TLS sessions in your data feed. The ExtraHop session key forwarder can decrypt sessions from Java SSL/TLS (Java versions 6 through 10), or dynamically linked OpenSSL (1.0.x) libraries. OpenSSL is only supported on Linux with kernel versions 4.4 and later or RHEL 7.6 and later.

Depending on your environment, you can configure the Discover appliance for session key forwarding with or without a server certificate and private keys.

- (Recommended) If your environment does not require a server certificate, you can disable the private key requirement and configure global port mappings for the protocol traffic you want to decrypt.
- If your environment requires a server certificate, first complete the steps in the Decrypt SSL traffic with certificates and private keys guide, and then complete the steps below to install the forwarder software.

Before you begin

- Review the list of supported cipher suites that can be decrypted by the Discover appliance when session key forwarding is configured.
- Make sure that the Discover appliance is licensed for SSL Decryption and SSL Shared Secrets.
- 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.

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 into 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 and then click **Next**.
6. Click **Install**.
7. 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 into 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 up to two 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>
```

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 Discover appliance before the appliance can receive and decrypt sessions keys from the session key forwarder. By default, this service is disabled.

1. Log into the Admin UI on the Discover appliance.
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 into the Admin UI on the Discover appliance.
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 Discover appliance. Note that this page only

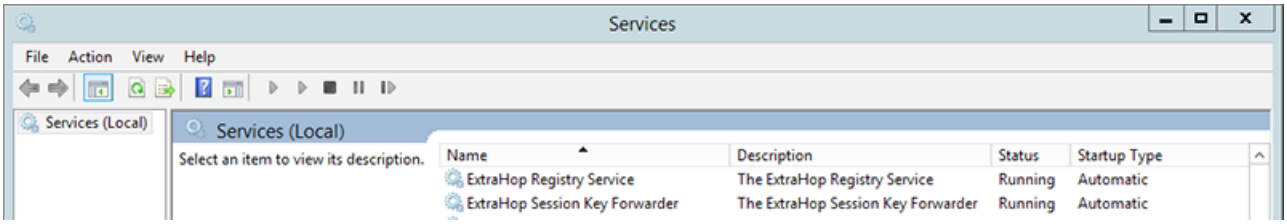
displays session key forwarders that have connected over the last few minutes, not all session key forwarders that are currently connected.

1. Log into the Admin UI on the Discover appliance.
2. In the System Configuration section, click **Capture**.
3. Click **SSL Shared Secrets**.

Validate session key forwarding

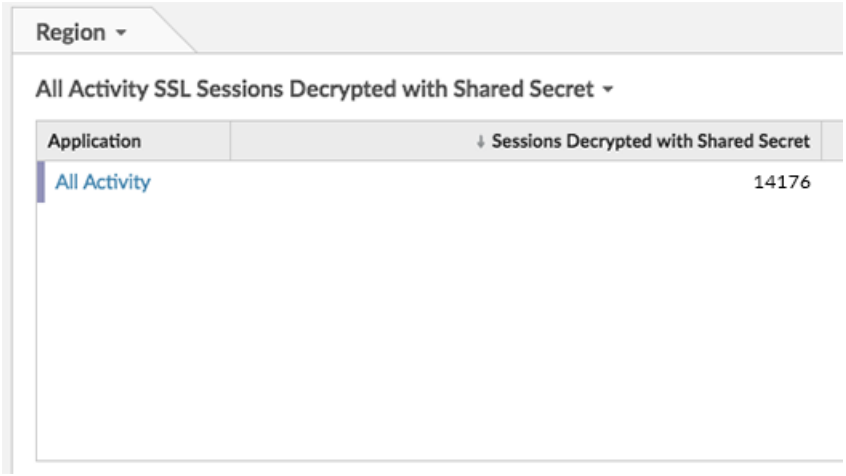
Perform these steps to make sure that the installation was successful and the session key forwarder is forwarding the keys to the Discover appliance.

1. Log into the Windows server.
2. Open the Services MMC snap-in. Ensure both services, "ExtraHop Secret Agent" 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 Discover appliance to verify that secret-based decryption is working.

When the Discover appliance 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.



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 connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond`	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.
`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

Message	Cause	Solution
		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 into the Windows server and 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.
2. Click **Yes** to confirm.
3. 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. Two additional parameters, `EDA_CERTIFICATEPATH` or `SERVERNAMEOVERRIDE`, 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 Admin UI instead of specifying this parameter.

Supported SSL cipher suites

To decrypt SSL traffic in real time, you must configure your server applications to encrypt traffic with supported ciphers. The following information provides a list of supported cipher suites and the best practices you should consider when implementing SSL encryption.

- Turn off SSLv2 to reduce security issues at the protocol level.
- Turn off SSLv3, unless required for compatibility with older clients.
- Turn off SSL compression to avoid the CRIME security vulnerability.
- Turn off session tickets unless you are familiar with the risks that might weaken Perfect Forward Secrecy.
- Configure the server to select the cipher suite in order of the server preference.

The following cipher suites can be decrypted by the ExtraHop appliance and are listed in from strongest to weakest and by server preference:

- AES256-GCM-SHA384
- AES128-GCM-SHA256
- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DES-CBC3-SHA

The following list includes some common cipher suites that support Perfect Forward Secrecy (PFS) and can be decrypted by the ExtraHop appliance when session key forwarding is configured. To configure session

key forwarding, see Install the ExtraHop session key forwarder on a Windows server or Install the ExtraHop session key forwarder on a Linux server.

- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The following list of cipher suites support Perfect Forward Secrecy (PFS) but cannot be decrypted by the ExtraHop appliance:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES128-SHA256