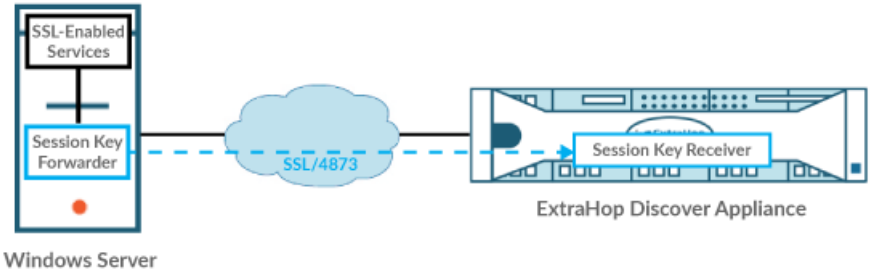
Install the ExtraHop session key forwarder on a Windows server

Published: 2018-01-11

The ExtraHop session key forwarder runs as a process on a monitored Windows server running SSL services. The forwarder establishes an SSL-secured connection to an ExtraHop Discover appliance to send all SSL session keys. The session keys enable the Discover appliance to decrypt SSL/TLS sessions that otherwise could not be decrypted, either because the session is encrypted with Perfect Forward Secrecy (PFS) ciphers or the Discover appliance does not have the private key for RSA handshakes. After the session keys are forwarded, We should proactively zero-out secrets immediately after sending



After the session keys are forwarded, they are immediately deleted from memory on the Windows server.

Before you begin

- Read our blog post: What is Perfect Forward Secrecy?
- Make sure that the Discover appliance is running firmware version 7.0 or later.
- Make sure that the Discover appliance is licensed for SSL Decryption.
- Install the session key forwarder on one or more Windows 2008 or Windows 2012 servers running SSL-based services with the native Windows SSL framework. OpenSSL on Windows is not currently supported.
- Session key processing on the Discover appliance requires that you upload the server certificate and private key file for any monitored SSL-encrypted service to the Discover appliance. Go to the **Capture** > **SSL Decryption Keys** page in the Admin UI to upload a .pem file that includes both a private key and certificate.
- The session key forwarder on the Windows server must be able to access a trusted CA certificate from the Windows certificate store to validate the certificate (or chain of certificates) that the Discover appliance presents.
- Make sure that the server certificates have an RSA public key. DSA and ECDSA public keys are not currently supported.
- The traffic for each monitored SSL server must be part of the data feed to the Discover appliance.

Important: The session key forwarder software is provided as an .msi file. While it is possible to double-click the .msi file to start the installation process, we strongly recommend that you install the software from a command prompt.

When the installation parameters are provided through the command line, the installation process incorporates the specified parameters into the registry and certificate store. If the installation is completed through the installer UI, there are no prompts for any parameters and you must configure them manually in the registry after the installation is complete.

If you inadvertently install the software from the installer UI, uninstall the software and then reinstall from the command prompt.

Install the software

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.

Before you begin
Contact your ExtraHop account representative for a download link to the session key forwarder software.

1. Log into the Windows 2008 or 2012 server.
2. Download the session key forwarder software.
3. Run the following command:

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

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

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

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

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**.

View connected session key forwarders

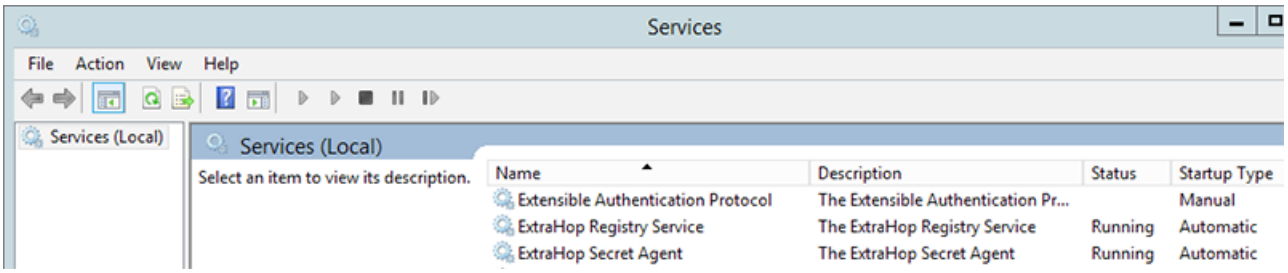
You can view connected session key forwarders after you install the session key forwarder on your Windows server and enable the SSL session key receiver service on the Discover appliance.

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

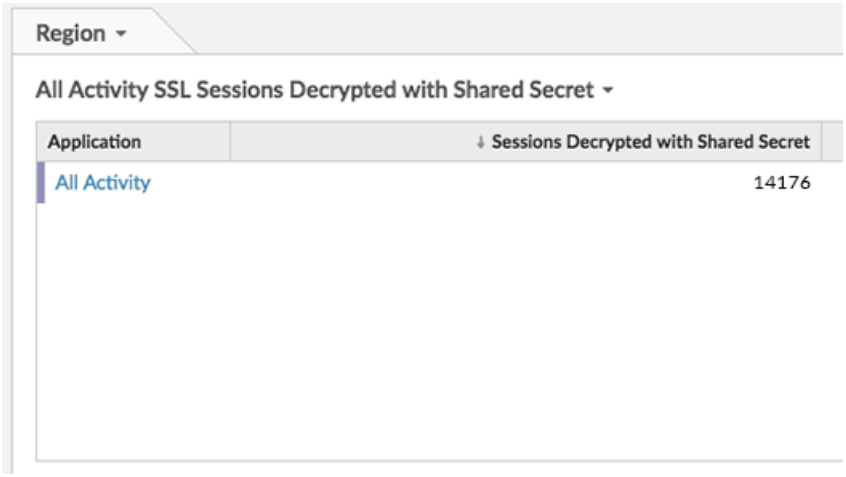
Perform these steps to make sure that the installation was successful and the session key forwarder is forwarding the keys to the Discover appliance.

1. Log into the Windows 2008 or 2012 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`	The monitored server cannot route any traffic to the Discover appliance.	Ensure firewall rules allow SSL connections to be initiated from the monitored server to the Discover appliance.

Message	Cause	Solution
`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 Secret Agent 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 into the Windows server.

2. Run the following command to remove the software and associated registry entries:

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

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

Appendix

Installation parameters

The session key forwarder software is provided as an MSI package. A complete installation of the forwarder requires specifying up to three parameters, which 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.