RevealX Enterprise Secure Technical Implementation Guide

Published: 2025-04-10

The following sections provide information and recommendations about configuring your ExtraHop RevealX Enterprise system with optimal security controls.

Data protection

The following sections provide guidance on settings that ensure your data is secured.

Create a certificate signing request from your ExtraHop system

A certificate signing request (CSR) is a block of encoded text that is given to your Certificate Authority (CA) when you apply for a TLS certificate. The CSR is generated on the ExtraHop system where the TLS certificate will be installed and contains information that will be included in the certificate such as the common name (domain name), organization, locality, and country. The CSR also contains the public key that will be included in the certificate. The CSR is created with the private key from the ExtraHop system, making a key pair.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **TLS Certificate**.
3. Click **Manage certificates** and then click **Export a Certificate Signing Request (CSR)**.
4. In the Subject Alternative Names section, type the DNS name of the ExtraHop system.
   You can add multiple DNS names and IP addresses to be protected by a single TLS Certificate.
5. In the Subject section, complete the following fields.
   Only the **Common Name** field is required.

Field	Description	Examples
Common Name	The fully qualified domain name (FQDN) of the ExtraHop system. The FQDN must match one of the Subject Alternative Names.	*.example.com discover.example.com
E-mail Address	The email address of the primary contact for your organization.	webmaster@example.com
Organizational Unit	The division of your organization handling the certificate.	IT Department
Organization	The legal name of your organization. This entry should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.	Example, Inc.
Locality/City	The city where your organization is located.	Seattle
State/Province	The state or province where your organization is located. This entry should not be abbreviated.	Washington

Field	Description	Examples
Country Code	The two-letter ISO code for the country where your organization is located.	US

6. Click **Export**.

   The CSR file is automatically downloaded to your computer.

Next steps

Send the CSR file to your certificate authority (CA) to have the CSR signed. When you receive the TLS certificate from the CA, return to the TLS Certificate page in the Administration settings and upload the certificate to the ExtraHop system.

Tip: If your organization requires that the CSR contains a new public key, generate a self-signed certificate to create new key pairs before creating the CSR.

Encryption Controls

The following sections provide guidance on settings that control encryption.

Encryption at rest

Data on a stolen unencrypted disk can still be accessed, however encryption at rest further secures your data, because an encryption key is required to access disk data.

Encryption at rest can be configured on supported appliances.

Encryption in transit

The following settings in the Running Configuration file help secure your encrypted data in transit.

Some of the following settings might not appear in the Running Configuration file by default, but if they have been added by an administrator, you should ensure these settings are configured for the most secure option.

Most of these settings are configured to the most secure mode by default, but here is a list of the settings.

Replace DNS license traffic with HTTPS through ExtraHop Cloud Services

This setting allows license check-ins to connect through HTTPS to ExtraHop Cloud Services instead of through DNS. Setting `use_dns` to `false` ensures the firmware connects through an encrypted tunnel to ExtraHop Cloud Services for license check-ins. The setting is set to `true` by default, but should be modified to `false` to maximize security:

```
"license_server": {
    "use_dns": false
}
```

Note that when this value is set to `false`, if the appliance cannot connect to ExtraHop Cloud Services through HTTPS, all functionality is halted.

Enable FIPS mode

This setting configures the appliance to limit encryption for data transfer to FIPS-validated algorithms. This setting is set to `false` by default, but should be set to `true` for customers who are required to comply with FIPS-validated algorithms.

The setting should appear as follows for FedRAMP compliance:

```
"fips": {
    "enabled": true
```

```
}
```

ExtraHop Cloud Services Certificate Verification

When a customer node joins ExtraHop Cloud Services, ExtraHop verifies the TLS certificate by default. While this certificate can be disabled, the inner tunnels will continue to validate certificates. The setting should appear as follows:

```
"hopcloud": {
    "verify_outer_tunnel_cert": true
}
```

HTTP Strict Transport Security (HSTS)

Enables HTTP Strict Transport Security (HSTS), a web security policy mechanism that helps to protect websites against protocol downgrade attacks and cookie hijacking. The setting should appear as follows:

```
"webserver": {
    "hsts": true
}
```

Web Server SSL/TLS profile

Determines the SSL/TLS profile configured for the appliance webserver. The SSL/TLS profile should be left at its default value of `modern`:

```
"webserver": {
    "ssl_profile": "modern"
}
```

Content Security Policy (CSP)

This flag enables the addition of the Content-Security-Policy Header. The flag currently defaults to false. The CSP is defined as `default-src 'self' 'unsafe-inline'; img-src * data:`. The setting should appear as follows:

```
"webserver": {
    "enable_csp": true,
}
```

Session key forwarding

To configure session key forwarding, see the following guides:

- Install the ExtraHop session key forwarder on a Windows server
- Install the ExtraHop session key forwarder on a Linux server
- Download session keys with packet captures

Important: Make sure that access is open for TCP port 4873 on the ExtraHop sensor.

TLS decryption

To configure TLS decryption, see the following guides:

- Decrypt TLS traffic with certificates and private keys
- TLS decryption

Configure packet capture

Packet capture enables you to collect, store, and retrieve data packets from your network traffic. You can download a packet capture file for analysis in a third-party tool, such as Wireshark. Packets can be inspected to diagnose and resolve network problems and to verify that security policies are being followed.

By adding a packet capture disk to the ExtraHop sensor, you can store the raw payload data sent to your ExtraHop system. This disk can be added to your virtual sensor or an SSD that is installed in your physical sensor.

These instructions only apply to ExtraHop systems that have a precision packet capture disk. To store packets on an ExtraHop packetstore appliance, see the packetstore deployment guides.

Important: Systems with self-encrypting disks (SEDs) cannot be configured for software encryption on packet captures. For information on enabling security on these systems, see Configure self-encrypting disks (SEDs).

Packet slicing

By default, the packetstore saves whole packets. If packets are not already sliced, you can configure the sensor to store packets sliced to a fixed number of bytes for improved privacy and lookback.

For more information on configuring this feature in your running configuration file, contact ExtraHop Support.

Enable packet capture

Your ExtraHop system must be licensed for packet capture and configured with a dedicated storage disk. Physical sensors require an SSD storage disk and virtual sensors require a disk configured on your hypervisor.

Before you begin

Verify that your ExtraHop system is licensed for Packet Capture by logging in to the Administration settings and clicking **License**. Packet Capture is listed under Features and **Enabled** should appear.

Important: The capture process restarts when you enable the packet capture disk.

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 **Disks**.
3. Depending on your sensor type and menu options, configure the following settings.
   - For physical sensors click **Enable** next to SSD Assisted Packet Capture, and then click **OK**.
   - For virtual sensors, verify that `running` appears in the Status column and that the disk size you configured for packet capture appears in the Size column. Click **Enable** in the Actions column of the row for the packet capture disk, and then click **OK**.

Next steps

Your packet capture disk is now enabled and ready to store packets. Click **Configure** if you want to encrypt the disk, or configure global or precision packet captures.

Encrypt the packet capture disk

Packet capture disks can be secured with 256-bit AES encryption.

Here are some important considerations before you encrypt a packet capture disk:

- You cannot decrypt a packet capture disk after it is encrypted. You can clear the encryption, but the disk is formatted, and all data is deleted.
- You can lock an encrypted disk to prevent any read or write access to stored packet capture files. If the ExtraHop system is restarted, encrypted disks are automatically locked and remain locked until they are unlocked with the passphrase. Unencrypted disks cannot be locked.
- You can reformat an encrypted disk, but all data is permanently deleted. You can reformat a locked disk without unlocking the disk first.
- You can perform a secure delete (or system wipe) of all system data. For instructions, see the ExtraHop Rescue Media Guide.

Warning: When you encrypt a packet capture disk, all packets stored on the disk are deleted.

Important: Systems with self-encrypting disks (SEDs) cannot be configured for software encryption on packet captures. For information on enabling security on these systems, see Configure self-encrypting disks (SEDs).

1. In the Appliance Settings section, click **Disks**.
2. On the Disks page, select one of the following options based on your sensor type.
   - For virtual sensors, click **Configure** in the Actions column of the row for the packet capture disk.
   - For physical sensors, click **Configure** next to SSD Assisted Packet Capture.
3. Click **Encrypt Disk**.
4. Specify a disk encryption key from one of the following options:
   - Type a passphrase into the Passphrase and Confirm fields.
   - Click **Choose File** and select an encryption key file.
5. Click **Encrypt**.

Next steps
You can change the disk encryption key by returning to the Disks page and clicking **Configure** and then **Change Disk Encryption Key**.

Format the packet capture disk
You can format an encrypted packet capture disk to permanently remove all packet captures. Formatting an encrypted disk removes the encryption. If you want to format an unencrypted packet capture disk, you must remove the disk, and then enable the disk again.

Warning: This action cannot be reversed.

1. In the Appliance Settings section, click **Disks**.
2. On the Disks page, choose one of the following options based on your appliance platform.
   - For virtual sensors, click **Configure** in the Actions column of the row for the packet capture disk.
   - For physical sensors, click **Configure** next to SSD Assisted Packet Capture.
3. Click **Clear Disk Encryption**.
4. Click **Format**.

Remove the packet capture disk
If you want to replace a packet capture disk, you must first remove the disk from the system. When a packet capture disk is removed from the system, all of the data on the disk is permanently deleted.

Removing the disk requires selecting a format option. On physical appliances, you can safely remove the disk from the appliance after this procedure is complete.

1. In the Appliance Settings section, click **Disks**.
2. On the Disks page, choose one of the following options based on your appliance platform.
   - For virtual appliances, click **Configure** next to Triggered Packet Capture.
   - For physical devices, click **Configure** next to SSD Assisted Packet Capture.
3. Click **Remove Disk**.
4. Select one of the following format options:
   - **Quick Format**
   - **Secure Erase**
5. Click **Remove**.

Configure a global packet capture
A global packet capture collects every packet that is sent to the ExtraHop system for the duration that matches the criteria.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Packet Captures section, click **Global Packet Capture**.

   When configuring packet captures, you only need to specify the criteria you want for the packet capture.
3. In the Name field, type a name to identify the packet capture.
4. In the Max Packets field, type the maximum number of packets to capture.
5. In the Max Bytes field, type the maximum number of bytes to capture.
6. In the Max Duration (milliseconds) field, type the maximum duration of the packet capture in milliseconds.

   ExtraHop recommends the default value of 1000 (1 second). The maximum value is up to 60000 milliseconds (1 minute).
7. In the Snaplen field, type the maximum number of bytes copied per frame.

   The default value is 96 bytes, but you can set this value to a number between 1 and 65535.
8. Click **Start**.

   Tip: Make a note of the time you start the capture to make it easier to locate the packets.
9. Click **Stop** to stop the packet capture before any of the maximum limits are reached.

Download your packet capture.

- On RevealX Enterprise systems, click **Packets** from the top menu and then click **Download PCAP**.

  To help locate your packet capture, click and drag on the Packet Query timeline to select the time range when you started the packet capture.
- On ExtraHop Performance systems, click the System Settings icon, click **All Administration**, and then click **View and Download Packet Captures** in the Packet Capture section.

Configure a precision packet capture
Precision packet captures require ExtraHop Triggers, which enable you to capture only the packets that meet your specifications. Triggers are highly customizable user-defined code that run upon defined system events.

Before you begin
Packet capture must be licensed and enabled on your ExtraHop system.

It is recommended that you have familiarity with writing triggers before configuring a precision packet capture. Here are some resources to help you learn about ExtraHop Triggers:

- Trigger concepts
- Build a trigger
- Trigger API Reference
- Walkthough: Initiate precision packet captures to analyze zero window conditions

In the following example, the trigger captures an HTTP flow with the name `HTTP host <hostname>` and stops the capture after a maximum of 10 packets are collected.

1. Click the System Settings icon and then click **Triggers**.
2. Click **Create**.
3. Type a name for the trigger and select the HTTP_REQUEST and HTTP_RESPONSE events.
4. Type or paste the following trigger code in the right pane.

```
Flow.captureStart("HTTP host " + HTTP.host, {maxPackets: 10});
```

5. Assign the trigger to a device or group of devices.

Warning: Running triggers on unnecessary devices and networks exhausts system resources. Minimize performance impact by assigning a trigger only to the specific sources that you need to collect data from.

6. Select **Enable trigger**.
7. Click **Save**.

Next steps
Download the packet capture file.

- On RevealX Enterprise systems, click **Records** from the top menu. Select **Packet Capture** from the Record Type drop-down menu. After the records associated with your packet capture appear, click the Packets icon, and then click **Download PCAP**.
- On ExtraHop Performance systems, click the System Settings icon, click **All Administration**, and then click **View and Download Packet Captures** in the Packet Capture section.

View and download packet captures
If you have packet captures stored on a virtual disk or on an SSD disk in your sensor, you can manage those files from the View Packet Captures page in the Administration settings. For RevealX systems and on ExtraHop packetstores, view the Packets page.

The View and Download Packet Captures section only appears on ExtraHop Performance systems. On RevealX systems, precision packet capture files are found by searching Records for the packet capture record type.

- Click **Configure packet capture settings** to automatically delete stored packet captures after the specified duration (in minutes).
- View statistics about your packet capture disk.
- Specify criteria to filter packet captures and limit the number of files displayed in the Packet Capture List.
- Select a file from the Packet Capture list and then download or delete the file.

Note: You cannot delete individual packet capture files from RevealX systems.

Infrastructure security

Always place management interfaces on secure internal networks, not untrusted networks including the public internet.

We recommend the following best practices:

- Be sure to restrict outbound connectivity to the ExtraHop Cloud Services IP addresses for the specific region assigned for your organization, and only allow access to those IP addresses over HTTPS (TCP 443). If you are connecting to ExtraHop Cloud Services through an explicit proxy, you can monitor traffic sent to the licensing server.
- Configure your management interface and restrict network access as much as possible.
- Disable SSH access from the Services pages in the Administration settings.

Ensure that ExtraHop consoles are connected to sensors over HTTPS on port 443.

Identity and access management

Configure best practices for users who have access to the ExtraHop system.

Authentication

We recommend that you disable default accounts or have complex passwords only for administrator or emergency access, and enforce SSO rules and LDAP groups for all other users.

Configure sensors with an identity provider that has strong authentication features such as two-factor or multi-factor authentication.

You can configure secure remote authentication for users through the following methods:

- SSO SAML
- LDAP

You can also configure stricter password policies through a global policy setting.

User sessions

There are a number of Running Configuration options that you can configure around session expiration.

Session Expiration Configuration

Configure the length of time a local user can stay logged in to the ExtraHop system by adding the `session` section to the Running Configuration file.

- The lifetime is in seconds. The default is `1209600` (2 weeks).
- Lifetimes less than `3600` (1 hour) are automatically set to `3600`.
- The session can be configured for up to twice the configured lifetime.

```
"session": {
    "lifetime": 654321
}
```

Remote Auth Session Expiration

Configure the length of time a remote authentication user can stay logged in to the ExtraHop system, in seconds. The default value is `43200` (12 hours); minimum is `3600` (1 hour), maximum is `86400` (1 day).

```
"session": {
    "remote_lifetime": 4800
}
```

Idle-Based Session Expiration

Configure the length of time a user can be logged in and idle, represented by an integer value in seconds. When the time expires, the user is logged out. When `idle_lifetime` is not set, the default value is `-1`, which indicates no idle timeout and is insecure.

We recommend that you set this value to `900` seconds or less.

```
"session": {
    "idle_lifetime": 900
}
```

API keys

API keys are powerful and never expire, which can create a security risk. We recommend that you deny API key generation for users, and limit access to administrators.

Access control

Privileges should be assigned with the minimal access needs of each user. Note that users with administrative privileges have the ability to reconfigure the system to no longer comply with the recommendations in this guide.

Users must be assigned privileges before they can access the E+xtraHop system.

Auditing

The AU–11 guidelines require that data is retained for 12 months of active storage and 18 months of cold storage.

The ExtraHop system can be configured to send audit log data and system notifications to a remote syslog server, as well as export API interactions for the Machine Learning service. We recommend that you configure an external storage that enables you to retain data for the required times.