ExtraHop 9.4
Admin UI Guide

© 2024ExtraHop Networks, Inc. All rights reserved.

This manual in whole or in part, may not be reproduced, translated, or reduced to any machine-readable form without prior written approval from ExtraHop Networks, Inc.

For more documentation, see https://docs.extrahop.com.

Published: 2024-05-08

ExtraHop Networks
Seattle, WA 98101
877-333-9872 (US)
+44 (0)203 7016850 (EMEA)
+65-31585513 (APAC)
www.extrahop.com

Contents

Introduction to the ExtraHop Admin UI 8
Supported browsers 8

Status and Diagnostics 9
Health 9
Audit Log 10
Send audit log data to a remote syslog server 11
Audit log events 12
Fingerprint 16
Exception Files 16
Support Scripts 16
Run the default support script 16
Run a custom support script 17

Network Settings 18
Connect to ExtraHop Cloud Services 18
Configure your firewall rules 19
Connect to ExtraHop Cloud Services through a proxy 19
Bypass certificate validation 20
Connectivity 20
Configure an interface 21
Interface throughput 22
Set a static route 23
Enable IPv6 for an interface 23
Global proxy server 24
ExtraHop Cloud proxy 24
Bond interfaces 24
Create a bond interface 24
Modify bond interface settings 25
Destroy a bond interface 25
Netskope settings 26
Flow Networks 26
Collect traffic from NetFlow and sFlow devices 26
Configure the interface on your ExtraHop system 27
Configure the flow type and the UDP port 27
Add the pending flow networks 27
View configured flow networks 28
Configure Cisco NetFlow devices 28
Configure an exporter on the Cisco Nexus switch 28
Configure Cisco switches through the Cisco IOS CLI 29
Set up shared SNMP credentials for your NetFlow or sFlow networks 30
Manually refresh SNMP information 30
Notifications 30
Configure email settings for notifications 31
Configure an email notification group 31
Configure settings to send notifications to an SNMP manager 32
Download the ExtraHop SNMP MIB 32
Extract the ExtraHop vendor object OID 33
Send system notifications to a remote syslog server 33
SSL Certificate 34

Upload an SSL certificate 34
Generate a self-signed certificate 35
Create a certificate signing request from your ExtraHop system 35
Trusted Certificates 36
Add a trusted certificate to your ExtraHop system 36

Access Settings 37

Global Policies 37
Passwords 37
Change the default password for the setup user 37
Support Access 38
Generate SSH key 38
Regenerate or revoke the SSH key 38
Users 38
Users and user groups 38
Local users 38
Remote Authentication 39
Remote users 39
User groups 39
User privileges 40
Add a local user account 45
Add an account for a remote user 45
Sessions 46
Remote Authentication 46
Configure remote authentication through LDAP 46
Configure user privileges for remote authentication 48
Configure remote authentication through SAML 49
Configure SAML single sign-on with Okta 52
Enable SAML on the ExtraHop system 52
Configure SAML settings in Okta 52
Assign the ExtraHop system to Okta groups 55
Add identity provider information on the ExtraHop system 55
Log in to the ExtraHop system 57
Configure SAML single sign-on with Google 57
Enable SAML on the ExtraHop system 57
Add user custom attributes 57
Add identity provider information from Google to the ExtraHop system 58
Add ExtraHop service provider information to Google 60
Assign user privileges 61
Log in to the ExtraHop system 62
Configure remote authentication through RADIUS 62
Configure remote authentication through TACACS+ 63
Configure the TACACS+ server 64
API Access 66
Manage API key access 67
Configure cross-origin resource sharing (CORS) 67
Generate an API key 67
Privilege levels 67

System Configuration 71

Capture 71
Exclude protocol modules 71
Exclude MAC addresses 72
Exclude an IP address or range 72
Exclude a port 72

Filtering and deduplication 72
Protocol classification 73
Add a custom protocol classification 77
Configure Device Discovery 78
Discover local devices 78
Discover remote devices by IP address 79
Discover VPN clients 79
SSL decryption 80
Upload a PEM certificate and RSA private key 80
Upload a PKCS#12/PFX file 80
Add encrypted protocols 81
Add a global port to protocol mapping 81
Install the ExtraHop session key forwarder on a Windows server 82
Install the ExtraHop session key forwarder on a Linux server 92
Supported SSL/TLS cipher suites 103
Store SSL session keys on connected packetstores 106
View connected session key forwarders 106
Decrypt domain traffic with a Windows domain controller 106
Connect a domain controller to a sensor 107
Connect a domain controller to a Reveal(x) 360 sensor 107
Validate the configuration settings 108
Import external data to your ExtraHop system 109
Enable the Open Data Context API 109
Write a Python script to import external data 109
Write a trigger to access imported data 110
Open Data Context API example 111
Install the packet forwarder on a Linux server 113
Download and install on RPM-based systems 113
Download and install on other Linux systems 113
Download and install on Debian-based systems 114
Install the packet forwarder on a Windows server 114
Monitoring multiple interfaces on a Linux server 117
Monitoring multiple interfaces on a Windows server 118
Enable network overlay decapsulation 119
Enable GRE or NVGRE decapsulation 119
Enable VXLAN decapsulation 120
Enable GENEVE decapsulation 120
Analyze a packet capture file 120
Set the offline capture mode 120
Datastore 121
Local and extended datastores 121
Calculate the size needed for your extended datastore 122
Configure an extended CIFS or NFS datastore 123
Add a CIFS mount 123
(Optional) Configure Kerberos for NFS 123
Add an NFS mount 124
Specify a mount as an active extended datastore 124
Archive an extended datastore for read-only access 125
Connect your ExtraHop system to the archived datastore 125
Import metrics from an extended datastore 126
Reset the local datastore and remove all device metrics from the ExtraHop system 126
Troubleshoot issues with the extended datastore 127
Device name precedence 128
Inactive sources 128
Detection Tracking 129

Configure endpoint lookup links 129
Geomap Data Source 130
Change the GeoIP database 130
Override an IP location 131
Open Data Streams 131
Configure an HTTP target for an open data stream 132
Configure a Kafka target for an open data stream 133
Configure a MongoDB target for an open data stream 135
Configure a raw data target for an open data stream 135
Configure a syslog target for an open data stream 136
ODS Details 137
Trends 138
Back up and restore a sensor or console 138
Back up a Sensor or ECA VM 138
Restore a sensor or console from a system backup 139
Restore a sensor or console from a backup file 140
Transfer settings to a new console or sensor 141
Reconnect sensors to the console 142

Appliance Settings 143

Running Config 143
Save system settings to the running configuration file 143
Edit the running config 144
Download the running configuration as a text file 144
Disable ICMPv6 Destination Unreachable messages 144
Disable specific ICMPv6 Echo Reply messages 144
Services 145
SNMP Service 145
Configure the SNMPv1 and SNMPv2 service 145
Configure the SNMPv3 service 146
Firmware 146
Upgrade the firmware on your ExtraHop system 146
Pre-upgrade checklist 147
Upgrade the firmware on a console and sensor 148
Upgrade the firmware on recordstores 148
Upgrade the firmware on packetstores 148
Upgrade connected sensors in Reveal(x) 360 149
System Time 149
Configure the system time 151
Shutdown or Restart 151
Sensor Migration 151
Migrate an ExtraHop sensor 152
Prepare the source and target sensors 153
Start the migration 154
Configure the target sensor 155
License 155
Register your ExtraHop system 155
Register the appliance 156
Troubleshoot license server connectivity 156
Apply an updated license 157
Update a license 157
Disks 158
Replace a RAID 0 disk 158
Install a new packet capture disk 159
Console Nickname 161

Configure packet capture 162
Packet slicing 162
Enable packet capture 162
Encrypt the packet capture disk 162
Format the packet capture disk 163
Remove the packet capture disk 163
Configure a global packet capture 164
Configure a precision packet capture 164
View and download packet captures 165

Recordstore 166
Send records from ExtraHop to Google BigQuery 166
Send records from ExtraHop to BigQuery 166
Transfer recordstore settings 167
Send records from ExtraHop to Splunk 167
Send records from ExtraHop to Splunk 168
Transfer recordstore settings 168

ExtraHop Command Settings 170
Generate Token 170
Connect to a console from a sensor 170
Connect an ExtraHop console to an ExtraHop sensor 171
Generate a token on the sensor 171
Connect the console and sensors 171
Manage Discover Appliances 171

ExtraHop Recordstore Settings 173
Connect the console and sensors to ExtraHop recordstores 173
Disconnect the recordstore 174
Manage Explore Appliances 175
Collect flow records 175
ExtraHop Recordstore Status 176

ExtraHop Packetstore Settings 177
Connect sensors and console to the packetstore 177
Manage Trace Appliances 178

Appendix 179
Common acronyms 179
Configure Cisco NetFlow devices 180
Configure an exporter on Cisco Nexus switch 180
Configure Cisco switches through Cisco IOS CLI 181

Introduction to the ExtraHop Admin UI

The Admin UI Guide provides detailed information about the administrator features and functionality of ExtraHop sensors and consoles. This guide provides an overview of the global navigation and information about the controls, fields, and options available throughout the UI.

After you have deployed your sensor or console, see the Sensor and console post-deployment checklist.

We value your feedback. Please let us know how we can improve this document. Send your comments or suggestions to documentation@extrahop.com.

Supported browsers

The following browsers are compatible with all ExtraHop systems. Apply the accessibility and compatibility features provided by your browser to access content through assistive technology tools.

- Firefox
- Google Chrome
- Microsoft Edge
- Safari

Important: Internet Explorer 11 is no longer supported. We recommend that you install the latest version of any supported browser.

Status and Diagnostics

The Status and Diagnostics section provides metrics about the overall health of your ExtraHop system.

Health

The Health page provides a collection of metrics that helps you to monitor the operation of your ExtraHop system and enables ExtraHop Support to troubleshoot system errors if necessary.

System

Reports the following information about the system CPU usage and hard disk.

CPU User

The percentage of CPU usage associated with the ExtraHop system user.

CPU System

The percentage of CPU usage associated with the ExtraHop system.

CPU Idle

The CPU Idle percentage associated with the ExtraHop system.

CPU IO

The percentage of CPU usage associated with the ExtraHop system IO functions.

Bridge Status

Reports the following information about the ExtraHop system bridge component.

VM RSS

The bridge process physical memory in use.

VM Data

The bridge process heap virtual memory in use.

VM Size

The bridge process total virtual memory in use.

Start Time

Specifies the start time for the ExtraHop system bridge component.

Capture Status

Reports the following information about the ExtraHop system network capture status.

VM RSS

The network capture process physical memory in use.

VM Data

The network capture process heap virtual memory in use.

VM Size

The network capture process total virtual memory in use.

Start Time

The start time for the ExtraHop network capture.

Service Status

Reports the status of ExtraHop system services.

exalerts

The amount of time the ExtraHop system alert service has been running.

extrend
The amount of time the ExtraHop system trend service has been running.

exconfig
The amount of time the ExtraHop system config service has been running.

exportal
The amount of time the ExtraHop system web portal service has been running.

exshell
The amount of time the ExtraHop system shell service has been running.

Interfaces
Reports the status of ExtraHop system interfaces.

RX packets
The number of packets received by the specified interface on the ExtraHop system.

RX Errors
The number of received packet errors on the specified interface.

RX Drops
The number of received packets dropped by the specified interface.

TX Packets
The number of packets transmitted by the specified interface on the ExtraHop system.

TX Errors
The number of transmitted packet errors on the specified interface.

TX Drops
The number of transmitted packets dropped by the specified interface.

RX Bytes
The number of bytes received by the specified interface on the ExtraHop system.

TX Bytes
The number of bytes transmitted by the specified interface on the ExtraHop system.

Partitions
Reports the memory that has been allocated to system components for the ExtraHop system.

Name
The system components that have a memory partition in NVRAM.

Options
The read-write options for the system components.

Size
The partition size in gigabytes that is allocated for the system component.

Utilization
The amount of memory that is currently consumed by the system components, as a quantity and as a percentage of the total partition.

Audit Log

The audit log provides data about the operations of your ExtraHop system, broken down by component. The audit log lists all known events by timestamp, in reverse chronological order.

If you experience an issue with the ExtraHop system, consult the audit log to view detailed diagnostic data to determine what might have caused the issue.

Send audit log data to a remote syslog server

The audit log collects data about ExtraHop system operations, broken down by component. The log stored on the system has a capacity of 10,000 entries, and entries older than 90 days are automatically removed. You can view these entries in the Administration settings, or you can send the audit log events to a syslog server for long-term storage, monitoring, and advanced analysis. All logged events are listed in the table below.

The following steps show you how to configure the ExtraHop system to send audit log data to a remote syslog server.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Status and Diagnostics section, click **Audit Log**.
3. Click **Configure Syslog Settings**.
4. In the Destination field, type the IP address of the remote syslog server.
5. From the Protocol drop-down menu, select **TCP** or **UDP**. This option specifies the protocol over which the information is sent to your remote syslog server.
6. In the Port field, type the port number for your remote syslog server. By default, this value is set to 514.
7. Click **Test Settings** to verify that your syslog settings are correct. If the settings are correct, you should see an entry in the syslog log file on the syslog server similar to the following:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```

8. Click **Save**.
9. (Optional) Modify the format of syslog messages.

   By default, syslog messages are not compliant with RFC 3164 or RFC 5424. However, you can format syslog messages to be compliant by modifying the running config.

   a) Click **Admin**.
   b) Click **Running Config (Unsaved Changes)**.
   c) Click **Edit Config**.
   d) Add an entry under `auditlog_rsyslog` where the key is `rfc_compliant_format` and the value is either `rfc5424` or `rfc3164`.

      The `auditlog_rsyslog` section should look similar to the following code:

      ```
      "auditlog_rsyslog": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```

   e) Click **Update**.
   f) Click **Done**.

10. (Optional) Modify the timezone referenced in syslog timestamps.

    By default, syslog timestamps reference UTC time. However, you can modify timestamps to reference the ExtraHop system time by modifying the running config.

    a) Click **Admin**.
    b) Click **Running Config (Unsaved Changes)**.
    c) Click **Edit Config**.
    d) Add an entry under `auditlog_rsyslog` where the key is `syslog_use_localtime` and the value is `true`.

The `auditlog_rsyslog` section should look similar to the following code:

```
    "auditlog_rsyslog": {
        "syslog_destination": "192.168.0.0",
        "syslog_ipproto": "udp",
        "syslog_port": 514,
        "syslog_use_localtime": true
    }
```

e) Click **Update**.
f) Click **Done**.

Next steps
After you confirm that your new settings are working as expected, preserve your configuration changes by saving the running configuration file.

Audit log events
The following events on an ExtraHop system generate an entry in the audit log.

Category	Event
Agreements	• A EULA or POC agreement is agreed to
API	• An API key is created • An API key is deleted • A user is created. • A user is modified.
Sensor Migration	• A sensor migration is started • A sensor migration succeeded • A sensor migration failed
Browser sessions	• A specific browser session is deleted • All browser sessions are deleted
Cloud Services	• Status of a connected sensor is retrieved
Console	• A sensor connects to a console • A sensor disconnects from a console • An ExtraHop recordstore or packetstore establishes a tunneled connection to a console • Console information is set • A console nickname is set • Enable or disable a sensor • The sensor is remotely viewed • A license for a sensor is checked by a console • A license for a sensor is set by a console
Dashboards	• A dashboard is created • A dashboard is renamed • A dashboard is deleted • A dashboard permalink, also known as a short code, is modified • Dashboard sharing options are modified

Category	Event
Datastore	• The extended datastore configuration is modified • The datastore is reset • A datastore reset completed • Customizations are saved • Customizations are restored • Customizations are deleted
Detections	• A detection status is updated • A detection assignee is updated • Detection notes are updated • An external ticket is updated • A tuning rule is created • A tuning rule is deleted • A tuning rule is modified • A tuning rule description is updated • A tuning rule is enabled • A tuning rule is disabled • A tuning rule is extended
Exception files	• An exception file is deleted
ExtraHop recordstore records	• All ExtraHop recordstore records are deleted
ExtraHop recordstore cluster	• A new ExtraHop recordstore node is initialized • A node is added to an ExtraHop recordstore cluster • A node is removed from an ExtraHop recordstore cluster • A node joins an ExtraHop recordstore cluster • A node leaves an ExtraHop recordstore cluster • A sensor or console is connected to an ExtraHop recordstore • A sensor or console is disconnected from an ExtraHop recordstore • An ExtraHop recordstore node is removed or missing, but not through a supported interface
ExtraHop Update Service	• A detection category is updated • A detection definition is updated • A detection trigger is updated • A ransomware definition is updated • Detection metadata is updated • Expanded detection content is updated
Firmware	• Firmware is upgraded
Global Policies	• Global policy for device group edit control is updated

Category	Event
Integrations	• An integration is updated
License	• A new static license is applied • License server connectivity is tested • A product key is registered with the license server • A new license is applied
Login to the ExtraHop system	• A login succeeds • A login fails
Login from SSH or REST API	• A login succeeds • A login fails
Modules	• NDR module access control is enabled • NPM module access control is enabled
Network	• A network interface configuration is edited • The hostname or DNS setting is changed • A network interface route is changed
Offline capture	• An offline capture file is loaded
PCAP	• A packet capture (PCAP) file is downloaded
Remote Access	• Remote access for ExtraHop Support Team is enabled • Remote access for ExtraHop Support Team is disabled • Remote access for ExtraHop Atlas Analysts is enabled • Remote access for ExtraHop Atlas Analysts is disabled • Remote access for ExtraHop Support is enabled • Remote access for ExtraHop Support is disabled
RPCAP	• An RPCAP configuration is added • An RPCAP configuration is deleted
Running Config	• The running configuration file changes
SAML Identity Provider	• An identity provider is added • An identity provider is modified • An identity provider is deleted
SAML login	• A login succeeds • A login fails
SAML privileges	• A privilege level is granted

Category	Event
	• A privilege level is denied
SSL decryption	• An SSL decryption key is saved
SSL session keys	• A PCAP session key is downloaded
Support account	• The support account is disabled • The support account is enabled • The support SSH key is regenerated
Support Script	• A default support script is running • A past support script result is deleted • A support script is uploaded
Syslog	• Remote syslog settings are updated
System and service status	• The system starts up • The system shuts down • The system is restarted • The bridge, capture, or portal process is restarted • A system service is enabled (such as SNMP, web shell, management, SSH) • A system service is disabled (such as SNMP, web shell, /management, SSH)
System time	• The system time is set • The system time is changed • The system time is set backwards • NTP servers are set • The time zone is set • A manual NTP synchronization is requested
System user	• A user is added • User metadata is edited • A user is deleted • A user password is set • A user other than the `setup` user attempts to modify the password of another user • A user password is updated
Threat briefings	• A threat briefing is archived • A threat briefing is restored
ExtraHop packetstore	• A new ExtraHop packetstore is initialized • A sensor or console is connected to an ExtraHop packetstore • A sensor or console is disconnected from an ExtraHop packetstore • An ExtraHop packetstore is reset

Category	Event
Trends	• A trend is reset
Triggers	• A trigger is added • A trigger is edited • A trigger is deleted
User Groups	• A local user group is created • A local user group is deleted • A local user group is enabled • A local user group is disabled

Fingerprint

Fingerprints help secure appliances from machine-in-the-middle attacks by providing a unique identifier that can be verified when connecting ExtraHop appliances.

When connecting an Explore or Trace appliance with a Discover appliance or Command appliance, make sure that the fingerprint displayed is exactly the same as the fingerprint shown on the join or pairing page.

If the fingerprints do not match, communications between the devices might have been intercepted and altered.

Exception Files

Exception files are a core file of the data stored in memory. When you enable the Exception File setting, the core file is written to the disk if the system unexpectedly stops or restarts. This file can help ExtraHop Support diagnose the issue.

- Click **Enable Exception Files** or **Disable Exception Files** to enable or disable the saving of exception files.

Support Scripts

ExtraHop Support might provide a support script that can apply a special setting, make a small adjustment to the ExtraHop system, or provide help with remote support or enhanced settings. The Administration settings enable you to upload and run support scripts.

Run the default support script

The default support script gathers information about the state of the ExtraHop system for analysis by ExtraHop Support.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Status and Diagnostics section, click **Support Scripts**.
3. Click **Run Default Support Script**.
4. Click **Run**.
   When the script completes, the Support Script Results page appears.
5. Click the name of the diagnostic support package that you want to download. The file saves to the default download location on your computer.
   Send this file, typically named `diag-results-complete.expk`, to ExtraHop Support.

The `.expk` file is encrypted and the contents are only viewable by ExtraHop Support. However, you can download the `diag-results-complete.manifest` file to view a list of the files collected.

Run a custom support script

If you receive a custom support script from ExtraHop Support complete the following procedure to make a small adjustment to the system or apply enhanced settings.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Status and Diagnostics section, click **Support Scripts**.
3. Click **Run Custom Support Script**.
4. Click **Choose File**, navigate to the diagnostic support script you want to upload, and then click **Open**.
5. Click **Upload** to run the file on the ExtraHop system.
   ExtraHop Support will confirm that the support script achieved the desired results.

Network Settings

The Network Settings section provides configuration settings for your ExtraHop system. These settings enable you to set a hostname, configure notifications, and manage connections to your system.

Connect to ExtraHop Cloud Services

ExtraHop Cloud Services provides access to ExtraHop cloud-based services through an encrypted connection. The services you are connected to are determined by your system license.

After the connection is established, information about the available services appear on the ExtraHop Cloud Services page.

- ExtraHop Machine Learning Service enables detections for your ExtraHop system. In Reveal(x) Enterprise, you can enable security-only or security and performance detections.
- Reveal(x) Enterprise users can send data to the Machine Learning Service by enabling ExtraHop Cloud Services in the Administration settings. For example, the system can send external plaintext IP addresses, domain names, and hostnames that are associated with detected suspicious behavior. This setting is enabled in Reveal(x)360 by default and can not be disabled. See the Collective Threat Analysis FAQ for more information. For a full list of data types sent to the ExtraHop Machine Learning Service, and to see how the data is applied to improve threat detection, see the Machine Learning section of the ExtraHop Security, Privacy and Trust Overview.
- ExtraHop Update Service enables automatic updates of resources to the ExtraHop system, such as ransomware packages.
- ExtraHop Remote Access enables you to allow ExtraHop account team members, ExtraHop Atlas analysts, and ExtraHop Support to connect to your ExtraHop system for configuration help. If you have signed up for the Atlas Remote Analysis service, ExtraHop analysts can perform an unbiased analysis of your network data and report on areas in your IT infrastructure where improvements can be made. See the Remote Access FAQ for more information about remote access users.

Before you begin

- Reveal(x) 360 systems are automatically connected to ExtraHop Cloud Services, however, you might need to allow access through network firewalls.
- You must apply the relevant license on the ExtraHop system before you can connect to ExtraHop Cloud Services. See the License FAQ for more information.
- You must have setup or system and access administration privileges to access Administration settings.

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 **ExtraHop Cloud Services**.
3. Click **Terms and Conditions** to read the content.
4. Read the terms and conditions, and then select the checkbox.
5. Click **Connect to ExtraHop Cloud Services**.

   After you are connected, the page updates to show status and connection information for each service.
6. (Optional) In the Machine Learning Service section, select the checkbox for **Contribute to the Machine Learning Service for collective threat analysis** and then select one of the following options:
   - External IP addresses
   - External IP addresses, domains, and hostnames

If the connection fails, there might be an issue with your firewall rules.

Configure your firewall rules

If your ExtraHop system is deployed in an environment with a firewall, you must open access to ExtraHop Cloud Services. For Reveal(x) 360 systems that are connected to self-managed sensors, you must also open access to the ExtraHop Cloud Recordstore.

Open access to Cloud Services

For access to ExtraHop Cloud Services, your sensors must be able to resolve DNS queries for *.extrahop.com and access TCP 443 (HTTPS) from the IP address that corresponds to your sensor license:

- 35.161.154.247 (Portland, U.S.A.)
- 54.66.242.25 (Sydney, Australia)
- 52.59.110.168 (Frankfurt, Germany)

Open access to Cloud Recordstore

For access to the ExtraHop Cloud Recordstore, your sensors must be able to access outbound TCP 443 (HTTPS) to these fully-qualified domain names:

- `bigquery.googleapis.com`
- `bigquerystorage.googleapis.com`
- `oauth2.googleapis.com`
- `www.googleapis.com`
- `www.mtls.googleapis.com`
- `iamcredentials.googleapis.com`

You can also review the public guidance from Google about computing possible IP address ranges for googleapis.com.

In addition to configuring access to these domains, you must also configure the global proxy server settings.

Connect to ExtraHop Cloud Services through a proxy

If you do not have a direct internet connection, you can try connecting to ExtraHop Cloud Services through an explicit proxy.

Before you begin
Verify whether your proxy vendor is configured to perform machine-in-the-middle (MITM) when tunneling SSH over HTTP CONNECT to localhost:22. ExtraHop Cloud Services deploys an encrypted inner SSH tunnel, so traffic will not be visible to MITM inspection. We recommend that you create a security exception and disable MITM inspection for this traffic.

> **Important:** If you are unable to disable MITM on your proxy, you must disable certificate validation in the ExtraHop system running configuration file. For more information, see Bypass certificate validation.

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 **Connectivity**.
3. Click **Enable ExtraHop Cloud Proxy**.
4. Type the hostname for your proxy server, such as `proxyhost`.
5. Type the port for your proxy server, such as `8080`.
6. (Optional) If required, type a user name and password for your proxy server.
7. Click **Save**.

Bypass certificate validation

Some environments are configured so that encrypted traffic cannot leave the network without inspection by a third-party device. This device can act as an SSL/TLS endpoint that decrypts and re-encrypts the traffic before sending the packets to ExtraHop Cloud Services.

If an appliance is connecting to ExtraHop Cloud Services through a proxy server and the certificate validation fails, disable certificate validation and attempt the connection again. The security provided by ExtraHop system authentication and encryption ensures that communication between appliances and ExtraHop Cloud services cannot be intercepted.

Note: The following procedure requires familiarity with modifying the ExtraHop running configuration file.

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 **Running Config**.
3. Click **Edit config**.
4. Add the following line to the end of the running configuration file:

```
"hopcloud": { "verify_outer_tunnel_cert": false }
```

5. Click **Update**.
6. Click **View and Save Changes**.
7. Review the changes and click **Save**.
8. Click **Done**.

Connectivity

The Connectivity page contains controls for your appliance connections and network settings.

Interface Status

On physical appliances, a diagram of interface connections appears, which updates dynamically based on the port status.

- The blue Ethernet port is for management
- A black Ethernet port indicates a licensed and enabled port that is currently down
- A green Ethernet port indicates an active, connected port
- A gray Ethernet port indicates a disabled or unlicensed port

Network Settings

- Click **Change Settings** to add a hostname for your ExtraHop appliance or to add DNS servers.

Proxy Settings

- Enable a global proxy to connect to an ExtraHop Command appliance
- Enable a cloud proxy to connect to ExtraHop Cloud Services

Bond Interface Settings

- Create a bond interface to bond multiple interfaces together into one logical interface with a single IP address.

Interfaces

View and configure your management and monitoring interfaces. Click any interface to display setting options.

- Collect traffic from NetFlow and sFlow devices
- Packet Forwarding with RPCAP

Netskope Settings

- Enable Netskope packet ingest on your sensor to discover and monitor devices through a Netskope integration.

Configure an interface

1. In the Network Settings section, click **Connectivity**.
2. In the Interfaces section, click the name of the interface you want to configure.
3. On the Network Settings for Interface *<interface number>* page, select one of the following options from the **Interface Mode** drop-down:

Option	Description
Disabled	The interface is disabled.
Monitoring (receive only)	Monitors network traffic.
Management	Manages the ExtraHop sensor.
Management + RPCAP/ERSPAN/VXLAN/ GENEVE Target	Manages the ExtraHop sensor and captures traffic forwarded from a packet forwarder, ERSPAN*, VXLAN**, or GENEVE***. While 10 GbE management + capture interfaces on this sensor can conduct management functions at 10 Gbps speeds, processing traffic such as ERSPAN, VXLAN, and GENEVE is limited to 1 Gbps. **Tip:** In environments with asymmetric routing adjacent to the high-performance interfaces, ping replies might not get back to the sender.
High-Performance ERSPAN/VXLAN/GENEVE Target	Captures traffic forwarded from ERSPAN*, VXLAN**, or GENEVE***. This interface mode enables the port to handle more than 1 Gbps. Set this interface mode if the ExtraHop sensor has a 10 GbE port. This interface mode only requires that you configure an IPv4 address.

*The ExtraHop system supports the following ERSPAN implementations:

- ERSPAN Type I
- ERSPAN Type II
- ERSPAN Type III
- Transparent Ethernet Bridging. ERSPAN-like encapsulation commonly found in virtual switch implementations such as the VMware VDS and Open vSwitch.

**Virtual Extensible LAN (VXLAN) packets are received on UDP port 4789.

***Generic Network Virtualization Encapsulation (GENEVE) packets are received on UDP port 6081. To configure GENEVE-encapsulated traffic forwarded from an AWS Gateway Load Balancer (GWLB) acting as a VPC Traffic Mirroring target, see the AWS documentation.

Note: For Amazon Web Services (AWS) deployments with one interface, you must select **Management + RPCAP/ERSPAN/VXLAN/GENEVE Target** for Interface 1. If you are configuring two interfaces, you must select **Management + RPCAP/ERSPAN/VXLAN/ GENEVE Target** for Interface 1 and **Management + RPCAP/ERSPAN/VXLAN/GENEVE Target** for Interface 2.

Note: For Azure deployments, some instances running older NICs might not support High-Performance ERSPAN/VXLAN/GENEVE Target mode.

4. (Optional) Select an interface speed. **Auto-negotiate** is selected by default, however, you should manually select a speed if it is supported on your sensor, network transceiver, and network switch.
   - **Auto-negotiate**
   - **10 Gbps**
   - **25 Gbps**
   - **40 Gbps**
   - **100 Gbps**

   Important: When you change the interface speed to **Auto-negotiate**, you might need to restart the sensor before the change takes effect.
5. (Optional) Select a forward error correction (FEC) type. We recommend Auto-negotiate, which is optimal for most environments.

   • **Auto-negotiate:** Automatically enables either RS-FEC or Firecode FEC or disables FEC based on the capabilities of connected interfaces.

   • **RS-FEC:** Always enables Reed-Solomon FEC.

   • **Firecode:** Always enables Firecode (FC) FEC, also known as BaseR FEC.

   • **Disabled:** Disables FEC.
6. DHCPv4 is enabled by default. If your network does not support DHCP, you can clear the DHCPv4 checkbox to disable DHCP and then type a static IP address, netmask, and default gateway.

   Note: Only one interface should be configured with a default gateway. Configure static routes if your network requires routing through multiple gateways.
7. Configure the TCP health check port. This setting is only configurable on high-performance interfaces and is required when ingesting GENEVE traffic from an AWS Gateway Load Balancer (GWLB). The port number value must match the value configured in AWS. For more information, see Forward GENEVE-encapsulated traffic from an AWS Gateway Load Balancer.
8. (Optional) Enable IPv6.

   For more information about configuring IPv6, see Enable IPv6 for an interface.
9. (Optional) Manually add routes.
10. Click **Save**.

Interface throughput
ExtraHop sensor models EDA 6100, EDA 8100 and EDA 9100 are optimized to capture traffic exclusively on 10GbE ports.

Enabling the 1GbE interfaces for monitoring traffic can impact performance, depending on the ExtraHop sensor. While you can optimize these sensors to capture traffic simultaneously on both the 10GbE ports and the three non-management 1GbE ports, we recommend that you contact ExtraHop Support for assistance to avoid reduced throughput.

Note: EDA 6200, EDA 8200, EDA 9200, and EDA 10200 sensors are not susceptible to reduced throughput if you enable 1GbE interfaces for monitoring traffic.

ExtraHop Sensor	Throughput	Details
EDA 9100	Standard 40Gbps throughput	If the non-management 1GbE interfaces are disabled, you can use up to four of the 10GbE interfaces for a combined throughput of up to 40Gbps.

ExtraHop Sensor	Throughput	Details
EDA 8100	Standard 20Gbps throughput	If the non-management 1GbE interfaces are disabled, you can use either one or both of the 10GbE interfaces for a combined throughput of up to 20Gbps.
EDA 6100	Standard 10Gbps throughput	If the non-management 1GbE interfaces are disabled, the maximum total combined throughput is 10Gbps.
EDA 3100	Standard 3Gbps throughput	No 10GbE interface
EDA 1100	Standard 1Gbps throughput	No 10GbE interface

Set a static route

Before you begin
You must disable DHCPv4 before you can add a static route.

1. On the Edit Interface page, ensure that the **IPv4 Address** and **Netmask** fields are complete and saved, and click **Edit Routes**.
2. In the Add Route section, type a network address range in CIDR notation in the **Network** field and IPv4 address in the **Via IP** field and then click **Add**.
3. Repeat the previous step for each route you want to add.
4. Click **Save**.

Enable IPv6 for an interface

1. In the Network Settings section, click **Connectivity**.
2. In the Interfaces section, click the name of the interface you want to configure.
3. On the Network Settings for Interface *<interface number>* page, select **Enable IPv6**.
   IPv6 configuration options appear below **Enable IPv6**.
4. (Optional) Configure IPv6 addresses for the interface.
   - To automatically assign IPv6 addresses through DHCPv6, select **Enable DHCPv6**.

     Note: If enabled, DHCPv6 will be used to configure DNS settings.
   - To automatically assign IPv6 addresses through stateless address autoconfiguration, select one of the following options from the Stateless Address Autoconfiguration list:

     Use MAC address

     Configures the appliance to automatically assign IPv6 addresses based on the MAC address of the appliance.

     Use stable private address

     Configures the appliance to automatically assign private IPv6 addresses that are not based on hardware addresses. This method is described in RFC 7217.
   - To manually assign one or more static IPv6 addresses, type the addresses in the Static IPv6 Addresses field.
5. To enable the appliance to configure Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) information according to router advertisements, select **RDNSS/DNSSL**.
6. Click **Save**.

Global proxy server

If your network topology requires a proxy server to enable your ExtraHop system to communicate either with a console or with other devices outside of the local network, you can enable your ExtraHop system to connect to a proxy server you already have on your network. Internet connectivity is not required for the global proxy server.

Note: Only one global proxy server can be configured per ExtraHop system.

Complete the following fields and click **Save** to enable a global proxy.

- **Hostname :** The hostname or IP address for your global proxy server.
- **Port :** The port number for your global proxy server.
- **Username :** The name of a user that has privileged access to your global proxy server.
- **Password :** The password for the user specified above.

ExtraHop Cloud proxy

If your ExtraHop system does not have a direct internet connection, you can connect to the internet through a proxy server specifically designated for ExtraHop Cloud services connectivity. Only one proxy can be configured per system.

Complete the following fields and click **Save** to enable a cloud proxy.

- **Hostname:** The hostname or IP address for your cloud proxy server.
- **Port:** The port number for your cloud proxy server.
- **Username:** The name of a user that has for access to your cloud proxy server.
- **Password:** The password for the user specified above.

Bond interfaces

You can bond multiple interfaces on your ExtraHop system together into a single logical interface that has one IP address for the combined bandwidth of the member interfaces. Bonding interfaces enable a larger throughput with a single IP address. This configuration is also known as link aggregation, port channeling, link bundling, Ethernet/network/NIC bonding, or NIC teaming. Bond interfaces cannot be set to monitoring mode.

Note: When you modify bond interface settings, you lose connectivity to your ExtraHop system. You must make changes to your network switch configuration to restore connectivity. The changes required are dependent on your switch. Contact ExtraHop Support for assistance before you create a bond interface.

- Bonding is only configurable on Management or Management + interfaces.
- Port channeling on traffic monitoring ports is supported on the ExtraHop sensors.

Interfaces chosen as members of a bond interface are no longer independently configurable and are shown as Disabled (bond member) in the Interfaces section of the Connectivity page. After a bond interface is created, you cannot add more members or delete existing members. The bond interface must be destroyed and recreated.

- Create a bond interface
- Modify a bond interface
- Destroy a bond interface

Create a bond interface

You can create a bond interface with at least one interface member and up to the number of members that are available for bonding.

1. Click **Create Bond Interface**.

2. Configure the following options:

   • **Members:** Select the checkbox next to each interface you want to include in the bonding. Only ports that are currently available for bond membership appear.

   • **Take Settings From:** Select the interface that has the settings you want to apply to the bond interface. Settings for all non-selected interfaces will be lost.

   • **Bond Type:** Specify whether to create a static bond or a dynamic bond through IEEE 802.3ad Link Aggregation (LACP).

   • **Hash Policy:** Specify the hash policy. The **Layer 3+4** policy balances the distribution of traffic more evenly across interfaces; however, this policy is not fully compliant with 802.3ad standards. The **Layer 2+3** policy balances traffic less evenly and is compliant with 802.3ad standards.
3. Click **Create**.

Refresh the page to display the Bond Interfaces section. Any bond interface member whose settings were not selected in the **Take Settings From** drop-down menu are shown as **Disabled (bond member)** in the Interfaces section.

Modify bond interface settings
After a bond interface is created, you can modify most settings as if the bond interface is a single interface.

1. In the Network Settings section, click **Connectivity**.
2. In the Bond Interfaces section, click the bond interface you want to modify.
3. On the Network Settings for Bond Interface <interface number> page, modify the following settings as needed:

   • **Members:** The interface members of the bond interface. Members cannot be changed after a bond interface is created. If you need to change the members, you must destroy and recreate the bond interface.

   • **Bond Mode:** Specify whether to create a static bond or a dynamic bond through IEEE 802.3ad Link Aggregation (LACP).

   • **Interface Mode:** The mode of the bond membership. A bond interface can be **Management** or **Management+RPCAP/ERSPAN Target** only.

   • **Enable DHCPv4**: If DHCP is enabled, an IP address for the bond interface is automatically obtained.

   • **Hash Policy:** Specify the hash policy. The **Layer 3+4** policy balances the distribution of traffic more evenly across interfaces; however, it is not fully compliant with 802.3ad standards. The **Layer 2+3** policy balances traffic less evenly; however, it is compliant with 802.3ad standards.

   • **IPv4 Address:** The static IP address of the bond interface. This setting is unavailable if DHCP is enabled.

   • **Netmask**: The network netmask for the bond interface.

   • **Gateway**: The IP address of the network gateway.

   • **Routes:** The static routes for the bond interface. This setting is unavailable if DHCP is enabled.

   • **Enable IPv6:** Enable configuration options for IPv6.
4. Click **Save**.

Destroy a bond interface
When a bond interface is destroyed, the separate interface members of the bond interface return to independent interface functionality. One member interface is selected to retain the interface settings for the bond interface and all other member interfaces are disabled. If no member interface is selected to retain the settings, the settings are lost and all member interfaces are disabled.

1. In the Network Settings section, click **Connectivity**.
2. In the Bond Interfaces section, click the red **X** next to the interface you want to destroy.

3. On the Destroy Bond Interface <interface number> page, select the member interface to move the bond interface settings to. Only the member interface selected to retain the bond interface settings remains active, and all other member interfaces are disabled.
4. Click **Destroy**.

Netskope settings

This integration enables you to configure ExtraHop sensors to ingest packets from your Netskope solution to detect threats, discover and monitor devices, and gain insight into traffic.

Before you begin

Important: The Reveal(x) integration with Netskope Intelligent Security Service Edge (SSE) is currently only available to Netskope Cloud TAP Early Access Program participants. If you would like to learn more about this integration and be notified as soon as it is publicly available, reach out to your ExtraHop account team.

- Your user account must have full write privileges or higher on Reveal(x) Enterprise or System and Access Administration privileges on Reveal(x) 360.
- Your Reveal(x) system must be connected to an ExtraHop sensor with firmware version 9.4 or later.
- Your ExtraHop sensor must be dedicated to ingesting Netskope packets only.
- You must configure at least one interface on your ExtraHop sensor; all interfaces must specify a mode that includes GENEVE encapsulation.
- You must configure TAP mode in your Netskope environment.

1. Log in to the Administration settings on the sensor through https://<extrahop-hostname-or-IP-address>/admin.
2. From the Network Settings section, click **Connectivity**.
3. From the Netskope Settings section, select **Enable Netskope packet ingest**.
4. Click **Save**.

Next steps

- From the Assets page, you can search for this sensor to view traffic and detections observed from the Netskope data.
- Log into Administration settings on the connected Reveal(x) Enterprise or Reveal(x) 360 console to check the status of sensors integrated with Netskope.

Flow Networks

You must configure network interface and port settings on the ExtraHop system before you can collect NetFlow or sFlow data from remote flow networks (flow exporters). Flow networks cannot be configured on Reveal(x) Enterprise systems. The ExtraHop system supports the following flow technologies: Cisco NetFlow Version 5 (v5) and Version 9 (v9), AppFlow, IPFIX, and sFlow.

In addition to configuring the ExtraHop system, you must configure your network devices to send sFlow or NetFlow traffic. Refer to your vendor documentation or see sample Cisco configurations in the appendix.

Collect traffic from NetFlow and sFlow devices

You must configure network interface and port settings on the ExtraHop system before you can collect NetFlow or sFlow data from remote flow networks (flow exporters). Flow networks cannot be configured on Reveal(x) Enterprise systems. The ExtraHop system supports the following flow technologies: Cisco NetFlow v5 and v9, AppFlow, IPFIX, and sFlow.

Note: For information on the EFC 1292v NetFlow sensor virtual appliance, see Deploy the ExtraHop EFC 1292v NetFlow Sensor.

You must log in as a user with System and Access Administration privileges to complete the following steps.

Configure the interface on your ExtraHop system

In addition to configuring the ExtraHop system, you must configure your network devices to send sFlow or NetFlow traffic. Refer to your vendor documentation or see the sample Cisco configurations at the end of this document. Note that Cisco ASA firewalls with NetFlow Secure Event Logging (NSEL) are not supported.

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 **Connectivity**.
3. In the Interfaces section, click the name of the interface that should receive the flow data.
4. From the Interface Mode drop-down list, select **Management + Flow Target**.

   Note: The EDA 1100v must be configured for either flow data or wire data because this sensor cannot process flow data and wire data simultaneously. If the sensor is configured for flow data, you must set the monitoring port to **Disabled**.
5. If Enable DHCPv4 is selected, click **Save**.

   Otherwise, configure the remaining network settings and then click **Save**.

Configure the flow type and the UDP port

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. In the Network Settings section, click **Flow Networks**.
3. In the Ports section, from the Port field, type the UDP port number.

   The default port for Net Flow is `2055`, and the default port for sFlow is `6343`. You can add additional ports as needed for your environment.

   Note: Port numbers must be 1024 or greater
4. From the Flow Type drop-down menu, select **NetFlow** or **sFlow**.

   For AppFlow traffic, select **NetFlow**.
5. Click the plus icon (**+**) to add the port.
6. Save the running configuration file to preserve your changes by clicking **View and Save Changes** at the top of the Flow Networks page.
7. Click **Save**.

Add the pending flow networks

You can now add pending flow networks.

Before you begin

You must log in as a user with System and Access Administration privileges to complete the following steps.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. In the Network Settings section, click **Flow Networks**.
3. In the Pending Flow Networks section, click **Add Flow Network**.
4. Type a name to identify this flow network in the Flow Network ID field.
5. Select the **Automatic records** checkbox to send records from this flow network to a connected recordstore.
6. Select the **Enable SNMP polling** checkbox to enable SNMP polling.
7. If you enable SNMP polling, select one of the following options from the SNMP credentials drop-down menu:
   - **Inherit from CIDR**. If you select this option, the SNMP credentials are applied based on the Shared SNMP Credentials settings.
   - **Custom credentials**. Select v1, v2, or v3 from the SNMP version drop-down list, and then configure the remaining settings for the specific polling type.
8. Click **Save**.

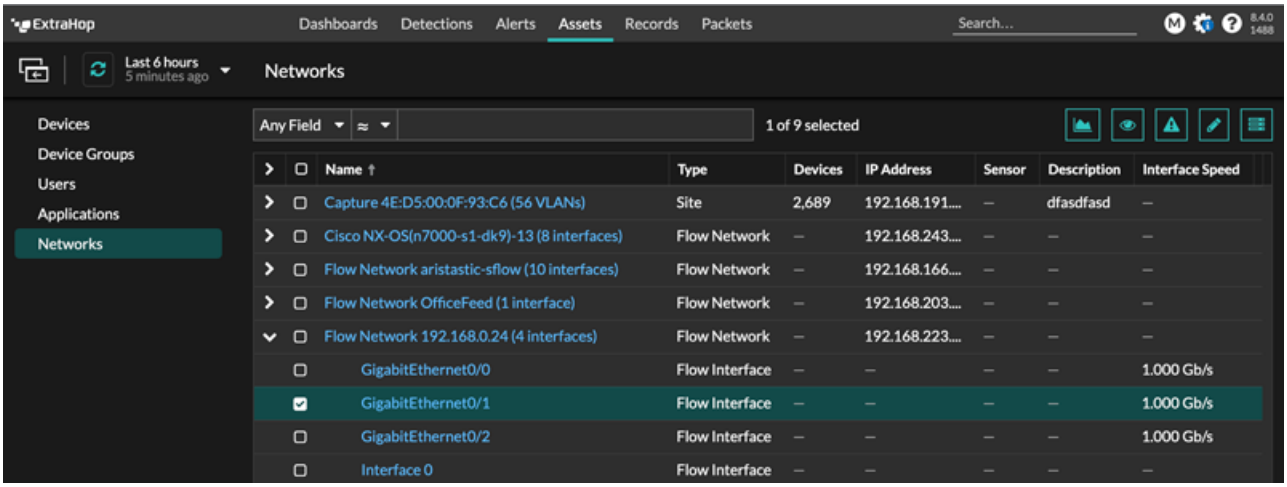
The flow network appears in the Approved Flow Networks table. If you do not see the flow network, you can add it manually by clicking **Add Flow Network** in the Approved Flow Networks section and completing the information as described above.

View configured flow networks

After you configure your flow networks, log in to the ExtraHop system to view built-in charts and modify settings and configurations.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click **Assets**, and then click **Networks**.
3. Click the drop-down arrow next to the flow network name to see a list of flow interfaces and their attributes.
4. Select the checkbox next to the flow network or interface name.

   From the top bar, you can create a chart, assign a trigger, assign an alert, rename the flow interface, and set the interface speed.



Note: Each NetFlow record contains the interface index (ifIndex) of the reporting interface. The interface table (ifTable) is then polled by the ExtraHop system to obtain the interface speed (ifSpeed).

5. Click the flow network name or flow interface name to view built-in charts on summary pages.

   From the summary pages, you can click the regions and charts and add them to a new or existing dashboard.

Configure Cisco NetFlow devices

The following examples of basic Cisco router configuration for NetFlow. NetFlow is configured on a per-interface basis. When NetFlow is configured on the interface, IP packet flow information is exported to the ExtraHop system.

Important: NetFlow takes advantage of the SNMP ifIndex value to represent ingress and egress interface information in flow records. To ensure consistency of interface reporting, enable SNMP ifIndex persistence on devices sending NetFlow to the ExtraHop system. For more information on how to enable SNMP ifIndex persistence on your network devices, refer to the configuration guide provided by the device manufacturer.

For more information on configuring NetFlow on Cisco switches, see your Cisco router documentation or the Cisco website at www.cisco.com.

Configure an exporter on the Cisco Nexus switch

Define a flow exporter by specifying the export format, protocol, and destination.

1. Log in to the switch command-line interface and run the following commands.

2. Enter global configuration mode.

```
config t
```

3. Create a flow exporter and enter flow exporter configuration mode.

```
flow exporter <name>
```

For example:

```
flow exporter Netflow-Exporter-1
```

4. (Optional) Enter a description.

```
description <string>
```

For example:

```
description Production-Netflow-Exporter
```

5. Set the destination IPv4 or IPv6 address for the exporter.

```
destination <eda_mgmt_ip_address>
```

For example:

```
destination 192.168.11.2
```

6. Specify the interface needed to reach the NetFlow collector at the configured destination.

```
source <interface_type> <number>
```

For example:

```
source ethernet 2/2
```

7. Specify the NetFlow export version.

```
version 9
```

Configure Cisco switches through the Cisco IOS CLI

1. Log in to the Cisco IOS command-line interface and run the following commands.
2. Enter global configuration mode.

```
config t
```

3. Specify the interface, and then enter interface configuration mode.
   - Cisco 7500 series routers:

     ```
     interface <type> <slot>/<port-adapter>/<port>
     ```

     For example:

     ```
     interface fastethernet 0/1/0
     ```

- Cisco 7200 series routers:

  ```
  interface <type> <slot>/<port>
  ```

  For example:

  ```
  interface fastethernet 0/1
  ```

4. Enable NetFlow.

   ```
   ip route-cache flow
   ```

5. Export NetFlow statistics, where *<ip-address>* is the Management + Flow Target interface on the ExtraHop system and *<udp-port>* is the configured collector UDP port number.

   ```
   ip flow-export <ip-address> <udp-port> version 5
   ```

Set up shared SNMP credentials for your NetFlow or sFlow networks

If you enable SNMP polling on your flow network configuration, you must specify the credentials that allow you to poll the network device. The SNMP authentication credentials apply to all flow networks in a CIDR block and are automatically applied to every discovered flow network unless custom credentials are configured.

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 **Flow Networks**.
3. In the Shared SNMP Credentials section, click **Add SNMP Credentials**.
4. Type the IPv4 CIDR block in the CIDR field. For example, type `10.0.0.0/8` to match any IP address that starts with 10 or `10.10.0.0/16` to match any IP address that starts with 10.10. You cannot configure an IP address to match all traffic.
5. Select **v1**, **v2c**, or **v3** from the SNMP version drop-down list and then complete the remaining fields.
6. Click **Save**.

Manually refresh SNMP information

You can poll and retrieve data on demand from the SNMP agent on a flow network device. Instead of waiting for automatic polling to occur after each configuration change to confirm that the change is correct (automatic polling occurs every 24 hours), you can poll immediately.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Actions column for the approved flow network, click **Poll**.
   The ExtraHop system polls for the following information:
   - The system name of the SNMP agent. This identifier is assigned by SNMP to the flow network. OID: `1.3.6.1.2.1.1.5.0`.
   - The interface name of each interface on the SNMP agent. These identifiers are for each flow interface on the flow network. OID: `1.3.6.1.2.1.2.2.1.2`.
   - The interface speed of each interface on the SNMP agent. OID: `1.3.6.1.2.1.2.2.1.5` and `1.3.6.1.2.1.31.1.1.1.15`.

Notifications

The ExtraHop system can send notifications about configured alerts through email, SNMP traps, and syslog exports to remote servers. If an email notification group is specified, then emails are sent to the groups assigned to the alert.

Configure email settings for notifications

You must configure an email server and sender before the ExtraHop system can send alert notifications or scheduled dashboard reports.

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 **Notifications**.
3. Click **Email Server and Sender**.
4. In the SMTP Server field, type the IP address or hostname for the outgoing SMTP mail server. The SMTP server should be the fully qualified domain name (FQDN) or IP address of an outgoing mail server that is accessible from the ExtraHop system. If the DNS server is set, then the SMTP server can be a FQDN, otherwise you must type an IP address.
5. In the SMTP Port field, type the port number for SMTP communication. Port 25 is the default value for SMTP and port 465 is the default value for SSL/TLS encrypted SMTP.
6. Select one of the following encryption methods from the Encryption drop-down list:
   - **None**. SMTP communication is not encrypted.
   - **SSL/TLS**. SMTP communication is encrypted through the Secure Socket Layer/Transport Layer Security protocol.
   - **STARTTLS**. SMTP communication is encrypted through STARTTLS.
7. In the Alert Sender Address field, type the email address for the notification sender.

   Note: The displayed sender address might be changed by the SMTP server. When sending through a Google SMTP server, for example, the sender email is changed to the username supplied for authentication, instead of the originally entered sender address.
8. (Optional) Select the Validate SSL Certificates checkbox to enable certificate validation. If you select this option, the certificate on the remote endpoint is validated against the root certificate chains specified by the trusted certificates manager. Note that the host name specified in the certificate presented by the SMTP server must match the hostname specified in your SMTP configuration or validation will fail. In addition, you must configure which certificates you want to trust on the Trusted Certificates page. For more information, see Add a trusted certificate to your ExtraHop system
9. In the Report Sender Address field, type the email address responsible for sending the message. This field is only applicable when sending scheduled dashboard reports from a Command appliance or Reveal(x) 360.
10. Select the Enable SMTP authentication checkbox and then type the SMTP server setup credentials in the Username and Password fields.
11. (Optional) Click **Test Settings**, type your email address, and then click **Send**. You should receive an email message with the subject title `ExtraHop Test Email`.
12. Click **Save**.

Next steps

After you confirm that your new settings are working as expected, preserve your configuration changes through system restart and shutdown events by saving the Running Config file.

Configure an email notification group

Add a list of email addresses to a group, then select the group when you configure email settings for an alert or scheduled dashboard report. Although you can specify individual email addresses, email groups are an effective way to manage your recipient list.

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 **Notifications**.
3. Click **Email Notification Groups**.
4. Click **Add Group**.

5. In the Group Info section, configure the following information:

   • **Name:** Type a name for the email group.

   • **System Health Notifications:** Select this checkbox if you want to send system storage alerts to the email group. These alerts are generated under the following conditions:

   - A virtual disk is in a degraded state.
   - A physical disk is in a degraded state.
   - A physical disk has an increasing error count.
   - A necessary disk partition is missing for firmware, datastore, or packet capture data.

6. In the Email Addresses text box, type the recipient email addresses that should receive the emails sent to this group. Email addresses can be entered one per line or separated by a comma, semicolon, or space. Email addresses are checked only for [*name*]@[*company*].[*domain*] format validation. There must be at least one email address in this text box for the group to be valid.
7. Click **Save**.

Configure settings to send notifications to an SNMP manager

The state of the network can be monitored through the Simple Network Management Protocol (SNMP). SNMP collects information by polling devices on the network or SNMP enabled devices send alerts to SNMP management stations. SNMP communities define the group that devices and management stations running SNMP belong to, which specifies where information is sent. The community name identifies the group.

Note: Most organizations have an established system for collecting and displaying SNMP traps in a central location that can be monitored by their operations teams. For example, SNMP traps are sent to an SNMP manager, and the SNMP management console displays them.

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 **Notifications**.
3. Under Notifications, click **SNMP**.
4. On the SNMP Settings page, in the **SNMP Monitor** field, type the hostname for the SNMP trap receiver. Multiple names can be entered, separated by commas.
5. In the **SNMP Community** field, enter the SNMP community name.
6. In the **SNMP Port** field, type the SNMP port number for your network that is used by the SNMP agent to respond back to the source port on the SNMP manager.
   The default response port is `162`.
7. Click **Test Settings** to verify that your SNMP settings are correct. If the settings are correct, you should see an entry in the SNMP log file on the SNMP server similar to the following:

   ```
   Connection from UDP: [192.0.2.0]:42164->[ 192.0.2.255]:162
   ```

   Where `192.0.2.0` is the IP address of your ExtraHop system and `192.0.2.255` is the IP address of the SNMP server.
8. Click **Save**.

Download the ExtraHop SNMP MIB

SNMP does not provide a database of information that an SNMP-monitored network reports. SNMP information is defined by third-party management information bases (MIBs) that describe the structure of the collected data.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. Go to the Network Settings section and click **Notifications**.
3. Under Notifications, click **SNMP**.

4. Under SNMP MIB, click the **Download ExtraHop SNMP MIB**.
   The file is typically saved to the default download location for your browser.

Extract the ExtraHop vendor object OID
Before you can monitor a device with SNMP, you need the `sysObjectID`, which contains an OID that is the vendor-reported identity of the device.

The SNMP vendor object ID (OID) for the ExtraHop system is iso.3.6.1.4.1.32015. You can also extract this value with `snmpwalk`.

1. Log in to the command-line interface on your management workstation.
2. Extract the OID, where *ip-address* is the IP address for your ExtraHop system:
   In this example, you query with `sysObjectID`:

   ```
   snmpwalk -v 2c -c public <ip-address> SNMPv2-MIB::sysObjectID
   ```

   A response similar to this example displays:

   ```
   SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.32015
   ```

   In this example, you query with the OID:

   ```
   snmpwalk -v 2c -c public <ip-address> 1.3.6.1.2.1.1.2
   ```

   A response similar to this example displays:

   ```
   SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.32015
   ```

Send system notifications to a remote syslog server

The syslog export option enables you to send alerts from an ExtraHop system to any remote system that receives syslog input for long-term archiving and correlation with other sources.

Only one remote syslog server can be configured for each ExtraHop system.

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 **Notifications**.
3. In the Destination field, type the IP address of the remote syslog server.
4. From the Protocol drop-down menu, select **TCP** or **UDP**. This option specifies the protocol over which the information will be sent to your remote syslog server.
5. In the Port field, type the port number for your remote syslog server. By default, this value is set to 514.
6. Click **Test Settings** to verify that your syslog settings are correct. If the settings are correct, you should see an entry in the syslog log file on the syslog server similar to the following:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```

7. Click **Save**.
8. (Optional) Modify the format of syslog messages.

   By default, syslog messages are not compliant with RFC 3164 or RFC 5424. However, you can format syslog messages to be compliant by modifying the running configuration file.

   a) Click **Admin**.
   b) Click **Running Config (Unsaved Changes)**.
   c) Click **Edit Config**.
   d) Add an entry under `syslog_notification` where the key is `rfc_compliant_format` and the value is either `rfc5424` or `rfc3164`.

The `syslog_notification` section should look similar to the following code:

```
    "syslog_notification": {
        "syslog_destination": "192.168.0.0",
        "syslog_ipproto": "udp",
        "syslog_port": 514,
        "rfc_compliant_format": "rfc5424"
    }
```

e) Click **Update**.
f) Click **Done**.

9. (Optional) Modify the timezone referenced in syslog timestamps.

   By default, syslog timestamps reference UTC time. However, you can modify timestamps to reference the ExtraHop system time by modifying the running configuration file.

   a) Click **Admin**.
   b) Click **Running Config (Unsaved Changes)**.
   c) Click **Edit Config**.
   d) Add an entry under `syslog_notification` where the key is `syslog_use_localtime` and the value is `true`.

      The `syslog_notification` section should look similar to the following code:

```
    "syslog_notification": {
        "syslog_destination": "192.168.0.0",
        "syslog_ipproto": "udp",
        "syslog_port": 514,
        "syslog_use_localtime": true
    }
```

   e) Click **Update**.
   f) Click **Done**.

Next steps
After you confirm that your new settings are working as expected, preserve your configuration changes through system restart and shutdown events by saving the running configuration file.

SSL Certificate

SSL certificates provide secure authentication to the ExtraHop system.

You can designate a self-signed certificate for authentication instead of a certificate signed by a Certificate Authority. However, be aware that a self-signed certificate generates an error in the client browser, which reports that the signing certificate authority is unknown. The browser provides a set of confirmation pages to trust the certificate, even though the certificate is self-signed. Self-signed certificates can also degrade performance by preventing caching in some browsers. We recommend that you create a certificate-signing request from your ExtraHop system and upload the signed certificate instead.

Important: When replacing an SSL certificate, the web server service is restarted. Tunneled connections from Discover appliances to Command appliances are lost but then re-established automatically.

Upload an SSL certificate

You must upload a .pem file that includes both a private key and either a self-signed certificate or a certificate-authority certificate.

Note: The .pem file must not be password protected.

Note: You can also automate this task through the REST API.

1. In the Network Settings section, click **SSL Certificate**.
2. Click **Manage certificates** to expand the section.
3. Click **Choose File** and navigate to the certificate that you want to upload.
4. Click **Open**.
5. Click **Upload**.

Generate a self-signed certificate

1. In the Network Settings section, click **SSL Certificate**.
2. Click **Manage certificates** to expand the section.
3. Click **Build SSL self-signed certificate based on hostname**.
4. On the Generate Certificate page, click **OK** to generate the SSL self-signed certificate.

   Note: The default hostname is `extrahop`.

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 an SSL certificate. The CSR is generated on the ExtraHop system where the SSL 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 **SSL 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 SSL 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

Field	Description	Examples
State/Province	The state or province where your organization is located. This entry should not be abbreviated.	Washington
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 SSL certificate from the CA, return to the SSL 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.

Trusted Certificates

Trusted certificates enable you to validate SMTP, LDAP, HTTPS ODS and MongoDB ODS targets, as well as Splunk recordstore connections from your ExtraHop system.

Add a trusted certificate to your ExtraHop system

Your ExtraHop system only trusts peers who present a Transport Layer Security (TLS) certificate that is signed by one of the built-in system certificates and any certificates that you upload. SMTP, LDAP, HTTPS ODS and MongoDB ODS targets, as well as Splunk recordstore connections can be validated through these certificates.

Before you begin
You must log in as a user with setup or system and access administration privileges to add or remove trusted certificates.

When uploading a custom trusted certificate, a valid trust path must exist from the uploaded certificate to a trusted self-signed root in order for the certificate to be fully trusted. Either upload the entire certificate chain for each trusted certificate or (preferably) ensure that each certificate in the chain has been uploaded to the trusted certificates system.

Important: To trust the built-in system certificates and any uploaded certificates, you must also enable SSL/TLS or STARTTLS encryption and certificate validation when configuring the settings for the external server.

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 **Trusted Certificates**.
3. (Optional) The ExtraHop system ships with a set of built-in certificates. Select **Trust System Certificates** if you want to trust these certificates, and then click **Save**.
4. To add your own certificate, click **Add Certificate** and then paste the contents of the PEM-encoded certificate chain into the Certificate field
5. Type a name into the Name field and click **Add**.

Access Settings

In the Access Settings section, you can change user passwords, enable the support account, manage local users and user groups, configure remote authentication, and manage API access.

Global Policies

Administrators can configure global policies that apply to all users who access the system.

Password policy

- Choose between two password policies; the default password policy of 5 or more characters or a more secure strict password policy that has the following restrictions:
  - 8 or more characters
  - Upper and lowercase characters
  - At least one number
  - At least one symbol

  Note: If you select the strict password policy of 8 or more characters, passwords will expire every 60 days.

Device Group Edit Control

- Control whether users with limited write privileges can create and edit device groups. When this policy is selected, all limited write users can create device groups and add other limited write users as editors to their device groups.

Default Dashboard

- Specify the dashboard that users see when they log in to the system. Only dashboards shared with all users can be set as a global default. Users can override this default setting from the command menu of any dashboard.

Passwords

Users with privileges to the Administration page can change the password for local user accounts.

- Select any user and change their password
  - You can only change passwords for local users. You cannot change passwords for users authenticated through LDAP or other remote authentication servers.

For more information about privileges for specific Administration page users and groups, see the Users section.

Change the default password for the setup user

It is recommended that you change the default password for the setup user on the ExtraHop system after you log in for the first time. To remind administrators to make this change, there is a blue **Change Password** button at the top of the page while the setup user is accessing the Administration settings. After the setup user password is changed, the button at the top of the page no longer appears.

Note: The password must be a minimum of 5 characters.

1. In the Administration settings, click the blue **Change default password** button.
   The Password page displays without the drop-down menu for accounts. The password will change for the setup user only.
2. Type the default password in the Old password field.
3. Type the new password in the New password field.
4. Retype the new password in the Confirm password field.
5. Click **Save**.

Support Access

Support accounts provide access for the ExtraHop Support team to help customers troubleshoot issues with the ExtraHop system.

These settings should be enabled only if the ExtraHop system administrator requests hands-on assistance from the ExtraHop Support team.

Generate SSH key

Generate an SSH key to enable ExtraHop Support to connect to your ExtraHop system when remote access is configured through ExtraHop Cloud Services.

1. In the Access Settings section, click **Support Access**.
2. Click **Generate SSH Key**.
3. Click **Generate SSH Key**.
4. Copy the encrypted key from the text box and email the key to your ExtraHop representative.
5. Click **Done**.

Regenerate or revoke the SSH key

To prevent SSH access to the ExtraHop system with an existing SSH key, you can revoke the current SSH key. A new SSH key can also be regenerated if needed.

1. In the Access Settings section, click **Support Access**.
2. Click **Generate SSH Key**.
3. Choose one of the following options:
   - Click **Regenerate SSH Key** and then click **Regenerate**.

     Copy the encrypted key from the text box and email the key to your ExtraHop representative and then click **Done**.
   - Click **Revoke SSH Key** to prevent SSH access to the system with the current key.

Users

The Users page enables you to control local access to the ExtraHop appliance.

Users and user groups

Users can access the ExtraHop system in three ways: through a set of pre-configured user accounts, through local user accounts configured on the appliance, or through remote user accounts configured on existing authentication servers, such as LDAP, SAML, Radius, and TACACS+.

Local users

This topic is about default and local accounts. See Remote Authentication to learn how to configure remote accounts.

The following accounts are configured by default on ExtraHop systems but do not appear in the list of names on the Users page. These accounts cannot be deleted and you must change the default password upon initial login.

setup

This account provides full system read and write privileges to the browser-based user interface and to the ExtraHop command-line interface (CLI). On physical sensors, the default password for this account is the service tag number on the front of the appliance. On virtual sensors, the default password is `default`.

shell

The `shell` account, by default, has access to non-administrative shell commands in the ExtraHop CLI. On physical sensors, the default password for this account is the service tag number on the front of the appliance. On virtual sensors, the default password is `default`.

Note: The default ExtraHop password for either account when deployed in Amazon Web Services (AWS) and Google Cloud Platform (GCP) is the instance ID of the virtual machine.

Next steps

- Add a local user account

Remote Authentication

The ExtraHop system supports remote authentication for user access. Remote authentication enables organizations that have authentication systems such as LDAP (OpenLDAP or Active Directory, for example) to enable all or a subset of their users to log in to the system with their existing credentials.

Centralized authentication provides the following benefits:

- User password synchronization.
- Automatic creation of ExtraHop accounts for users without administrator intervention.
- Management of ExtraHop privileges based on user groups.
- Administrators can grant access to all known users or restrict access by applying LDAP filters.

Next steps

- Configure remote authentication through LDAP
- Configure remote authentication through SAML
- Configure remote authentication through TACACS+
- Configure remote authentication through RADIUS

Remote users

If your ExtraHop system is configured for SAML or LDAP remote authentication, you can create an account for those remote users. Preconfiguring accounts on the ExtraHop system for remote users enables you to share system customizations with those users before they log in.

If you choose to auto-provision users when you configure SAML authentication, then the user is automatically added to the list of local users when they log in for the first time. However, you can create a remote SAML user account on the ExtraHop system when you want to provision a remote user before that user has logged in to the system. Privileges are assigned to the user by the provider. After the user is created, you can add them to local user groups.

Next steps

- Add an account for a remote user

User groups

User groups enable you to manage access to shared content by group instead of by individual user. Customized objects such as activity maps can be shared with a user group, and any user who is added to the group automatically has access. You can create a local user group—which can include remote and local users. Alternatively, if your ExtraHop system is configured for remote authentication through LDAP, you can configure settings to import your LDAP user groups.

- Click **Create User Group** to create a local group. The user group appears in the list. Then, select the checkbox next to the user group name and select users from the **Filter users...** drop-down list. Click **Add Users to Group**.
- (LDAP only) Click **Refresh All User Groups** or select multiple LDAP user groups and click **Refresh Users in Groups**.
- Click **Reset User Group** to remove all shared content from a selected user group. If the group no longer exists on the remote LDAP server, the group is removed from the user group list.
- Click **Enable User Group** or **Disable User Group** to control whether any group member can access shared content for the selected user group.
- Click **Delete User Group** to remove the selected user group from the system.
- View the following properties for listed user groups:

  Group Name

  Displays the name of the group. To view the members in the group, click the group name.

  Type

  Displays Local or Remote as the type of user group.

  Members

  Displays the number of users in the group.

  Shared Content

  Displays the number of user-created objects that are shared with the group.

  Status

  Displays whether the group is enabled or disabled on the system. When the status is `Disabled`, the user group is considered empty when performing membership checks; however, the user group can still be specified when sharing content.

  Members Refreshed (LDAP only)

  Displays the amount of time elapsed since the group membership was refreshed. User groups are refreshed under the following conditions:

  - Once per hour, by default. The refresh interval setting can be modified on the **Remote Authentication** > **LDAP Settings** page.
  - An administrator refreshes a group by clicking **Refresh All User Groups** or **Refresh Users in Group**, or programmatically through the REST API. You can refresh a group from the User Group page or from within the Member List page.
  - A remote user logs in to the ExtraHop system for the first time.
  - A user attempts to load a shared dashboard that they do not have access to.

User privileges

Administrators determine the module access level for users in the ExtraHop system.

For information about user privileges for the REST API, see the REST API Guide.

For information about remote user privileges, see the configuration guides for LDAP, RADIUS, SAML, and TACACS+.

Privilege Levels

Set the privilege level for your user to determine which areas of the ExtraHop system they can access.

Module Access privileges

These privileges determine the features that users can access in the ExtraHop system. Administrators can grant users role-based access to one or all of the NDR, NPM, and Packet Forensics modules. A module license is required to access module features.

Network Detection and Response (NDR)

Allows the user to access security features such as attack detections, investigations, and threat briefings.

Network Performance and Monitoring (NPM)

Allows the user to access performance features such as operations detections and the ability to create custom dashboards.

Packet Forensics

Allows the user to view and download packets and session keys, packets only, or packet slices only.

System Access privileges

These privileges determine the level of functionality users have within the modules where they have been granted access.

For Reveal(x) Enterprise, users with system access and administration privileges can access all features, packets, and session keys for their licensed modules.

For Reveal(x) 360, system access and administration privileges, access to licensed modules, packets, and session keys must be assigned separately. Reveal(x) 360 also offers an additional System Administration account that grants full system privileges except for the ability to manage users and API access.

The following table contains ExtraHop features and their required privileges. If no module requirement is noted, the feature is available in both the NDR and NDM modules.

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Activity Maps							
Create, view, and load shared activity maps	Y	Y	Y	Y	Y	Y	N
Save activity maps	Y	Y	Y	Y	Y	N	N
Share activity maps	Y	Y	Y	Y	N	N	N
Alerts	NPM module license and access required.						
View alerts	Y	Y	Y	Y	Y	Y	Y
Create and modify alerts	Y	Y	Y	N	N	N	N
Analysis Priorities							
View Analysis Priorities page	Y	Y	Y	Y	Y	Y	N
Add and modify	Y	Y	Y	N	N	N	N

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
analysis levels for groups							
Add devices to a watchlist	Y	Y	Y	N	N	N	N
Transfer priorities management	Y	Y	Y	N	N	N	N
Bundles							
Create a bundle	Y	Y	Y	N	N	N	N
Upload and apply a bundle	Y	Y	Y	N	N	N	N
View list of bundles	Y	Y	Y	Y	Y	Y	N
Dashboards	NPM module license and access required to create and modify dashboards.						
View and organize dashboards	Y	Y	Y	Y	Y	Y	Y
Create and modify dashboards	Y	Y	Y	Y	Y	N	N
Share dashboards	Y	Y	Y	Y	N	N	N
Detections	NDR module license and access required to view and tune security detections and create investigations. NPM module license and access required to view and tune performance detections.						
View detections	Y	Y	Y	Y	Y	Y	Y
Acknowledge Detections	Y	Y	Y	Y	Y	N	N
Modify detection status and notes	Y	Y	Y	Y	N	N	N
Create and modify investigations	Y	Y	Y	Y	N	N	N

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Create and modify tuning rules	Y	Y	Y	N	N	N	N
Device Groups	Administrators can configure the Device Group Edit Control global policy to specify whether users with limited write privileges can create and edit device groups.						
Create and modify device groups	Y	Y	Y	Y (If the global privilege policy is enabled)	N	N	N
Metrics							
View metrics	Y	Y	Y	Y	Y	Y	N
Notification Rules	NDR module license and access required to create and modify notifications for security detections and threat briefings. NPM module license and access required to create and modify notifications for performance detections.						
Create and modify detection notification rules	Y	Y	Y	N	N	N	N
Create and modify threat briefing notification rules	Y	Y	Y	N	N	N	N
Create and modify system notification rules (Reveal(x) only)	Y	Y	N	N	N	N	N
Records	Recordstore required.						
View record queries	Y	Y	Y	Y	Y	Y	N
View record formats	Y	Y	Y	Y	Y	Y	N

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Create, modify, and save record queries	Y	Y	Y	N	N	N	N
Create, modify, and save record formats	Y	Y	Y	N	N	N	N
Dashboard Reports	Console required.						
Create, view, and manage scheduled reports	Y	Y	Y	Y	N	N	N
Threat Intelligence	NDR module license and access required.						
Manage threat collections	Y	Y	N	N	N	N	N
View threat intelligence information	Y	Y	Y	Y	Y	Y	N
Triggers							
Create and modify triggers	Y	Y	Y	N	N	N	N
Administrative Privileges							
Access the ExtraHop Administration settings	Y	Y	N	N	N	N	N
Connect to other appliances	Y	Y	N	N	N	N	N
Manage other appliances (Console)	Y	Y	N	N	N	N	N

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Manage users and API access	Y	N	N	N	N	N	N

Add a local user account

By adding a local user account, you can provide users with direct access to your ExtraHop system and restrict their privileges as needed by their role in your organization.

To learn about default system user accounts, see Local users.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Users**.
3. Click **Add User**.
4. In the Personal Information section, type the following information:

   • Login ID: The username that users will log in to the sensor with, which cannot contain any spaces. For example, `adalovelace`.

   • Full Name: A display name for the user, which can contain spaces. For example, `Ada Lovelace`.

   • Password: The password for this account.

   Note: On sensors and consoles, the password must meet the criteria specified by the global password policy. On ExtraHop recordstores and packetstores, passwords must be 5 characters or more.

   • Confirm Password: Re-type the password from the Password field.
5. In the Authentication Type section, select Local.
6. In the User Type section, select the type of privileges for the user.
   - System and access administration privileges enables full read and write access to the ExtraHop system, including Administration settings.
   - Limited privileges enable you to select from a subset of privileges and options.

   Note: For more information, see the User privileges section.
7. Click **Save**.

Tip:
- To modify settings for a user, click the username from the list to bring up the Edit user page.
- To delete a user account, click the red **X** icon. If you delete a user from a remote authentication server, such as LDAP, you must also delete the entry for that user on the ExtraHop system.

Add an account for a remote user

Add a user account for LDAP or SAML users when you want to provision the remote user before that user logs in to the ExtraHop system. After the user is added to the system, you can add them to local groups or share items directly with them before they log in through the LDAP or SAML provider.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Users**.
3. Click **Add User**.

4. In the Personal Information section, type the following information:
   - **Login ID:** The email address that the user logs in to their LDAP or SAML SSO identity provider with.

     Note: Only lowercase email addresses are supported for remote users.

   - **Full Name:** The first and last name of the user.
5. In the Authentication Type section, select **Remote**.
6. Click **Save**.

Sessions

The ExtraHop system provides controls to view and delete user connections to the web interface. The Sessions list is sorted by expiration date, which corresponds to the date the sessions were established. If a session expires or is deleted, the user must log in again to access the web interface.

Remote Authentication

The ExtraHop system supports remote authentication for user access. Remote authentication enables organizations that have authentication systems such as LDAP (OpenLDAP or Active Directory, for example) to enable all or a subset of their users to log in to the system with their existing credentials.

Centralized authentication provides the following benefits:

- User password synchronization.
- Automatic creation of ExtraHop accounts for users without administrator intervention.
- Management of ExtraHop privileges based on user groups.
- Administrators can grant access to all known users or restrict access by applying LDAP filters.

Next steps

- Configure remote authentication through LDAP
- Configure remote authentication through SAML
- Configure remote authentication through TACACS+
- Configure remote authentication through RADIUS

Configure remote authentication through LDAP

The ExtraHop system supports the Lightweight Directory Access Protocol (LDAP) for authentication and authorization. Instead of storing user credentials locally, you can configure your ExtraHop system to authenticate users remotely with an existing LDAP server. Note that ExtraHop LDAP authentication only queries for user accounts; it does not query for any other entities that might be in the LDAP directory.

Before you begin

- This procedure requires familiarity with configuring LDAP.
- Ensure that each user is in a permission-specific group on the LDAP server before beginning this procedure.
- If you want to configure nested LDAP groups, you must modify the Running Configuration file. Contact ExtraHop Support for help.

When a user attempts to log onto an ExtraHop system, the ExtraHop system tries to authenticate the user in the following ways:

- Attempts to authenticate the user locally.
- Attempts to authenticate the user through the LDAP server if the user does not exist locally and if the ExtraHop system is configured for remote authentication with LDAP.

- Logs the user onto the ExtraHop system if the user exists and the password is validated either locally or through LDAP. The LDAP password is not stored locally on the ExtraHop system. Note that you must enter the username and password in the format that your LDAP server is configured for. The ExtraHop system only forwards the information to the LDAP server.
- If the user does not exist or an incorrect password is entered, an error message appears on the login page.

Important: If you change LDAP authentication at a later time to a different remote authentication method, the users, user groups, and associated customizations that were created through remote authentication are removed. Local users are unaffected.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Remote Authentication**.
3. From the Remote authentication method drop-down list, select **LDAP** and then click **Continue**.
4. On the LDAP Settings page, complete the following server information fields:
   a) In the Hostname field, type the hostname or IP address of the LDAP server. If you are configuring a hostname, make sure that the DNS entry of the ExtraHop system is properly configured.
   b) In the Port field, type the port number on which the LDAP server is listening.
   c) From the Server Type drop-down list, select **Posix** or **Active Directory**.
   d) (Optional) In the Bind DN field, type the bind DN. The bind DN is the user credentials that allow you to authenticate with the LDAP server to perform the user search. The bind DN must have list access to the base DN and any OU, groups, or user account required for LDAP authentication. If this value is not set, then an anonymous bind is performed. Note that anonymous binds are not enabled on all LDAP servers.
   e) (Optional) In the Bind Password field, type the bind password. The bind password is the password required when authenticating with the LDAP server as the bind DN specified above. If you are configuring an anonymous bind, leave this field blank. In some cases, an unauthenticated bind is possible, where you supply a Bind DN value but no bind password. Consult your LDAP administrator for the proper settings.
   f) From the Encryption drop-down list, select one of the following encryption options.

      • **None:** This options specifies cleartext TCP sockets. All passwords are sent across the network in cleartext in this mode.

      • **LDAPS:** This option specifies LDAP wrapped inside SSL.

      • **StartTLS:** This option specifies TLS LDAP. (SSL is negotiated before any passwords are sent.)
   g) Select **Validate SSL Certificates** to enable certificate validation. If you select this option, the certificate on the remote endpoint is validated against the root certificates as specified by the trusted certificates manager. You must configure which certificates you want to trust on the Trusted Certificates page. For more information, see Add a trusted certificate to your ExtraHop system.
   h) Type a time value in the Refresh Interval field or leave the default setting of 1 hour. The refresh interval ensures that any changes made to user or group access on the LDAP server are updated on the ExtraHop system.
5. Configure the following user settings:
   a) Type the base DN in the Base DN field. The Base DN is the point from where a server will search for users. The base DN must contain all user accounts that will have access to the ExtraHop system. The users can be direct members of the base DN or nested within an OU within the base DN if the **Whole Subtree** option is selected for the Search Scope specified below.
   b) Type a search filter in the Search Filter field. Search filters enable you to define search criteria when searching the LDAP directory for user accounts.

Important: The ExtraHop system automatically adds parentheses to wrap the filter and will not parse this parameter correctly if you add parentheses manually. Add your search filters in this step and in step 5b, similar to the following example:

```
cn=atlas*
|(cn=EH-*)(cn=IT-*)
```

In addition, if your group names include the asterisk (*) character, the asterisk must be escaped as `\2a`. For example, if your group has a CN called `test*group`, type `cn=test\2agroup` in the Search Filter field.

c) From the Search Scope drop-down list, select one of the following options. Search scope specifies the scope of the directory search when looking for user entities.

- **Whole subtree:** This option looks recursively under the group DN for matching users.
- **Single level:** This option looks for users that exist in the base DN only; not any subtrees.

6. (Optional) Import user groups. Select the **Import user groups from LDAP server** checkbox and configure the following settings.

Note: Importing LDAP user groups enables you to share dashboards with those groups. The imported groups appear on the User Group page in the Administration settings.

a) Type the base DN in the Base DN field. The Base DN is the point from where a server will search for user groups. The base DN must contain all user groups that will have access to the ExtraHop system. The user groups can be direct members of the base DN or nested within an OU within the base DN if the **Whole Subtree** option is selected for the Search Scope specified below.

b) Type a search filter in the Search Filter field. Search filters enable you to define search criteria when searching the LDAP directory for user groups.

Important: For group search filters, the ExtraHop system implicitly filters on the objectclass=group, and so objectclass=group should not be added to this filter.

c) From the Search Scope drop-down list, select one of the following options. Search scope specifies the scope of the directory search when looking for user group entities.

- **Whole subtree:** This option looks recursively under the base DN for matching user groups.
- **Single level:** This option looks for user groups that exist in the base DN; not any subtrees.

7. Click **Test Settings**. If the test succeeds, a status message appears near the bottom of the page. If the test fails, click **Show details** to see a list of errors. You must resolve any errors before you continue.
8. Click **Save and Continue**.

Next steps

Configure user privileges for remote authentication

Configure user privileges for remote authentication

You can assign user privileges to individual users on your ExtraHop system or configure and manage privileges through your LDAP server.

When assigning user privileges through LDAP, you must complete at least one of the available user privilege fields. These fields require groups (not organizational units) that are pre-specified on your LDAP server. A user account with access must be a direct member of a specified group. User accounts that are not a member of a group specified above will not have access. Groups that are not present are not authenticated on the ExtraHop system.

The ExtraHop system supports both Active Directory and POSIX group memberships. For Active Directory, `memberOf` is supported. For POSIX, `memberuid`, `posixGroups`, `groupofNames`, and `groupofuniqueNames` are supported.

1. Choose one of the following options from the Privilege assignment options drop-down list:
   - **Obtain privileges level from remote server**

This option assigns privileges through your remote authentication server. You must complete at least one of the following distinguished name (DN) fields.

• **System and Access Administration DN:** Create and modify all objects and settings on the ExtraHop system, including Administration settings.

• **Full Write DN:** Create and modify objects on the ExtraHop system, not including Administration settings.

• **Limited Write DN:** Create, modify, and share dashboards.

• **Personal Write DN:** Create personal dashboards and modify dashboards shared with the logged-in user.

• **Full read-only DN:** View objects in the ExtraHop system.

• **Restricted Read-only DN:** View dashboards shared with the logged-in user.

• **Packet Slices Access DN:** View and download the first 64 bytes of packets captured through the ExtraHop Trace appliance.

• **Packet Access DN:** View and download packets captured through the ExtraHop Trace appliance.

• **Packet and Session Keys Access DN:** View and download packets and any associated SSL session keys captured through the ExtraHop Trace appliance.

• **NDR Module Access DN:** View, acknowledge, and hide security detections that appear in the ExtraHop system.

• **NPM Module Access DN:** View, acknowledge, and hide performance detections that appear in the ExtraHop system.

- **Remote users have full write access**

  This option grants remote users full write access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, NDR module access, and NPM module access.
- **Remote users have full read-only access**

  This option grants remote users read-only access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, NDR module access, and NPM module access.

2. (Optional) Configure packet and session key access. Select one of the following options to allow remote users to download packet captures and SSL session keys.
   - **No access**
   - **Packet slices only**
   - **Packets only**
   - **Packets and session keys**
3. (Optional) Configure NDR and NPM module access.
   - **No access**
   - **Full access**
4. Click **Save and Finish**.
5. Click **Done**.

Configure remote authentication through SAML

You can configure secure, single sign-on (SSO) authentication to the ExtraHop system through one or more security assertion markup language (SAML) identity providers.

When a user logs in to an ExtraHop system that is configured as a service provider (SP) for SAML SSO authentication, the ExtraHop system requests authorization from the appropriate identity provider (IdP).

The identity provider authenticates the user's credentials and then returns the authorization for the user to the ExtraHop system. The user is then able to access the ExtraHop system.

Configuration guides for specific identity providers are linked below. If your provider is not listed, apply the settings required by the ExtraHop system to your identity provider.

Identity providers must meet the following criteria:

- SAML 2.0
- Support SP-initiated login flows. IdP-initiated login flows are not supported.
- Support signed SAML Responses
- Support HTTP-Redirect binding

The example configuration in this procedure enables access to the ExtraHop system through group attributes.

If your identity provider does not support group attribute statements, configure user attributes with the appropriate privileges for module access, system access, and packet forensics.

Enable SAML remote authentication

Warning: If your system is already configured with a remote authentication method, changing these settings will remove any users and associated customizations created through that method, and remote users will be unable to access the system. Local users are unaffected.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Remote Authentication**.
3. Select **SAML** from the remote authentication method drop-down list and then click **Continue**.

- Click **View SP Metadata** to view the Assertion Consumer Service (ACS) URL and Entity ID of the ExtraHop system. These strings are required by your identity provider to configure SSO authentication. You can also download a complete XML metadata file that you can import into your identity provider configuration.

  Note: The ACS URL includes the hostname configured in Network Settings. If the ACS URL contains an unreachable hostname, such as the default system hostname `extrahop`, you must edit the URL when adding the ACS URL to your identity provider and specify the fully qualified domain name (FQDN) of the ExtraHop system.
- Click **Add Identity Provider** to add the following information:

  • **Provider Name:** Type a name to identify your specific identity provider. This name appears on the ExtraHop system log in page after the **Log in with** text.

  • **Entity ID:** Paste the entity ID provided by your identity provider into this field.

  • **SSO URL:** Paste the single sign-on URL provided by your identity provider into this field.

  • **Public Certificate:** Paste the X.509 certificate provided by your identity provider into this field.

  • **Auto-provision users:** When this option is selected, ExtraHop user accounts are automatically created when the user logs in through the identity provider. To manually control which users can log in, clear this checkbox and manually configure new remote users through the ExtraHop Administration settings or REST API. Any manually-created remote username should match the username configured on the identity provider.

  • **Enable this identity provider:** This option is selected by default and allows users to log in to the ExtraHop system. To prevent users from logging in through this identity provider, clear the checkbox.

  • **User Privilege Attributes:** You must configure user privilege attributes before users can log in to the ExtraHop system through an identity provider. Values are not case sensitive and can include spaces.

The names and values of user privilege attributes must match the names and values your identity provider includes in SAML responses, which are configured when you add the ExtraHop application to a provider. For example, in Azure AD, you configure claim names and claim condition values that must match the names and values of user privilege attributes in the ExtraHop system. For more detailed examples, see the following topics:

- Configure SAML single sign-on with JumpCloud
- Configure SAML single sign-on with Google
- Configure SAML single sign-on with Okta
- Configure SAML single sign-on with Azure AD

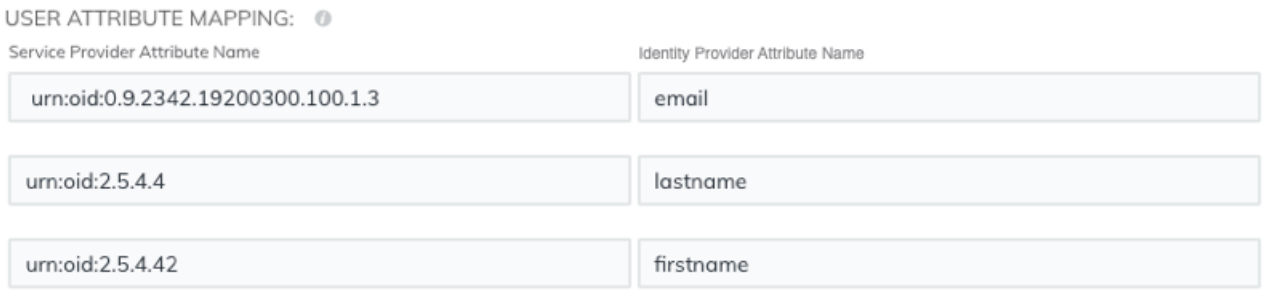
Note: If a user matches multiple attribute values, the user is granted the most permissive access privilege. For example, if a user matches both Limited write and Full write values, the user is granted Full write privileges. For more information about privilege levels, see Users and user groups.

- **NDR Module Access:** NDR attributes enable users to access NDR features.
- **NPM Module Access:** NPM attributes enable users to access NPM features.
- **Packets and Session Key Access:** Packets and session key attributes enable users to access packets and session keys. Configuring packets and session key attributes is optional and only required when you have a connected ExtraHop packetstore.

User attribute mapping

You must configure the following set of user attributes in the application attribute mapping section on your identity provider. These attributes identify the user throughout the ExtraHop system. Refer to your identity provider documentation for the correct property names when mapping attributes.

ExtraHop Attribute Name	Friendly Name	Category	Identity Provider Attribute Name
`urn:oid:0.9.2342.19200300.100.1.3`	mail	Standard Attribute	Primary email address
`urn:oid:2.5.4.4`	sn	Standard Attribute	Last name
`urn:oid:2.5.4.42`	givenName	Standard Attribute	First name



Group attribute statements

The ExtraHop system supports group attribute statements to easily map user privileges to all members of a specific group. When you configure the ExtraHop application on your identity provider, specify a group attribute name. This name is then entered in the Attribute Name field when you configure the identity provider on the ExtraHop system.

If your identity provider does not support group attribute statements, configure user attributes with the appropriate privileges for module access, system access, and packet forensics.

Next steps

- Configure SAML single sign-on with JumpCloud
- Configure SAML single sign-on with Google
- Configure SAML single sign-on with Okta

Configure SAML single sign-on with Okta

You can configure your ExtraHop system to enable users to log in to the system through the Okta identity management service.

Before you begin

- You should be familiar with administering Okta. These procedures are based on the Okta Classic UI. If you are configuring Okta through the Developer Console, the procedure might be slightly different.
- You should be familiar with administering ExtraHop systems.

These procedures require you to copy and paste information between the ExtraHop system and the Okta Classic UI, so it is helpful to have each system open side-by-side.

Enable SAML on the ExtraHop system

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Remote Authentication**.
3. From the Remote authentication method drop-down list, select **SAML**.
4. Click **Continue**.
5. Click **View SP Metadata**. You will need to copy the ACS URL and Entity ID to paste into the Okta configuration in the next procedure.

Configure SAML settings in Okta

This procedure requires you to copy and paste information between the ExtraHop Administration settings and the Okta Classic UI, so it is helpful to have each UI open side-by-side.

1. Log in to Okta.
2. In the upper-right corner of the page, change the view from **Developer Console** to **Classic UI**.

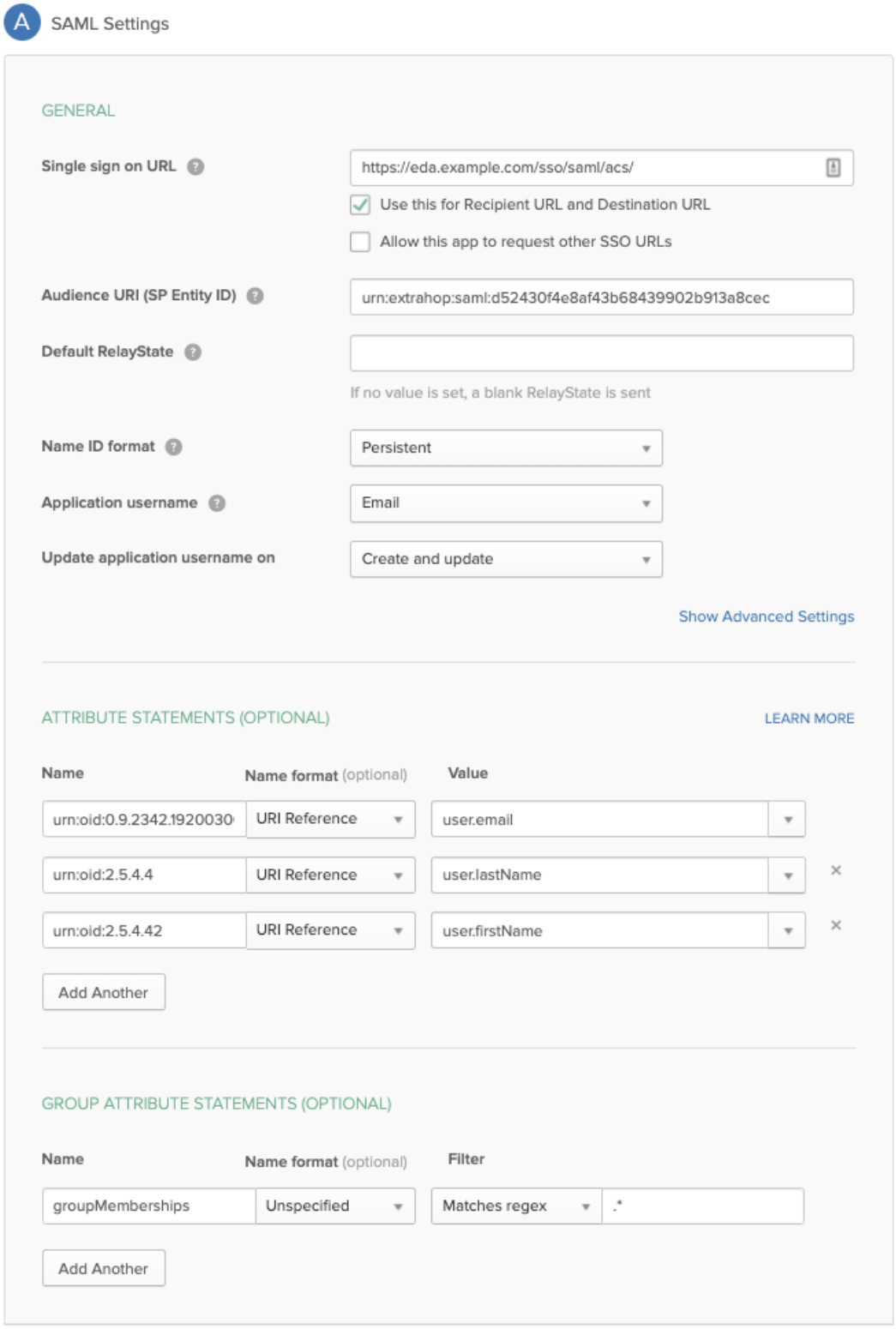
3. From the top menu, click **Applications**.
4. Click **Add Application**.
5. Click **Create New App**.
6. From the Platform drop-down list, select **Web**.
7. For the Sign on method, select **SAML 2.0**.
8. Click **Create**.

9. In the General Settings section, type a unique name in the App name field to identify the ExtraHop system.
10. (Optional) Configure the App logo and App visibility fields as required for your environment.
11. Click **Next**.
12. In the SAML Settings sections, paste the Assertion Consumer Service (ACS) URL from the ExtraHop system into the Single sign on URL field in Okta.

    Note: You might need to manually edit the ACS URL if the URL contains an unreachable hostname, such as the default system hostname `extrahop`. We recommend that you specify the fully qualified domain name for the ExtraHop system in the URL.
13. Paste the SP Entity ID from the ExtraHop system into the Audience URI (SP Entity ID) field in Okta.
14. From the Name ID format drop-down list, select **Persistent**.
15. From the Application username drop-down list, select a username format.
16. In the Attribute Statements section, add the following attributes. These attributes identify the user throughout the ExtraHop system.

Name	Name format	Value
`urn:oid:0.9.2342.19200300.100.1.3`	URI Reference	user.email
`urn:oid:2.5.4.4`	URI Reference	user.lastName
`urn:oid:2.5.4.42`	URI Reference	user.firstName

17. In the Group Attribute Statement section, type a string in the Name field and configure a filter. You will specify the group attribute name when you configure user privilege attributes on the ExtraHop system. The following figure shows a sample configuration.



18. Click **Next** and then click **Finish**.
    You are returned to the Sign On settings page.
19. In the Settings section, click **View Setup Instructions**.
    A new browser window opens and displays information that is required to configure the ExtraHop system.

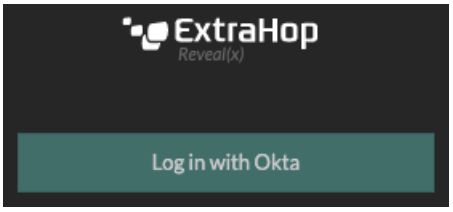
Assign the ExtraHop system to Okta groups

We assume that you already have users and groups configured in Okta. If you do not, refer to the Okta documentation to add new users and groups.

1. From the Directory menu, select **Groups**.
2. Click the group name.
3. Click **Manage Apps**.
4. Locate the name of the application you configured for the ExtraHop system and click **Assign**.
5. Click **Done**.

Add identity provider information on the ExtraHop system

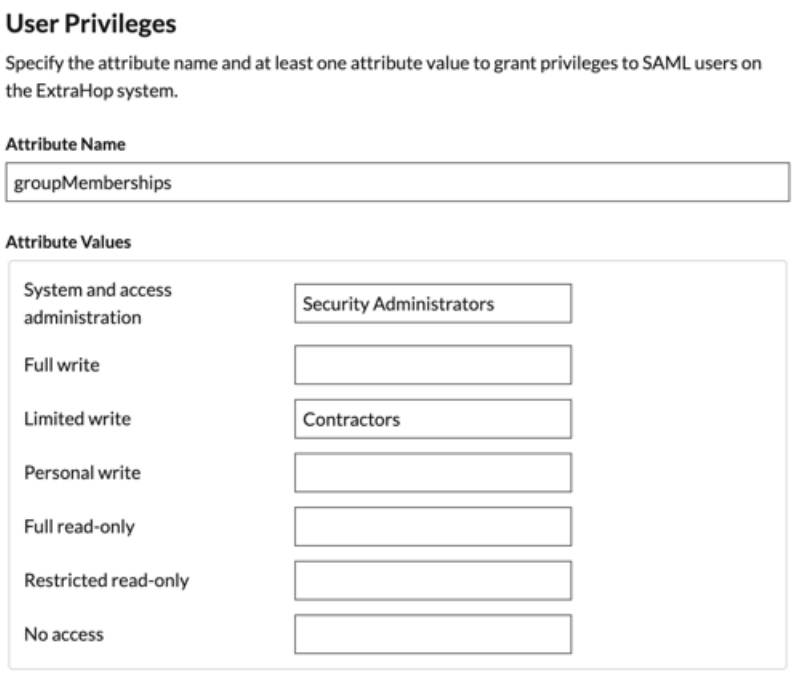
1. Return to the Administration settings on the ExtraHop system. Close the Service Provider metadata window if it is still open, and then click **Add Identity Provider**.
2. Type a unique name in the Provider Name field. This name appears on the ExtraHop system login page.



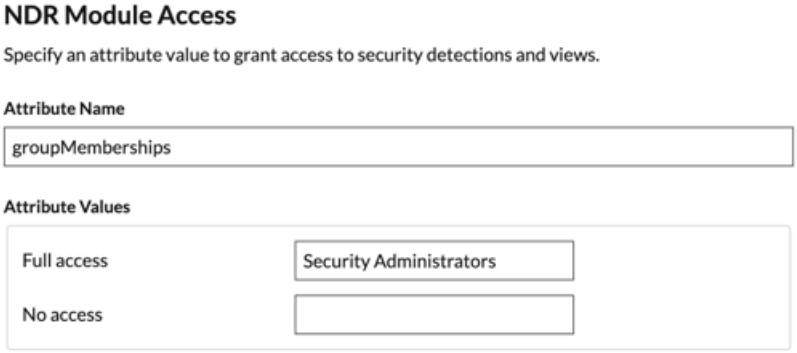
3. From Okta, copy the Identity Provider Single Sign-On URL and paste into the SSO URL field on the ExtraHop system.
4. From Okta, copy the Identity Provider Issuer URL and paste into the Entity ID field on the ExtraHop system.
5. From Okta, copy the X.509 certificate and paste into the Public Certificate field on the ExtraHop system.
6. Choose how you would like to provision users from one of the following options.
   - Select Auto-provision users to create a new remote SAML user account on the ExtraHop system when the user first logs in.
   - Clear the Auto-provision users checkbox and manually configure new remote users through the ExtraHop Administration settings or REST API. Access and privilege levels are determined by the user configuration in Okta.
7. The **Enable this identity provider** option is selected by default and allows users to log in to the ExtraHop system. To prevent users from logging in, clear the checkbox.
8. Configure user privilege attributes. You must configure the following set of user attributes before users can log in to the ExtraHop system through an identity provider. Values are user-definable; however, they must match the attribute names that are included in the SAML response from your identity provider. Values are not case sensitive and can include spaces. For more information about privilege levels, see Users and user groups.

   Important: You must specify the attribute name and configure at least one attribute value other than **No access** to enable users to log in.

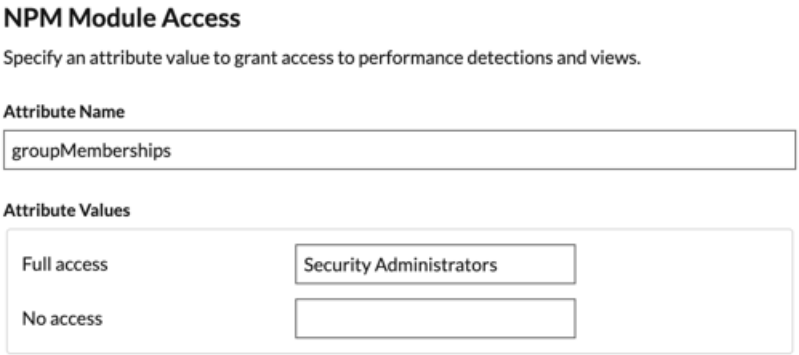
   In the examples below, the Attribute Name field is the group attribute configured when creating the ExtraHop application on the identity provider and the Attribute Values are the names of your user groups. If a user is a member of more than one group, the user is granted the most permissive access privilege.



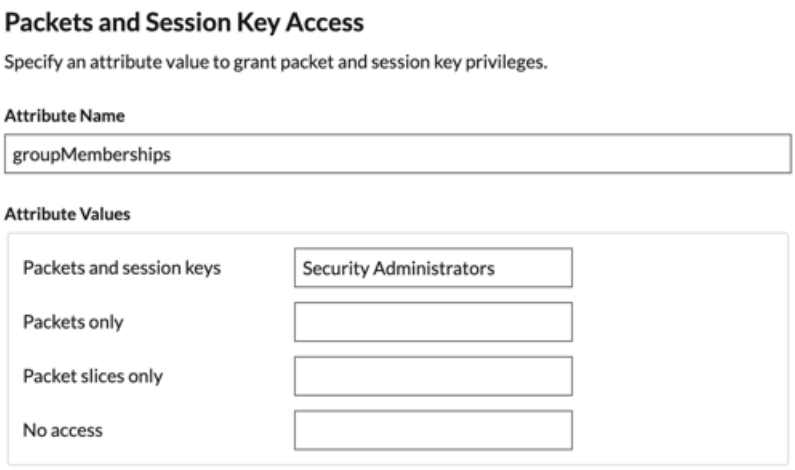
9. Configure NDR module access.



10. Configure NPM module access.



11. (Optional) Configure packets and session key access. This step is optional and is only required when you have a connected packetstore and the Packet Forensics module.



12. Click **Save**.
13. Save the Running Config.

Log in to the ExtraHop system

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click **Log in with** *<provider name>*.
3. Sign in to your provider with your email address and password. You are automatically directed to the ExtraHop Overview page.

Configure SAML single sign-on with Google

You can configure your ExtraHop system to enable users to log in to the system through the Google identity management service.

Before you begin

- You should be familiar with administering Google Admin.
- You should be familiar with administering ExtraHop systems.

These procedures require you to copy and paste information between the ExtraHop system and Google Admin console, so it is helpful to have each system open side-by-side.

Enable SAML on the ExtraHop system

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Remote Authentication**.
3. From the Remote authentication method drop-down list, select **SAML**.
4. Click **Continue**.
5. Click **View SP Metadata**.
6. Copy the ACS URL and Entity ID to a text file. You will paste this information into the Google configuration in a later procedure.

Add user custom attributes

1. Log in to the Google Admin console.
2. Click **Users**.
3. Click the Manage custom attributes icon .
4. Click **Add Custom Attribute**.
5. In the Category field, type `ExtraHop`.

6. (Optional) Type a description in the Description field.
7. In the Custom fields section, enter the following information.
   a) In the Name field, type `writelevel`.
   b) From the Info Type drop-down list, select **Text**.
   c) From the Visibility drop-down list, select **Visible to domain**.
   d) From the No. of values drop-down list, select **Single Value**.
8. Enable NDR module access
   a) In the Name field, type `ndrlevel`.
   b) From the Info Type drop-down list, select **Text**.
   c) From the Visibility drop-down list, select **Visible to domain**.
   d) From the No. of values drop-down list, select **Single Value**.
9. Enable NPM module access
   a) In the Name field, type `npmlevel`.
   b) From the Info Type drop-down list, select **Text**.
   c) From the Visibility drop-down list, select **Visible to domain**.
   d) From the No. of values drop-down list, select **Single Value**.
10. (Optional) If you have connected packetstores, enable packet access by configuring a custom field with the following information.
    a) In the Name field, type `packetslevel`.
    b) From the Info Type drop-down list, select **Text**.
    c) From the Visibility drop-down list, select **Visible to domain**.
    d) From the No. of values drop-down list, select **Single Value**.
11. Click **Add**.

Add identity provider information from Google to the ExtraHop system

1. In the Google Admin console, click the Main menu icon and select **Apps** > **SAML apps**.
2. Click the Enable SSO for a SAML application icon.
3. Click **SETUP MY OWN CUSTOM APP**.
4. On the Google IdP Information screen, click the **Download** button to download the certificate (`GoogleIDPCertificate.pem`).
5. Return to the Administration settings on the ExtraHop system.
6. Click **Add Identity Provider**.
7. Type a unique name in the Provider Name field. This name appears on the ExtraHop system login page.
8. From the Google IdP Information screen, copy the SSO URL and paste it into the SSO URL field on the ExtraHop appliance.
9. From the Google IdP Information screen, copy the Entity ID and paste into the Entity ID field on the ExtraHop system.
10. Open the `GoogleIDPCertificate` in a text editor, copy the contents and paste into the Public Certificate field on the ExtraHop system.
11. Choose how you would like to provision users from one of the following options.
    - Select **Auto-provision users** to create a new remote SAML user account on the ExtraHop system when the user first logs in.
    - Clear the **Auto-provision users** checkbox and manually configure new remote users through the ExtraHop Administration settings or REST API. Access and privilege levels are determined by the user configuration in Google.
12. The **Enable this identity provider** option is selected by default and allows users to log in to the ExtraHop system. To prevent users from logging in, clear the checkbox.

13. Configure user privilege attributes. You must configure the following set of user attributes before users can log in to the ExtraHop system through an identity provider. Values are user-definable; however, they must match the attribute names that are included in the SAML response from your identity provider. Values are not case sensitive and can include spaces. For more information about privilege levels, see Users and user groups..

    Important: You must specify the attribute name and configure at least one attribute value other than **No access** to enable users to log in.

    In the example below, the Attribute Name field is the application attribute and the Attribute Value is the user field name configured when creating the ExtraHop application on the identity provider.

Field Name	Example Attribute Value
Attribute Name	`urn:extrahop:saml:2.0:writelevel`
System and access administration	`unlimited`
Full write privileges	`full_write`
Limited write privileges	`limited_write`
Personal write privileges	`personal_write`
Full read-only privileges	`full_readonly`
Restricted read-only privileges	`restricted_readonly`
No access	`none`

14. Configure NDR module access.

Field	Example Attribute Value
Attribute Name	`urn:extrahop:saml:2.0:ndrlevel`
Full access	`full`
No access	`none`

15. Configure NPM module access.

Field	Example Attribute Value
Attribute Name	`urn:extrahop:saml:2.0:npmlevel`
Full access	`full`
No access	`none`

16. (Optional) Configure packets and session key access. Configuring packets and session key attributes is optional and only required when you have a connected packetstore.

Field Name	Example Attribute Value
Attribute Name	`urn:extrahop:saml:2.0:packetslevel`
Packets and session keys	`full_with_keys`
Packets only	`full`
Packets slices only	`slices`
No access	`none`

17. Click **Save**.
18. Save the Running Config.

Add ExtraHop service provider information to Google

1. Return to the Google Admin console and click **Next** on the Google Idp Information page to continue to step 3 of 5.

2. Type a unique name in the Application Name field to identify the ExtraHop system. Each ExtraHop system that you create a SAML application for needs a unique name.
3. (Optional) Type a description for this application or upload a custom logo.
4. Click **Next**.
5. Copy the Assertion Consumer Service (ACS) URL from the ExtraHop system and paste into the ACS URL field in Google Admin.

   Note: You might need to manually edit the ACS URL if the URL contains an unreachable hostname, such as the default system hostname `extrahop`. We recommend that you specify the fully qualified domain name for the ExtraHop system in the URL.
6. Copy the SP Entity ID from the ExtraHop system and paste into the Entity ID field in Google Admin.
7. Select the **Signed Response** checkbox.
8. In the Name ID section, leave the default **Basic Information** and **Primary Email** settings unchanged.
9. From the Name ID Format drop-down list, select **PERSISTENT**.
10. Click **Next**.

11. On the Attribute Mapping screen, click **ADD NEW MAPPING**.
12. Add the following attributes exactly as shown. The first four attributes are required. The `packetslevel` attribute is optional and is only required if you have a connected packetstore. If you have a packetstore and you do not configure the `packetslevel` attribute, users will be unable to view or download packet captures in the ExtraHop system.

Application Attribute	Category	User Field
`urn:oid:0.9.2342.19200300.100.1.3`	Basic Information	Primary Email
`urn:oid:2.5.4.4`	Basic Information	Last Name
`urn:oid:2.5.4.42`	Basic Information	First Name
`urn:extrahop:saml:2.0:writelevel`	ExtraHop	writelevel
`urn:extrahop:saml:2.0:ndrlevel`	ExtraHop	ndrlevel
`urn:extrahop:saml:2.0:npmlevel`	ExtraHop	npmlevel
`urn:extrahop:saml:2.0:packetslevel`	ExtraHop	packetslevel

13. Click **Finish** and then click **OK**.
14. Click **Edit Service**.
15. Select **On for everyone**, and then click **Save**.

Assign user privileges

1. Click **Users** to return to the table of all users in your organizational units.
2. Click the name of the user you want to allow to log in to the ExtraHop system.
3. In the User information section, click **User details**.
4. In the ExtraHop section, click **writelevel** and type one of the following privilege levels.

   - `unlimited`
   - `full_write`
   - `limited_write`
   - `personal_write`
   - `full_readonly`
   - `restricted_readonly`
   - `none`

   For information about user privileges, see Users and user groups.
5. (Optional) If you added the `packetslevel` attribute above, click **packetslevel** and type one of the following privileges.

   - `full`
   - `full_with_write`
   - `none`

6. (Optional) If you added the `detectionslevel` attribute above, click **detectionslevel** and type one of the following privileges.
   - `full`
   - `none`
7. Click **Save**.

Log in to the ExtraHop system

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click **Log in with** *<provider name>*.
3. Sign in to your provider with your email address and password. You are automatically directed to the ExtraHop Overview page.

Configure remote authentication through RADIUS

The ExtraHop system supports Remote Authentication Dial In User Service (RADIUS) for remote authentication and local authorization only. For remote authentication, the ExtraHop system supports unencrypted RADIUS and plaintext formats.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Remote Authentication**.
3. From the Remote authentication method drop-down list, select **RADIUS** and then click **Continue**.
4. On the Add RADIUS Server page, type the following information:

   Host
   : The hostname or IP address of the RADIUS server. Make sure that the DNS of the ExtraHop system is properly configured if you specify a hostname.

   Secret
   : The shared secret between the ExtraHop system and the RADIUS server. Contact your RADIUS administrator to obtain the shared secret.

   Timeout
   : The amount of time in seconds that the ExtraHop system waits for a response from the RADIUS server before attempting the connection again.
5. Click **Add Server**.
6. (Optional) Add additional servers as needed.
7. Click **Save and Finish**.
8. From the Privilege assignment options drop-down list, choose one of the following options:
   - **Remote users have full write access**

This option grants remote users full write access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, NDR module access, and NPM module access.

- **Remote users have full read-only access**

  This option grants remote users read-only access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, NDR module access, and NPM module access.

9. (Optional) Configure packet and session key access. Select one of the following options to allow remote users to download packet captures and SSL session keys.
   - **No access**
   - **Packet slices only**
   - **Packets only**
   - **Packets and session keys**
10. (Optional) Configure NDR and NPM module access.
    - **No access**
    - **Full access**
11. Click **Save and Finish**.
12. Click **Done**.

Configure remote authentication through TACACS+

The ExtraHop system supports Terminal Access Controller Access-Control System Plus (TACACS+) for remote authentication and authorization.

Ensure that each user to be remotely authorized has the ExtraHop service configured on the TACACS+ server before beginning this procedure.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Remote Authentication**.
3. From the Remote authentication method drop-down list, select **TACACS+**, and then click **Continue**.
4. On the Add TACACS+ Server page, type the following information:

   • Host: The hostname or IP address of the TACACS+ server. Make sure that the DNS of the ExtraHop system is properly configured if you are entering a hostname.

   • Secret: The shared secret between the ExtraHop system and the TACACS+ server. Contact your TACACS+ administrator to obtain the shared secret.

   Note: The secret cannot include the number sign (#).

   • Timeout: The amount of time in seconds that the ExtraHop system waits for a response from the TACACS+ server before attempting to connect again.
5. Click **Add Server**.
6. (Optional) Add additional servers as needed.
7. Click **Save and Finish**.
8. From the Permission assignment options drop-down list, choose one of the following options:
   - **Obtain privileges level from remote server**

     This option allows remote users to obtain privilege levels from the remote server. You must also configure permissions on the TACACS+ server.
   - **Remote users have full write access**

This option grants remote users full write access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, NDR module access, and NPM module access.

- **Remote users have full read-only access**

  This option grants remote users read-only access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, NDR module access, and NPM module access.

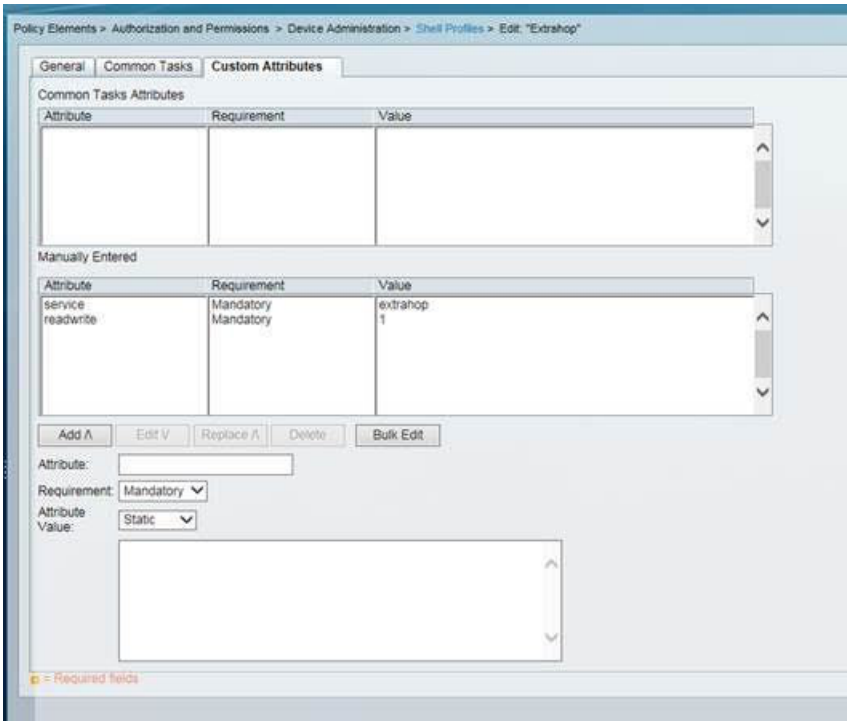
9. (Optional) Configure packet and session key access. Select one of the following options to allow remote users to download packet captures and SSL session keys.
   - **No access**
   - **Packet slices only**
   - **Packets only**
   - **Packets and session keys**
10. (Optional) Configure NDR and NPM module access.
    - **No access**
    - **Full access**
11. Click **Save and Finish**.
12. Click **Done**.

Configure the TACACS+ server

In addition to configuring remote authentication on your ExtraHop system, you must configure your TACACS+ server with two attributes, one for the ExtraHop service and one for the permission level. If you have an ExtraHop packetstore, you can optionally add a third attribute for packet capture and session key logging.

1. Log in to your TACACS+ server and navigate to the shell profile for your ExtraHop configuration.
2. For the first attribute, add `service`.
3. For the first value, add `extrahop`.
4. For the second attribute, add the privilege level, such as `readwrite`.
5. For the second value, add `1`.

For example, the following figure shows the `extrahop` attribute and a privilege level of `readwrite`.



Here is a table of available permission attributes, values, and descriptions:

Attribute	Value	Description
`setup`	`1`	Create and modify all objects and settings on the ExtraHop system and manage user access
`readwrite`	`1`	Create and modify all objects and settings on the ExtraHop system, not including Administration settings
`limited`	`1`	Create, modify, and share dashboards
`readonly`	`1`	View objects in the ExtraHop system
`personal`	`1`	Create personal dashboards for themselves and modify any dashboards that have been shared with them
`limited_metrics`	`1`	View shared dashboards
`ndrfull`	`1`	View, acknowledge, and hide security detections
`npmfull`	`1`	View, acknowledge, and hide performance detections
`packetsfull`	`1`	View and download packets stored on a connected packetstore.

Attribute	Value	Description
packetslicesonly	1	View and download packet slices on a connected packetstore.
packetsfullwithkeys	1	View and download packets and associated session keys stored on a connected packetstore.

6. (Optional) Add the following attribute to allow users to view, acknowledge, and hide security detections

Attribute	Value
ndrfull	1

7. (Optional) Add the following attribute to allow users to view, acknowledge, and hide performance detections that appear in the ExtraHop system.

Attribute	Value
npmfull	1

8. (Optional) If you have an ExtraHop packetstore, add an attribute to allow users to download packet captures or packet captures with associated session keys.

Attribute	Value	Description
packetslicesonly	1	Users with any privilege level can view and download the first 64 bytes of packets.
packetsfull	1	Users with any privilege level can view and download packets stored on a connected packetstore.
packetslicesonly	1	View and download packet slices on a connected packetstore.
packetsfullwithkeys	1	Users with any privilege level can view and download packets and associated session keys stored on a connected packetstore.

API Access

The API Access page enables you to generate, view, and manage access for the API keys that are required to perform operations through the ExtraHop REST API.

Manage API key access

Users with system and access administration privileges can configure whether users can generate API keys for the ExtraHop system. You can allow only local users to generate keys, or you can also disable API key generation entirely.

Users must generate an API key before they can perform operations through the ExtraHop REST API. Keys can be viewed only by the user who generated the key or system administrators with unlimited privileges. After a user generates an API key, they must append the key to their request headers.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **API Access**.
3. In the Manage API Access section, select one of the following options:
   - **Allow all users to generate an API key**: Local and remote users can generate API keys.
   - **Only local users can generate an API key**: Remote users cannot generate API keys.
   - **No users can generate an API key**: No API keys can be generated by any user.
4. Click **Save Settings**.

Configure cross-origin resource sharing (CORS)

Cross-origin resource sharing (CORS) allows you to access the ExtraHop REST API across domain-boundaries and from specified web pages without requiring the request to travel through a proxy server.

You can configure one or more allowed origins or you can allow access to the ExtraHop REST API from any origin. Only users with system and access administration privileges can view and edit CORS settings.

1. In the **Access Settings** section, click **API Access**.
2. In the CORS Settings section, specify one of the following access configurations.
   - To add a specific URL, type an origin URL in the text box, and then click the plus (+) icon or press ENTER.

     The URL must include a scheme, such as `HTTP` or `HTTPS`, and the exact domain name. You cannot append a path; however, you can provide a port number.
   - To allow access from any URL, select the Allow API requests from any Origin checkbox.

     Note: Allowing REST API access from any origin is less secure than providing a list of explicit origins.
3. Click **Save Settings** and then click **Done**.

Generate an API key

You must generate an API key before you can perform operations through the ExtraHop REST API. Keys can be viewed only by the user who generated the key or by users with system and access administration privileges. After you generate an API key, add the key to your request headers or the ExtraHop REST API Explorer.

Before you begin
Make sure the ExtraHop system is configured to allow API key generation.

1. In the Access Settings section, click **API Access**.
2. In the Generate an API Key section, type a description for the new key, and then click **Generate**.
3. Scroll down to the API Keys section, and copy the API key that matches your description.

You can paste the key into the REST API Explorer or append the key to a request header.

Privilege levels

User privilege levels determine which ExtraHop system and administration tasks the user can perform through the ExtraHop REST API.

You can view the privilege levels for users through the `granted_roles` and `effective_roles` properties. The `granted_roles` property shows you which privilege levels are explicitly granted to the user. The `effective_roles` property shows you all privilege levels for a user, including those received outside of the granted role, such as through a user group.

The `granted_roles` and `effective_roles` properties are returned by the following operations:

- GET /users
- GET /users/{username}

The `granted_roles` and `effective_roles` properties support the following privilege levels. Note that the type of tasks for each ExtraHop system vary by the available resources listed in the REST API Explorer and depend on the modules enabled on the system and user module access privileges.

Privilege level	Actions allowed
"system": "full"	• Enable or disable API key generation for the ExtraHop system. • Generate an API key. • View the last four digits and description for any API key on the system. • Delete API keys for any user. • View and edit cross-origin resource sharing. • Perform any administration task available through the REST API. • Perform any ExtraHop system task available through the REST API.
"write": "full"	• Generate your own API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform any ExtraHop system task available through the REST API.
"write": "limited"	• Generate an API key. • View or delete their own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform all GET operations through the REST API. • Perform metric and record queries.
"write": "personal"	• Generate an API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform all GET operations through the REST API. • Perform metric and record queries.
"metrics": "full"	• Generate an API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform metric and record queries.
"metrics": "restricted"	• Generate an API key. • View or delete your own API key.

Privilege level	Actions allowed
	• Change your own password, but you cannot perform any other administration tasks through the REST API.
"ndr": "full"	• View security detections • View and create investigations This is a module access privilege that can be granted to a user in addition to one of the following system access privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"ndr": "none"	• No access to NDR module content This is a module access privilege that can be granted to a user in addition to one of the following system access privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"npm": "full"	• View performance detections • View and create dashboards • View and create alerts This is a module access privilege that can be granted to a user in addition to one of the following system access privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"npm": "none"	• No access to NPM module content This is a module access privilege that can be granted to a user in addition to one of the following system access privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"

Privilege level	Actions allowed
"packets": "full"	• View and download packets through the `GET/packetcaptures/{id}` operation. This is an add-on privilege that can be granted to a user with one of the following privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"packets": "full_with_keys"	• View and download packets through the `GET/packetcaptures/{id}` operation. This is an add-on privilege that can be granted to a user with one of the following privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"packets": "slices_only"	• View and download the first 64 bytes of packets through the `GET/packetcaptures/{id}` operation. This is an add-on privilege that can be granted to a user with one of the following privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"

System Configuration

In the System Configuration section, you can modify the following settings.

Capture
Configure the network capture settings. (Sensors only)

Datastore
Configure an extended datastore or reset the local datastore. (Sensors only)

Device Naming
Configure the order of precedence when multiple names are found for a device.

Inactive Sources
Remove devices and applications that have been inactive between 1 and 90 days from search results.

Detection Tracking
Select whether to track detection investigations with the ExtraHop system or from an external ticketing system.

Endpoint Lookup
Configure links to an external IP address lookup tool for endpoints in the ExtraHop system.

Geomap Data Source
Modify the information in geomaps.

Open Data Streams
Send log data to a third-party system, such as a syslog system, MongoDB database, or HTTP server. (Sensors only)

Trends
Reset all trends and trend-based alerts. (Sensors only).

Backup and Restore
Create, view, or restore system backups.

Capture

The Capture page provides controls to adjust how the ExtraHop system collects your network traffic for analysis.

Exclude protocol modules

By default, all supported modules on the ExtraHop system are included in the capture unless you manually exclude them.

1. Click **System Configuration** > **Capture**.
2. Click **Excluded Protocol Modules**.
3. Add **Module to Exclude**.
4. On the Select Protocol Module to Exclude page, from the **Module Name** dropdown, select the module that you want to exclude from the capture.
5. Click **Add**.
6. On the Excluded Protocol Modules page, click **Restart Capture**.
7. After the capture restarts, click **OK**.

To re-include the module, click the red X to delete it from the Current Excluded Modules list.

Exclude MAC addresses

Add filters to exclude specific MAC addresses or vendor device traffic from the network capture

1. In the System Configuration section, click **Capture**.
2. Click **MAC Address Filters**.
3. Click **Add Filter**.
4. In the MAC Address field, type the MAC address to exclude.
5. In the Mask field, type the mask to indicate how many bits, from left to right, the filter checks against the MAC address.
6. Click **Add**.

   In the following example, the full MAC address is excluded from the capture:

   - **MAC Address:** `60:98:2D:B1:EC:42`
   - **Mask:** `FF:FF:FF:FF:FF:FF`

   In this example, only the first 24 bits are evaluated for exclusion:

   - **MAC Address:** `60:98:2D:B1:EC:42`
   - **Mask:** `FF:FF:FF:00:00:00`

To re-include a MAC address, click **Delete** to remove the address from the list.

Exclude an IP address or range

Add filters to exclude specific IP addresses and IP ranges from the network capture on the ExtraHop system.

1. Click **System Configuration** > **Capture**.
2. Click **IP Address Filters**.
3. Click **Add Filter**.
4. On the IP Address Filters page, enter either a single IP address you want to exclude, or an IP address mask in CIDR format for a range of IP addresses you want to exclude.
5. Click **Add**.

To re-include an IP address or range, click **Delete** next to the filter for each address.

Exclude a port

Add filters to exclude traffic from specific ports from the network capture on the ExtraHop system.

1. In the System Configuration section,click **Capture**.
2. Click **Port Filters**.
3. Click **Add Filter**.
4. On the Add Port Filter page, type the port you want to exclude.
   - To specify a source port you want to exclude, type the port number in the Source Port field.
   - To specify a destination port you want to exclude, type the port number in the Destination Port field.
5. From the **IP Protocol** drop-down list, select the protocol you want to exclude on the indicated port.
6. Click **Add**.

To re-include a port, click **Delete** next to the port.

Filtering and deduplication

Refer to the following table to view the effects of filtering and deduplication on metrics, packet capture, and device discovery. Deduplication is enabled by default on the system.

Packet Dropped by	MAC address filter	IP address filter	Port filter	L2 dedup	L3 dedup
Network VLAN L2 Metrics	Not collected	Not collected	Not fragmented*: Not collected Fragmented: Collected	Not collected	Collected
Network VLAN L3 Metrics	Not collected	Not collected	Not fragmented: Not collected Fragmented: Collected	Not collected	Collected
Device L2/L3 Metrics	Not collected	Not collected	Not fragmented: Not collected Fragmented, top-level: Collected Fragmented, detail: Not collected	Not collected	Collected
Global PCAP Packets	Captured	Captured	Captured	Captured	Captured
Precision PCAP Packets	Not captured	Not captured	Not captured	Not captured	Captured
L2 Device Discovery	No discovery	Discovery	Discovery	--	--
L3 Device Discovery	No discovery	No discovery	Not fragmented: No discovery Fragmented: Discovery	--	--

*For port filters, when IP fragments are present in the data feed, a port number is not determined during fragment reassembly. The ExtraHop system might collect metrics, capture packets, or discover a device even if the port filtering rule otherwise precludes it.

L2 duplicates are identical Ethernet frames. The duplicate frames do not usually exist on the wire, but are an artifact of the data feed configuration. L3 duplicates are frames that differ only in L2 header and IP TTL. These frames usually result from tapping on both sides of a router. Because these frames exist on the monitored network, they are counted at L2 and L3 in the locations referenced above. L3 deduplication is targeted toward L4 and above, for example, to avoid counting the L3 duplicates as TCP retransmissions.

Protocol classification

Protocol classification relies on specific payloads to identify custom protocols over specific ports. These protocols are Layer 7 (application-layer) protocols that sit above the Layer 4 (TCP or UDP) protocol. These applications have their own custom protocol, and they also use the TCP protocol.

The Protocol Classification page provides an interface to perform the following functions:

- List applications and ports for the following network entities:
  - Widely-known applications that are mapped to non-standard ports.
  - Lesser-known and custom networking applications.
  - Unnamed applications with TCP and UDP traffic (for example, TCP 1234).
- Add custom protocol-to-application mapping that includes the following information:

  Name

  The user-specified protocol name.

  Protocol

  The selected Layer 4 protocol (TCP or UDP).

  Source

  (Optional) The specified source port. Port 0 indicates any source port.

  Destination

  The destination port or range of ports.

  Loose Initiation

  Select this checkbox if you want the classifier to attempt to categorize the connection without seeing the connection open. ExtraHop recommends selecting loose initiation for long-lived flows.

  By default, the ExtraHop system uses loosely-initiated protocol classification, so it attempts to classify flows even after the connection was initiated. You can turn off loose initiation for ports that do not always carry the protocol traffic (for example, the wildcard port 0).
- Delete protocols with the selected application name and port mapping from the list.

  The application name and port do not display in the ExtraHop system or in reports based on any future data capture. The device will appear in reports with historical data, if the device was active and discoverable within the reported time period.
- Restart the network capture.
  - You must restart the network capture before any protocol classification changes take effect.
  - Previously-collected capture data is preserved.

The ExtraHop system recognizes most protocols on their standard ports with some exceptions. On the Performance edition, the following protocols are recognized on any port:

- AJP
- DTLS
- FIX
- HTTP
- HTTP2
- IIOP
- Java RMI
- LDAP
- RPC
- SSH
- SSL

On Reveal(x) 360, the following protocols are recognized on any port:

- ethminer
- getblocktemplate
- RDP
- RFB
- Stratum
- LDAP

- Java RMI
- IIOP

In some cases, if a protocol is communicating over a non-standard port, it is necessary to add the non-standard port on the Protocol Classification page. In these cases, it is important to properly name the non-standard port. The table below lists the standard ports for each of the protocols, along with the protocol name that must be specified when adding the custom port numbers on the Protocol Classification page.

In most cases, the name you enter is the same as the name of the protocol. The most common exceptions to this rule are Oracle (where the protocol name is TNS) and Microsoft SQL (where the protocol name is TDS).

If you add a protocol name that has multiple destination ports, add the entire port range separated by a dash (-). For example, if your protocol requires adding ports 1434, 1467, and 1489 for database traffic, type `1434-1489` in the Destination Port field. Alternatively, add each of the three ports in three separate protocol classifications with the same name.

Canonical Name	Protocol Name	Transport	Default Source Port	Default Destination Port
ActiveMQ	ActiveMQ	TCP	0	61616
AJP	AJP	TCP	0	8009
CIFS	CIFS	TCP	0	139, 445
DB2	DB2	TCP	0	50000, 60000
DHCP	DHCP	TCP	68	67
Diameter	AAA	TCP	0	3868
DICOM	DICOM	TCP	0	3868
DNS	DNS	TCP, UDP	0	53
FIX	FIX	TCP	0	0
FTP	FTP	TCP	0	21
FTP-DATA	FTP-DATA	TCP	0	20
HL7	HL7	TCP, UDP	0	2575
HTTPS	HTTPS	TCP	0	443
IBM MQ	IBMMQ	TCP, UDP	0	1414
ICA	ICA	TCP	0	1494, 2598
IKE	IKE	UDP	0	500
IMAP	IMAP	TCP	0	143
IMAPS	IMAPS	TCP	0	993
Informix	Informix	TCP	0	1526, 1585
IPSEC	IPSEC	TCP, UDP	0	1293
IPX	IPX	TCP, UDP	0	213
IRC	IRC	TCP	0	6660-6669
ISAKMP	ISAKMP	UDP	0	500
iSCSI	iSCSI	TCP	0	3260

Canonical Name	Protocol Name	Transport	Default Source Port	Default Destination Port
Kerberos	Kerberos	TCP, UDP	0	88
LDAP	LDAP	TCP	0	389, 390, 3268
LLDP	LLDP	Link Level	N/A	N/A
L2TP	L2TP	UDP	0	1701
Memcache	Memcache	TCP	0	11210, 11211
Modbus	Modbus	TCP	0	502
MongoDB	MongoDB	TCP	0	27017
MS SQL Server	TDS	TCP	0	1433
MSMQ	MSMQ	TCP	0	1801
MSRPC	MSRPC	TCP	0	135
MySQL	MySQL	TCP	0	3306
NetFlow	NetFlow	UDP	0	2055
NFS	NFS	TCP	0	2049
NFS	NFS	UDP	0	2049
NTP	NTP	UDP	0	123
OpenVPN	OpenVPN	UDP	0	1194
Oracle	TNS	TCP	0	1521
PCoIP	PCoIP	UDP	0	4172
POP3	POP3	TCP	0	143
POP3S	POP3S	TCP	0	995
PostgreSQL	PostgreSQL	TCP	0	5432
RADIUS	AAA	TCP	0	1812, 1813
RADIUS	AAA	UDP	0	1645, 1646, 1812, 1813
RDP	RDP	TCP	0	3389
Redis	Redis	TCP	0	6397
RFB	RFB	TCP	0	5900
SCCP	SCCP	TCP	0	2000
SIP	SIP	TCP	0	5060, 5061
SMPP	SMPP	TCP	0	2775
SMTP	SMTP	TCP	0	25
SNMP	SNMP	UDP	0	162
SSH	SSH	TCP	0	0
SSL	SSL	TCP	0	443

Canonical Name	Protocol Name	Transport	Default Source Port	Default Destination Port
Sybase	Sybase	TCP	0	10200
SybaseIQ	SybaseIQ	TCP	0	2638
Syslog	Syslog	UDP	0	514
Telnet	Telnet	TCP	0	23
VNC	VNC	TCP	0	5900
WebSocket	WebSocket	TCP	0	80, 443
Windows Update Delivery Optimization	Windows Update Delivery Optimization	TCP	0	7860

The name specified in the Protocol Name column in the table appears on the Protocol Classification page to classify a common protocol that communicates over non-standard ports.

Protocols in the ExtraHop system that do not appear in this table include the following:

HTTP
The ExtraHop system classifies HTTP on all ports.

HTTP-AMF
This protocol runs on top of HTTP and is automatically classified.

Protocols in this table that do not appear in the ExtraHop system include the following:

FTP-DATA
The ExtraHop system does not handle FTP-DATA on non-standard ports.

LLDP
This is a link-level protocol, so port-based classification does not apply.

Add a custom protocol classification

The following procedure describes how to add custom protocol classification labels with the TDS (MS SQL Server) protocol as an example.

By default, the ExtraHop system looks for TDS traffic on TCP port 1433. To add MS SQL Server TDS parsing on another port, complete the following steps.

1. In the System Configuration section, click **Capture**.
2. Click **Protocol Classification**.
3. Click **Add Protocol**.
4. On the Protocol Classification page, enter the following information:

   Name
   From the drop-down, select **Add custom label...**.

   Name
   Enter TDS for the custom protocol name.

   Protocol
   From the drop-down, select an L4 protocol to associate with the custom protocol (TCP in this example).

   Source
   The source port for the custom protocol. (The default value of 0 specifies any source port.)

Destination

The destination port for the custom protocol. To specify a range of ports, put a hyphen between the first and last port in the range. For example, `3400-4400`.

Loose Initiation

Select this checkbox if you want the classifier to attempt to categorize the connection without seeing the connection open. ExtraHop recommends selecting loose initiation for long-lived flows.

By default, the ExtraHop system uses loosely-initiated protocol classification, so it attempts to classify flows even after the connection was initiated. You can turn off loose initiation for ports that do not always carry the protocol traffic (for example, the wildcard port 0).

5. Click **Add**.
6. Confirm the setting change, and then click **Restart Capture** for the change to take effect. This will briefly interrupt the collection of data.
7. After the capture restarts, a confirmation message appears. Click **Done**.
8. This change has been applied to the running config. When you save the change to the running config, it will be reapplied when the ExtraHop system restarts. Click **View and Save Changes** at the top of the screen.
9. Click **Save** to write the change to the default configuration.
10. After the configuration is saved, a confirmation message appears. Click **Done**.

Database statistics now appear for any devices running TDS on the added port (in this example, 65000). This setting is applied across the capture, so you do not need to add it on a per-device basis.

Configure Device Discovery

The ExtraHop system can discover and track devices by their MAC address (L2 Discovery) or by their IP addresses (L3 Discovery). L2 Discovery offers the advantage of tracking metrics for a device even if the IP address is changed or reassigned through a DHCP request. The system can also automatically discover VPN clients.

Before you begin

Learn how device discovery and L2 discovery works in the ExtraHop system. Changing these settings affects how metrics are associated with devices.

Note: Packet brokers can filter ARP requests. The ExtraHop system relies on ARP requests to associate L3 IP addresses with L2 MAC addresses.

Discover local devices

If you enable L3 Discovery, local devices are tracked by their IP address. The system creates an L2 parent entry for the MAC address and an L3 child entry for the IP address. Over time, if the IP address changes for a device, you might see a single entry for an L2 parent with a MAC address with multiple L3 child entries with different IP addresses.

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 **Device Discovery**.
4. In the Local Device Discovery section, select from the following choices:
   - Select the **Enable local device discovery** checkbox to enable L3 Discovery.
   - Clear the **Enable local device discovery** checkbox to enable L2 Discovery.
5. Click **Save**.

Discover remote devices by IP address

You can configure the ExtraHop system to automatically discover devices on remote subnets by adding a range of IP addresses.

Note: If your ExtraHop system is configured for L2 Discovery and your remote devices request IP addresses through a DHCP relay agent, you can track devices by their MAC address, and you do not need to configure Remote L3 Discovery. Learn more about device discovery.

Important considerations about Remote L3 Discovery:

- L2 information, such as device MAC address and L2 traffic, is not available if the device is on a different network from the one being monitored by the ExtraHop system. This information is not forwarded by routers, and therefore is not visible to the ExtraHop system.
- Exercise caution when specifying CIDR notation. A /24 subnet prefix might result in 255 new devices discovered by the ExtraHop system. A wide /16 subnet prefix might result in 65,535 new devices discovered, which might exceed your device limit.
- If an IP address is removed from the Remote L3 Device Discovery settings, the IP address will persist in the ExtraHop system as a remote L3 device as long as there are existing active flows for that IP address or until the capture is restarted. After a restart, the device is listed as an inactive remote L3 device.

  If the same IP address is later added through the local data feed, that remote L3 device can transition to a local L3 device, but only if the capture process is restarted and the Local Device Discovery setting is enabled.

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 **Device Discovery**.
4. In the Remote Device Discovery section, type the IP address in the IP address ranges field. You can specify one IP address or a CIDR notation, such as `192.168.0.0/24` for an IPv4 network or `2001:db8::/32` for an IPv6 network.

   Important: Every actively communicating remote IP address that matches the CIDR block will be discovered as a single device in the ExtraHop system. Specifying wide subnet prefixes such as /16 might result in thousands of discovered devices, which might exceed your device limit.
5. Click the green plus icon (**+**) to add the IP address. You can add another IP address or range of IP addresses by repeating steps 5-6.

   Important: The capture process must be restarted when removing IP address ranges before the changes take effect. We recommend deleting all entries before restarting the capture process. The capture process does not need to be restarted when adding IP address ranges.

Discover VPN clients

Enable the discovery of internal IP addresses that are associated with VPN client devices.

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 **Device Discovery**.
4. In the VPN Client Discovery section, select from the following choices:
   - Select the **Enable VPN client discovery** checkbox to enable VPN client discovery.
   - Clear the **Enable VPN client discovery** checkbox to disable VPN client discovery.
5. Click **Save**.

SSL decryption

The ExtraHop system supports real-time decryption of SSL traffic for analysis. Before the system can decrypt your traffic, you must configure session key forwarding or upload an SSL server certificate and private key. The server certificate and private keys are uploaded over an HTTPS connection from a web browser to the ExtraHop system.

Note: Your server traffic must be encrypted through one of these supported cipher suites.

Help on this page

- Decrypt SSL traffic with session key forwarding without private keys.
  - Clear the checkbox for **Require Private Keys**.
  - Install session key forwarding software on your Linux or Windows servers.
  - Add a global port to protocol mapping for each protocol you want to decrypt.
- Decrypt SSL traffic by uploading a certificate and private key.
  - Upload a PEM certificate and RSA private key or Upload a PKCS#12/PFX file
  - Add encrypted protocols

Note: SSL decryption requires a license. However, if you have a license for MS SQL, you can also upload an SSL certificate to decrypt MS SQL traffic from these settings.

Upload a PEM certificate and RSA private key

Tip: You can export a password-protected key to add to your ExtraHop system by running the following command on a program such as OpenSSL:

```
openssl rsa -in yourcert.pem -out new.key
```

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, select the checkbox for **Require Private Keys**.
5. Click **Save**.
6. In the Private Keys section, click **Add Keys**.
7. In the Add PEM Certificate and RSA Private Key section, enter the following information:

   Name

   A descriptive name to identify this certificate and key.

   Enabled

   Clear this checkbox if you want to disable this SSL certificate.

   Certificate

   The public key certificate.

   Private Key

   The RSA private key.
8. Click **Add**.

Next steps

Add the encrypted protocols you want to decrypt with this certificate.

Upload a PKCS#12/PFX file

PKCS#12/PFX files are archived in a secure container on the ExtraHop system and contains both public and private key pairs, which can only be accessed with a password.

Tip: To export private keys from a Java KeyStore to a PKCS#12 file, run the following command on your server, where `javakeystore.jks` is the path of your Java KeyStore:

```
keytool -importkeystore -srckeystore javakeystore.jks -
destkeystore
pkcs.p12 -srcstoretype jks -deststoretype pkcs12
```

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, select the checkbox for **Require Private Keys**.
5. Click **Save**.
6. In the Private Keys section, click **Add Keys**.
7. In the Add PKCS#12/PFX File With Password section, enter the following information:

   Description

   A descriptive name to identify this certificate and key.

   Enabled

   Clear this checkbox to disable this SSL certificate.
8. Next to PKCS#12/PFX file, click **Choose File**.
9. Browse to the file and select it, then click **Open**.
10. In the Password field, type the password for the PKCS#12/PFX file.
11. Click **Add**.
12. Click **OK**.

Next steps
Add the encrypted protocols you want to decrypt with this certificate.

Add encrypted protocols
You must add each protocol that you want to decrypt for each uploaded certificate.

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 Protocol to Port Mapping by Key section, click **Add Protocol**.
5. On the Add Encrypted Protocol page, enter the following information:

   Protocol

   From the drop-down list, select the protocol you want to decrypt.

   Key

   From the drop-down list, select an uploaded private key.

   Port

   Type the source port for the protocol. By default this value is set to 443, which specifies HTTP traffic. Specify 0 to decrypt all protocol traffic.
6. Click **Add**.

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**.

Install the ExtraHop session key forwarder on a Windows server

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. Communication between the key forwarder and the sensor is encrypted with TLS 1.2 or TLS 1.3, and 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.
- Make sure the server where you install the session key forwarder trusts the SSL certificate of the ExtraHop sensor.
- Make sure your firewall rules allow connections to be initiated by the monitored server to TCP port 4873 on the sensor.

  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 2016 or Windows 2019 servers that are 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, applications that include SSL-enabled features, such as EDR agents and Windows Store applications, 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

1. Log in to the Windows server.
2. Download the latest version of the session key forwarder software.
3. Double-click the `ExtraHopSessionKeyForwarder.exe` file and click **Next**.
4. If the system prompts you to authorize the installer to run with administrator privileges, click **OK**.
5. Select the box to accept the terms of the license agreement and then click **Next**.
6. Type the hostname or IP address of the sensor where you want to forward session keys.

   Note: You can forward session keys to more than one sensor by entering comma-separated hostnames. For example:

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

7. (Optional) Select the **Advanced options** checkbox. Accept the default TCP listen port value of 598 (recommended), or type a custom port value.
8. Click **Install**.
9. When the installation completes, click **Finish**.

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

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

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

   Note: The `-q` option installs the forwarder in non-interactive mode, which does not prompt for confirmation. You can omit the `-q` option to install the forwarder in interactive mode.

   Note: You can specify multiple sensors in a comma-separated list. For example, the following command specifies two sensors:

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

   For more information about installation options, see Installation parameters.

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**.

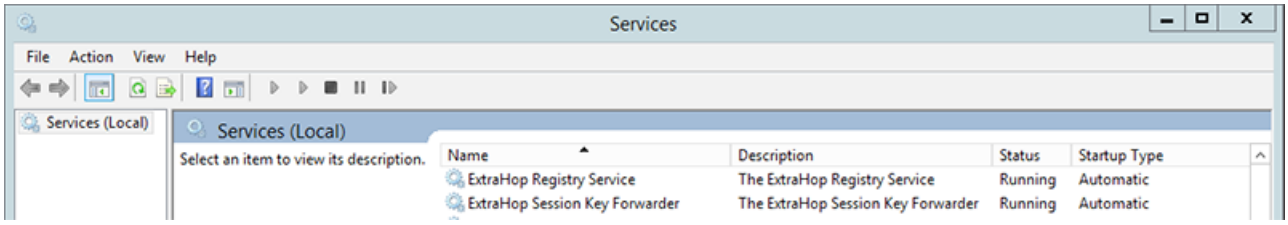
4. In the Private Key Decryption section, clear the Require Private Keys checkbox.
5. In the Global Protocol to Port Mapping section, click **Add Global Protocol**.
6. From the Protocol drop-down list, select the protocol for the traffic that you want to decrypt.
7. In the Port field, type the number 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**.

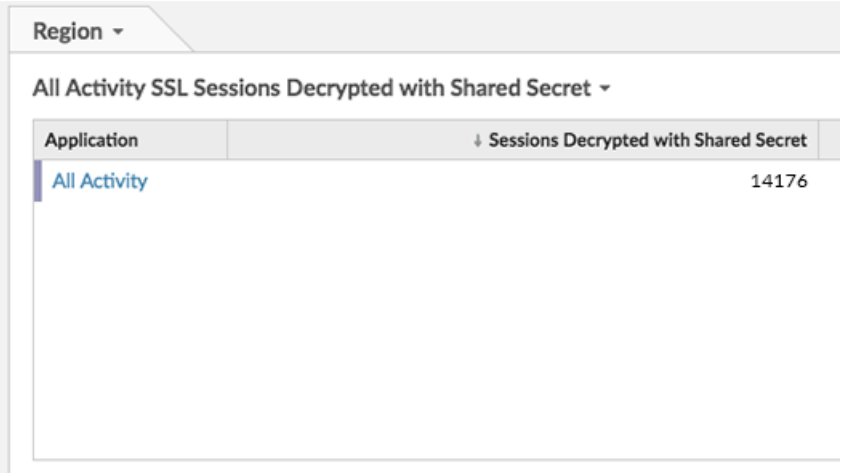
Validate session key forwarding
Perform these steps to make sure that the installation was successful and the session key forwarder is forwarding the keys to the ExtraHop system.

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 sensor is successfully receiving session keys from the monitored servers.



Verify the configuration from the command line

In cases where you might have problems with the configuration, the session key forwarder binary includes a test mode you can access from the command line to test your configuration.

1. Log in to your Windows server.
2. Open the Windows PowerShell application.
3. Perform a verification test by running the following command:

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

   Where `<eda hostname>` is the fully qualified domain name of the sensor you are forwarding secrets to.

   The following output should appear:

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

   If there is a configuration issue, troubleshooting tips appear in the output to help you correct the issue. Follow the suggestions to resolve the issue and then run the test again.
4. You can optionally test the certificate path and server name override by adding the following options to the command above.
   - Specify this option to test the certificate without adding it to the certificate store.

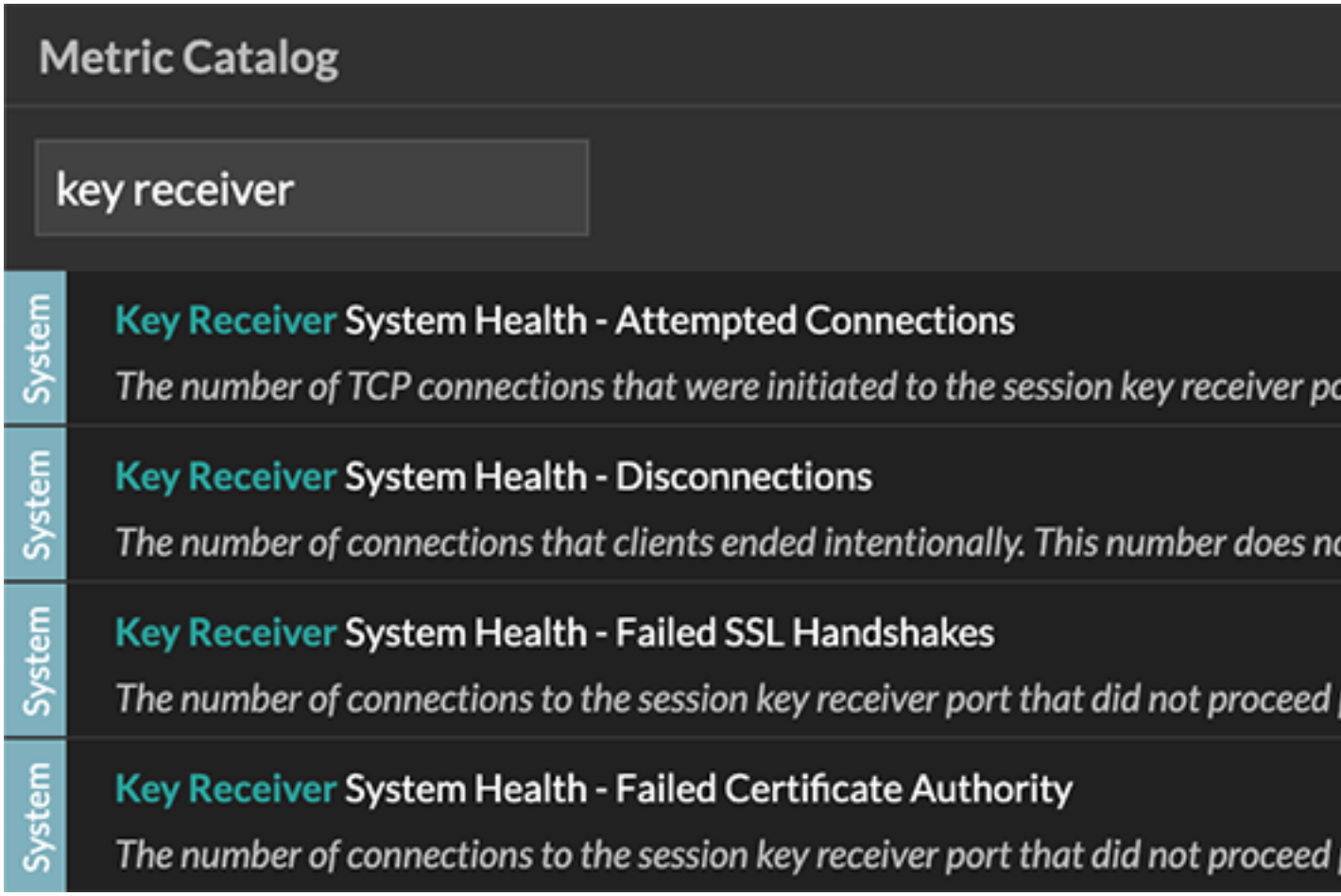
     ```
     -cert <file path to certificate>
     ```
   - Specify this option to test the connection if there is a mismatch between the ExtraHop system hostname that the forwarder knows (SERVER) and the common name (CN) that is presented in the SSL certificate of the ExtraHop system.

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

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.



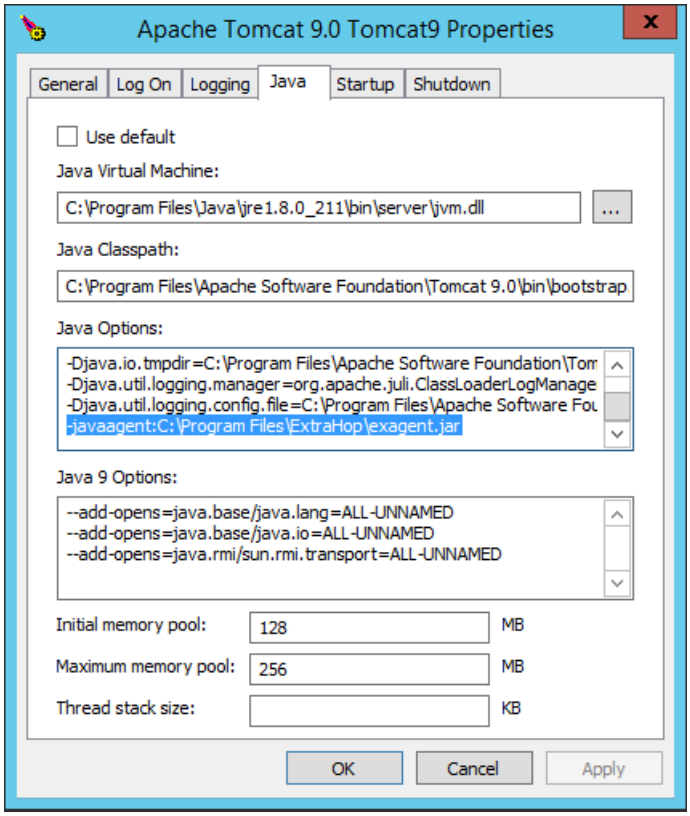
Tip: To learn how to create a new dashboard chart, see Edit a chart with the Metric Explorer.

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
```



Appendix

Troubleshoot common error messages

Error messages are saved to log files in the following locations, where TMP is the value of your TMP environment variable:

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

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 sensor.	Ensure firewall rules allow connections to be initiated by the monitored server to TCP port 4873 on the sensor.
`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 sensor, but the receiving process is not listening.	Ensure that the sensor is licensed for both the SSL Decryption and SSL Shared Secrets features.

Message	Cause	Solution
`connect: x509: certificate signed by unknown authority`	The monitored server is not able to chain up the sensor 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 sensor.
`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 sensor 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 sensor with, and that hostname matches the subject name in the sensor certificate, uninstall and reinstall the forwarder, specifying that hostname as the value of `EDA_HOSTNAME`. • If the server is required to connect to the sensor by IP address, uninstall and reinstall the forwarder, specifying the subject name from the sensor certificate as the value of `SERVERNAMEOVERRIDE`. • Re-issue the sensor 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 (sensor 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**.

- Open a PowerShell command prompt and run the following commands to remove the software and associated registry entries:

  1. ```
     $app=Get-WMIObject -class win32_product | where-object {$_.name -eq
      "ExtraHop Session Key Forwarder"}
     ```
  2. ```
     $app.Uninstall()
     ```

4. Click **Yes** to confirm.
5. After the software is removed, click **Yes** to restart the system

Installation parameters

You can specify the following MSI parameters:

MSI Installation Parameter	EDA_HOSTNAME
Registry Entry	HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\EDAHost
Description	The sensor 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 sensor SSL certificate through the server's certificate store. In some environments, the sensor 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 sensor 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 sensor hostname that the forwarder knows (EDA_HOSTNAME) and

	the common name (CN) that is presented in the SSL certificate of the sensor, 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	`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 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

Hex Value	Name (IANA)	Name (OpenSSL)	Supported Decryption
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
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

Hex Value	Name (IANA)	Name (OpenSSL)	Supported Decryption
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
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

Export the MSI file from the executable file
You can export the MSI file from the executable file to support a custom installation workflow.

Open a PowerShell command prompt and run the following command:

```
ExtraHopSessionKeyForwarderSetup.exe -e
```

Note: You can append `<directory>` to the `-e` parameter to save the `.msi` file to a directory other than the current working directory. For example, the following command saves the file to the `install_dir` directory:

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

Install the ExtraHop session key forwarder on a Linux server

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. Communication between the key forwarder and the sensor is encrypted with TLS 1.2 or TLS 1.3, and 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.
- Make sure the server where you install the session key forwarder trusts the SSL certificate of the ExtraHop sensor.
- Make sure your firewall rules allow connections to be initiated by the monitored server to TCP port 4873 on the sensor.

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 RHEL, CentOS, Fedora, or Debian-Ubuntu Linux distributions. The session key forwarder might not function correctly on other distributions.
- The session key forwarder has not been extensively tested with SELinux and might not be compatible when enabled on some Linux distributions.

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**.

Install the software
RPM-based distributions

Tip: You can install the forwarder without user interaction by specifying environment variables in the installation command.

1. Log in to your RPM-based Linux server.
2. Download the latest version of the ExtraHop session key forwarder software.
3. Open a terminal application and run the following command:

```
sudo rpm --install <path to installer file>
```

4. Open the initialization script in a text editor (vi or vim, for example).

```
sudo vi /opt/extrahop/etc/extrahop-key-forwarder.conf
```

5. Depending on how your sensors are managed, choose one of the following options:

   - For self-managed sensors, remove the hash symbol (#) before the EDA_HOSTNAME field and type the fully qualified domain name of your sensor, similar to the following example.

     ```
     EDA_HOSTNAME=discover.example.com
     ```

     Note: You can forward session keys to more than one sensor by entering comma-separated hostnames. For example:

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

   - For ExtraHop-manged sensors, remove the hash symbol (#) before the `EDA_HOSTED_PLATFORM` field and type `aws`, similar to the following example.

     ```
     EDA_HOSTED_PLATFORM=aws
     ```

6. (Optional) 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 `LOCAL_LISTENER_PORT` field. We recommended that this port remain set to the default of 598. If you change the port number, you must modify the `-javaagent` argument to account for the new port.
7. (Optional) If you prefer that syslog writes to a different facility than `local3` for key forwarder log messages, you can edit the `SYSLOG` field.
   For a self-managed sensor, the contents of the `extrahop-key-forwarder.conf` file should appear similar to the following example:

```
#EDA_HOSTED_PLATFORM=aws
EDA_HOSTNAME=sensor.example.com
LOCAL_LISTENER_PORT=598
SYSLOG=local3
ADDITIONAL_ARGS=''
```

8. Save the file and exit the text editor.
9. If your server is managing containers with the containerd runtime, you must add the following parameters to the `/opt/extrahop/etc/extrahop-key-forwarder.conf` configuration file:

   - `-containerd-enable`
   - `-containerd-socket`
   - `-containerd-state`
   - `-containerd-state-rootfs-subdir`

   For more information about these parameters and other optional parameters, see Session key forwarder options.
10. Start the `extrahop-key-forwarder` service:

```
sudo service extrahop-key-forwarder start
```

Debian-Ubuntu distributions

Tip: You can install the forwarder without user interaction by specifying environment variables in the installation command.

1. Log in to your Debian or Ubuntu Linux server.
2. Download the latest version of the ExtraHop session key forwarder software.

3. Open a terminal application and run the following command.

```
sudo dpkg --install <path to installer file>
```

4. Depending on how your sensors are managed, choose one of the following options:

   - 1. For self-managed sensors, select **direct** and then press ENTER.
     2. Type the fully qualified domain name or IP address of the ExtraHop system where session keys will be forwarded and then press ENTER.

        Note: You can forward session keys to more than one sensor by entering comma-separated hostnames. For example:

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

   - For ExtraHop managed sensors, select **hosted** and then press ENTER.

5. If your server is managing containers with the containerd runtime, you must add the following parameters to the `/opt/extrahop/etc/extrahop-key-forwarder.conf` configuration file:

   - `-containerd-enable`
   - `-containerd-socket`
   - `-containerd-state`
   - `-containerd-state-rootfs-subdir`

   For more information about these parameters and other optional parameters, see Session key forwarder options.

6. Ensure that the `extrahop-key-forwarder` service started:

   ```
   sudo service extrahop-key-forwarder status
   ```

   The following output should appear:

   ```
   extrahop-key-forwarder.service - LSB: ExtraHop Session Key Forwarder
   Loaded: loaded (/etc/rc.d/init.d/extrahop-key-forwarder; bad; vendor
    preset: disabled)
   Active: active (running) since Tue 2018-04-10 10:55:47 PDT; 5s ago
   ```

   If the service is not active, run the following command:

   ```
   sudo service extrahop-key-forwarder start
   ```

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, many Tomcat environments support customization of Java options in the `/etc/default/tomcat7` file. In the following example, adding the `-javaagent` option to the JAVA_OPTS line 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.

```
JAVA_OPTS="... -javaagent:/opt/extrahop/lib/exagent.jar
```

Validate and troubleshoot your installation
If your Linux server has network access to the ExtraHop system and the server SSL configuration trusts the certificate presented by the ExtraHop system that you specified when you installed the session key forwarder, then the configuration is complete.

In cases where you might have problems with the configuration, the session key forwarder binary includes a test mode you can access from the command-line to test your configuration.

1. Log in to your Linux server.
2. To validate your installation, perform an initial test by running the following command:

   ```
   /opt/extrahop/sbin/extrahop-agent -t=true -server <eda hostname>
   ```

   The following output should appear:

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

   If there is a configuration issue, troubleshooting tips appear in the output to help you correct the issue. Follow the suggestions to resolve the issue and then run the test again.
3. You can optionally test the certificate path and server name override by adding the following options to the command above.
   - Specify this option to test the certificate without adding it to the certificate store.

     ```
     -cert <file path to certificate>
     ```
   - Specify this option to test the connection if there is a mismatch between the ExtraHop system hostname that the forwarder knows (SERVER) and the common name (CN) that is presented in the SSL certificate of the ExtraHop system.

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

(Optional) Configure a server name override
If there is a mismatch between the ExtraHop system hostname that the forwarder knows (SERVER) and the common name (CN) that is presented in the SSL certificate of the ExtraHop system, then the forwarder must be configured with the correct CN.

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.

1. Log in to your Linux server.
2. Open the configuration file in a text editor.

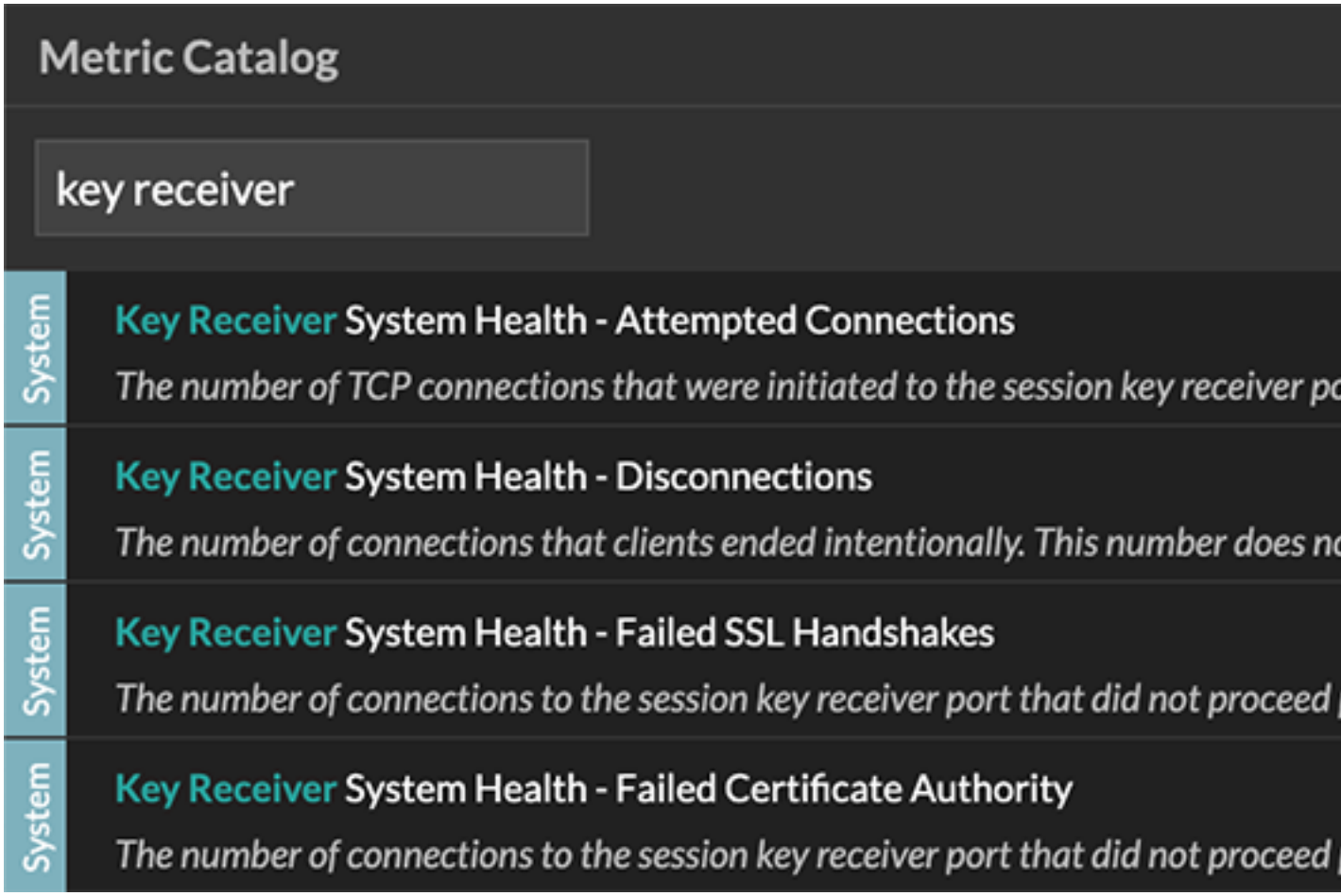
   ```
   vi /opt/extrahop/etc/extrahop-key-forwarder.conf
   ```
3. Add a `SERVER_NAME_OVERRIDE` parameter with a value of the name found in the ExtraHop system SSL certificate, similar to the following example:

   ```
   SERVER_NAME_OVERRIDE=altname.example.com
   ```
4. Save the file and exit the text editor.
5. Start the `extrahop-key-forwarder` service.

   ```
   sudo service extrahop-key-forwarder start
   ```

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.

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**.

Uninstall the software

If you no longer want the ExtraHop session key forwarder software installed, complete the following steps.

1. Log in to the Linux server.
2. Open a terminal application and choose one of the following options to remove the software.
   - For RPM-based servers, run the following command:

     ```
     sudo rpm --erase extrahop-key-forwarder
     ```
   - For Debian and Ubuntu servers, run the following command:

     ```
     sudo apt-get --purge remove extrahop-key-forwarder
     ```

Type `Y` at the prompt to confirm the software removal and then press ENTER.

3. Click **Yes** to confirm.
4. After the software is removed, click **Yes** to restart the system

Common error messages
Errors created by the session key forwarder are logged to the Linux system log file.

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 sensor.	Ensure firewall rules allow connections to be initiated by the monitored server to TCP port 4873 on the sensor.
`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 sensor, but the receiving process is not listening.	Ensure that the sensor 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 sensor certificate to a trusted Certificate Authority (CA).	Ensure that the Linux certificate store for the computer account has trusted root certificate authorities that establish a chain of trust for the sensor.
`connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANs`	An IP address was supplied as the `SERVER` parameter when installing the forwarder, but the SSL certificate presented by the sensor does not include an IP address as a Subject Alternate Name (SAN).	Select from the following three solutions. • Replace the IP address for the `SERVER` value in the `/etc/init.d/extrahop-key-forwarder` file with a hostname. The hostname must match the subject name in the sensor certificate. • If the server is required to connect to the sensor by IP address, uninstall and reinstall the forwarder, specifying the subject name from the sensor certificate as the value of `server-name-override`. • Re-issue the sensor certificate to include an IP Subject Alternative Name

Message	Cause	Solution
		(SAN) for the given IP address.

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 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

Hex Value	Name (IANA)	Name (OpenSSL)	Supported Decryption
0x9C	TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Cert RSA + Cert
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
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Cert

Hex Value	Name (IANA)	Name (OpenSSL)	Supported Decryption
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

Session key forwarder options
You can configure the session key forwarder by editing the `/opt/extrahop/etc/extrahop-key-forwarder.conf` file.

The table below lists all of the configurable options.

Important: If you add options to `extrahop-key-forwarder.conf` that do not have dedicated variables, they must be in the `ADDITIONAL_ARGS` field. For example:

```
ADDITIONAL_ARGS="-v=true -libcrypto=/some/path/libcrypto.so
-libcrypto=/some/other/path/libcrypto.so"
```

Option	Description
`-cert <path>`	Specifies the path to the server certificate. Only specify this option if the server certificate is not signed by a trusted certificate authority.
`-containerd-enable`	Enables the enumeration of containers managed with the containerd runtime. This option is disabled by default. You must type `-containerd-enable` to enable containerd support.
`-containerd-socket <string>`	The full path of the containerd socket file.
`-containerd-state <string>`	The full path of the containerd state directory.
`-containerd-state-rootfs-subdir <string>`	The relative path of the `rootfs` subdirectory of the containerd state directory.
`-docker-enable`	Enables the enumeration of Docker containers. This option is enabled by default. You must type `-docker-enable=false` to disable Docker support.
`-docker-envoy <path>`	Specifies additional Envoy paths within Docker containers. You can specify this option multiple times.
`-docker-go-binary <value>`	Specifies glob patterns to find Go binaries within Docker containers. You can specify this option multiple times.
`-docker-libcrypto <path>`	Specifies the path to libcrypto within Docker containers. You can specify this option multiple times.

Option	Description
`-envoy <path>`	Specifies additional Envoy paths on the host. You can specify this option multiple times.
`-go-binary <value>`	Specifies glob patterns to find Go binaries. You can specify this option multiple times.
`-hearbeat-interval`	Specifies the time interval in seconds between heartbeat messages. The default interval is 30 seconds.
`-host-mount-path <path>`	Specifies the path where the host file system is mounted when running the session key forwarder inside a container.
`-hosted <platform>`	Specifies that the agent is running in the specified hosted platform. The platform is currently limited to `aws`.
`-ldconfig-cache <path>`	Specifies the path to the ldconfig cache, ld.so.cache. The default path is `/etc/ld.so.cache`. You can specify this option multiple times.
`-libcrypto <path>`	Specifies the path to the OpenSSL library, `libcrypto`. You can specify this option multiple times if you have multiple installations of OpenSSL.
`-no-docker-envoy`	Disables Envoy support within Docker containers.
`-no-envoy`	Disables Envoy support on the host.
`-openssl-discover`	Automatically discovers `libcrypto` implementations. The default value is "true". You must type `-openssl-discover=false` to disable OpenSSL decryption.
`-pidfile <path>`	Specifies the file where this server records its process ID (PID).
`-port <value>`	Specifies the TCP port that the sensor is listening on for forwarded session keys. The default port is 4873.
`-server <string>`	Specifies the fully qualified domain name of the ExtraHop Discover appliance.
`-server-name-override <value>`	Specifies the subject name from the sensor certificate. Specify this option if this server can only connect to the packet sensor by IP address.
`-syslog <facility>`	Specifies the facility sent by the key forwarder. The default facility is local3.
`-t`	Perform a connectivity test. You must type `-t=true` to run with this option.
`-tcp-listen-port <value>`	Specifies the TCP port that the key forwarder is listening on for forwarded session keys.
`-username <string>`	Specifies the user that the session key forwarder runs under after the forwarder software is installed.

Option	Description
`-v`	Enable verbose logging. You must type `-v=true` to run with this option.

Linux environment variables

The following environment variables enable you to install the session key forwarder without user interaction.

Variable	Description	Example
`EXTRAHOP_CONNECTION_MODE`	Specifies the connection mode to the session key receiver. Options are `direct` for self-managed sensors and `hosted` for ExtraHop-managed sensors.	`sudo EXTRAHOP_CONNECTION_MODE=hosted rpm --install extrahop-key-forwarder.x86_64.rpm`
`EXTRAHOP_EDA_HOSTNAME`	Specifies the fully qualified domain name of the self-managed sensor.	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c dpkg --install extrahop-key-forwarder_amd64.deb`
`EXTRAHOP_LOCAL_LISTENER_PORT`	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 `LOCAL_LISTENER_PORT` field. We recommended that this port remain set to the default of 598. If you change the port number, you must modify the `-javaagent` argument to account for the new port.	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_LOCAL_LISTENER_PORT=900 rpm --install extrahop-key-forwarder.x86_64.rpm`
`EXTRAHOP_SYSLOG`	Specifies the facility, or machine process, that created the syslog event. The default facility is `local3`, which is system daemon processes.	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_SYSLOG=local1 dpkg --install extrahop-key-forwarder_amd64.deb`
`EXTRAHOP_ADDITIONAL_ARGS`	Specifies additional key forwarder options.	`sudo EXTRAHOP_CONNECTION_MODE=hosted EXTRAHOP_ADDITIONAL_ARGS="-v=true -libcrypto=/some/path/libcrypto.so libcrypto=/some/other/path/libcrypto.so" rpm --install extrahop-key-forwarder.x86_64.rpm`

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 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
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

Hex Value	Name (IANA)	Name (OpenSSL)	Supported Decryption
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
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

Store SSL session keys on connected packetstores

When session key forwarding is configured on an ExtraHop system that is connected to a packetstore, the ExtraHop system can store encrypted session keys along with the collected packets.

Before you begin
Learn more about decrypting packets with stored keys.

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 Session Key Storage**.
4. Select **Enable SSL Session Key Storage**.
5. Click **Save**.

Next steps

For more information about downloading session keys, see Download session keys with packet captures.

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**.

Decrypt domain traffic with a Windows domain controller

The ExtraHop system can be configured to retrieve and store domain keys from a domain controller. When the system observes encrypted traffic that matches the stored keys, all of the Kerberos-encrypted traffic in the domain is decrypted for supported protocols. The system only synchronizes Kerberos and NTLM decryption keys and does not modify any other properties in the domain.

A domain controller like Active Directory is a frequent target for attackers because a successful attack campaign yields high-value targets. Critical attacks can be obscured by Kerberos or NTLM decryption, such as Golden Ticket, PrintNightmare, and Bloodhound. Decrypting this type of traffic can provide deeper insight for security detections.

You can enable decryption on an individual sensor or through an integration on Reveal(x) 360.

The following requirements must be met for decryption:

- You must have an Active Directory domain controller (DC) that is not configured as a Read-only Domain Controller (RODC).
- Only Windows Server 2016 and Windows Server 2019 are supported.
- Only one domain controller can be configured on a sensor, which means you can decrypt the traffic from one domain per sensor.
- The ExtraHop system synchronizes keys for up to 50,000 accounts in a configured domain. If your DC has more than 50,000 accounts, some traffic will not be decrypted.
- The ExtraHop system must observe the network traffic between the DC and connected clients and servers.
- The ExtraHop system must be able to access the domain controller over the following ports: TCP 88 (Kerberos), TCP 445 (SMB), TCP 135 (RPC), and TCP ports 49152-65535 (RPC dynamic range).

Warning: If you enable these settings, the ExtraHop system is granted access to all of the account keys in the Windows domain. The ExtraHop system should be deployed at the same security level as the domain controller. Here are some best practices to consider:

- Strictly limit end-user access to sensors that are configured with access to the domain controller. Ideally, only permit end-user access to a connected console.
- Configure sensors with an identity provider that has strong authentication features such as two-factor or multi-factor authentication.
- Restrict inbound and outbound traffic to and from the sensor to only what is needed.
- In Active Directory, limit the Logon Workstations for the account to only communicate with the domain controller that the ExtraHop system is configured with.

Connect a domain controller to a sensor

Before you begin
You must have a user account with setup or system and access administration privileges on the sensor.

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 **Domain Controller**.
4. Select the **Enable connection to the domain controller** checkbox.
5. Complete the following fields:
   - **Hostname:** The fully qualified domain name of the domain controller.
   - **Computer Name (sAMAccountName):** The name of the domain controller.
   - **Realm Name:** The Kerberos realm name of the domain controller.
   - **User Name:** The name of a user who is a member of the built-in Administrators group for the domain (not to be confused with the Domain Admins group). To prevent possible connection errors, specify a user account created after the domain controller was established.
   - **Password:** The password of the privileged user.
6. Click **Test Connection** to confirm that the sensor can communicate with the domain controller.
7. Click **Save**.

Connect a domain controller to a Reveal(x) 360 sensor

Before you begin
Your user account must have privileges on Reveal(x) 360 for System and Access Administration.

1. Log into Reveal(x) 360.
2. Click the System Settings icon and then click **Integrations**.
3. Click the **Microsoft Protocol Decryption** tile.
4. Complete the following fields to specify credentials for the Microsoft Active Directory domain controller you want to connect to a Reveal(x) 360 sensor:
   - **Hostname:** The fully qualified domain name of the domain controller.
   - **Computer Name (sAMAccountName):** The name of the domain controller.
   - **Realm Name:** The Kerberos realm name of the domain controller.
   - **User Name:** The name of a user who is a member of the built-in Administrators group for the domain (not to be confused with the Domain Admins group). To prevent possible connection errors, specify a user account created after the domain controller was established.
   - **Password:** The password of the privileged user.

5. From the drop-down list, select the Reveal(x) 360 sensor the domain controller will connect to. Only one domain controller can be connected to a Reveal(x) 360 sensor.
6. Click **Test Connection** to confirm that the sensor can communicate with the domain controller.
7. Click **Save**.

Validate the configuration settings

To validate that the ExtraHop system is able to decrypt traffic with the domain controller, create a dashboard that identifies successful decryption attempts.

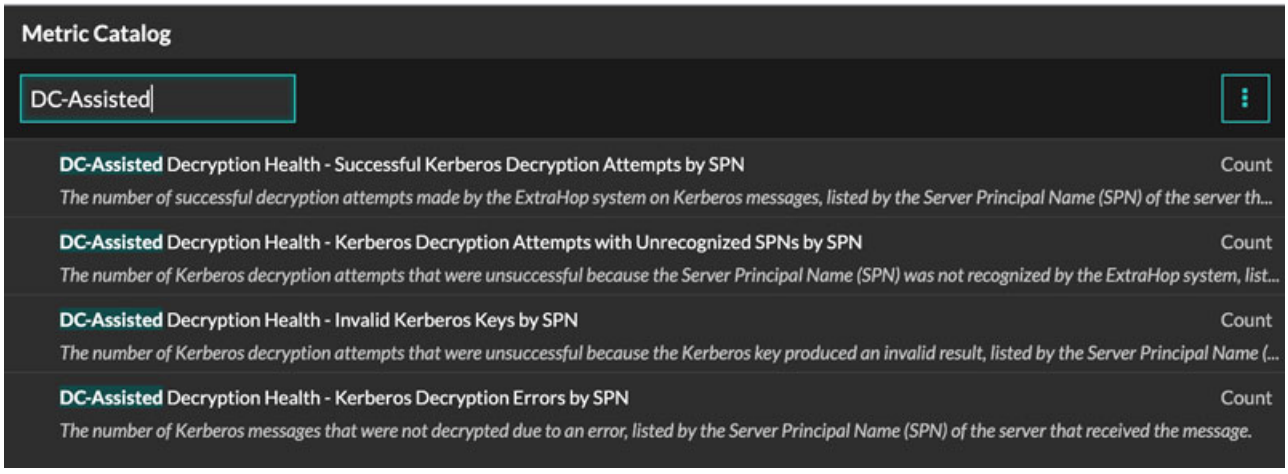
1. Create a new dashboard.
2. Click the chart widget to add the metric source.
3. Click **Add Source**.
4. In the Sources field, type the name of the sensor communicating with a domain controller and then select the sensor from the list.
5. In the Metrics field, type `DC` in the search field and then select **DC-Assisted Decryption Health - Successful Kerberos Decryption Attempts by SPN**.
6. Click **Save**.

The chart appears with a count of successful decryption attempts.

Additional system health metrics

The ExtraHop system provides metrics that you can add to a dashboard to monitor DC-assisted decryption health and functionality.

To view a list of available metrics, click the System Settings icon and then click **Metric Catalog**. Type `DC-Assisted` in the filter field to display all available DC-assisted decryption metrics.



Import external data to your ExtraHop system

The ExtraHop Open Data Context API enables you to import data from an external host into the session table on your ExtraHop sensor. That data can then be accessed to create custom metrics that you can add to ExtraHop charts, store in records on a recordstore, or export to a external analysis tool.

After you enable the Open Data Context API on your sensor, you can import data by running a Python script from a memcached client on an external host. That external data is stored in key-value pairs, and can be accessed by writing a trigger.

For example, you might run a memcached client script on an external host to import CPU load data into the session table on your sensor. Then, you can write a trigger that accesses the session table and commits the data as custom metrics.

Warning: The connection between the external host and the ExtraHop system is not encrypted and should not transmit sensitive information.

Enable the Open Data Context API

You must enable the Open Data Context API on your sensor before it can receive data from an external host.

Before you begin

- You must have setup or system and access administration privileges to access the Administration page on your ExtraHop system.
- If you have a firewall, your firewall rules must allow external hosts to access the specified TCP and UDP ports. The default port number is 11211.

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 **Open Data Context API**.
4. Click **Enable Open Data Context API**.
5. Configure each protocol that you want to allow external data transmissions through:

Option	Description
TCP	1. Select the **TCP Port enabled** checkbox. 2. In the **TCP Port** field, type the port number that will receive external data.
UDP	1. Select the **UDP Port enabled** checkbox. 2. In the **UDP Port** field, type the port number that will receive external data.

6. Click **Save and Restart Capture**.

   Important: The sensor will not collect metrics while it is restarting.

7. Click **Done**.

Write a Python script to import external data

Before you can import external data into the session table on your sensor, you must write a Python script that identifies your sensor and contains the data you want to import into the session table. The script is then run from a memcached client on the external host.

This topic provides syntax guidance and best practices for writing the Python script. A complete script example is available at the end of this guide.

Before you begin

Ensure that you have a memcached client on the external host machine. You can install any standard memcached client library, such as http://libmemcached.org/ or https://pypi.python.org/pypi/pymemcache. The sensor acts as a memcached version 1.4 server.

Here are some important considerations about the Open Data Context API:

- The Open Data Context API supports most memcached commands, such as `get`, `set`, and `increment`.
- All data must be inserted as strings that are readable by the sensor. Some memcached clients attempt to store type information in the values. For example, the Python memcache library stores floats as pickled values, which cause invalid results when calling `Session.lookup` in triggers. The following Python syntax correctly inserts a float as a string:

```
mc.set("my_float", str(1.5))
```

- Although session table values can be almost unlimited in size, committing large values to the session table might cause performance degradation. In addition, metrics committed to the datastore must be 4096 bytes or fewer, and oversized table values might result in truncated or imprecise metrics.
- Basic statistics reporting is supported, but detailed statistics reporting by item size or key prefix is not supported.
- Setting item expiration when adding or updating items is supported, but bulk expiration through the `flush` command is not supported.
- Keys expire at 30-second intervals. For example, if a key is set to expire in 50 seconds, it can take from 50 to 79 seconds to expire.
- All keys set with the Open Data Context API are exposed through the `SESSION_EXPIRE` trigger event as they expire. This behavior is in contrast to the Trigger API, which does not expose expiring keys through the `SESSION_EXPIRE` event.

1. In a Python editor, open a new file.
2. Add the IP address of your sensor and the port number where the memcached client will send data, similar to the following syntax:

```
client = memcache.Client(["eda_ip_address:eda_port"])
```

3. Add the data you want to import to the session table through the memcached `set` command, formatted in key-value pairs, similar to the following syntax:

```
client.set("some_key", "some_value")
```

4. Save the file.
5. Run the Python script from the memcached client on the external host.

Write a trigger to access imported data
You must write a trigger before you can access the data in the session table.

Before you begin
This topic assumes experience with writing triggers. If you are unfamiliar with triggers, check out the following topics:

- Triggers
- Build a trigger
- Learn how to build a trigger to collect custom metrics

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Triggers**.
3. Click **New**, and then click the Configuration tab.
4. In the **Name** field, type a unique name for the trigger.
5. In the **Events** field, begin typing an event name and then select an event from the filtered list.

6. Click the **Editor** tab.
7. In the Trigger Script textbox, write a trigger script that accesses and applies the session table data. A complete script example is available at the end of this guide.

   The script must include the `Session.lookup` method to locate a specified key in the session table and return the corresponding value.

   For example, the following code looks up a specific key in the session table to return the corresponding value, and then commits the value to an application as a custom metric:

```
var key_lookup = Session.lookup("some_key");
                 Application("My
 App").metricAddDataset("my_custom_metric",
                 key_lookup);
```

   Tip: You can also add, modify, or delete key-value pairs in the session table through methods described in the Session class of the ExtraHop Trigger API Reference.
8. Click **Save and Close**.

Next steps
You must assign the trigger to a device or device group. The trigger will not run until it has been assigned.

Open Data Context API example
In this example, you will learn how to check the reputation score and potential risk of domains that are communicating with devices on your network. First, the example Python script shows you how to import domain reputation data into the session table on your sensor. Then, the example trigger script shows you how to check IP addresses on DNS events against that imported domain reputation data and how to create a custom metric from the results.

Example Python script

This Python script contains a list of 20 popular domain names and can reference domain reputation scores obtained from a source such as DomainTools.

This script is a REST API that accepts a POST operation where the body is the domain name. Upon a POST operation, the memcached client updates the session table with the domain information.

```
#!/usr/bin/python
import flask
import flask_restful
import memcache
import sqlite3

top20 = { "google.com", "facebook.com", "youtube.com", "twitter.com",
          "microsoft.com", "wikipedia.org", "linkedin.com",
          "apple.com","adobe.com", "wordpress.org", "instagram.com",
          "wordpress.com", "vimeo.com", "blogspot.com", "youtu.be",
          "pinterest.com", "yahoo.com", "goo.gl", "amazon.com", "bit.ly}

dnsnames = {}

mc = memcache.Client(['10.0.0.115:11211'])

for dnsname in top20:
    dnsnames[dnsname] = 0.0

dbc = sqlite3.Connection('./dnsreputation.db')
cur = dbc.cursor()
cur.execute('select dnsname, score from dnsreputation;')
for row in cur:
    dnsnames[row[0]] = row[1]
dbc.close()
```

```
app = flask.Flask(__name__)
api = flask_restful.Api(app)

class DnsReputation(flask_restful.Resource):
    def post(self):
        dnsname = flask.request.get_data()
        #print dnsname
        mc.set(dnsname, str(dnsnames.get(dnsname, 50.0)), 120)
        return 'added to session table'

api.add_resource(DnsReputation, '/dnsreputation')

if __name__ == '__main__':
     app.run(debug=True,host='0.0.0.0')
```

Example trigger script

This example trigger script canonicalizes (or converts) IP addresses that are returned on DNS events into domain names, and then checks for the domain and its reputation score in the session table. If the score value is greater than 75, the trigger adds the domain to an application container called "DNSReputation" as a detail metric called "Bad DNS reputation".

```
//Configure the following trigger settings:
//Name: DNSReputation
//Debugging: Enabled
//Events: DNS_REQUEST, DNS_RESPONSE

if (DNS.errorNum != 0 || DNS.qname == null
    || DNS.qname.endsWith("in-addr.arpa") || DNS.qname.endsWith("local")
    || DNS.qname.indexOf('.') == -1 ) {
    // error or null or reverse lookup, or lookup of local namereturn
    return;
}

//var canonicalname = DNS.qname.split('.').slice(-2).join('.');
var canonicalname = DNS.qname.substring(DNS.qname.lastIndexOf('.',
 DNS.qname.lastIndexOf('.')-1)+1)

//debug(canonicalname);


//Look for this DNS name in the session table
var score = Session.lookup(canonicalname)
if (score === null) {
    // Send to the service for lookup
    Remote.HTTP("dnsrep").post({path: "/dnsreputation", payload:
 canonicalname});
} else {
    debug(canonicalname + ':' +score);
    if (parseFloat(score) > 75) {
  //Create an application in the ExtraHop system and add custom metrics
        //Note: The application is not displayed in the ExtraHop system
 after the
  //initial request, but is displayed after subsequent requests.
        Application('DNSReputation').metricAddDetailCount('Bad DNS
 reputation', canonicalname + ':' + score, 1);
    }
}
```

Install the packet forwarder on a Linux server

You must install the packet forwarder software on each server to be monitored to forward packets to the ExtraHop system.

RPCAP installation files and instructions are available from the ExtraHop Downloads and Resources web page.

Download and install on RPM-based systems

1. Download the RPCAP installer file from the ExtraHop Downloads and Resources web page.
2. Install the software on the server by running the following command:

```
sudo rpm -i rpcapd-<extrahop_firmware_version>.x86_64.rpm
```

3. Open and edit the `rpcapd.ini` file in a text editor by running one of the following commands:

```
vim /opt/extrahop/etc/rpcapd.ini
```

```
nano /opt/extrahop/etc/rpcapd.ini
```

Example output:

```
#ActiveClient = <TARGETIP>,<TARGETPORT>
NullAuthPermit = YES
```

Replace <TARGETIP> with the IP address of the ExtraHop system, and <TARGETPORT> with 2003. In addition, uncomment the line by deleting the number sign (#) at the beginning of the line.

For example:

```
ActiveClient = 10.10.10.10,2003
NullAuthPermit = YES
```

4. Start sending traffic to the ExtraHop system by running the following command:

```
sudo /etc/init.d/rpcapd start
```

5. (Optional) Verify the ExtraHop system is receiving traffic by running the following command:

```
sudo service rpcapd status
```

Download and install on other Linux systems

1. Download the RPCAP installer file from the ExtraHop Downloads and Resources web page.
2. Install the software on the server by running the following commands:
   a) Extract the packet forwarder files from the archive file:

```
tar xf rpcapd-<extrahop_firmware_version>.tar.gz
```

   b) Change to the `rpcapd` directory:

```
cd rpcapd
```

   c) Run the installation script:

```
sudo ./install.sh <extrahop_ip> 2003
```

3. (Optional) Verify the ExtraHop system is receiving traffic by running the following command:

```
sudo /etc/init.d/rpcapd status
```

To run the software on servers with multiple interfaces, See Monitoring multiple interfaces on a Linux server.

Download and install on Debian-based systems
To download and install the packet forwarder on Debian-based systems:

1. Download the RPCAP installer file from the ExtraHop Downloads and Resources web page.
2. Install the software on the server by running the following command:

```
sudo dpkg -i rpcapd_<extrahop_firmware_version>_amd64.deb
```

3. At the prompt, enter the ExtraHop system IP address, confirm the default connection to port 2003, and press ENTER.
4. (Optional) Verify the ExtraHop system is receiving traffic by running the following commands:

```
sudo dpkg --get-selections | grep rpcapd
```

```
sudo service rpcapd status
```

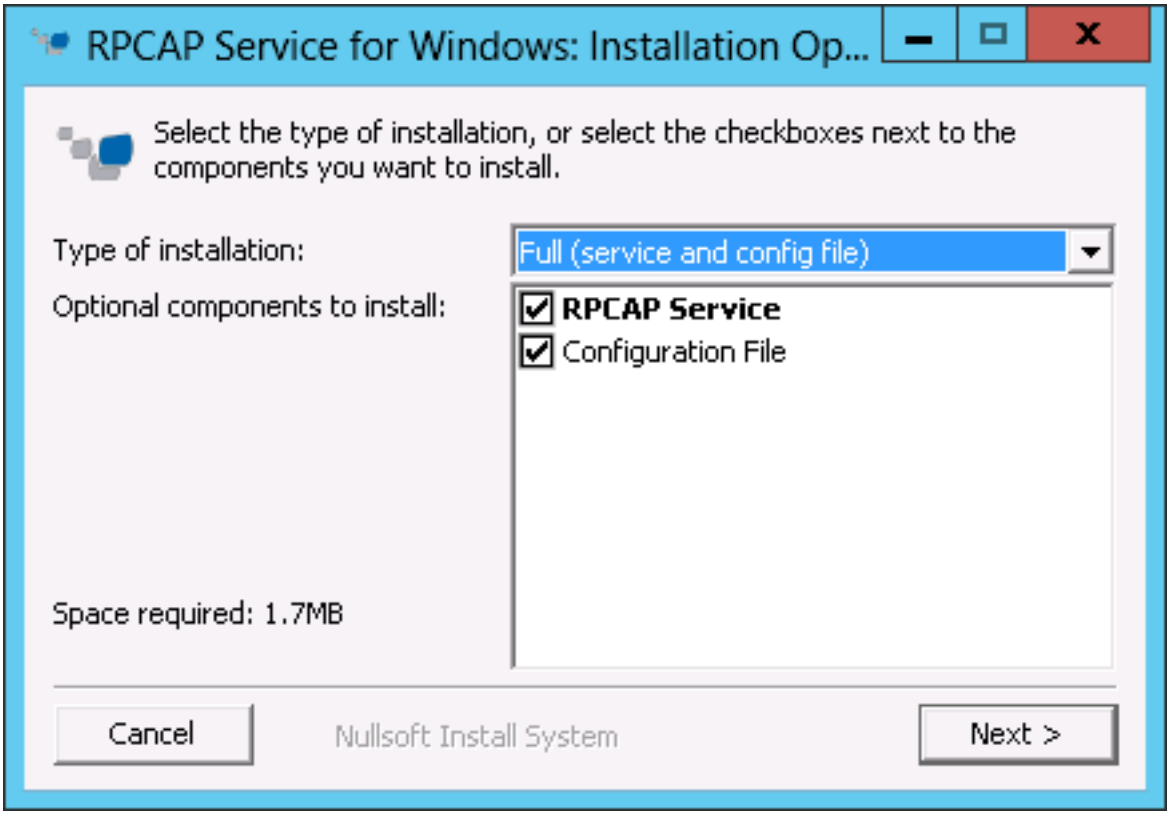
5. (Optional) To change the ExtraHop system IP address, port number, or arguments to the service, run the following command.

```
sudo dpkg-reconfigure rpcapd
```

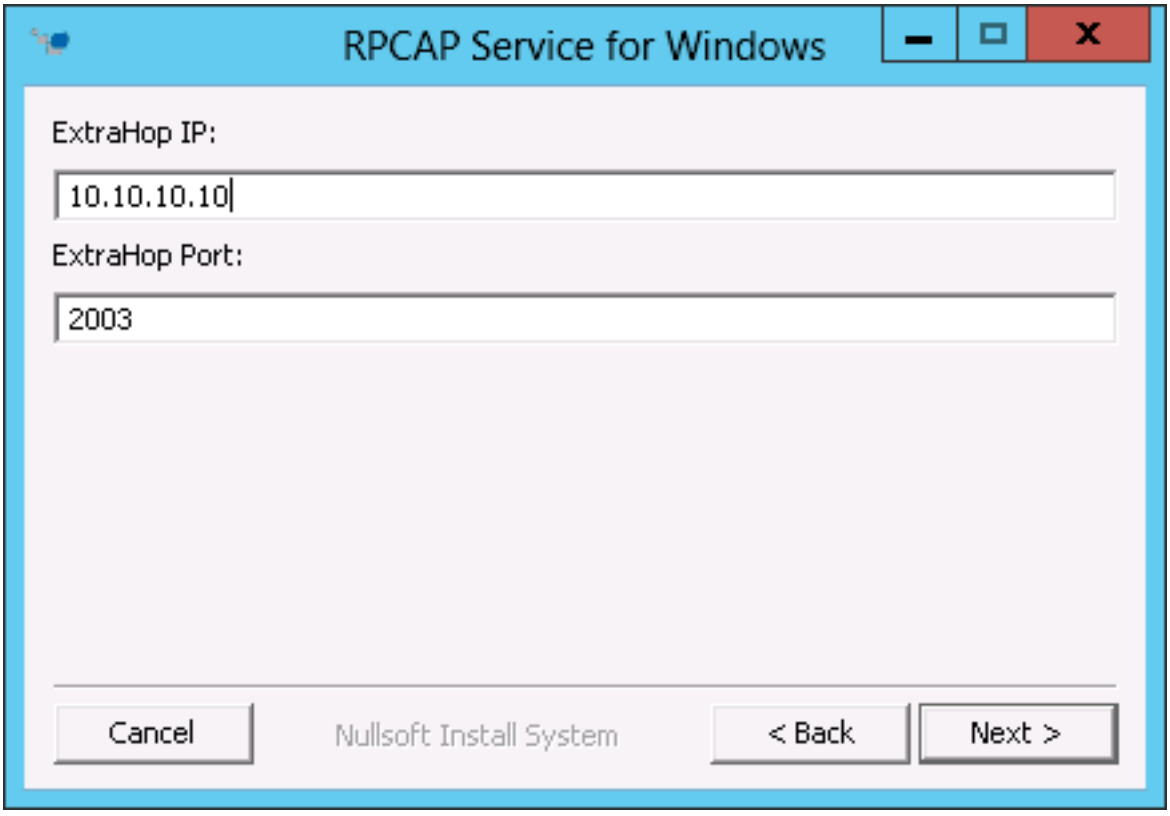
Install the packet forwarder on a Windows server

You must install the packet forwarder software on each server to be monitored in order to forward packets to the ExtraHop system.

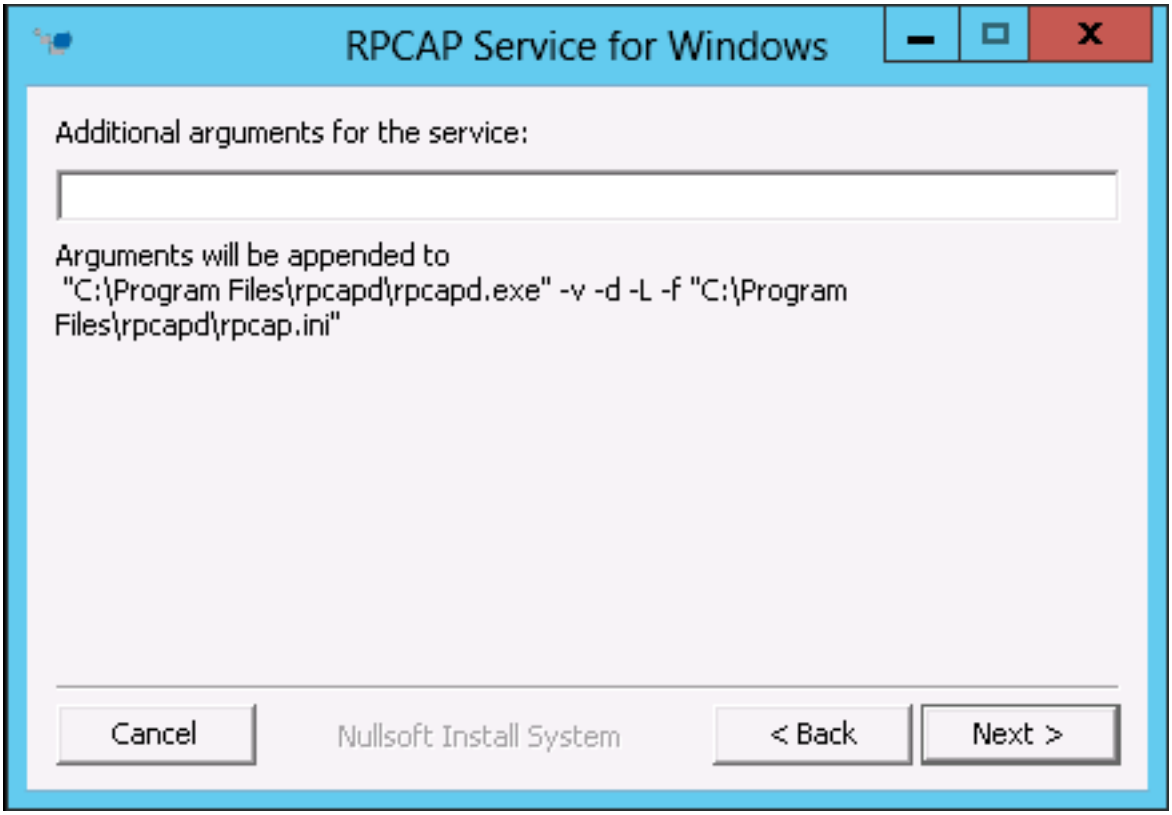
1. Download the RPCAP Service for Windows installer file from the ExtraHop Downloads and Resources web page.
2. Double-click the file to start the installer.
3. In the wizard, select the components to install.



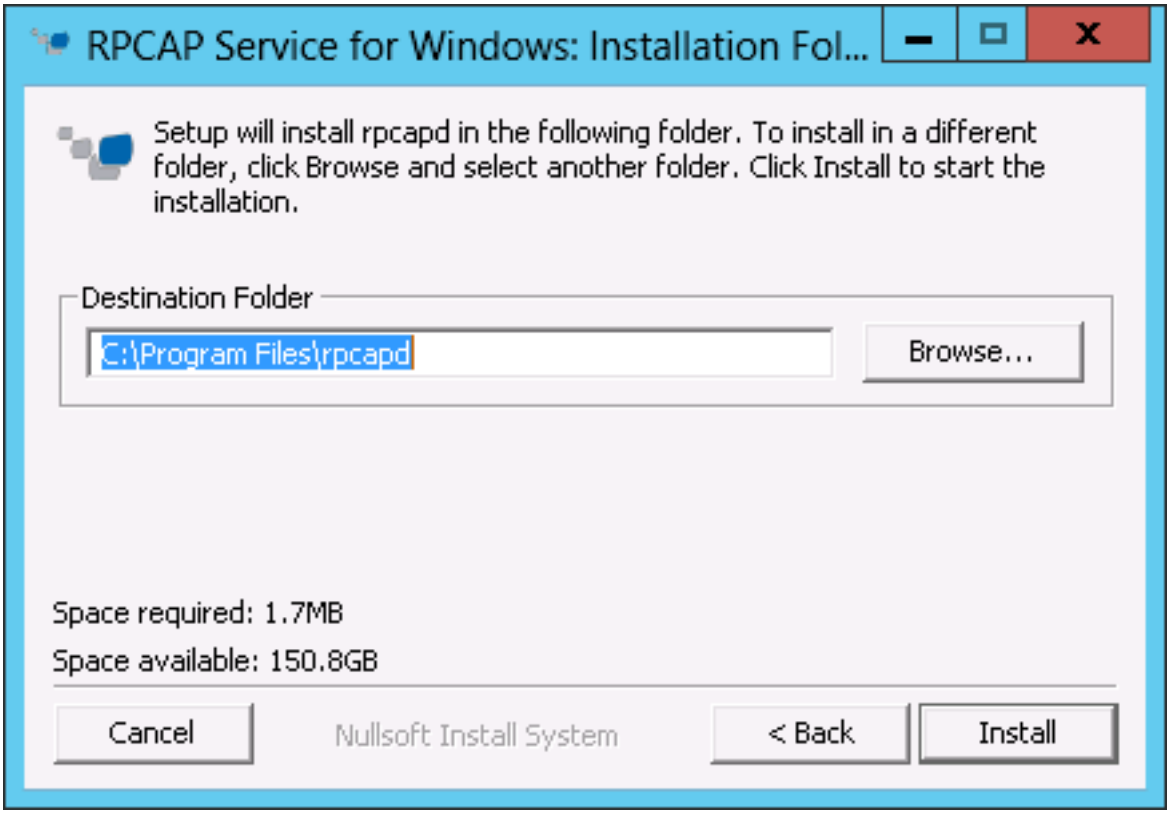
4. Complete the **ExtraHop IP** and **ExtraHop Port** fields and click **Next**. The default port is 2003.



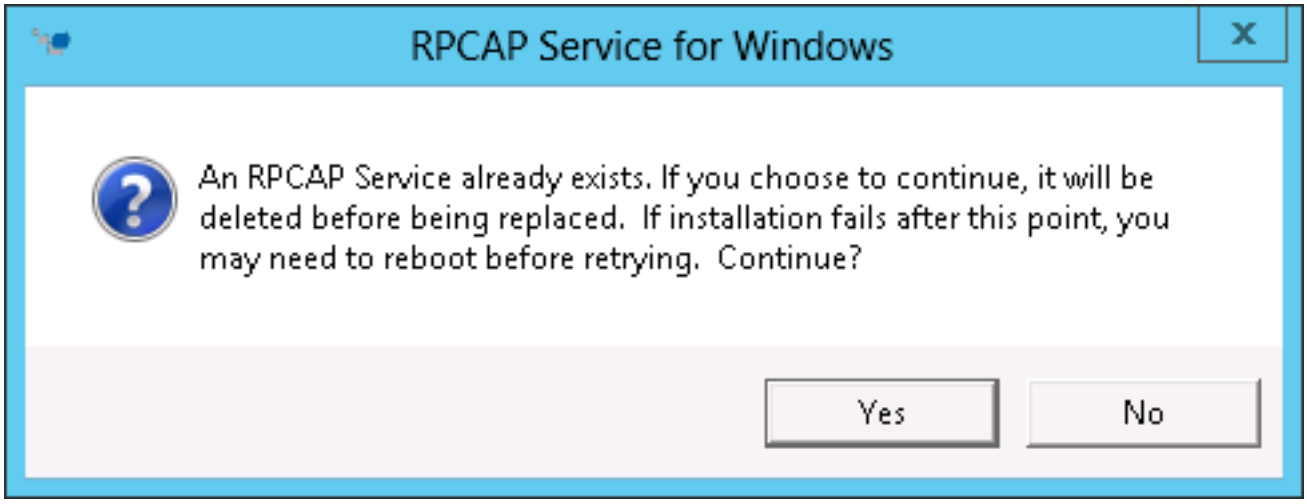
5. (Optional) Enter additional arguments in the text box and click **Next**.



6. Browse to and select the destination folder to install RPCAP Service.



7. If RPCAP Service was previously installed, click **Yes** to delete the previous service.



8. When the installation is complete, click **Close**.

Monitoring multiple interfaces on a Linux server

For servers with multiple interfaces, you can configure the packet forwarder to forward packets from a particular interface or from multiple interfaces by editing its configuration file on the server.

To edit the configuration file, complete the following steps.

1. After installing the packet forwarder, open the configuration file, `/opt/extrahop/etc/rpcapd.ini`.

   The configuration file contains this text or similar:

   ```
   ActiveClient = 10.0.0.100,2003
   NullAuthPermit = YES
   ```

2. Modify the existing `ActiveClient` line and create an `ActiveClient` line for each additional interface to be monitored. Specify each interface by its interface name or IP address.

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_name>
   ```

   or

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_address>
   ```

   Where *<interface_name>* is the name of the interface from which you want to forward packets, and *<interface_address>* is the IP address of the interface from which the packets are forwarded. The *<interface_address>* variable can be either the IP address itself, such as 10.10.1.100, or a CIDR specification (network IP address/subnet prefix length) that contains the IP address, such as 10.10.1.0/24.

   For every `ActiveClient` line, the packet forwarder independently forwards packets from the interface specified in the line.

   The following is an example of the configuration file specifying two interfaces by the interface name:

   ```
   ActiveClient = 10.10.6.45, 2003, ifname=eth0
   ActiveClient = 10.10.6.45, 2003, ifname=eth1
   NullAuthPermit = YES
   ```

The following is an example of the configuration file specifying two interfaces by the interface IP address:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
```

The following is an example of the configuration file specifying two interfaces using CIDR specifications that contain the interface IP address:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
```

3. Save the configuration file. Make sure to save the file in ASCII format to prevent errors.
4. Restart the packet forwarder by running the command:

```
sudo /etc/init.d/rpcapd restart
```

Note: To reinstall the packet forwarder after changing the configuration file, run the installation command and replace *<extrahop_ip>* and *<extrahop_port>* with the `–k` flag in order to preserve the modified configuration file. For example:

```
sudo sh ./install-rpcapd.sh –k
```

Monitoring multiple interfaces on a Windows server

For servers with multiple interfaces, you can configure the packet forwarder to forward packets from a particular interface or from multiple interfaces by editing its configuration file on the server.

To edit the configuration file, complete the following steps.

1. After installing the packet forwarder on the server, open the configuration file: `C:\Program Files \rpcapd\rpcapd.ini`

   The configuration file contains this text or similar:

   ```
   ActiveClient = 10.0.0.100,2003
   NullAuthPermit = YES
   ```

2. Modify the existing ActiveClient line and create an ActiveClient line for each additional interface to be monitored. Specify each interface by its interface name or IP address.

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_address>
   ```

   Where *<interface_address>* is the IP address of the interface from which the packets are forwarded and *<interface_address>* can be either the IP address itself, such as 10.10.1.100, or a CIDR specification (network IP address/subnet prefix length) that contains the IP address, such as 10.10.1.0/24.

   or

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_name>
   ```

   Where *<interface_name>* is the name of the interface from which the packets are forwarded. The name is formatted as `\Device\NPF_{<GUID>}`, where *<GUID>* is the globally unique identifier (GUID) of the interface. For example, if the interface GUID is `2C2FC212-701D-42E6-9EAE-BEE969FEFB3F`, the interface name is `\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}`.

The following is an example of the configuration file specifying two interfaces with the interface IP address:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
```

The following is an example of the configuration file specifying two interfaces with CIDR specifications that contain the interface IP address:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
```

The following is an example of the configuration file specifying two interfaces with the interface name:

```
ActiveClient = 10.10.6.45, 2003, ifname=\Device
\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
ActiveClient = 10.10.6.45, 2003, ifname=\Device
\NPF_{3C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
NullAuthPermit = YES
```

3. Save the configuration (.ini) file. Make sure to save the file in ASCII format to prevent errors.
4. Restart the packet forwarder by running the following command:

```
restart-service rpcapd
```

Note: To reinstall the packet forwarder software after changing the configuration file, run the installation command and replace `-RpcapIp` and `-RpcapPort` with the `-KeepConfig` flag to preserve the modified configuration file. For example:

```
.\install-rpcapd.ps1 -MgmtIp <extrahop_ip> -KeepConfig
```

or

```
.\install-rpcapd.ps1 –InputDir . -KeepConfig
```

Enable network overlay decapsulation

Network overlay encapsulation wraps standard network packets in outer protocol headers to perform specialized functions, such as smart routing and virtual machine networking management. Network overlay decapsulation enables the ExtraHop system to remove these outer encapsulating headers and then process the inner packets.

Note: Enabling Generic Routing Encapsulation (GRE), Network Virtualization using Generic Routing Encapsulation (NVGRE), VXLAN, and GENEVE decapsulation on your ExtraHop system can increase your device count as virtual devices are discovered on the network. Discovery of these virtual devices can affect Advanced Analysis and Standard Analysis capacity and the additional metrics processing can cause performance to degrade in extreme cases.

MPLS, TRILL, and Cisco FabricPath protocols are automatically decapsulated by the ExtraHop system.

Enable GRE or NVGRE decapsulation

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 **Network Overlay Decapsulation**.

4. In the Settings section, select the **Enabled** checkbox next to **NVGRE** or **GRE**.

   Note: Selecting GRE also enables NVGRE even if you do not select the NVGRE checkbox.

5. Click **Save**.
6. Click **OK**.

Enable VXLAN decapsulation

VXLAN is a UDP tunneling protocol configured for specific destination ports. Decapsulation is not attempted unless the destination port in a packet matches the UDP destination port or ports listed in the VXLAN decapsulation settings.

To configure the ExtraHop system as an endpoint for VXLAN-encapsulated traffic, see Configure an interface.

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 **Network Overlay Decapsulation**.
4. In the Settings section, select the **Enabled** checkbox next to **VXLAN**.
5. In the **VXLAN UDP Destination Port** field, type a port number and click the green plus (+) .

   By default, port 4789 is added to the UDP Destination Port list. You can add up to eight destination ports.
6. Click **Save**.
7. Click **OK**.

Enable GENEVE decapsulation

To configure the ExtraHop system as an endpoint for GENEVE-encapsulated traffic, see Configure an interface.

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 **Network Overlay Decapsulation**.
4. In the Settings section, select the **Enabled** checkbox next to **GENEVE**. The default destination port is 6081.
5. Click **Save**.
6. Click **OK**.

Analyze a packet capture file

The offline capture mode enables administrators to upload and analyze a capture file recorded by packet analyzer software, such as Wireshark or tcpdump, in the ExtraHop system.

Here are some important considerations before enabling offline capture mode:

- When the capture is set to offline mode, the system datastore is reset. All previously recorded metrics are deleted from the datastore. When the system is set to online mode, the datastore is reset again.
- In offline mode, no metrics are collected from the capture interface until the system is set to online mode again.
- Only capture files in the pcap format are supported. Other formats such as pcpapng are not supported.

Set the offline capture mode

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 **Offline Capture File**.
4. Select **Upload** and then click **Save**.
5. Click **OK** to confirm the datastore reset.
   The capture process is stopped, the capture state is set to offline, and the datastore is cleared of all data. When the system has set the capture to offline mode, the Offline Capture File page appears.
6. Click **Choose File**, browse to the capture file that you want to upload, select the file, and then click **Open**.
7. Click **Upload**.
   The ExtraHop system displays the Offline Capture Results page when the capture file uploads successfully.
8. Click **View Results** to analyze the packet capture file as you would when the system is in live capture mode.

Return the system to live capture mode

1. In the System Configuration section, click **Capture (offline)**.
2. Click **Restart Capture**.
3. Select **Live**, and then click **Save**.

The system removes the performance metrics collected from the previous capture file and prepares the datastore for real-time analysis from the capture interface.

Datastore

The ExtraHop system includes a self-contained, streaming datastore for storing and retrieving performance and health metrics in real time. This local datastore bypasses the operating system and accesses the underlying block devices directly, rather than going through a conventional relational database.

Local and extended datastores

The ExtraHop system includes a self-contained, streaming datastore for storing and retrieving performance and health metrics in real time. This local datastore bypasses the operating system and accesses the underlying block devices directly, rather than going through a conventional relational database.

The local datastore maintains entries for all devices discovered by the ExtraHop system as well as metrics for those devices. By storing this information, the ExtraHop system is able to provide both quick access to the latest network capture and historic and trend-based information about selected devices.

Extended datastore

The ExtraHop system can connect to an external storage device to expand your metric storage. By default, the ExtraHop system stores fast (30-second), medium (5-minute), and slow (1-hour) metrics locally. However, you can store 5-minute, 1-hour, and 24-hour metrics on an extended datastore.

To store metrics externally, you must first mount an external datastore, and then configure the ExtraHop system to store data in the mounted directory. You can mount an external datastore through NFS v4 (with optional Kerberos authentication) or CIFS (with optional authentication).

Note that you can configure only one active extended datastore at a time to collect all configured metric cycles. For example, if you configure your extended datastore to collect 5-minute, 1-hour, and 24-hour metrics, all three metric cycles are stored in the same extended datastore. In addition, you can archive an extended datastore and those metrics are available for read-only requests from multiple ExtraHop systems.

Here are some important things to know about configuring an external datastore:

- If an extended datastore contains multiple files with overlapping timestamps, the metrics will be incorrect.

- If an extended datastore has metrics committed by an ExtraHop system running a later firmware version, the system with the older firmware cannot read those metrics.
- If an extended datastore becomes unreachable, the ExtraHop system buffers metrics until the allocated memory is full. After the memory is full, the system overwrites older blocks until the connection is restored. When the mount reconnects, all of the metrics stored in memory are written to the mount.
- If an extended datastore file is lost or corrupted, metrics contained in that file are lost. Other files in the extended datastore remain intact.
- As a security measure, the system does not allow access to the stored plaintext password for the datastore.

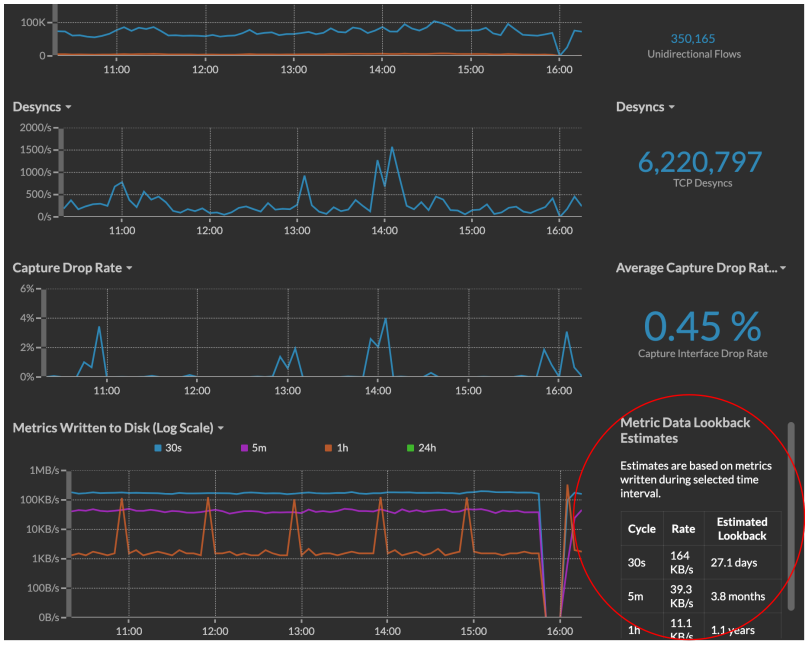
Calculate the size needed for your extended datastore

The extended datastore must have enough space to contain the amount of data generated by the ExtraHop system. The following procedure explains how you can calculate approximately how much free space you need for your extended datastore.

Before you begin
Familiarize yourself with ExtraHop datastore concepts.

In the following example, we show you how to calculate the amount of storage space required for 30 days worth of 5-minute metrics.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon, and then click **System Health**.
3. Scroll down to the Data Feed section.
4. In the Metric Data Lookback Estimates chart, note the Rate and Estimated Lookback for each metric cycle (or time period) that you want to store on the external datastore. Estimates are based on metrics written during the selected time interval.



5. Calculate the amount of required space by applying the following formula: `<rate> x <lookback_time>`, and then convert the value to standard units.
   For example, in the figure above the rate for 5-minute metrics is 39.3 KB/s.
   1. Convert the rate from seconds to days: `39.3 * 60 (seconds) * 60 (minutes) * 24 (hours) * 30 (days) = 101865600 KB` for 30 days of lookback.

2. Convert the rate from kilobytes to megabytes: `101865600 / 1024 = 99478 MB` for 30 days of lookback.
3. Convert the rate from megabytes to gigabytes:`99478 / 1024 = 97 GB` for 30 days of lookback.

To store all of the 5 minute metrics from this ExtraHop system for 30 days, you need 97 GB of free space.

Next steps
Configure an extended CIFS or NFS datastore.

Configure an extended CIFS or NFS datastore

The following procedures show you how to configure an external datastore for the ExtraHop system.

Before you begin
Calculate the size needed for your extended datastore

To configure an extended datastore, you will complete the following steps:

- First, you mount the NFS or CIFS share where you want to store data.
- For NFS, optionally configure Kerberos authentication before you add the NFS mount.
- Finally, specify the newly added mount as the active datastore.

Add a CIFS mount

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 **Datastore**.
3. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
4. Click **Add Mount**.
5. Click **Add CIFS Mount**.
6. On the Configure CIFS Mount page, enter the following information:

   Mount Name
   A name for the mount; for example, `EXDS_CIFS`.

   Remote Share Path
   The path for the share in the following format:

   ```
   \\host\mountpoint
   ```

   For example:

   ```
   \\herring\extended-datastore
   ```

   SMB Version
   The SMB version that is compatible with your file server.

   Domain
   The site domain.
7. If password protection is required, complete the following steps:
   a) From the Authentication drop-down menu, select **password**.
   b) In the User and Password fields, type a valid username and password.
8. Click **Save**.

(Optional) Configure Kerberos for NFS

You must configure any desired Kerberos authentication before you add an NFS mount.

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 **Datastore and Customizations**.
3. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
4. Click **Add Kerberos Config**, then complete the following information.
   a) In the Admin Server field, type the IP address or hostname of the master Kerberos server that issues tickets.
   b) In the Key Distribution Center (KDC) field, type the IP address or hostname of the server that holds the keys.
   c) In the Realm field, type the name of the Kerberos realm for your configuration.
   d) In the Domain field, type the name of the Kerberos domain for your configuration.
5. In the Keytab File section, click **Choose File**, select a saved keytab file, and then click **Open**.
6. Click **Upload**.

Add an NFS mount

Before you begin

- Configure any applicable Kerberos authentication before you add an NFS mount.
- Either allow read/write access for all users on the share or assign the 'extrahop' user as the owner of the share and allow read/write access.
- You must have NFS version 4.

1. In the System Configuration section, click **Datastore and Customizations**.
2. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
3. Click **Add NFSv4 Mount**.
4. On the Configure NFSv4 Mount page, complete the following information:
   a) In the Mount Name field, type a name for the mount, such as EXDS.
   b) In the Remote Share Point field, type the path for the mount in the following format: `host:/mountpoint`, such as `herring:/mnt/extended-datastore`.
5. From the Authentication drop-down, select from the following options:
   - **None**, For no authentication
   - **Kerberos**, For krb5 security.
   - **Kerberos (Secure Auth and Data Integrity)**, for krb5i security.
   - **Kerberos (Secure Auth, Data Integrity, Privacy)**, for krb5p security
6. Click **Save**.

Specify a mount as an active extended datastore

After you add a CIFS or NFS mount, set the mount as your active extended datastore. Remember that only one datastore can collect metrics at a time.

Note: If you decide to store 5-minute and 1-hour metrics on the extended datastore, this option causes any 5-minute and 1-hour metrics collected from the local ExtraHop system datastore to be migrated to the extended datastore. Migrating 5-minute and 1-hour metrics to an extended datastore leaves more room to store 30-second metrics on the local datastore, which increases the amount of high-resolution lookback available.

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 **Datastore and Customizations**.
3. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
4. From the Mount Name drop-down, select the name of the mount you want to specify as the extended datastore.

5. In the Datastore Directory field, type a name for the datastore directory. The directory is automatically created on the mount point by the ExtraHop system.
6. From the Configure as options, select the **Active** radio button.
7. In the Datastore Size field, specify the maximum amount of data that can be stored on the datastore.
8. Select the checkbox to store 5-minute and 1-hour metrics on the extended datastore. 24-hour metrics are always stored on the extended datastore.
9. Specify whether to migrate existing metrics to the extended datastore by selecting from one of the following options.
   - To migrate existing metrics, click **Move existing metrics to the extended datastore**.
   - To retain existing metrics on the local datastore, click **Keep existing metrics on the ExtraHop**.

   Warning: While data is migrated, the ExtraHop system stops collecting data and system performance is degraded. The migration process takes more time under the following circumstances:
   - If there is a large amount of data to migrate
   - If the network connection to the NAS device hosting the datastore is slow
   - If the write performance of the NAS device hosting the datastore is slow
10. Select **Move existing**.
11. Specify what the system should do if the datastore becomes full by selecting from the following options.
    - To overwrite older data when the datastore becomes full, click **Overwrite**.
    - To stop storing new metrics on the extended datastore when the datastore becomes full, click **Stop writing**.
12. Click **Configure**.
13. After the storage is added, the Status displays `Nominal`.

Next steps

- Troubleshoot issues with an extended datastore
- Archive an extended datastore for read-only access

Archive an extended datastore for read-only access

By disconnecting an active datastore from an ExtraHop system, you can create a read-only archive of the stored metrics data. Any number of ExtraHop systems can read from an archived datastore.

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 **Datastore and Customizations**.
3. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
4. Click the name of the mount that contains the datastore you want to archive.
5. In the row of that datastore, click **Disconnect Extended Datastore**.
6. Type YES to confirm and then click **OK**.

The datastore is disconnected from the system and marked for read-only access. Wait at least ten minutes before connecting any other ExtraHop systems to the archive.

Connect your ExtraHop system to the archived datastore

Warning: To connect to an archived datastore, the ExtraHop system must scan through the data contained in the datastore. Depending on the amount of data stored in the archived datastore, connecting to the archived datastore might take a long time. When connecting to the archived datastore, the system does not collect data and system performance is degraded. The connection process takes more time under the following circumstances:

- If there is a large amount of data in the datastore
- If the network connection to the NAS device hosting the datastore is slow
- If the read performance of the NAS device hosting the datastore is slow

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration, click **Datastore and Customizations**.
3. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
4. Click the name of the mount that contains the archived datastore.
5. In the Datastore Directory field, type the path of the archived datastore directory.
6. Click **Archive (Read Only)**.
7. Click **Configure**.

Your extended database is now a read-only archive that can be accessed by multiple ExtraHop systems.

Import metrics from an extended datastore

If you stored metric data on an extended datastore that is connected to your ExtraHop system, you can move that data during an upgrade or datastore reset.

Contact ExtraHop Support if you need to transfer metrics from an extended datastore.

Reset the local datastore and remove all device metrics from the ExtraHop system

In certain circumstances, such as moving a sensor from one network to another, you might need to clear the metrics in the local and extended datastores. Resetting the local datastore removes all metrics, baselines, trend analyses, and discovered devices—and affects any customizations on your ExtraHop system.

Before you begin
Familiarize yourself with ExtraHop database concepts.

Customizations are changes that were made to the default settings on the system, such as triggers, dashboards, alerts, and custom metrics. These settings are stored in a file on the system, and this file is also deleted when the datastore is reset. Most customizations are applied to devices, which are identified by an ID on the system. When the local datastore is reset, those IDs might change and any device-based assignments must be re-assigned to the devices by their new IDs. The reset procedure includes an option to save and restore your customizations.

If your device IDs are stored on the extended datastore, and that datastore is disconnected when the local datastore is reset and then later reconnected, those device IDs are restored to the local datastore and you do not need to reassign your restored customizations.

Configured alerts are retained on the system, but they are disabled and must be enabled and reapplied to the correct network, device, or device group. System settings and user accounts are unaffected.

Warning: This procedure deletes device IDs and device metrics from the ExtraHop system.

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 **Datastore and Customizations**.
3. Disconnect your extended datastore by completing the following steps:
   a) In the Extended Datastore Settings section, click **Configure Extended Datastore**.
   b) Click the name of the mount that contains the datastore you want to disconnect.
   c) In the row of that datastore, click **Disconnect Extended Datastore**.
   d) Type YES to confirm and then click **OK**.
4. Navigate back to the Datastore and Customizations page.
5. In the Local Datastore Settings section, click **Reset Datastore**.
6. On the Reset Datastore page, specify whether to save customizations before you reset the datastore.

- To retain the current customizations after the datastore is reset, select the **Save Customizations** checkbox.
- To delete the current customizations after the datastore is reset, clear the **Save Customizations** checkbox.

7. Type YES in the confirmation text box.
8. Click **Reset Datastore**.
   If you opted to save your customizations, a prompt appears with a detailed list after about one minute. Click **OK** to restore the saved customizations.

Troubleshoot issues with the extended datastore

To view the status for your mounts and datastores, and identify applicable troubleshooting steps, complete the following steps.

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 **Datastore and Customizations**.
3. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
4. In the Extended Datastores table, view the entry in the Status column for each mount or datastore. The following table provides guidance on each entry and identifies any applicable action.

Table 1: Mounts

Status	Description	User Action
Mounted	The mount configuration was successful.	None required
NOT MOUNTED	The mount configuration was unsuccessful.	• Verify that the mount configuration information for accuracy and correct spelling. • Verify that the remote system is available. • Verify that the server is a supported type and version. • Verify credentials, if using authentication.
NOT READABLE	The mount has permissions or network-related issues that prevent reading.	• Verify that the correct permissions are set on the share. • Verify the network connection and availability.
NO SPACE AVAILABLE	The mount has no space remaining.	Detach the mount and create a new one.
INSUFFICIENT SPACE	• First appearance: The system anticipates that not enough space is available. • Second appearance: Less than 128MB of space is available.	Detach the mount and create a new one.

Status	Description	User Action
AVAILABLE SPACE WARNING	Less than 1GB of space is available.	Detach the mount and create a new one.
NOT WRITEABLE	The mount has permissions or network-related issues that prevent writing.	• Verify permissions. • Verify the network connection and availability.

Table 2: Datastores

Status	Description	User Action
Nominal	The datastore is in a normal state.	None required
INSUFFICIENT SPACE on: <MOUNT NAME>	The datastore has insufficient space on the named mount and it cannot be written to.	Create a new datastore. For the new datastore, consider selecting the `Overwrite` option, if appropriate.
NOT READABLE	The datastore has permissions or network-related issues that prevent reading.	• Verify permissions. • Verify the network connection and availability.
NOT WRITEABLE	The datastore has permissions or network-related issues that prevent writing.	• Verify permissions. • Verify the network connection and availability.

Device name precedence

Discovered devices are automatically named based on multiple sources of network data. When multiple names are found for a device, a default order of precedence is applied. You can change the order of precedence.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **All Administration**.
3. In the System Configuration section, click **Device Name Precedence**.
4. Click and drag device names to create a new order of precedence.
5. Click **Save**.
   Click **Revert to Default** to undo your changes.

Inactive sources

Devices and applications appear in search results until they are inactive for over 90 days. If you want to remove sources from search results before the 90-day expiration, you can remove all sources that have been inactive between 1 and 90 days, on-demand.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. Type a value from 1 to 90 in the inactive days field.
3. Click **Remove**.

Detection Tracking

Detection tracking enables you to assign a detection to a user, set the status, and add notes. You can track detections with ExtraHop, or with a 3rd-party external ticketing system.

- Select **Track detections with the ExtraHop system** to manage detection tracking with ExtraHop.
- Select **Track detections with an external ticketing system** to create and manage tickets in a third-party ticket tracking system and view the assignee and status in the ExtraHop system.

  Optional: To create an HTML link from the detection to the ticket in your ticket tracking system, specify a URL template. Type the URL in the template field for your ticketing system and add the `$ticket_id` variable at the appropriate location. Type a complete URL, such as `https://jira.example.com/browse/$ticket_id`. The `$ticket_id` variable is replaced with the ticket ID associated with the detection.

  After the URL template is configured, you can click the ticket ID in a detection to open the ticket in a new browser tab.

While you can enable ticket tracking and configure a URL template through the Administration settings, ticket tracking requires further configuration through ExtraHop Triggers and the REST API. For more information about ticket tracking, see Configure ticket tracking for detections.

Note: You must enable ticket tracking on all connected sensors.

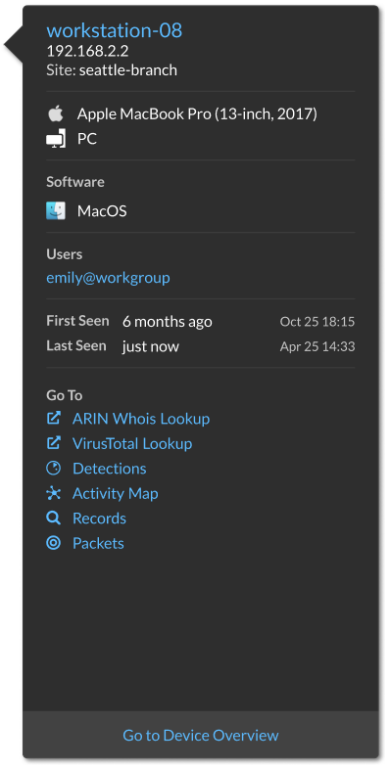
If you disable external ticket tracking by changing to detection tracking with the ExtraHop system, previously stored status and assignee ticket information is converted to ExtraHop detection tracking. You will be able to view tickets that already existed when you disabled external ticket tracking, but changes to that external ticket will not appear in the ExtraHop system.

Configure endpoint lookup links

Endpoint lookup enables you to specify external IP address tools that are available for retrieving up information about endpoints within the ExtraHop system. For example, when you click or hover over an IP address, lookup tool links are displayed so that you can easily find information about that endpoint.

The following lookup links are configured by default and can be modified or deleted:

- ARIN Whois Lookup
- VirusTotal Lookup



1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. From the System Configuration section, click **Endpoint Lookup**.
3. In the **URL Template** field, type the URL of the lookup tool.

   The URL must include the `$ip` variable, which is replaced with the IP address of the endpoint upon lookup. For example, `https://search.arin.net/rdap/?query=$ip`
4. In the **Display Name** field, type the name link as you want it to appear.
5. Select one of the following Display Options:
   - Show this link on all endpoints
   - Show this link on external endpoints
   - Show this link on internal endpoints
   - Do not show this link
6. Click Save.

Geomap Data Source

Geomaps and triggers reference a GeoIP database to identify the approximate location of an IP address.

Change the GeoIP database

You can upload your own GeoIP database to the ExtraHop system to ensure that you have the latest version of the database or if your database contains internal IP addresses that only you or your company know the location of.

You can upload a database file in MaxMind DB format (.mmdb) that include city-level details and country-level details.

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 **Geomap Data Source**.
3. Click **GeoIP Database**.
4. In the City-level Database section, select **Upload New Database**.
5. Click **Choose File** and navigate to the new city-level database file on your computer.
6. Click **Save**.

Next steps
For more information about geomaps, see the following resources:

- Geomaps FAQ
- Generate a geomap

Override an IP location

You can override missing or incorrect IP addresses that are in the GeoIP database. You can enter a comma-delimited list or tabbed list of overrides into the text box.

Each override must include an entry in the following seven columns:

- IP address (a single IP address or CIDR notation)
- Latitude
- Longitude
- City
- State or region
- Country name
- ISO alpha-2 country code

You can edit and delete items as necessary, but you must ensure that there is data present for each of the seven columns. For more information about ISO country codes, refer to https://www.iso.org/obp/ui/#search and click **Country Codes**.

1. Under System Configuration, click **Geomap Data Source**.
2. Click **IP Location Override**.
3. In the text box, type or paste a tab or comma-delimited list of overrides in the following format:

```
IP address, latitude, longitude, city, state or region, country name, ISO
alpha-2 country code
```

For example:

```
10.10.113.0/24, 38.907231, -77.036464, Washington, DC, United States, US
10.10.225.25, 47.6204, -122.3491, Seattle, WA, United States, US
```

4. Click **Save**.

To verify the change, go to the Geomaps interface and mouse over a location included in your IP location overrides.

Open Data Streams

By configuring an open data stream, you can send the data collected by your ExtraHop system to an external third-party system, such as syslog systems, MongoDB databases, HTTP servers, Kafka servers. In addition, you can send raw data to any external server by configuring the target with port and protocol specifications.

You can configure up to 16 open data stream targets of each external system type.

Important: After you configure an open data stream (ODS) for an external system, you must create a trigger that specifies what data to manage through the stream.

Similarly, if you delete an open data stream, you should also delete the associated trigger to avoid needlessly consuming system resources.

For more information, see Open data stream classes in the ExtraHop Trigger API Reference.

Configure an HTTP target for an open data stream

You can export data on an ExtraHop system to a remote HTTP server for long-term archiving and comparison with other sources.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.

   Repeat these steps on each sensor in your environment.
2. In the System Configuration section, click **Open Data Streams**.
3. Click **Add Target**.
4. From the Target Type drop-down menu, select **HTTP**.
5. In the Name field, type a name to identify the target.
6. In the Host field, type the hostname or IP address of the remote HTTP server.
7. In the Port field, type the port number of the remote HTTP server.
8. From the Type drop-down menu, select one of the following protocols:
   - **HTTP**
   - **HTTPS**
9. If you selected HTTPS, select **Skip certificate verification** to bypass certificate verification of encrypted data. Data can be verified by trusted certificates that you upload to the ExtraHop system.

   Note: Secure connections to the HTTPS ODS server can be verified through trusted certificates that you upload to the ExtraHop system.
10. Select **Multiple connections** to enable concurrent requests through multiple connections, which can improve throughput speed.
11. In the Additional HTTP Header field, type an additional HTTP header.

    The format for the additional header is *Header* : *Value*.

    Note: Headers configured in a trigger take precedence over an additional header. For example, if the Additional HTTP Header field specifies `Content-Type: text/plain` but a trigger script for the same ODS target specifies `Content-Type: application/json`, then `Content-Type: application/json` is included in the HTTP request.
12. (Optional) From the Authentication drop-down menu, select the type of authentication from the following options.

Option	Description
Basic	Authenticates through a username and password.
Amazon AWS	Authenticates through Amazon Web Services.
Microsoft Azure Storage	Authenticates through Microsoft Azure.
Microsoft Azure Active Directory	Authenticates through Microsoft Azure Active Directory (v1.0). **Note:** Microsoft identity platform (v2.0) is not supported.
CrowdStrike	Authenticates through CrowdStrike.

13. Select **Connect through global proxy** to send requests through the global proxy server configured for the ExtraHop system.

14. (Optional) Click **Test** to establish a connection between the ExtraHop system and the remote HTTP server and send a test message to the server.
    The dialog box displays a message that indicates whether the connection succeeded or failed. If the test fails, edit the target configuration and test the connection again.
15. (Optional) Send a test request to the remote HTTP server.

    The request is for testing purposes only; it is not included in any trigger scripts.

    a) From the Method drop-down menu, select one of the following HTTP request methods:

    - **DELETE**
    - **GET**
    - **HEAD**
    - **OPTIONS**
    - **PUT**
    - **POST**
    - **TRACE**

    b) In the Options field, specify the parameters of the HTTP request in the following format:

```
    "headers": {},
    "payload": "",
    "path": "/"
}
```

    The parameters are defined as follows:

    headers

    The headers of the HTTP request. You must specify headers as an array, even if you specify only one header. For example:

```
"headers": {"content-type":["application/json"]},
```

    path

    The path that the HTTP request will be applied to.

    payload

    The payload of the HTTP request.

    c) Click **Test** to establish a connection between the ExtraHop system and the remote server and send the request.
    The dialog box displays a message that indicates whether the request succeeded or failed, and displays any requested content.
16. Click **Save**.

Next steps
Create a trigger that specifies what HTTP message data to send and initiates the transmission of data to the target. For more information, see the Remote.HTTP class in the ExtraHop Trigger API Reference.

Configure a Kafka target for an open data stream

You can export data on an ExtraHop system to any Kafka server for long-term archiving and comparison with other sources.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.

   Repeat these steps on each sensor in your environment.
2. In the System Configuration section, click **Open Data Streams**.
3. Click **Add Target**.

4. From the Target Type drop-down menu, select **Kafka**.
5. In the Name field, type a name to identify the target.
6. From the Compression drop-down list, select one of the following compression methods that will be applied to the transmitted data:
   - **None**
   - **GZIP**
   - **Snappy**
7. From the Partition strategy drop-down list, select one of the following partitioning methods that will be applied to the transmitted data:
   - **Default (Hash Key)**
   - **Manual**
   - **Random**
   - **Round Robin**
8. (Optional) Configure SASL/SCRAM authentication.
   a) From the Authentication drop-down menu, select **SASL/SCRAM**.
   b) In the **Username** field, type the name of the SASL/SCRAM user.
   c) In the **Password** field, type the password of the SASL/SCRAM user.
   d) From the Hashing Algorithm drop-down menu, select the hashing algorithm for SASL authentication.
9. From the Protocol drop-down menu, select one of the following protocols over which to transmit data:
   - **TCP**
   - **SSL/TLS**
10. (Optional) If you selected the **SSL/TLS** protocol, specify certificate options.
    a) If the Kafka server requires client authentication, specify a TLS client certificate to send to the server in the **Client certificate** field.
    b) If you specified a client certificate, specify the private key of the certificate in the **Client key** field.
    c) If you do not want to verify the certificate of the Kafka server, select **Skip server certificate verification**.
    d) If you want to verify the certificate of the Kafka server, but the certificate has not been signed by a valid Certificate Authority (CA), specify trusted certificates to verify the server certificate with in the **CA certificates (optional)** field. Specify the certificates in PEM format. If this option is not specified, the server certificate is validated with the built-in list of valid CA certificates.
11. Specify at least one Kafka broker, also referred to as a node in a Kafka cluster, that can receive transmitted data.

    Note: You can add multiple brokers that are part of the same Kafka cluster to ensure connectivity in case a single broker is unavailable. All brokers must be part of the same cluster.

    a) In the Host field, type the hostname or IP address of the Kafka broker.
    b) In the Port field, type the port number of the Kafka broker.
    c) Click the plus (**+**) icon.
12. (Optional) Click **Test** to establish a connection between the ExtraHop system and the remote Kafka server and send a test message to the server.
    The dialog box displays a message that indicates whether the connection succeeded or failed. If the test fails, edit the target configuration and test the connection again.
13. Click **Save**.

Next steps
Create a trigger that specifies what Kafka message data to send and initiates the transmission of data to the target. For more information, see the Remote.Kafka class in the ExtraHop Trigger API Reference.

Configure a MongoDB target for an open data stream

You can export data on an ExtraHop system to any system that receives MongoDB input for long-term archiving and comparison with other sources.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.

   Repeat these steps on each sensor in your environment.
2. In the System Configuration section, click **Open Data Streams**.
3. Click **Add Target**.
4. From the Target Type drop-down menu, select **MongoDB**.
5. In the Name field, type a name to identify the target.
6. In the Host field, type the hostname or IP address of the remote MongoDB server.
7. In the Port field, type the port number of the remote MongoDB server.
8. Select **SSL/TLS Encryption** to encrypt transmitted data.
9. Select **Skip certificate verification** to bypass certificate verification of encrypted data.

   Note: Secure connections to the MongoDB target server can be verified through trusted certificates that you upload to the ExtraHop system.
10. (Optional) Add users that have permission to write to a MongoDB database on the target server.
    a) In the Database field, type the name of the MongoDB database.
    b) In the Username field, type the username of the user.
    c) In the Password field, type the password of the user.
    d) Click the plus (**+**) icon.
11. (Optional) Click **Test** to establish a connection between the ExtraHop system and the remote MongoDB server and send a test message to the server.
    The dialog box displays a message that indicates whether the connection succeeded or failed. If the test fails, edit the target configuration and test the connection again.
12. Click **Save**.

Next steps

Create a trigger that specifies what MongoDB message data to send and initiates the transmission of data to the target. For more information, see the Remote.MongoDB class in the ExtraHop Trigger API Reference.

Configure a raw data target for an open data stream

You can export raw data on an ExtraHop system to any server for long-term archiving and comparison with other sources. In addition, you can select an option to compress the data through GZIP.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.

   Repeat these steps on each sensor in your environment.
2. In the System Configuration section, click **Open Data Streams**.
3. Click **Add Target**.
4. From the Target Type drop-down menu, select **Raw**.
5. In the Name field, type a name to identify the target.
6. In the Host field, type hostname or IP address of the remote server.
7. In the Port field, type the port number of the remote server.
8. From the Protocol drop-down menu, select one of the following protocols over which to transmit data:
   - **TCP**
   - **UDP**
9. (Optional) Enable GZIP compression of the transmitted data.

a) Select **GZIP compression**.
b) Provide a value for each of the following fields:

Number of bytes after which to refresh GZIP

The default value is 64000 bytes.

Number of seconds after which to refresh GZIP

The default value is 300 seconds.

10. (Optional) Click **Test** to establish a connection between the ExtraHop system and the remote server and send a test message to the server.
The dialog box displays a message that indicates whether the connection succeeded or failed. If the test fails, edit the target configuration and test the connection again.
11. Click **Save**.

Next steps
Create a trigger that specifies what raw message data to send and initiates the transmission of data to the target. For more information, see the Remote.Raw class in the ExtraHop Trigger API Reference.

Configure a syslog target for an open data stream

You can export data on an ExtraHop system to any system that receives syslog input (such as Splunk, ArcSight, or Q1 Labs) for long-term archiving and comparison with other sources.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
Repeat these steps on each sensor in your environment.
2. In the System Configuration section, click **Open Data Streams**.
3. Click **Add Target**.
4. From the Target Type drop-down menu, select **Syslog**.
5. In the Name field, type a name to identify the target.
6. In the Host field, type the hostname or IP address of the remote syslog server.
7. In the Port field, type the port number of the remote syslog server.
8. From the Protocol drop-down menu, select one of the following protocols over which to transmit data:
   - **TCP**
   - **UDP**
   - **SSL/TLS**
9. (Optional) Select **Local Time** to send syslog information with timestamps in the local time zone of the ExtraHop system. If this option is not selected, timestamps are sent in GMT.
10. (Optional) Select **Length-prefix framing** to prepend the number of bytes in a message to the beginning of each message. If this option is not selected, the end of each message is delimited by a trailing newline.
11. (Optional) In the **Batch min bytes** field, type the minimum number of bytes to send to the syslog server at a time.
12. (Optional) In the **Concurrent connections** field, type the number of concurrent connections to send messages over.
13. (Optional) If you selected the **SSL/TLS** protocol, specify certificate options.
    a) If the Syslog server requires client authentication, specify a TLS client certificate to send to the server in the **Client certificate** field.
    b) If you specified a client certificate, specify the private key of the certificate in the **Client key** field.
    c) If you do not want to verify the certificate of the Syslog server, select **Skip server certificate verification**.
    d) If you want to verify the certificate of the Syslog server, but the certificate has not been signed by a valid Certificate Authority (CA), specify trusted certificates to verify the server certificate with

in the **CA certificates (optional)** field. Specify the certificates in PEM format. If this option is not specified, the server certificate is validated with the built-in list of valid CA certificates.

14. (Optional) Click **Test** to establish a connection between the ExtraHop system and the remote syslog server and send a test message to the server.
    The dialog box displays a message that indicates whether the connection succeeded or failed. If the test fails, edit the target configuration and test the connection again.
15. Click **Save**.

Next steps
Create a trigger that specifies what syslog message data to send and initiates the transmission of data to the target. For more information, see the Remote.Syslog class in the ExtraHop Trigger API Reference.

ODS Details

The Open Data Stream (ODS) details page provides information about the amount of data that has been sent to the ODS target and how many errors have occurred.

Note: The ODS Details page is currently available only for HTTP ODS targets.

Connection attempts
The number of times the ExtraHop system attempted to connect to the ODS target.

Connection errors
The number of errors that occurred during attempts to connect to the ODS target.

IPC errors
The number of errors that occurred during data transfer between triggers and the exremote process. If IPC errors occur, contact ExtraHop Support for help.

Bytes sent to target
The number of bytes that were forwarded by the exremote process to the ODS target.

Messages sent to target
The number of messages that were forwarded by the exremote process to the ODS target.

Bytes sent from triggers
The number of bytes that triggers sent to the exremote process to be forwarded to the ODS target.

Messages sent from triggers
The number of messages that triggers sent to the exremote process to be forwarded to the ODS target.

Messages dropped by exremote
The number of messages that triggers sent to the exremote process but were never forwarded to the ODS target.

Error Details

Time
The time that the error occurred.

URL
The URL of the ODS target.

Status
The HTTP status code returned by the ODS target.

Request Headers
The headers of the HTTP request sent to the ODS target.

Request Body
The body of the HTTP request sent to the ODS target.

Response Headers

The headers of the HTTP response sent by the ODS target.

Response Body

The body of the HTTP response sent by the ODS target.

Trends

Trend-based alerts are generated when a monitored metric deviates from the normal trends observed by the ExtraHop system. If needed, you can delete all configured trends and trend-based alerts.

- Click **Reset Trends** to erase all trend data from the ExtraHop system.

Back up and restore a sensor or console

After you have configured your ExtraHop console and sensor with customizations such as bundles, triggers, and dashboards or administrative changes such as adding new users, ExtraHop recommends that you periodically back up your settings to make it easier to recover from a system failure.

Daily backups are automatically saved to the local datastore, however, we recommend that you manually create a system backup prior to upgrading firmware or before making a major change in your environment (changing the data feed to the sensor, for example). Then, download the backup file and save it to a secure location.

Back up a Sensor or ECA VM

Create a system backup and store the backup file to a secure location.

Important: System backups contain sensitive information, including SSL keys. When you create a system backup, make sure you store the backup file to a secure location.

The following customizations and resources are saved when you create a backup.

- User customizations such as bundles, triggers, and dashboards.
- Configurations made from Administration settings, such as locally-created users and remote imported user groups, running configuration file settings, SSL certificates, and connections to ExtraHop recordstores and packetstores.

The following customizations and resources are not saved when you create a backup or migrate to a new target.

- License information for the system. If you are restoring settings to a new target, you must manually license the new target.
- Precision packet captures. You can download saved packet captures manually by following the steps in View and download packet captures.
- When restoring an ECA VM console that has a tunneled connection from a sensor, the tunnel must be reestablished after the restore is complete and any customizations on the console for that sensor must be manually recreated.
- User-uploaded SSL keys for traffic decryption.
- Secure keystore data, which contains passwords. If you are restoring a backup file to the same target that created the backup, and the keystore is intact, you do not need to re-enter credentials. However, if you are restoring a backup file to a new target or migrating to a new target, you must re-enter the following credentials:
  - Any SNMP community strings provided for SNMP polling of flow networks.
  - Any bind password provided to connect with LDAP for remote authentication purposes.
  - Any password provided to connect to an SMTP server where SMTP authentication is required.
  - Any password provided to connect to an external datastore.

- Any password provided to access external resources through the configured global proxy.
- Any password provided to access ExtraHop Cloud Services through the configured ExtraHop cloud proxy.
- Any authentication credentials or keys provided to configure Open Data Stream targets.

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 **Backup and Restore**.
3. Click **Create System Backup**, and then click **OK**.
   A list of user-saved and automatic backups appear.
4. Click the name of the new backup file, **User saved <timestamp> (new)**. The backup file, with an .exbk file extension, is automatically saved to the default download location for your browser.

Restore a sensor or console from a system backup

You can restore the ExtraHop system from the user-saved or automatic backups stored on the system. You can perform two types of restore operations; you can restore only customizations (changes to alerts, dashboards, triggers, custom metrics, for example), or you can restore both customizations and system resources.

This procedure describes the steps required to restore a backup file to the same sensor or console that created the backup file. If you want to migrate the settings to a new sensor or console, see Transfer settings to a new console or sensor.

Before you begin
The target must be running the same firmware version, matching the first and second digits of the firmware that generated the backup file. If the versions are not the same, the restore operation will fail.

The following table shows examples of supported restore operations.

Source firmware	Target firmware	Supported
7.7.0	7.7.5	Yes
7.7.0	7.8.0	No

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 **Backup and Restore**.
3. Click **View or Restore System Backups**.
4. Click **Restore** next to the user backup or automatic backup that you want to restore.
5. Select one of the following restore options:

Option	Description
Restore system customizations	Select this option if, for example, a dashboard was accidentally deleted or any other user setting needs to be restored. Any customizations that were made after the backup file was created are not overwritten when the customizations are restored.
Restore system customizations and resources	Select this option if you want to restore the system to the state it was in when the backup was created. **Warning:** Any customizations that were made after the backup file was created are overwritten when the

Option	Description
	customizations and resources are restored.

6. Click **OK**.
7. (Optional) If you selected **Restore system customizations**, click **View import log** to see which customizations were restored.
8. Restart the system.
   a) Return to Administration settings.
   b) In the Appliance Settings section, click **Shutdown or Restart**.
   c) In the Actions column for the System entry, click **Restart**.
   d) Click **Restart** to confirm.

Restore a sensor or console from a backup file

This procedure describes the steps required to restore a system from a backup file to the same sensor or console that created the backup file.

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 **Backup and Restore**.
3. Click **Upload Backup File to Restore System**.
4. Select one of the following restore options:

Option	Description
Restore system customizations	Select this option if, for example, a dashboard was accidentally deleted or any other user setting needs to be restored. Any customizations that were made after the backup file was created are not overwritten when the customizations are restored.
Restore system customizations and resources	Select this option if you want to restore the system to the state it was in when the backup was created. **Warning:** Any customizations that were made after the backup file was created are overwritten when the customizations and resources are restored.

5. Click Choose File and navigate to a backup file that you saved previously.
6. Click **Restore**.
7. (Optional) If you selected **Restore system customizations**, click **View import log** to see which customizations were restored.
8. Restart the system.
   a) Return to Administration settings.
   b) In the Appliance Settings section, click **Shutdown or Restart**.
   c) In the Actions column for the System entry, click **Restart**.
   d) Click **Restart** to confirm.

Transfer settings to a new console or sensor

This procedure describes the steps required to restore a backup file to a new console or sensor. Only system settings from your existing console or sensor are transferred. Metrics on the local datastore are not transferred.

Before you begin

- Create a system backup and save the backup file to a secure location.
- Remove the source sensor or console from the network before transferring settings. The target and source cannot be active on the network at the same time.

  Important: Do not disconnect any sensors that are already connected to a console.
- Deploy and register the target sensor or console.
  - Ensure that the target is the same type of sensor or console (physical or virtual) as the source.
  - Ensure that the target is the same size or larger (maximum throughput on the sensor; CPU, RAM, and disk capacity on the console) as the source.
  - Ensure that the target has a firmware version that matches the firmware version that generated the backup file. If the first two digits of the firmware versions are not the same, the restore operation will fail.

    The following table shows examples of supported configurations.

Source firmware	Target firmware	Supported
7.7.0	7.7.0	Yes
7.7.0	7.7.5	Yes
7.7.5	7.7.0	No
7.7.0	7.6.0	No
7.7.0	7.8.0	No

- After transferring settings to a target console, you must manually reconnect all sensors.
- When transferring settings to a target console that is configured for a tunneled connection to the sensors, we recommend that you configure the target console with the same hostname and IP address as the source console.

1. Log in to the Administration settings on the target system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Backup and Restore**.
3. Click **Upload Backup File to Restore System**.
4. Select **Restore system customizations and resources**.
5. Click **Choose File**, navigate to the stored backup file, and then click **Open**.
6. Click **Restore**.

   Warning: If the backup file is incompatible with the local datastore, the datastore must be reset.

   After the restore is complete, you are logged out of the system.
7. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin` and verify that your customizations were correctly restored on the target sensor or console.

   Note: If the source sensor or console was connected to ExtraHop Cloud Services, you must manually connect the target to ExtraHop Cloud Services.

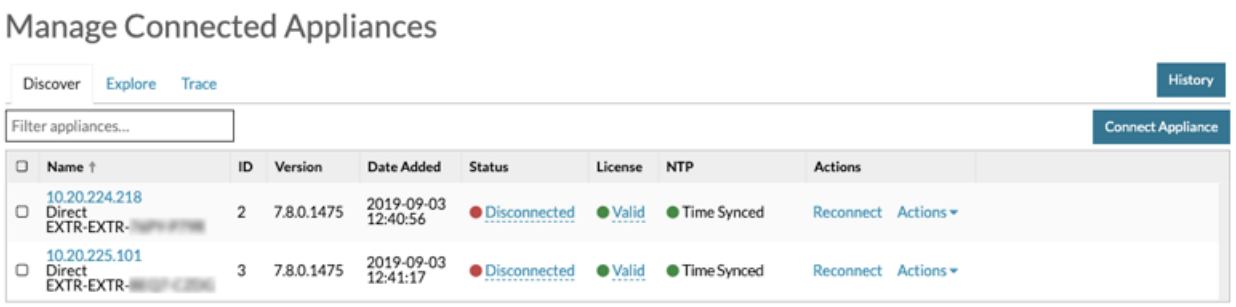
Reconnect sensors to the console

If you transferred settings to a new console, you must manually reconnect all previously connected sensors.

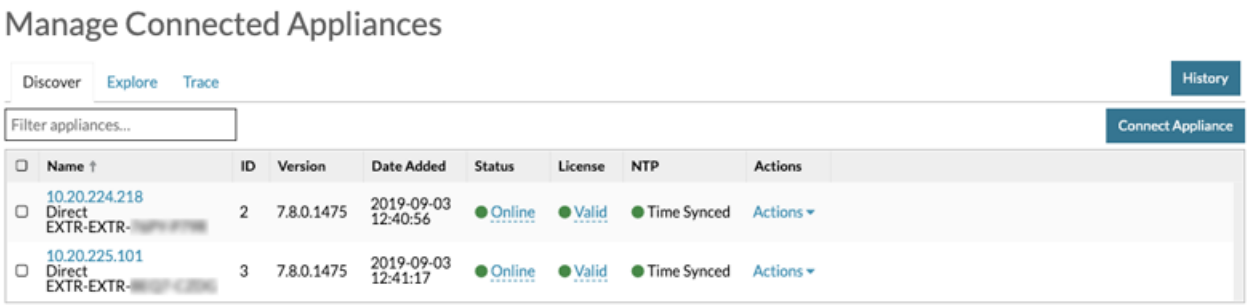
Before you begin

Important: If your console and sensors are configured for a tunneled connection, we recommend that you configure the source and target consoles with the same IP address and hostname. If you cannot set the same IP address and hostname, skip this procedure and create a new tunneled connection to the new IP address or hostname of the console.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Connected Appliance Administration section, under ExtraHop Discover Settings, click **Manage Discover Appliances**.
3. In the Actions column for the first sensor, click **Reconnect**.



4. Type the password for the setup user of the sensor.
5. Click **Connect**.
6. Repeat steps 3-5 for any remaining disconnected sensors.
All disconnected sensors are now online.



Appliance Settings

You can configure the following components of the ExtraHop appliance in the Appliance Settings section.

All appliances have the following components:

Running Config
Download and modify the running configuration file.

Services
Enable or disable the Web Shell, management GUI, SNMP service, SSH access, and SSL session key receiver. The SSL Session Key Receiver option appears only on the Discover appliance.

Firmware
Upgrade the ExtraHop system firmware.

System Time
Configure the system time.

Shutdown or Restart
Halt and restart system services.

License
Update the license to enable add-on modules.

Disks
Provides information about the disks in the appliance.

The following components only appear on the specified appliances:

Command Nickname
Assign a nickname to the Command appliance. This setting is available only on the Command appliance.

Reset Packetstore
Delete all packets stored on the ExtraHop Trace appliance. The Reset Packetstore page appears only on the Trace appliance.

Running Config

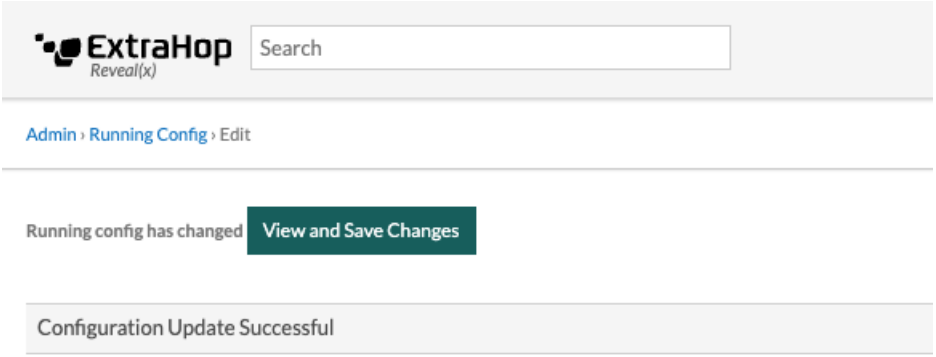
The running configuration file specifies the default system configuration. When you modify system settings, you must save the running configuration file to preserve those modifications after a system restart.

Note: Making configuration changes to the code from the Edit page is not recommended. You can make most system modifications through other pages in the Administration settings.

Save system settings to the running configuration file

When you modify any of the system configuration settings on an ExtraHop system, you must confirm the updates by saving the running configuration file. If you do not save the settings, the changes are lost when your ExtraHop system restarts.

To remind you that the running configuration has changed, (Unsaved changes) appears next to the Running Config link on the main Administration settings page, as well as a **View and Save Changes** button on all Administration settings pages, as shown below.



1. Click **View and Save Changes**.
2. Review the comparison between the old running configuration and the current (unsaved) running configuration, and then select from the following options:
   - If the changes are correct, click **Save**.
   - If the changes are not correct, click **Cancel** and then revert the changes by clicking **Revert config**.

Edit the running config

The ExtraHop Administration settings provide an interface to view and modify the code that specifies the default system configuration. In addition to making changes to the running configuration file through the Administration settings, changes can also be made on the Running Config page.

Note: Making configuration changes to the code from the Edit page is not recommended. You can make most system modifications through other Administration settings.

Download the running configuration as a text file

You can download the running configuration file to your workstation. You can open this text file and make changes to it locally, before copying those changes into the Running Config window.

1. Click **Running Config**.
2. Click **Download config as a File**.

The current running configuration file is downloaded as a text file to your default download location.

Disable ICMPv6 Destination Unreachable messages

You can prevent the ExtraHop system from generating ICMPv6 Destination Unreachable messages. You might want to disable ICMPv6 Destination Unreachable messages for security reasons per RFC 4443.

To disable ICMPv6 Destination Unreachable messages, you must edit the Running Configuration. However, we recommend that you do not manually edit the Running Configuration file without direction from ExtraHop Support. Manually editing the running config file incorrectly might cause the system to become unavailable or stop collecting data. You can contact ExtraHop Support.

Disable specific ICMPv6 Echo Reply messages

You can prevent the ExtraHop system from generating Echo Reply messages in response to ICMPv6 Echo Request messages that are sent to an IPv6 multicast or anycast address. You might want to disable these messages to reduce unnecessary network traffic.

To disable specific ICMPv6 Echo Reply messages, you must edit the running configuration file. However, we recommend that you do not manually edit the running configuration file without direction from ExtraHop Support. Manually editing this file incorrectly might cause the system to become unavailable or stop collecting data. You can contact ExtraHop Support.

Services

These services run in the background and perform functions that do not require user input. These services can be started and stopped through the Administration settings.

Enable or disable the Management GUI

The Management GUI provides browser-based access to the ExtraHop system. By default, this service is enabled so that ExtraHop users can access the ExtraHop system through a web browser. If this service is disabled, the Apache Web Server session is terminated and all browser-based access is disabled.

Warning: Do not disable this service unless you are an experienced ExtraHop administrator and you are familiar with the ExtraHop CLI.

Enable or disable the SNMP Service

Enable the SNMP service on the ExtraHop system when you want your network device monitoring software to collect information about the ExtraHop system. This service is disabled by default.

- Enable the SNMP service from the Services page by selecting the Disabled checkbox and then clicking **Save**. After the page refreshes, the Enabled checkbox appears.
- Configure the SNMP service and download the ExtraHop MIB file

Enable or disable SSH Access

SSH access is enabled by default to enable users to securely log in to the ExtraHop command-line interface (CLI).

Note: The SSH Service and the Management GUI Service cannot be disabled at the same time. At least one of these services must be enabled to provide access to the system.

Enable or disable the SSL Session Key Receiver (Sensor only)

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

Note: If you do not see this checkbox and have purchased the SSL Decryption license, contact ExtraHop Support to update your license.

SNMP Service

Configure the SNMP service on your ExtraHop system so that you can configure your network device monitoring software to collect information about your ExtraHop system through the Simple Network Management Protocol (SNMP).

For example, you can configure your monitoring software to determine how much free space is available on an ExtraHop system and send an alert if the system is over 95% full. Import the ExtraHop SNMP MIB file into your monitoring software to monitor all ExtraHop-specific SNMP objects. You can configure settings for SNMPv1/SNMPv2 and SNMPv3

Configure the SNMPv1 and SNMPv2 service

You can configure the SNMPv1 and SNMPv2 service on your ExtraHop system.

1. On the Services page, next to SNMP Service, click **Configure**.
2. Configure the following settings to enable the SNMPv1 and SNMPv2 service:

Enabled

Select the checkbox to enable the SNMP service.

SNMPv1 and SNMPv2 Enabled

Select the checkbox to enable the SNMPv1 and SNMPv2 service.

SNMP Community

Type a friendly name for the SNMP community.

SNMP System Contact

Type a valid name or email address for the SNMP system contact.

SNMP System Location

Type a location for the SNMP system.

3. Click **Save Settings**.

Next steps
Download the ExtraHop SNMP MIB file from the SNMP Service Configuration page.

Configure the SNMPv3 service
You can configure the SNMPv3 service on your ExtraHop system. The SNMPv3 security model provides additional support for authentication and privacy protocols.

1. On the Services page, next to SNMP Service, click **Configure**.
2. Configure the following settings to enable the SNMPv3 service:

SNMPv3 Enabled

Select the checkbox to enable the SNMPv3 service.

SNMPv3 User Name

Type the name of the user that can access the SNMPv3 service.

Authentication and Privacy Mode

Select **Authentication and Privacy** or **Authentication and No Privacy** from the drop-down list. If you select **Authentication and Privacy**, you must also complete the **Privacy Password** field.

Important: ExtraHop systems support AES-128 encryption for privacy of SNMPv3 messages.

Authentication Password

Type a password for the user to authenticate to the SNMPv3 service.

Authentication Algorithm

Select **SHA-256** or **SHA-1** as the authentication protocol from the drop-down list.

Privacy Password

Type the password to decrypt SNMPv3 traps. This field is required if you select **Authentication and Privacy**.

3. Click **Save Settings**.

Next steps
Download the ExtraHop SNMP MIB file from the SNMP Service Configuration page.

Firmware

The Administration settings provide an interface to upload and delete the firmware on ExtraHop appliances. The firmware file must be accessible from the computer where you will perform the upgrade.

Before you begin
Be sure to read the release notes for the firmware version that you want to install. Release notes contain upgrade guidance as well as known issues that might affect critical workflows in your organization.

Upgrade the firmware on your ExtraHop system

The following procedure shows you how to upgrade your ExtraHop system to the latest firmware release. While the firmware upgrade process is similar across all ExtraHop appliances, some appliances

have additional considerations or steps that you must address before you install the firmware in your environment. If you need assistance with your upgrade, contact ExtraHop Support.

Important: When settings migration fails during firmware upgrade, the previously installed firmware version and ExtraHop system settings are restored.

Pre-upgrade checklist
Here are some important considerations and requirements about upgrading ExtraHop appliances.

- A system notice appears on consoles and sensors connected to ExtraHop Cloud Services when a new firmware version is available.
- Verify that your Reveal(x) 360 system has been upgraded to version 9.2 before upgrading your self-managed sensors.
- If you are upgrading from firmware version 8.7 or earlier, contact ExtraHop Support for additional upgrade guidance.
- If you have multiple types of ExtraHop appliances, you must upgrade them in the following order:

  1. Console
  2. Sensors (EDA and Ultra)
  3. Recordstores
  4. Packetstores

Note: Your browser might time out after 5 minutes of inactivity. Refresh the browser page if the update appears incomplete.

If the browser session times out before the ExtraHop system is able to complete the update process, you can try the following connectivity tests to confirm the status up the upgrade process:

- Ping the appliance from the command line of another appliance or client workstation.
- From the Administration settings on a console, view the appliance status on the Manage Connected Appliances page.
- Connect to the appliance through the iDRAC interface.

Console upgrades

- For large console deployments (managing 50,000 devices or more), reserve a minimum of one hour to perform the upgrade.
- The console firmware version must be greater than or equal to the firmware version of all connected appliances. To ensure feature compatibility, all connected appliances should be running firmware version 8.7 or later.

Recordstore upgrades

- Do not upgrade recordstores to a firmware version that is newer than the version installed on connected consoles and sensors.
- After upgrading the console and sensors, disable record ingest on the recordstore before upgrading the recordstore.
- You must upgrade all recordstore nodes in a recordstore cluster. The cluster will not function correctly if nodes are on dissimilar firmware versions.

  Important: The message `Could not determine ingest status on some nodes` and `Error` appear on the Cluster Data Management page in the Administration settings of the upgraded nodes until all nodes in the cluster are upgraded. These errors are expected and can be ignored.
- You must enable record ingest and shard reallocation from the Cluster Data Management page after all nodes in the recordstore cluster are upgraded.

Packetstore upgrades

- Do not upgrade packetstores to a firmware version that is newer than the version installed on connected consoles and sensors.

Upgrade the firmware on a console and sensor

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 **Firmware**.
3. From the **Available Firmware** drop-down list, select the version of firmware that you want to install. The recommended version is selected by default.

   Note: For sensors, the list includes only firmware versions that are compatible with the version running on the connected console.
4. Click **Download and Install**.

After the firmware upgrade installs successfully, the ExtraHop appliance restarts.

Upgrade the firmware on recordstores

1. Download the firmware for the appliance from the ExtraHop Customer Portal to your computer.
2. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
3. Click **Cluster Data Management**.
4. Click **Disable Record Ingest**.
5. Click **Admin** to return to the main Administration page.
6. Click **Firmware**.
7. Click **Upgrade**.
8. On the Upgrade Firmware page, select one of the following options:
   - To upload firmware from a file, click **Choose File**, navigate to the `.tar` file you want to upload, and click **Open**.
   - To upload firmware from a URL, click **retrieve from URL** instead and then type the URL in the Firmware URL field.
9. Click **Upgrade**.
   The ExtraHop system initiates the firmware upgrade. You can monitor the progress of the upgrade with the Updating progress bar. The appliance restarts after the firmware is installed.
10. Repeat steps 6-9 on all remaining recordstore cluster nodes.

Next steps
After all nodes in the recordstore cluster are upgraded, re-enable record ingest and shard reallocation on the cluster. You only need to perform these steps on one recordstore node.

1. In the Explore Cluster Settings section, click **Cluster Data Management**.
2. Click **Enable Record Ingest**.
3. Click **Enable Shard Reallocation**.

Upgrade the firmware on packetstores

1. Download the firmware for the appliance from the ExtraHop Customer Portal to your computer.
2. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
3. Click **Upgrade**.
4. On the Upgrade Firmware page, select one of the following options:

- To upload firmware from a file, click **Choose File**, navigate to the `.tar` file you want to upload, and click **Open**.
- To upload firmware from a URL, click **retrieve from URL** instead and then type the URL in the Firmware URL field.

5. (Optional) If you do not want to automatically restart the appliance after the firmware is installed, clear the **Automatically restart appliance after installation** checkbox.
6. Click **Upgrade**.
   The ExtraHop system initiates the firmware upgrade. You can monitor the progress of the upgrade with the Updating progress bar. The appliance restarts after the firmware is installed.
7. If you did not choose to automatically restart the appliance, click **Reboot** to restart the system.
   After the firmware update is installed successfully, the ExtraHop appliance displays the version number of the new firmware on the Administration settings.

Upgrade connected sensors in Reveal(x) 360
Administrators can upgrade sensors that are connected to Reveal(x) 360.

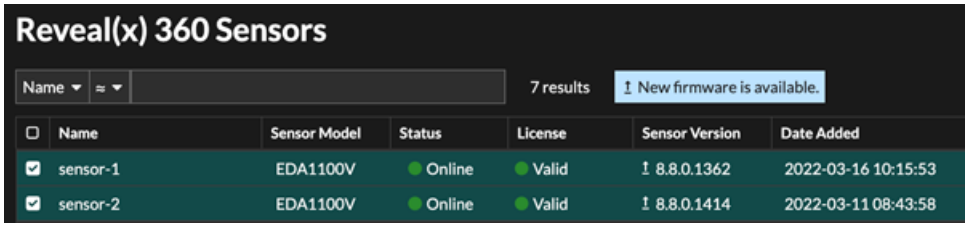
Before you begin

- Your user account must have privileges on Reveal(x) 360 for System and Access Administration or System Administration.

Here are some considerations about upgrading sensors:

- Sensors must be connected to ExtraHop Cloud Services
- Notifications appear when a new firmware version is available
- You can upgrade multiple sensors at the same time

1. Log in to Reveal(x) 360.
2. Click the System Settings icon and then click **Sensors**.
   Sensors that are eligible for upgrade display an up arrow in the Sensor Version field.



3. Select the checkbox next to each sensor that you want to upgrade.
4. In the Sensor Details pane, select the firmware version from the **Available Firmware** drop-down list.
   The drop-down list only displays versions that are compatible with the selected sensors.
   Only the selected sensors that have a firmware upgrade available appear in the Sensor Details pane.
5. Click **Install Firmware**.
   When the upgrade completes, the Sensor Version field is updated with the new firmware version.

System Time

The System Time page displays the current time settings configured for your ExtraHop system. View the current system time settings, the default display time for users, and details for configured NTP servers.

System time is the time and date tracked by services running on the ExtraHop system to ensure accurate time calculations. By default, the system time on the sensor or console is configured locally. For better accuracy, we recommend that you configure the system time through an NTP time server.

When capturing data, the system time must match the time on connected sensors to ensure that time stamps are correct and complete in scheduled dashboard reports, exported dashboards and chart metrics. If time sync issues occur, check that the configured system time, external time servers, or NTP servers are accurate. Reset the system time or sync NTP servers if needed

The table below contains details about the current system time configuration. Click **Configure Time** to configure system time settings.

Detail	Description
Time Zone	Displays the currently selected time zone.
System Time	Displays the current system time.
Time Servers	Displays a comma-separated list of configured time servers.

Default display time for users

The Default Display Time for Users section shows the time displayed to all users in the ExtraHop system unless a user manually changes their displayed time zone.

To modify the default display time, select one of the following options and then click **Save Changes**:

- Browser time
- System time
- UTC

NTP Status

The NTP Status table displays the current configuration and status of all NTP servers that keep the system clock in sync. The table below contains details about each configured NTP server. Click **Sync Now** to sync the current system time to a remote server.

remote	The host name or IP address of the remote NTP server you have configured to synchronize with.
st	The stratum level, 0 through 16.
t	The type of connection. This value can be `u` for unicast or manycast, `b` for broadcast or multicast, `l` for local reference clock, `s` for symmetric peer, `A` for a manycast server, `B` for a broadcast server, or `M` for a multicast server.
when	The last time when the server was queried for the time. The default value is seconds, or `m` is displayed for minutes, `h` for hours, and `d` for days.
poll	How often the server is queried for the time, with a minimum of 16 seconds to a maximum of 36 hours.
reach	Value that shows the success and failure rate of communicating with the remote server. Success means the bit is set, failure means the bit is not set. `377` is the highest value.
delay	The round trip time (RTT) of the ExtraHop appliance communicating with the remote server, in milliseconds.
offset	Indicates how far off the ExtraHop appliance clock is from the time reported by the server. The value can be positive or negative, displayed in milliseconds.
jitter	Indicates the difference, in milliseconds, between two samples.

Configure the system time

By default, the ExtraHop system synchronizes the system time through the *.extrahop.pool.ntp.org network time protocol (NTP) servers. If your network environment prevents the ExtraHop system from communicating with these time servers, you must configure an alternate time server source.

Before you begin

Important: Always configure more than one NTP server to increase the accuracy and reliability of time kept on the system.

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 **System Time**.
3. Click **Configure Time**.
4. Select your time zone from the drop-down list then click **Save and Continue**.
5. On the Time Setup page, select one of the following options:
   - Set time manually

     Note: You cannot manually set the time for sensors that are managed by a console or Reveal(x) 360.
   - Set time with NTP server
6. Select **Set time with NTP server** and then click **Select**.

   The ExtraHop time servers, `0.extrahop.pool.ntp.org`, `1.extrahop.pool.ntp.org`, `2.extrahop.pool.ntp.org`, and `3.extrahop.pool.ntp.org` appear in the first four Time Server fields by default.
7. Type the IP address or fully qualified domain name (FQDN) for the time servers in the Time Server fields. You can have up to nine time servers.

   Tip: After adding the fifth time server, click **Add Server** to display up to four additional timer server fields.
8. Click **Done**.

The NTP Status table displays a list of NTP servers that keep the system clock in sync. To sync the current system time a remote server, click the **Sync Now** button.

Shutdown or Restart

The Administration settings provides an interface to halt, shutdown, and restart the ExtraHop system and its system components. For each ExtraHop system component, the table includes a time stamp to show the start time.

- Restart or shutdown System to pause or shut down and restart the ExtraHop system.
- Restart Bridge Status (Sensor only) to restart the ExtraHop bridge component.
- Restart Capture (Sensor only) to restart the ExtraHop capture component.
- Restart Portal Status to restart the ExtraHop web portal.
- Restart Dashboard Reports (Console only) to restart the ExtraHop scheduled dashboard reports component.

Sensor Migration

You can migrate your stored metrics, customizations and system resources on your existing physical ExtraHop sensor to a new sensor.

Help on this page

- Migrate an ExtraHop sensor

Migrate an ExtraHop sensor

When you are ready to upgrade your existing sensor, you can easily migrate to new hardware without losing business critical metrics and time-consuming system configurations.

The following customizations and resources are not saved when you create a backup or migrate to a new target.

- License information for the system. If you are restoring settings to a new target, you must manually license the new target.
- Precision packet captures. You can download saved packet captures manually by following the steps in View and download packet captures.
- When restoring an ECA VM console that has a tunneled connection from a sensor, the tunnel must be reestablished after the restore is complete and any customizations on the console for that sensor must be manually recreated.
- User-uploaded SSL keys for traffic decryption.
- Secure keystore data, which contains passwords. If you are restoring a backup file to the same target that created the backup, and the keystore is intact, you do not need to re-enter credentials. However, if you are restoring a backup file to a new target or migrating to a new target, you must re-enter the following credentials:
  - Any SNMP community strings provided for SNMP polling of flow networks.
  - Any bind password provided to connect with LDAP for remote authentication purposes.
  - Any password provided to connect to an SMTP server where SMTP authentication is required.
  - Any password provided to connect to an external datastore.
  - Any password provided to access external resources through the configured global proxy.
  - Any password provided to access ExtraHop Cloud Services through the configured ExtraHop cloud proxy.
  - Any authentication credentials or keys provided to configure Open Data Stream targets.

Before you begin

Important: If the source sensor has an external datastore and the datastore is configured on a CIFS/SMB server requiring password authentication, contact ExtraHop Support to assist you with your migration.

- Source and target sensors must be running the same firmware version.
- Migrate only to same-edition sensors, such as Reveal(x). If you need to migrate between editions, contact your ExtraHop sales team for assistance.
- Migration is only supported between physical sensors. Virtual sensor migrations are not supported.
- Supported migration paths are listed in the following tables.

Table 3: Reveal(x) Compatibility Matrix

Source	Target				
	EDA 1200	EDA 6200	EDA 8200	EDA 9200	EDA 10200
EDA 1200	YES	YES	YES	YES	YES
EDA 6200	NO	YES*	YES	YES	YES
EDA 8200	NO	NO	YES*	YES*	YES
EDA 9200	NO	NO	NO	YES*	YES

Source	Target				
EDA 10200	NO	NO	NO	NO	YES*

*Migration is supported only if the source and target sensor were manufactured in May 2019 or later. Contact ExtraHop Support to verify compatibility.

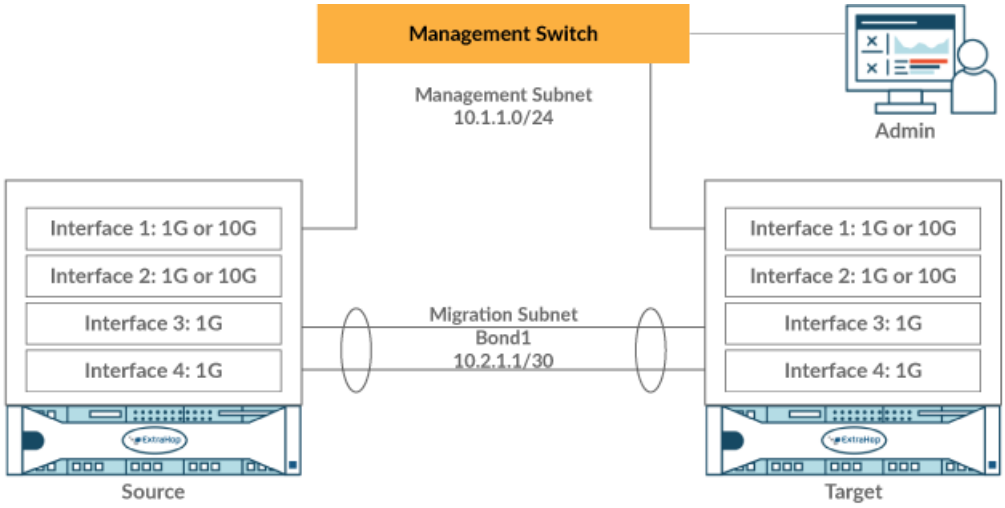
Table 4: Performance Edition Compatibility Matrix

Source	Target			
	EDA 6200	EDA 8200	EDA 9200	EDA 10200
EH3000	YES	YES	YES	YES
EH6000	YES	YES	YES	YES
EH8000	NO	YES	YES	YES
EDA 1100	YES	YES	YES	YES
EDA 3100	YES	YES	YES	YES
EDA 6100	YES	YES	YES	YES
EDA 8100	NO	YES	YES	YES
EDA 9100	NO	NO	YES	YES
EDA 6200	YES*	YES	YES	YES
EDA 8200	NO	YES*	YES*	YES
EDA 9200	NO	NO	YES*	YES
EDA 10200	NO	NO	NO	YES*

* Migration is supported only if the source and target sensor were manufactured in May 2019 or later. Contact ExtraHop Support to verify compatibility.

Prepare the source and target sensors

1. Follow the instructions in the deployment guide for your sensor model to deploy the target sensor.
2. Register the target sensor.
3. Make sure that the target and the source sensor are running the exact same firmware version. You can download current and previous firmware from the ExtraHop Customer Portal.
4. Choose one of the following networking methods to migrate to the target sensor.
   - (Recommended) To complete the migration in the fastest time possible, directly connect the sensors with 10G management interfaces.
   - Create a bond interface (optional) of available 1G management interfaces. With the appropriate network cables, directly connect the available port or ports on the source sensor to similar ports on the target sensor. The figure below shows an example configuration with bonded 1G interfaces.



Important: Make sure that your IP address and subnet configuration on both sensors route management traffic to your management workstation and migration traffic to the direct link.

- Migrate the sensor over your existing network. The source and target sensors must be able to communicate with each other over your network. Note that migration might take significantly longer with this configuration.

Create a bond interface (optional)
Follow the instructions below to bond 1G interfaces. Creating a bond interface decreases the amount of time it takes to complete the migration over 1G interfaces.

1. In the Network Settings section on the source sensor, click **Connectivity**.
2. In the Bond Interface Settings section, click **Create Bond Interface**.
3. In the Members section, Select the members of the bond interface depending on the sensor type. Do not include the current management interface, typically interface 1 or interface 3, in the bond interface.
4. From the Take Settings From drop-down list, select one of the members of the new bond interface.
5. For Bond Type, select **Static**.
6. Click **Create**.
7. On the Connectivity page, in the Bond Interfaces section, click **Bond Interface 1**.
8. From the Interface Mode drop-down menu, select **Management**.
9. Type the IPv4 Address, Netmask, and Gateway for your migration network.
10. Click **Save**.
11. Repeat this procedure on the target sensor.

Start the migration
Migration can take several hours to complete. During this time, neither the source nor the target sensor can collect data. The migration process cannot be paused or canceled.

1. Log in to the Administration settings on the source sensor.
2. In the Network Settings section, click **Connectivity**.
3. Write down the IP address of the management interface, DNS servers, and any static routes. You will configure these settings on the target after the migration completes.
4. In the Appliance Settings section, click **Appliance Migration**.
5. In the Target Appliance field, type the IP address of the interface you configured for migration on the target.

6. In the Setup User Password field, type the password of the setup user on the target. The default password is the system serial number of the target sensor.
7. Click **Continue**.
8. On the Confirm Fingerprint page, make sure that the fingerprint that appears on this page exactly matches the fingerprint that appears on the Fingerprint page in the Administration settings on the target. If the fingerprints do not match, make sure that you specified the correct hostname or IP address of the target that you entered in step 5.
9. Click **Start Migration**.
   Wait for the migration success message to appear, which can take several hours. During the migration, the ExtraHop system on the target is inaccessible. If you inadvertently close the Appliance Migration Status page on the source, you can return to `https://<source hostname>/admin/appliance_migration_status/` to continue monitoring the migration.

   If the migration fails for any reason, restart the migration. If the migration continues to fail, contact ExtraHop Support for assistance.

   Note: The target automatically reboots after the migration completes.
10. Click **Shut Down** to power off the source.

    Important: To prevent sensor ID conflicts, do not power on the source sensor while it is connected to the same network where the target sensor is located unless you reset the sensor through the ExtraHop Rescue Media.

Configure the target sensor
If sensor networking is not configured through DHCP, make sure connectivity settings are updated, including any assigned IP addresses, DNS servers, and static routes. Connections to ExtraHop consoles, recordstores, and packetstores on the source sensor are automatically established on the target sensor when network settings are configured.

1. Log in to the Administration settings on the target sensor.
2. In the Network Settings section, click **Connectivity**.
3. In the Interfaces section, click the management interface (typically interface 1 or interface 3, depending on the sensor model).
4. Type the IP address of the source sensor in the IPv4 Address field.
5. If static routes were configured on the source sensor, click **Edit Routes**, add any required route information, and then click **Save**.
6. Click **Save** to save the interface settings.
7. If you had to change any interface settings to perform the migration with bonded interfaces, make sure that the interface modes are configured as you expect them to be.
8. Restore any additional settings that are not automatically restored.

License

The License Administration page enables you to view and manage licenses for your ExtraHop system. You must have an active license to access the ExtraHop system, and your system must be able to connect to the ExtraHop licensing server for periodic updates and check-ins about your license status.

To learn more about ExtraHop licenses, see the License FAQ.

Register your ExtraHop system

This guide provides instructions on how to apply a new product key and activate all of your purchased modules. You must have privileges on the ExtraHop system to access the Administration settings.

Register the appliance

Before you begin

Note: If you are registering a sensor or a console, you can optionally enter the product key after you accept the EULA and log in to the ExtraHop system (`https://<extrahop_ip_address>/`).

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. Review the license agreement, select I Agree, and then click **Submit**.
3. On the login screen, type `setup` for the username.
4. For the password, select from the following options:
   - For 1U and 2U appliances, type the serial number printed on the label on the back of the appliance. The serial number can also be found on the LCD display on the front of the appliance in the `Info` section.
   - For the EDA 1100, type the serial number displayed in the `Appliance info` section of the LCD menu. The serial number is also printed on the bottom of the appliance.
   - For the EDA 1200, type the serial number printed on the back of the appliance.
   - For a virtual appliance in AWS, type the instance ID, which is the string of characters that follow i- (but not i- itself).
   - For a virtual appliance in GCP, type the instance ID.
   - For all other virtual appliances, type `default`.
5. Click **Log In**.
6. In the Appliance Settings section, click **License**.
7. Click **Manage License**.
8. If you have a product key, click **Register** and type your product key into the field.

   Note: If you received a license file from ExtraHop Support, click **Manage License**, click **Update**, then paste the contents of the file into the Enter License field. Click **Update**.
9. Click **Register**.

Next steps

Have more questions about ExtraHop licensing works? See the License FAQ.

Troubleshoot license server connectivity

For ExtraHop systems licensed and configured to connect to ExtraHop Cloud Services, registration and verification is performed through an HTTPS request to ExtraHop Cloud Services.

If your ExtraHop system is not licensed for ExtraHop Cloud Services or is not yet licensed, the system attempts to register the system through a DNS TXT request for `regions.hopcloud.extrahop.com` and an HTTPS request to all ExtraHop Cloud Services regions. If this request fails, the system tries to connect to the ExtraHop licensing server through DNS server port 53. The following procedure is useful to verify that the ExtraHop system can communicate with the licensing server through DNS.

Open a terminal application on your Windows, Linux, or macOS client that is on the same network as your ExtraHop system and run the following command:

```
nslookup -type=NS d.extrahop.com
```

If the name resolution is successful, output similar to the following appears:

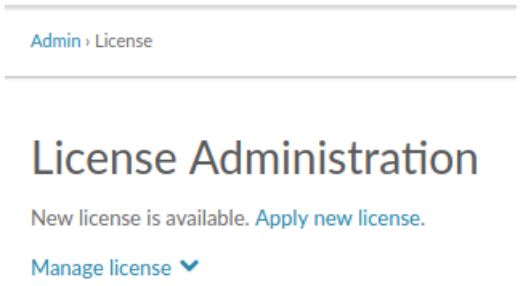
```
Non-authoritative answer:
d.extrahop.com  nameserver = ns0.use.d.extrahop.com.
d.extrahop.com  nameserver = ns0.usw.d.extrahop.com.
```

If the name resolution is not successful, make sure that your DNS server is properly configured to lookup the `extrahop.com` domain.

Apply an updated license

When you purchase a new protocol module, service, or feature, the updated license is automatically available on the ExtraHop system. However you must apply the updated license to the system through the Administration settings for the new changes to take effect.

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 **License**. A message appears about the availability of your new license, as shown in the following figure.



3. Click **Apply new license**. The capture process restarts, which might take a few minutes.

Note: If your license is not automatically updated, troubleshoot licensing server connectivity or contact ExtraHop Support.

Update a license

If ExtraHop Support provides you with a license file, you can install this file on your appliance to update the license.

Note: If you want to update the product key for your appliance, you must register your ExtraHop system.

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 **License**.
3. Click Manage License.
4. Click **Update**.
5. In the Enter License text box, enter the licensing information for the module.

   Paste the license text provided to you by ExtraHop Support. Be sure to include all of the text, including the `BEGIN` and `END` lines, as shown in the example below:

```
-----BEGIN EXTRAHOP LICENSE-----
serial=ABC123D;
dossier=1234567890abcdef1234567890abcdef;
mod_cifs=1;
mod_nfs=1;
mod_amf=0;
live_capture=1;
capture_upload=1;
...
ssl_decryption=0;
+++;
```

```
ABCabcDE/FGHIjklm12nopqrstuvwXYZAB12345678abcde901abCD;
12ABCDEFG1HIJklmnOP+1aA=;
=abcd;
-----END EXTRAHOP LICENSE-----
```

6. Click **Update**.

Disks

The Disks page displays a map of the drives on the ExtraHop system and lists their statuses. This information can help you determine whether drives need to be installed or replaced. Automatic system health checks and email notifications (if enabled) can provide timely notice about a disk that is in a degraded state. System health checks display disk errors at the top of the Settings page.

Self-encrypting disks (SEDs)

For sensors that include self-encrypting disks (SEDs), the `Hardware Disk Encryption` status can be set to `Disabled` or `Enabled`. This status set to `Unsupported` for sensors that do not include SEDs.

These sensors support SEDs:

- EDA 9300
- EDA 10300
- IDS 9380

For information about configuring SEDs, see Configure self-encrypting disks.

RAID

For information about configuring and repairing RAID10 functionality on the EDA 6200 sensors, see Upgrade from RAID 0 to RAID 10.

For help replacing a RAID 0 disk or installing an SSD drive, refer to the instructions below. The RAID 0 instructions apply to the following types of disks:

- Datastore
- Packet Capture
- Firmware

Do not attempt to install or replace the drive in Slot 0 unless instructed by ExtraHop Support.

Note: Ensure that your device has a RAID controller before attempting the following procedure. If unsure, contact ExtraHop Support. A persistently damaged disk might not be replaceable with this procedure.

Replace a RAID 0 disk

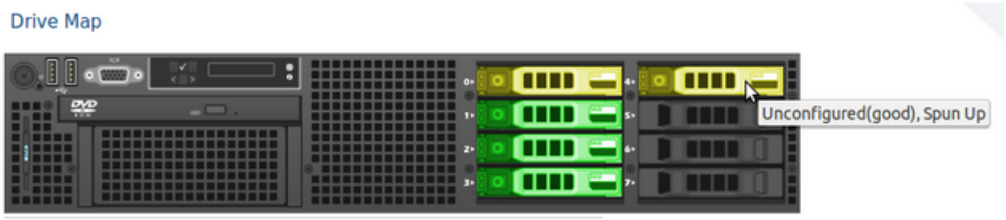
1. In the system health email notification, note which machine has the problematic disk.
2. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
3. In the Appliance Settings section, click **Disks**.
4. Under the section for the disk type (for example, **Datastore**), find the problematic disk and note the slot number.

   Click **RAID Disk Details** to display more details.

   Important: Keep the failed disk until data has been successfully copied to the new disk.
5. Insert an identical disk into an available slot.

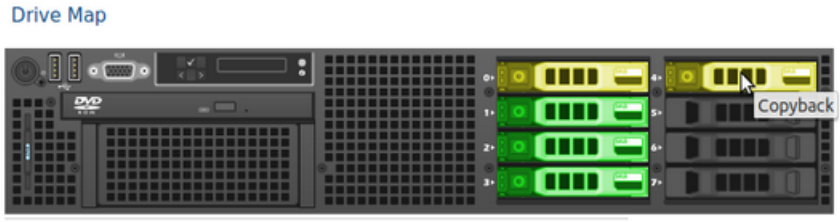
The system detects the new disk and adds a new row (Disk Error Action) with a link to replace the bad disk.

6. Verify the new disk information:
   - Under **Unused Disks** on the Disk Details page, verify that the new disk is the same size, speed, and type as the disk being replaced.
   - Mouse over the old and new disks in the Drive Map. The new disk displays the message "`Unconfigured(good), Spun Up`."



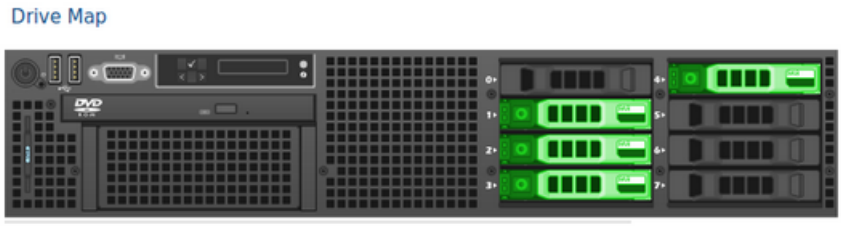
7. Under the section for the disk type, click **Replace with Disk in slot #n** in the Disk Error Action row.

   The data begins copying over. The Copy Status row displays the progress. Mousing over the disk in the Drive Map shows the status.



8. After copying is complete, make sure that the copy process was successful:
   - **Settings** button and Settings page no longer display error messages.
   - Disk page shows the old disk under the Unused Disk section
9. Remove the old disk.

   The Drive Map now shows the new disk in green.



Install a new packet capture disk

1. In the Appliance Settings section, click **Disks**.
   If the Drive Map shows the slot where the SSD is installed in red, you must replace the SSD.
2. Insert the SSD drive into the slot where the previous SSD was installed and wait for the LED on the drive to turn green.
3. In the Administration settings, refresh the browser.

   The Drive Map shows the SSD slot in yellow because the drive is not configured.

4. Next to SSD Assisted Packet Capture, click **Enable**.

Unused Disks

RAID Info	
Status	Unused
RAID Level	None

Disk / Span	Slot #	Status	Media Type
Disk #14	14	Unconfigured(good), Spun Up	Solid State Device

5. Click **OK** to add the packet capture drive.

   The page refreshes and the Drive Map shows the SSD as green and the Status changes to `Online, Spun Up`.

Packet Capture

RAID Info	
Status	Optimal
RAID Level	Primary-0, Secondary-0, RAID Level Qualifier-0
Encryption Status	Not Encrypted
SSD Assisted Packet Capture	Configure

Disk / Span	Slot #	Status	Media Type
Span 0: Row 0	14	Online, Spun Up	Solid State Device

Tip: If the SSD drive is dislodged and reinserted, you can re-enable it. This process requires reformatting the disk, which erases all data.

Console Nickname

By default, your ExtraHop console is identified by its hostname on connected sensors. However, you can optionally configure a custom name to identify your console.

Choose from the following options to configure the display name:

- Select **Display custom nickname** and type the name in the field you want to display for this console.
- Select **Display hostname** to display the hostname configured for this console.

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.

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** next to Triggered Packet Capture, 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.

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.

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** next to Triggered Packet Capture.
   - 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** next to Triggered Packet Capture.
   - 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**.
3. In the Start Global Packet Capture section, complete the following fields. You only need to specify the criteria you want for the packet capture:

   • **Name:** A name to identify the packet capture.

   • **Max Packets:** The maximum number of packets to capture.

   • **Max Bytes:** The maximum number of bytes to captures.

   • **Max Duration (milliseconds):** The maximum duration of the packet capture in milliseconds. We recommend the default value of 1000 (1 second), or configure up to 60000 milliseconds (1 minute).

   • **Snaplen:** 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.
4. Click **Start**.

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

Download your packet capture.

- On Reveal(x) 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 Reveal(x) Enterprise systems, click **Records** from the top menu. Select **Packet Capture** from the Record Type drop-down list. 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 Reveal(x) systems and on ExtraHop packetstores, view the Packets page.

The View and Download Packet Captures section only appears on ExtraHop Performance systems. On Reveal(x) 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 Reveal(x) systems.

Recordstore

You can send transaction-level records written by the ExtraHop system to a supported recordstore and then query those records from the Records page or REST API on your console and sensors.

Learn more about ExtraHop Records

- Records concepts

Send records from ExtraHop to Google BigQuery

You can configure your ExtraHop system to send transaction-level records to a Google BigQuery server for long-term storage, and then query those records from the ExtraHop system and the ExtraHop REST API. Records on BigQuery recordstores expire after 90 days.

Before you begin

- You need the BigQuery project ID
- You need the credential file (JSON) from your BigQuery service account. The service account requires the BigQuery Data Editor, BigQuery Data Viewer, and BigQuery User roles.
- For access to the ExtraHop Cloud Recordstore, your sensors must be able to access outbound TCP 443 (HTTPS) to these fully qualified domain names:
  - `bigquery.googleapis.com`
  - `bigquerystorage.googleapis.com`
  - `oauth2.googleapis.com`
  - `www.googleapis.com`
  - `www.mtls.googleapis.com`
  - `iamcredentials.googleapis.com`

  You can also review the public guidance from Google about computing possible IP address ranges for googleapis.com.
- If you want to configure the BigQuery recordstore settings with Google Cloud workload identity federation authentication, you need the configuration file from your workload identity pool.

  Note: The workload identity provider must be set up to provide a fully valid OIDC ID Token in response to a Client Credentials request. For more information about workload identity federation, see https://cloud.google.com/iam/docs/workload-identity-federation.

Send records from ExtraHop to BigQuery

Complete this procedure on all connected sensors and cosole.

Note: Any triggers configured to send records through `commitRecord` to an ExtraHop recordstore are automatically redirected to BigQuery. No further configuration is required.

Important: If your ExtraHop system includes a console, configure all appliances with the same recordstore settings or transfer management to manage settings from the console.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Records section, click **Recordstore**.
3. Select **Enable BigQuery as the recordstore**.

   Important: If you are migrating to BigQuery from a connected ExtraHop recordstore, you will no longer be able to access records stored on the recordstore.

4. In the Project ID field, type the ID for your BigQuery project. The project ID can be found in the BigQuery API console.
5. In the JSON Credential File field, click **Choose File** and select one of the following files:
   - The credential file saved from your BigQuery service account.

     See the Google Cloud documentation on how to create a service account and generate a service account key.

     Important: Create your service account with the following BigQuery roles:
     - BigQuery Data Editor
     - BigQuery Data Viewer
     - BigQuery User
   - The configuration file from your workload identity pool.
6. (Optional) If you chose the configuration file from your workload identity pool in the previous step, select **Authenticate through local Identity Provider for Workload Identity Federation** and enter the credentials from your identity provider in the following fields:
   - **Token URL**
   - **Client ID**
   - **Client Secret**
7. Click **Test Connection** to verify that your sensor can communicate with the BigQuery server.
8. Click **Save**.

After your configuration is complete, you can query for stored records in the ExtraHop system by clicking **Records**.

Important: Do not modify or delete the table in BigQuery where the records are stored. Deleting the table deletes all stored records.

Transfer recordstore settings

If you have an ExtraHop console connected to your ExtraHop sensors, you can configure and manage the recordstore settings on the sensor, or transfer the management of the settings to the console. Transferring and managing the recordstore settings on the console enables you to keep the recordstore settings up to date across multiple sensors.

Recordstore settings are configured for connected third-party recordstores and do not apply to the ExtraHop recordstore.

1. Log in to the Administration settings on the sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Records section, click **Recordstore**.
3. From the **Recordstore settings** drop-down list, select the Command appliance and then click **Transfer**.

   If you later decide to manage the settings on the sensor, select **this Discover appliance** from the Recordstore settings drop-down list and then click **Transfer**.

Send records from ExtraHop to Splunk

You can configure the ExtraHop system to send transaction-level records to a Splunk server for long-term storage, and then query those records from the ExtraHop system and the ExtraHop REST API.

Before you begin

- You must have version 7.0.3 or later of Splunk Enterprise and a user account that has administrator privileges.
- You must configure the Splunk HTTP Event Collector before your Splunk server can receive ExtraHop records. See the Splunk HTTP Event Collector documentation for instructions.

Note: Any triggers configured to send records through `commitRecord` to a recordstore are automatically redirected to the Splunk server. No further configuration is required.

Send records from ExtraHop to Splunk

Complete this procedure on all connected ExtraHop systems.

Important: If your ExtraHop system includes a console or Reveal(x) 360, configure all sensors with the same recordstore settings or transfer management to manage settings from the console or Reveal(x) 360.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Records section, click **Recordstore**.
3. Select **Enable Splunk as the recordstore**.

   Note: If you are migrating to Splunk from a connected ExtraHop recordstore, you will no longer be able to access records stored on the recordstore.
4. In the Record Ingest Target section, complete the following fields:
   - **Splunk Ingest Host:** The hostname or IP address of your Splunk server.
   - **HTTP Event Collector Port:** The port for the HTTP Event Collector to send records over.
   - **HTTP Event Collector Token:** The authentication token you created in Splunk for the HTTP Event Collector.
5. In the Record Query Target section, complete the following fields:
   - **Splunk Query Host:** The hostname or IP address of your Splunk server.
   - **REST API Port:** The port to send record queries over.
   - **Authentication Method:** The authentication method, which depends on your version of Splunk.

   For Splunk versions later than 7.3.0, select **Authenticate with token**, and then paste your Splunk authentication token. For instructions on how to create an authentication token, see the Splunk documentation.

   For Splunk versions earlier than 7.3.0, select **Authenticate with username and password**, and then type your Splunk credentials.
6. Clear the **Require certificate verification** checkbox if your connection does not require a valid SSL/TLS certificate.

   Note: Secure connections to the Splunk server can be verified through trusted certificates that you upload to the ExtraHop system.
7. In the Index Name field, type the name of the Splunk index where you want to store records.

   The default index on Splunk is called `main`, however, we recommend that you create a separate index for your ExtraHop records, and type the name of that index. For instructions for creating an index, see the Splunk documentation.
8. (ExtraHop sensor only) Click **Test Connection** to verify that the ExtraHop system can reach your Splunk server.
9. Click **Save**.

After your configuration is complete, you can query for stored records in the ExtraHop system by clicking **Records** from the top menu.

Transfer recordstore settings

If you have an ExtraHop console connected to your ExtraHop sensors, you can configure and manage the recordstore settings on the sensor, or transfer the management of the settings to the console. Transferring and managing the recordstore settings on the console enables you to keep the recordstore settings up to date across multiple sensors.

Recordstore settings are configured for connected third-party recordstores and do not apply to the ExtraHop recordstore.

1. Log in to the Administration settings on the sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Records section, click **Recordstore**.
3. From the **Recordstore settings** drop-down list, select the Command appliance and then click **Transfer**.

   If you later decide to manage the settings on the sensor, select **this Discover appliance** from the Recordstore settings drop-down list and then click **Transfer**.

ExtraHop Command Settings

The ExtraHop Command Settings section on the ExtraHop sensor enables you to connect an ExtraHop sensor to a console. Depending on your network configuration, you can establish a connection from the sensor (tunneled connection) or from the console (direct connection).

- We recommend that you log in to the Administration settings on your console and create a direct connection to the sensor. Direct connections are made from the console over HTTPS on port 443 and do not require special access. For instructions, see Connect an ExtraHop console to an ExtraHop sensor.
- If your sensor is behind a firewall, you can create an SSH tunnel connection from this sensor to your console. For instructions, see Connect to a console from a sensor.

Generate Token

You must generate a token on a sensor before you can connect to a console. The token ensures a secure connection, making the connection process less susceptible to machine-in-the-middle (MITM) attacks.

Click **Generate Token** and then complete the configuration on your console.

Connect to a console from a sensor

You can connect the ExtraHop sensor to the console through an SSH tunnel.

We recommend that you always connect sensors directly through the console; however, a tunneled connection might be required in network environments where a direct connection from the console is not possible because of firewalls or other network restrictions. After you connect the sensors, you can view and edit the sensor properties, assign a nickname, update firmware, check the license status, and create a diagnostic support package.

Before you begin

- You can only establish a connection to a sensor that is licensed for the same system edition as the console. For example, a console on Reveal(x) Enterprise can only connect to sensors on Reveal(x) Enterprise.

1. Log in to the Administration settings on the sensor.
2. In the ExtraHop Console Settings section, click **Connect Consoles**.
3. Click **Connect Console** and then and then configure the following fields:
   - **Host:** The hostname or IP address of the console.

     Note: You cannot specify an IPv6 link-local address.

   - **Setup password:** The password for the setup user on the console.
   - **Sensor nickname (Optional):** A friendly name for the sensor that appears on the Manage Connected Appliances page. If no friendly name is configured, the hostname for the sensor appears instead.
   - **Reset configuration:** If you select the Reset Configuration checkbox, existing sensor customizations such as device groups, alerts, and triggers will be removed from the sensor. Gathered metrics such as captures and devices will not be removed.
4. Click **Connect**.

Connect an ExtraHop console to an ExtraHop sensor

You can manage multiple ExtraHop sensors from a console. After you connect the sensors, you can view and edit the sensor properties, assign a nickname, upgrade firmware, check the license status, and create a diagnostic support package.

The console connects directly to the sensor over HTTPS on port 443. If it is not possible to establish a direct connection because of firewall restrictions in your network environment, you can connect to the console through a tunneled connection from the ExtraHop sensor.

Video Take the related training: Connect an Appliance to a Reveal(x) Enterprise Console (ECA)

Before you begin
You can only establish a connection to a sensor that is licensed for the same system edition as the console. For example, a console on Reveal(x) Enterprise can only connect to sensors on Reveal(x) Enterprise.

Important: We strongly recommend configuring a unique hostname. If the system IP address changes, the ExtraHop console can re-establish connection easily to the system by hostname.

Generate a token on the sensor

Generate a token on the sensor before beginning the connection procedure on the console.

1. Log in to the Administration settings on the sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the ExtraHop Command Settings section, click **Generate Token**.
3. Click **Generate Token**.
4. Copy the token and continue to the next procedure.

Connect the console and sensors

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Connected Appliance Administration section, click **Manage Sensors**.
3. In the ExtraHop Sensor section, click **Connect Sensor**.
4. Type the hostname or IP address of the sensor into the Host field.
5. Click **Connect**.
6. Configure the following fields:
   - **Token from ExtraHop Sensor:** The token that you generated on the sensor.
   - **Sensor Nickname (Recommended):** A friendly name for the ExtraHop system. If no nickname is entered, the system is identified by the hostname.
7. (Optional) Select **Reset configuration** to remove existing system customizations such as device groups, alerts, and triggers from the ExtraHop system. Gathered metrics such as captures and devices will not be removed.
8. Click **Connect**.

Manage Discover Appliances

From the Command appliance, you can view connected Discover appliances and manage some administrative tasks.

Select the checkbox for one or more connected Discover appliances. Then, select from the following administrative tasks.

- Click **Check License** to connect to the ExtraHop licensing server and retrieve the latest status for the selected Discover appliances. If your Command appliance is unable to access data from a connected Discover appliance, the license might be invalid.
- Click **Run Support Script** and then select from the following options:
  - Click **Run Default Support Script** to collect information about the selected Discover appliances. You can send this diagnostics file to ExtraHop Support for analysis.
  - Click **Run Custom Support Script** to upload a file from ExtraHop Support that provides small system changes or enhancements.
- Click **Upgrade Firmware** to upgrade the selected Discover appliance. You can enter a URL to the firmware on the Customer Portal website or upload the firmware file from your computer. With either option, we strongly recommend you read the firmware release notes and the firmware upgrade guide.
- Click **Disable** or **Enable** to temporarily alter the connection between Discover and Command appliances. When this connection is disabled, the Command appliance does not display the Discover appliance and cannot access the Discover appliance data.
- Click **Remove Appliance** to permanently disconnect selected Discover appliances.

ExtraHop Recordstore Settings

This section contains the following configuration settings for the ExtraHop recordstore.

- Configure automatic flow records (Sensors only)
- Connect to an ExtraHop recordstore
- Manage an ExtraHop recordstore (Console only)

Connect the console and sensors to ExtraHop recordstores

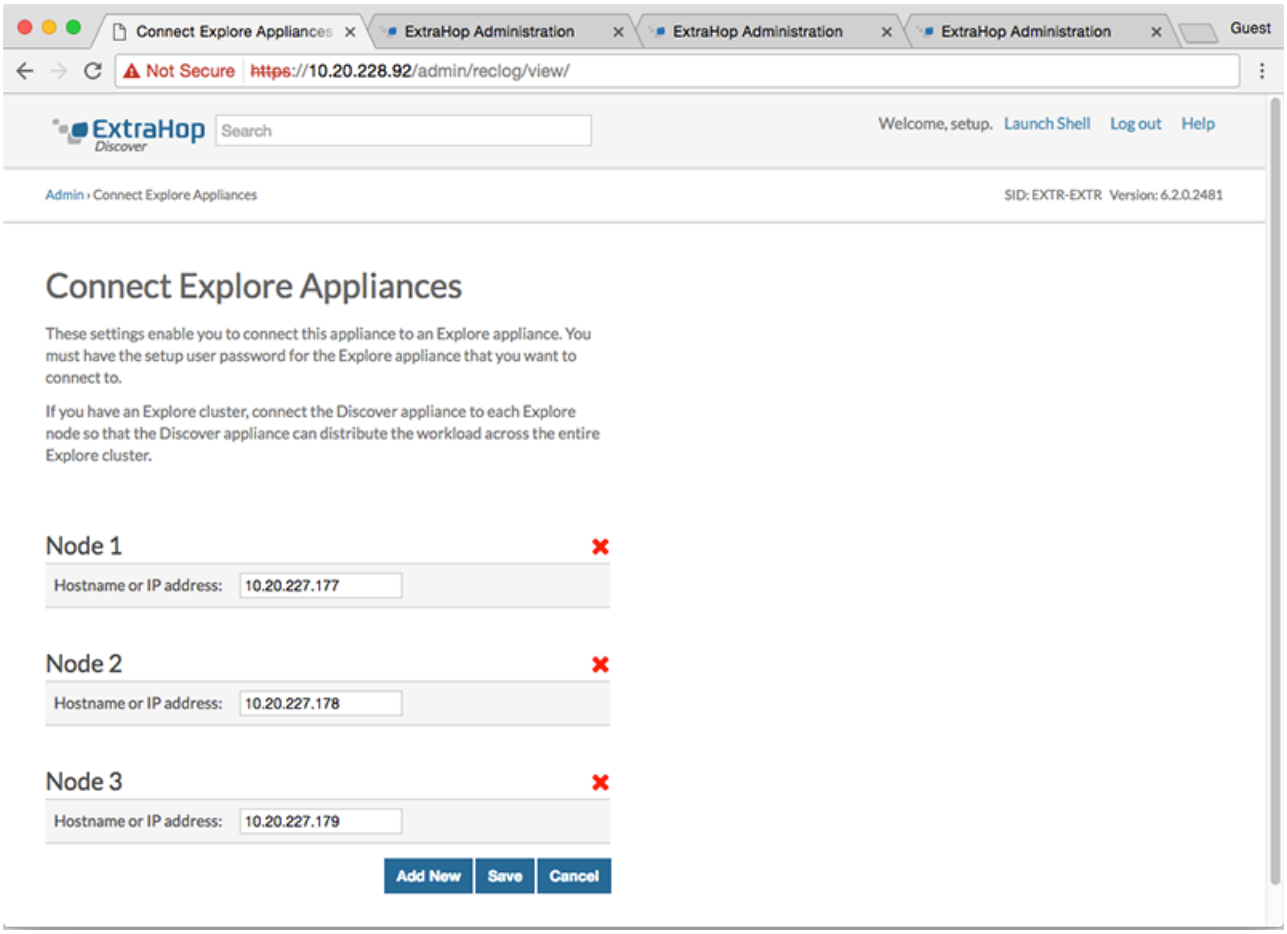
After you deploy an ExtraHop recordstore, you must establish a connection from all ExtraHop sensors and the console to the recordstore nodes before you can query for stored records.

Important: If your recordstore cluster is configured with manager-only nodes, only connect the sensors and console to the data-only nodes. Do not connect to the manager-only nodes.

1. Log in to the Administration settings on the console or sensor.

   Note: If the recordstore connections are managed from a console, you must perform this procedure from the console instead of from each sensor.
2. In the ExtraHop Recordstore Settings section, click **Connect Recordstores**.
3. Click **Add New**.
4. In the Node 1 field, type the hostname or IP address of any Explore appliance in the Explore cluster.

   Note: Only add data-only nodes if the cluster also contains manager-only nodes.
5. For each additional recordstore node in the cluster, click **Add New** and enter the individual hostname or IP address in the corresponding Node field.



6. Click **Save**.
7. Confirm that the fingerprint on this page matches the fingerprint of Node 1 of the cluster.
8. In the Explore Setup Password field, type the password for the Node 1 `setup` user account and then click **Connect**.
9. When the cluster settings are saved, click **Done**.
10. If the recordstore settings and not managed by a connected console, repeat this procedure on the console.

Disconnect the recordstore

To halt the ingest of records to the recordstore, disconnect all recordstore nodes from the console and sensors.

Note: If recordstore connections are managed by a console, you can only perform this procedure on the console.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the ExtraHop Recordstore Settings section, click **Connect Recordstores**.
3. Click the red **X** next to every node in the recordstore cluster.

4. Click **Save**.

Manage Explore Appliances

From the Command appliance, you can view connected Explore appliances and manage some administrative tasks.

View information about connected Explore appliances as individual appliances or as part of a cluster.

- Click **Explore Cluster** in the Name field to open the Cluster Properties. You can add a custom nickname for the Explore appliance and view the Cluster ID.
- Click any node name to open the node properties. By clicking **Open Admin UI**, you can access the Administration settings for the specific Explore appliance.
- View the date and time that the appliance was added to this Command appliance.
- View the license status for your appliances.
- View the list of actions that you can perform on this appliance.
- View the Job column to see the status of any running support scripts.

Select the Explore cluster or a single node in the cluster by clicking an empty area in the table, and then select from the following administrative tasks.

- Click **Run Support Script** and then select from the following options:
  - Select **Run Default Support Script** to collect information about the selected Explore appliance. You can send this diagnostics file to ExtraHop Support for analysis.
  - Select **Run Custom Support Script** to upload a file from ExtraHop Support that provides small system changes or enhancements.
- Click **Remove Cluster** to permanently disconnect the selected Explore appliance. This option only prevents you from performing the administrative tasks on this page from the Command appliance. The Explore appliance remains connected to your Discover appliance and continues to collect records.

Collect flow records

You can automatically collect and store all flow records, which are network-layer communications between two devices over an IP protocol. If you enable this setting, but do not add any IP addresses or port ranges, all detected flow records are captured. Configuring flow records for automatic collection is fairly straight-forward and can be a good way to test connectivity to your recordstore.

Before you begin
You must have access to an ExtraHop system with System and Access Administration privileges.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Records section, click **Automatic Flow Records**.
3. Select the **Enabled** checkbox.
4. In the Publish Interval field, type a number between 60 and 21600. This value determines how often records from an active flow are sent to the recordstore. The default value is 1800 seconds.
5. In the IP Address field, type a single IP address or IP address range in IPv4, IPv6, or CIDR format. Then, click the green plus (**+**) icon. (You can remove an entry by clicking the red delete (**X**) icon.)
6. In the Port Ranges field, type a single port or port range. Then, click the green plus (**+**) icon.
7. Click **Save**.

   Flow records that meet your criteria are now automatically sent to your configured recordstore. Wait a few minutes for records to be collected.
8. In the ExtraHop system, click **Records** from the top menu, and then click **View Records** to start a query.

If you do not see any records, wait a few minutes and try again. If no records appear after five minutes, review your configuration or contact ExtraHop Support.

ExtraHop Recordstore Status

If you have connected an ExtraHop recordstore to your sensor or console, you can access information about the recordstore.

The table on this page provides the following information about any connected recordstores.

Activity since

Displays the timestamp when record collection began. This value is automatically reset every 24 hours.

Record Sent

Displays the number of records sent to the recordstore from a sensor.

I/O Errors

Displays the number of errors generated.

Queue Full (Records Dropped)

Displays the number of records dropped when records are created faster than they can be sent to the recordstore.

ExtraHop Packetstore Settings

ExtraHop packetstores continuously collect and store raw packet data from your sensors. Connect the sensor to the packetstore to begin storing packets.

Connect sensors and console to the packetstore

Before you can query for packets, you must connect the console and all sensors to the packetstore.

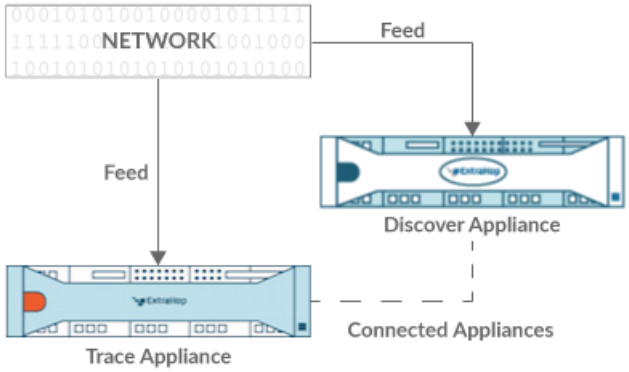


Figure 1: Connected to a sensor

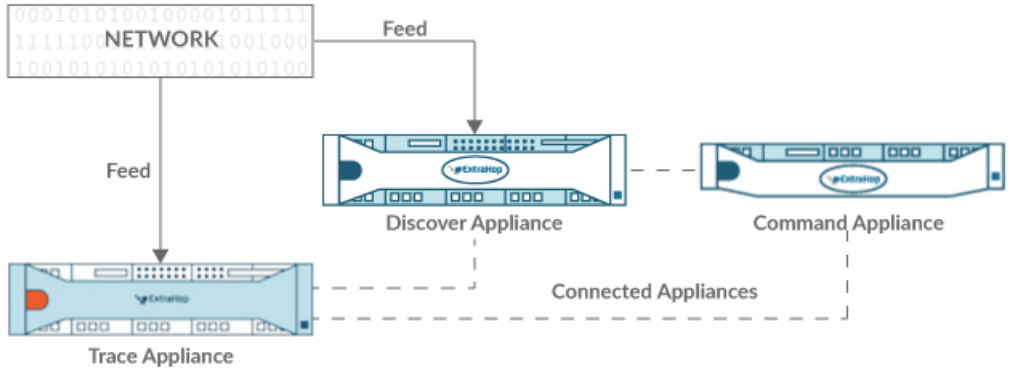


Figure 2: Connected to sensor and console

1. Log in to the Administration settings on the sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Packetstore Settings section, click **Connect Packetstores**.
3. In the Packetstore hostname field, type the hostname or IP address of the packetstore.
4. Click **Pair**.
5. Note the information listed in the Fingerprint field, and then verify that the fingerprint listed on this page matches the packetstore fingerprint on the Fingerprint page in the Administration settings of the packetstore.
6. In the Packetstore Setup Password field, type the password of the packetstore `setup` user.
7. Click **Connect**.
8. To connect additional packetstores, repeat steps 2 through 7.

Note: You can connect a sensor to twenty or fewer packetstores, and you can connect a console to fifty or fewer packetstores.

9. If you have a console, log in to the Administration settings on the console and repeat steps 3 through 7 for all packetstores.

Manage Trace Appliances

From the Command appliance, you can view connected Trace appliances and manage some administrative tasks.

View information about connected Trace appliances.

- Click **Trace Cluster** in the Name field to open the Cluster Properties. You can add a custom nickname for the Trace appliance and view the Cluster ID.
- Click any appliance to view the properties. By clicking **Open Admin UI**, you can access the Administration settings for the specific Trace appliance.
- View the date and time that the appliance was added to this Command appliance.
- View the license status for your appliances.
- View the list of actions that you can perform on this appliance.
- View the Job column to see the status of any running support scripts.

Select a Trace appliance. Then, select from the following administrative tasks.

- Click **Run Support Script** and then select from the following options:
  - Click **Run Default Support Script** to collect information about the selected Trace appliance. You can send this diagnostics file to ExtraHop Support for analysis.
  - Click **Run Custom Support Script** to upload a file from ExtraHop Support that provides small system changes or enhancements.
- Click **Upgrade Firmware** to upgrade the selected Trace appliance. You can enter a URL to the firmware on the Customer Portal website or upload the firmware file from your computer. With either option, we strongly recommend you read the firmware release notes and the firmware upgrade guide.
- Click **Remove Appliance** to permanently disconnect the selected Trace appliance. This option only prevents you from performing the administrative tasks on this page from the Command appliance. The Trace appliance remains connected to your Discover appliance and continues to collect packets.

Appendix

Common acronyms

The following common computing and networking protocol acronyms are used in this guide.

Acronym	Full Name
AAA	Authentication, authorization, and accounting
AMF	Action Message Format
CIFS	Common Internet File System
CLI	Command Line Interface
CPU	Central Processing Unit
DB	Database
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ERSPAN	Encapsulated Remote Switched Port Analyzer
FIX	Financial Information Exchange
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IBMMQ	IBM Message Oriented Middleware
ICA	Independent Computing Architecture
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
L2	Layer 2
L3	Layer 3
L7	Layer 7
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MIB	Management Information Base
NFS	Network File System
NVRAM	Non-Volatile Random Access Memory
RADIUS	Remote Authentication Dial-In User Service
RPC	Remote Procedure Call
RPCAP	Remote Packet Capture
RSS	Resident Set Size
SMPP	Short Message Peer-to-Peer Protocol

Acronym	Full Name
SMTP	Simple Message Transport Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SSD	Solid-State Drive
SSH	Secure Shell
SSL	Secure Socket Layer
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
UI	User Interface
VLAN	Virtual Local Area Network
VM	Virtual Machine

Configure Cisco NetFlow devices

The following are examples of basic Cisco router configuration for NetFlow. NetFlow is configured on a per-interface basis. When NetFlow is configured on the interface, IP packet flow information will be exported to the ExtraHop sensor.

Important: NetFlow takes advantage of the SNMP ifIndex value to represent ingress and egress interface information in flow records. To ensure consistency of interface reporting, enable SNMP ifIndex persistence on devices sending NetFlow to the sensor. For more information on how to enable SNMP ifIndex persistence on your network devices, refer the configuration guide provided by the device manufacturer.

For more information on configuring NetFlow on Cisco switches, see your Cisco router documentation or the Cisco website at www.cisco.com.

Configure an exporter on Cisco Nexus switch

Define a flow exporter by specifying the export format, protocol, and destination.

Log in to the switch command-line interface and run the following commands:

a) Enter global configuration mode:

```
config t
```

b) Create a flow exporter and enter flow exporter configuration mode.

```
flow exporter <name>
```

For example:

```
flow exporter Netflow-Exporter-1
```

c) (Optional) Enter a description:

```
description <string>
```

For example:

```
description Production-Netflow-Exporter
```

d) Set the destination IPv4 or IPv6 address for the exporter.

```
destination <eda_mgmt_ip_address>
```

For example:

```
destination 192.168.11.2
```

e) Specify the interface needed to reach the NetFlow collector at the configured destination.

```
source <interface_type> <number>
```

For example:

```
source ethernet 2/2
```

f) Specify the NetFlow export version:

```
version 9
```

Configure Cisco switches through Cisco IOS CLI

1. Log in to the Cisco IOS command-line interface and run the following commands.
2. Enter global configuration mode:

```
config t
```

3. Specify the interface, and enter interface configuration mode.
   - Cisco 7500 series routers:

     ```
     interface <type> <slot>/<port-adapter>/<port>
     ```

     For example:

     ```
     interface fastethernet 0/1/0
     ```

   - Cisco 7200 series routers:

     ```
     interface <type> <slot>/<port>
     ```

     For example:

     ```
     interface fastethernet 0/1
     ```

4. Enable NetFlow:

```
ip route-cache flow
```

5. Export NetFlow statistics:

```
ip flow-export <ip-address> <udp-port> version 5
```

Where *<ip-address>* is the Management + Flow Target interface on the ExtraHop system and *<udp-port>* is the configured collector UDP port number.

Help for early access features

For help about this early access feature, contact your ExtraHop sales representative.