ExtraHop 7.4
Admin UI Guide

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

Published: 2018-12-21

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

The Admin UI Guide provides detailed information about the administrator features and functionality of the ExtraHop Discover and Command appliances. 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 Discover or Command appliance, see the Discover and Command 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 appliances. We recommend that you install the latest version of the browser.

- Firefox
- Google Chrome
- Internet Explorer 11
- Safari

You must allow cookies and ensure that Adobe Flash Player is installed and enabled. Visit the Adobe website to confirm that Flash Player is installed and up-to-date.

Status and Diagnostics

The Status and Diagnostics section provides metrics about the overall health of the ExtraHop Discover appliance and diagnostic tools that enable ExtraHop Support to troubleshoot system errors.

Health

The Health page provides a collection of metrics that enable you check the operation of the Explore appliance.

View the metrics on this page to troubleshoot problems and determine why the ExtraHop appliance is not performing as expected.

System

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

CPU User

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

CPU System

The percentage of CPU usage associated with the ExtraHop appliance.

CPU Idle

The CPU Idle percentage associated with the ExtraHop appliance.

CPU IO

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

Bridge Status

Reports the following information about the ExtraHop appliance 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 appliance bridge component.

Capture Status

Reports the following information about the ExtraHop appliance 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 appliance services.

exalerts

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

extrend

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

exconfig

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

exportal

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

exshell

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

Interfaces

Reports the status of ExtraHop appliance system interfaces.

RX packets

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

RX Errors

The number of received packet errors on the specified interface.

RX Drops

The number of received packets dropped on the specified interface.

TX Packets

The number of packets transmitted by the ExtraHop appliance on the specified interface.

TX Errors

The number of transmitted packet errors on the specified interface.

TX Drops

The number of transmitted packets dropped on the specified interface.

RX Bytes

The number of bytes received by the ExtraHop appliance on the specified interface.

TX Bytes

The number of bytes transmitted by the ExtraHop appliance on the specified interface.

Partitions

Reports the non-volatile random-access memory (NVRAM) status and usage of ExtraHop appliance components. It identifies and provides status for specified components that have configuration settings that remain in memory when the power to the appliance is turned off.

Name

The ExtraHop settings that are held in NVRAM.

Options

The read-write options for the settings held in NVRAM.

Size

The size in gigabytes for the identified component.

Utilization

The amount of memory utilization for each of the identified components as a quantity and as percentage of total available NVRAM.

Audit Log

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

Send audit log data to a remote syslog server

The ExtraHop appliance audit log provides 90 days of lookback data about the operations of the system, broken down by component. You can view the audit log entries in the Admin UI 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 Audit log events table below.

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

1. Log into the Admin UI on the ExtraHop appliance.
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**.

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

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

Category	Event
Login from Web UI or Admin UI	• A login succeeds • A login fails
Login from SSH or REST API	• A login succeeds. • A login fails.
Running Config	The running configuration file changes
Support Script	• A default support script is running • A past support script result is deleted • A support script is uploaded
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)
Network	• A network interface configuration is edited

Category	Event
	• The hostname or DNS setting is changed • A network interface route is changed
Browser sessions	• A specific browser session is deleted • All browser sessions are deleted
Support account	• The support account is disabled • The support account is enabled • The support key is regenerated
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
Firmware	• Firmware is upgraded • Archived firmware is deleted
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
Command appliance	• A Discover appliance connects to a Command appliance • A Discover appliance disconnects from a Command appliance • An Explore or Trace appliance establishes a tunneled connection to a Command appliance • Command appliance information is set • A Command nickname is set • Enable or disable a Discover appliance • The Discover appliance Web UI is remotely viewed • A license for a Discover appliance is checked by a Command appliance • A license for a Discover appliance is set by a Command appliance
Agreements	A EULA or POC agreement is agreed to
SSL decryption	An SSL decryption key is saved
SSL session keys	A PCAP session key is downloaded
Appliance user	• A user is added • User metadata is edited • A user is deleted • A user password is set

Category	Event
	• A user other than the `setup` user attempts to modify the password of another user • A user password is updated
API	• An API key is created • An API key is deleted
Triggers	• A trigger is added • A trigger is edited • A trigger is deleted
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
Trends	A trend is reset
PCAP	A packet capture (PCAP) is downloaded
RPCAP	• An RPCAP configuration is added • An RPCAP configuration is deleted
Syslog	Remote syslog settings are updated
Support account	• The support account is enabled • The support account is disabled
Atlas	• The Atlas Remote UI account is enabled • The Atlas Remote UI account is disabled • The connection to the Atlas Service is reset • A Discover appliance disconnects from the Atlas Service
Datastore	• The extended datastore configuration is modified • The datastore is reset • A datastore reset completed • Customizations are saved • Customizations are restored • Customizations are deleted
Offline capture	An offline capture is loaded
Exception files	An exception file is deleted
Explore cluster	• A new Explore node is initialized • A node is added to an Explore cluster • A node is removed from an Explore cluster • A node joins an Explore cluster • A node leaves an Explore cluster

Category	Event
	• A Discover or Command appliance is paired to an Explore appliance • A Discover or Command appliance is unpaired from an Explore appliance • An Explore node is removed or missing, but not through a supported interface
Explore appliance records	All Explore appliance records are deleted
Trace appliance	• A new Trace appliance is initialized. • A Discover or Command appliance is paired to a Trace appliance. • A Discover or Command appliance is disconnected from a Trace appliance.
Trace appliance packetstore	A Trace appliance packetstore is reset.

Exception Files

Exception files are a core file of the data stored in memory. Enable exception files to help diagnose issues if the system unexpectedly stops or restarts.

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

Support Scripts

Support scripts are a way of collecting information about your ExtraHop system, and also a way to let ExtraHop support make adjustments to your system as part of a troubleshooting procedure.

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 into the Admin UI on your ExtraHop appliance.
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 into the Admin UI on your ExtraHop appliance.
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 appliance.
   ExtraHop Support will confirm that the support script achieved the desired results.

Network Settings

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

Connect to ExtraHop Cloud Services (Command appliance only)

ExtraHop Cloud Services provides access to ExtraHop cloud-based services through an encrypted connection. By enabling the Command appliance for remote access, you can allow designated ExtraHop staff to connect to your ExtraHop appliances for configuration help.

1. Log into the ExtraHop Admin UI on the Discover appliance.
2. In the Network Settings section, click **ExtraHop Cloud Services**.
3. Click **Terms and Conditions**.
4. After becoming familiar with the service terms and conditions, select the checkbox.
5. Click **Connect to ExtraHop Cloud Services**.

   After you are connected, the page updates to show status and connection information.

If the connection fails, there might be an issue with your firewall rules. See Troubleshoot your connection to ExtraHop Cloud Services to identify and resolve the issue. If connection problems persist, contact ExtraHop Support.

Connect to ExtraHop Cloud Services

ExtraHop Cloud Services provides access to ExtraHop cloud-based services through an encrypted connection. By connecting to the cloud-based ExtraHop Machine Learning Service (formerly Addy), you enable the Detections page for your ExtraHop system.

Detections are unexpected deviations from normal patterns in device or application behavior. The Machine Learning Service identifies detections from stored ExtraHop system data with a proprietary algorithm that combines time series decomposition, unsupervised learning, heuristics, and unique domain expertise from ExtraHop.

Before you begin

- You must apply the Machine Learning Service license on the Discover appliance before you can connect to ExtraHop Cloud Services. See the License FAQ for more information.
- You must have unlimited privileges to access the ExtraHop Admin UI and to connect to ExtraHop Cloud Services.

1. Log into the ExtraHop Admin UI on the Discover appliance.
2. In the Network Settings section, click **ExtraHop Cloud Services**.
3. Click **Terms and Conditions** to read the content.
4. After becoming familiar with the Machine Learning Service terms and conditions, select the checkbox.
5. Click **Connect to ExtraHop Cloud Services**.

   After you are connected, the page updates to show status and connection information.

If the connection fails, there might be an issue with your firewall rules. See Troubleshoot your connection to ExtraHop Cloud Services to identify and resolve the issue. If connection problems persist, contact ExtraHop Support.

Next steps
Learn how to navigate and interpret detections in Detections

Troubleshoot your connection to ExtraHop Cloud Services

You must establish a connection to ExtraHop Cloud Services to enable the Machine Learning Service (formerly Addy) and access the Detections page. However, if the connection fails or you do not have a direct internet connection, you can connect to the internet through a proxy server specifically designated for ExtraHop Cloud Services and Atlas connectivity. This guide explains how to troubleshoot common connectivity issues.

Before you begin

- You must have a valid license to connect to the ExtraHop Machine Learning Service. See the License FAQ for additional information. Note that it can take up to 24 hours for a license update to be available for your ExtraHop appliance after your request for a valid license is enabled.
- You must have unlimited privileges to access the ExtraHop Admin UI and to connect to ExtraHop Cloud Services.
- You must have familiarity with modifying the Running Config file. The Running Config file manages default system configurations and must be saved if you want the modified settings to be preserved after a system restart.

Configure your firewall rules

Before you can connect to the Machine Learning Service, you must allow access to the ExtraHop Cloud Services through any firewalls.

Connection to ExtraHop Cloud Services requires that your environment is able to meet the following conditions:

- The ability to perform a DNS lookup of *.extrahop.com
- The ability to connect to ExtraHop Cloud Services through HTTPS (port 443)

The server IP address for ExtraHop Cloud Services might change periodically, but you can identify the current IP address by running one of the following commands, based on your geographic location.

- **Portland, U.S.A.:**

```
nslookup pdx.hopcloud.extrahop.com
```

- **Sydney, Australia:**

```
nslookup syd.hopcloud.extrahop.com
```

- **Frankfurt, Germany:**

```
nslookup fra.hopcloud.extrahop.com
```

Connect to the Machine Learning Service through a proxy

If the connection fails or you do not have a direct internet connection, try connecting to the Machine Learning Service through an explicit proxy.

1. Log into the Admin UI of the Discover appliance.
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 username 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, which decrypts and re-encrypts the traffic before sending the packets to ExtraHop Cloud Services.

If the ExtraHop appliance cannot connect to the proxy server because the certificate validation has failed, you can bypass certificate validation and connect to ExtraHop Cloud Services.

1. Log into the ExtraHop Admin UI on the Discover appliance.
2. In the Appliance Settings section, click **Running Config**.
3. Click **Edit config**.
4. Add the following line to the end of the Running Config 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**.

Atlas Services

Atlas Services provide ExtraHop customers with a remote analysis report that is delivered monthly. The report contains specific recommendations for critical components across the application delivery chain.

Connect to Atlas services

Before you begin

You establish a connection to the Atlas server from the Admin UI of your ExtraHop Discover, Explore, or Trace appliance. If you have a firewall or proxy, you must first open access through those servers.
If you have signed up for the Atlas service, you will receive monthly customized reports about your ExtraHop data. This guide shows you how to connect to the service and how to troubleshoot common connectivity issues.

Important: The procedures in this guide require access to the appliance Admin UI and require that you modify the Running Config file. You can view and modify the code in the Running Config file, which specifies the default system configuration and saves changes to the current running configuration so the modified settings are enabled after a system restart. For more information, see the Running Config section of the ExtraHop Admin UI Guide.

Configure your firewall rules

Before you can connect to the Atlas server, you must allow access to the Atlas public IP server through any firewalls. If you do not have a firewall, you can skip this section.

Make sure that your environment meets the following conditions:

- The ability to complete a DNS lookup of *.a.extrahop.com
- The ability to connect to the Atlas server through HTTPS (port 443)

ExtraHop Networks can change the Atlas server IP address at any time, but you can identify the current IP address by selecting from one of the following options:

When connecting from EMEA, run the following command:

```
ping atlas-eu.a.extrahop.com
```

When connecting from all other locations, run the following command:

```
ping example.a.extrahop.com
```

Connect to Atlas through a proxy

If you want to connect to Atlas services through a proxy, configure the proxy settings in the ExtraHop Admin UI. If you do not have a proxy, you can skip this section.

1. In the Network Settings section, click **Connectivity**.
2. Click **Enable ExtraHop Cloud Proxy**. Click **Change ExtraHop Cloud Proxy** to modify an existing configuration.
3. Click **Enable ExtraHop Cloud Proxy**.
4. Type the hostname or IP address for your proxy server.
5. Type the port number for your proxy server, such as `8080`.
6. (Optional) If required, type a username 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, which decrypts and re-encrypts the traffic before sending the packets to the Atlas server. If your environment is not set up for inspection by third-party devices, you can skip this section.

The ExtraHop appliance cannot connect to the Atlas server if certificate validation has failed. To bypass certificate validation and connect to the Atlas server, you must modify the Running Config file.

1. Log into the Admin UI of the ExtraHop appliance you want to connect to Atlas services.
2. In the Appliance Settings section, click **Running Config**.
3. Click **Edit config**.
4. Add the entry to the Running Config file by completing the following steps:
   a) Add a comma after the second to last curly brace (}).
   b) Press ENTER to create a new line.
   c) Paste `"ecm": { "atlas_verify_cert": false }` on the new line before the final curly brace (}).
5. Click **Update**.
6. Click **View and Save Changes**.
7. Review the changes and click **Save**.
8. Click **Done**.

Establish a connection

After you have configured any optional firewall or proxy settings, complete the following steps to establish a connection to the Atlas server.

1. Log into the Admin UI on the ExtraHop Discover, Explore, or Trace appliance.
2. In the Network Settings section, click **Atlas Services**.
3. If you have not already changed the default password for the setup and shell users, you will see a message prompting you to change the password. Change the default password and then proceed to the next step.
4. On the Connect to Atlas Services page, click **Terms and Conditions** to read about the service agreement.

   The Atlas subscription services agreement opens in the browser or downloads the file to your computer.

5. Return to the Connect to Atlas Services page and select the checkbox next to **Terms and Conditions**.
6. Click **Test Connectivity** to make sure the connection is successful. If you have problems connecting to the Atlas service, see the previous sections to determine if you must open access through a firewall or connecting through a proxy.
7. Click **Connect**.

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** 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.

- Configure the Discover appliance to collect traffic from NetFlow and sFlow devices
- Packet Forwarding with RPCAP
- Configure ERSPAN with VMware

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 Port (receive only)	Monitors network traffic. This option is not available for Interface 1.
Management Port	Manages the ExtraHop appliance.
Management Port + Flow Target	Manages the ExtraHop appliance and captures traffic forwarded from a flow network. **Note:** If you enable NetFlow on the EDA 1100 or EDA 1000v, you must disable

Option	Description
	Interface 2. These appliances cannot process NetFlow and wire data simultaneously.
Management Port + RPCAP/ERSPAN/VXLAN Target	Manages the ExtraHop appliance and captures traffic forwarded from a software tap, ERSPAN*, or VXLAN**.
High-Performance ERSPAN/VXLAN Target	Captures traffic forwarded from ERSPAN* or VXLAN**. This interface mode enables the port to handle more than 1 Gbps. Set this interface mode if the ExtraHop appliance has a 10 GbE port.

*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.

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

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 appliance, 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 appliance before the change takes effect.

5. 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 gateway.
6. (Optional) Enable IPv6.

   For more information about configuring IPv6, see Enable IPv6 for an interface.
7. (Optional) Manually add routes.

   For more information about configuring static routes, see Set a static route.
8. Click **Save**.

Interface throughput
ExtraHop appliance models EH5000, EH6000, EDA 6100, EH8000, EDA 8100 and EDA 9100 are optimized to capture traffic exclusively on 10 GbE ports.

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

ExtraHop Appliance	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.
EDA 8000/8100	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 5000/6000/6100	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 appliance to communicate either with a Command appliance or with other devices outside of the local network, you can enable your ExtraHop appliance 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 appliance.

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 for access to your global proxy server.
- **Password:** The password for the user specified above.

ExtraHop Cloud proxy

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

Note: If no cloud proxy server is enabled, the ExtraHop appliance will attempt to connect through the global proxy. If no global proxy is enabled, the ExtraHop appliance will connect through an HTTP proxy to enable the services.

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 1GbE interfaces on your ExtraHop appliance 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. Only 1GbE interfaces are supported for bond interfaces. Bond interfaces cannot be set to monitoring mode.

Note: When you modify bond interface settings, you lose connectivity to your ExtraHop appliance. 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.

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 equivalent to the number of 1GbE interfaces on your ExtraHop appliance.

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 1GbE 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.
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**.

Flow Networks

You must configure network interface and port settings on the ExtraHop Discover appliance before you can collect NetFlow or sFlow data from remote flow networks (flow exporters). 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 your Discover appliance, 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.

Configure the Discover appliance to collect traffic from NetFlow and sFlow devices

You must configure network interface and port settings on the ExtraHop Discover appliance before you can collect NetFlow or sFlow data from remote flow networks (flow exporters). The ExtraHop system supports the following flow technologies: Cisco NetFlow v5 and v9, AppFlow, IPFIX, and sFlow.

Before you begin
You must log in as a user with unlimited privileges to complete the following steps.

Configure the interface on your Discover appliance

In addition to configuring your Discover appliance, you must configure your network devices to send sFlow or NetFlow traffic. Refer to your vendor documentation or see sample Cisco configurations at the end of this document.

1. Log into the Admin UI on your Discover appliance.
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. Select **Management Port + Flow Target** in the Interface Mode drop-down list.

   Note: The EDA 1100 and EDA 1000v must be configured for either flow data or wire data because these appliances cannot process flow data and wire data simultaneously. If these appliances are 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 over which flow data is collected

1. In the Network Settings section, click **Flow Networks**.
2. In the Ports section, type the UDP port number in the Port field. 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.
3. From the Flow Type drop-down menu, select **NetFlow** or **sFlow**. For AppFlow traffic, select **NetFlow**.
4. Click the plus icon (**+**) to add the port.
5. Save the running configuration file to preserve your changes by clicking **View and Save Changes** at the top of the Flow Networks page, and then click **Save**.

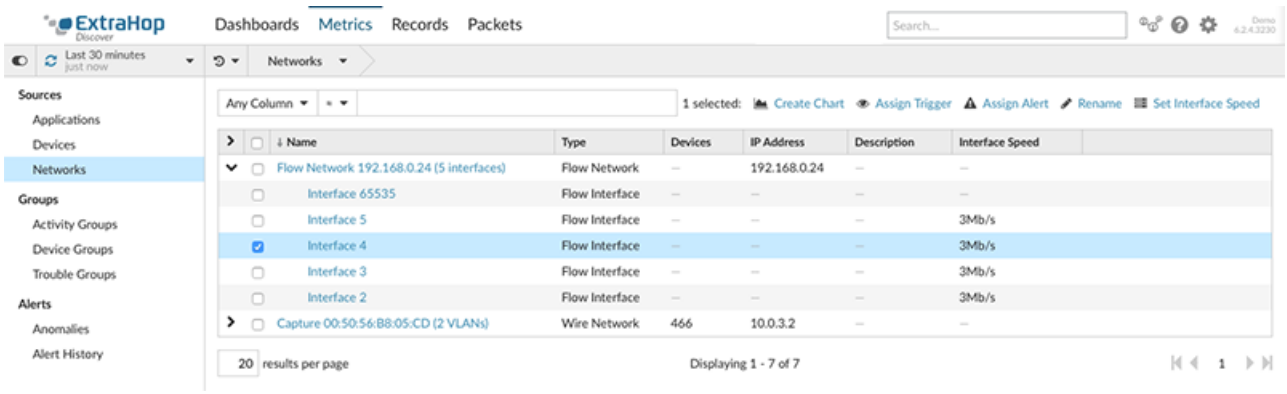
Add the pending flow networks on the Discover appliance

1. In the Network Settings section, click **Flow Networks**

2. In the Pending Flow Networks section click **Add Flow Network**.
3. Type a name to identify this flow network in the Flow Network ID field.
4. Select the Automatic records checkbox to send records from this flow network to a connected Explore appliance.
5. Select the Enable SNMP polling checkbox to enable SNMP polling.
6. 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.
7. Click **Save**.
   The flow network appears in the Approved Flow Networks table. If you do not see the flow network, you can manually add it 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 into the Web UI on the Discover appliance to view built-in charts and modify settings and configurations.



1. Log into the Web UI on your Discover appliance.
2. Click **Metrics** 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 will be exported to the Discover appliance.

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 Discover

appliance. 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 the 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 the Cisco IOS CLI

1. Log into 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 Port + Flow Target interface on the Discover appliance and <*udp-port*> is the configured collector UDP port number.

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 into the Admin UI on your Discover appliance.
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 into the Admin UI on your Discover appliance.
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 appliance 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 appliance can send notifications about system alerts by email or send scheduled reports from a Command appliance.

1. Log into the Admin UI on the ExtraHop appliance.
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 management network. 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 appliance
9. In the Report Sender Address field, type the email address responsible for sending the message. This field is only applicable when sending scheduled reports from an ExtraHop Command appliance.
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 on a Discover or Command appliance

Email notification groups can be designated to receive an email when a configured alert is generated. Although you can specify individual email addresses to receive emails for alerts, email groups are the most effective way to manage your alert recipient list.

1. Log into the Admin UI on the Discover or Command appliance.
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 for the team members who should receive the alert emails for 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. In the Network Settings section, click **Notifications**.
2. Under Notifications, click **SNMP**.
3. 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.
4. In the **SNMP Community** field, enter the SNMP community name.
5. 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`.
6. 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 appliance and `192.0.2.255` is the IP address of the SNMP server.
7. 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. Go to the Network Settings section and click **Notifications**.
2. Under Notifications, click **SNMP**.
3. Under SNMP MIB, click the **Download ExtraHop SNMP MIB**.
   The file is typically saved to the default download location for your browser.

Send system notifications to a remote syslog server

The syslog export option enables you to send alerts from an ExtraHop appliance 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 appliance.

1. Log into the Admin UI on the ExtraHop appliance.
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**.

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.

SSL Certificate

SSL provides secure authentication to the Admin UI of the ExtraHop appliance. To enable SSL, a SSL certificate must be uploaded to the appliance.

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. We recommend that you create a certificate signing request from your ExtraHop appliance and upload the signed certificate instead.

Important: When replacing an SSL certificate, the web server service is restarted. On a Command appliance, tunneled connections from Discover appliances are lost but are 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.

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 appliance

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 appliance 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 appliance, making a key pair.

1. Log into the Admin UI on your ExtraHop appliance.
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 appliance. 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 appliance. The FQDN must match one of the Subject Alternative Names.	*.example.com discover.example.com
E-mail Address	The email address of the primary contact for your organization.	webmaster@example.com
Organizational Unit	The division of your organization handling the certificate.	IT Department
Organization	The legal name of your organization. This entry should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.	Example, Inc.
Locality/City	The city where your organization is located.	Seattle
State/Province	The state or province where your organization is located.	Washington

Field	Description	Examples
	This entry should not be abbreviated.	
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 Admin UI and upload the certificate to the ExtraHop system.

Trusted Certificates

Trusted certificates enable you to validate SMTP and LDAP connections from your ExtraHop appliance.

Add a trusted certificate to your ExtraHop appliance

Your ExtraHop appliance 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. Only SMTP and LDAP connections are validated through these certificates.

Before you begin
You must log in as a user with unlimited 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. This can be achieved by either uploading the entire certificate chain for each trusted certificate or, preferably, by ensuring 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 certificate validation on the LDAP Settings page or Email Settings page.

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Network Settings section, click **Trusted Certificates**.
3. (Optional) The ExtraHop appliance 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**.

Next steps
Configure LDAP and SMTP settings to validate outbound connections with the trusted certificates.

Access Settings

In the Access Settings section, you can change passwords, enable the support account, and specify users in the ExtraHop appliances for remote authentication.

Password

Users with administrative privileges to the Admin UI can change the password for any user that has an account stored locally in the appliance.

- Select any user and change their password
  - You can only change passwords for local users, not for users authenticated with LDAP or other remote authentication servers.
  - The default password for Amazon Web Services (AWS) users is the string of numbers after the -i in the instance ID.

For more information about privileges for specific Admin UI 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 appliance 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 Admin UI. 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 Admin UI, 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 Account

Support accounts provide access for the ExtraHop Support team to help customers troubleshoot issues with the ExtraHop appliance. For the Discover appliance only, the Atlas Remote UI Account also provides remote analysis reports through Atlas Services.

These settings should be enabled only if the ExtraHop system administrator requests hands-on assistance from the ExtraHop Support team or if your organization is subscribed to Atlas Services.

Enable the Support account

1. In the Access Settings section, click **Support Account**.
2. Click **Support Account**.

   Note: On Command, Explore, and Trace appliances, this step is unnecessary.

3. Click **Enable Support Account**.

4. Copy the encrypted key from the text box and email the key to support@extrahop.com.
5. Click **Done**.

Regenerate the Support account key

1. In the Access Settings section, click **Support Account**.
2. Click **Support Account**.

   Note: On Command, Explore, and Trace appliances, this step is unnecessary.
3. Click **Regenerate Key**.
4. Click **Regenerate**.
5. Copy the encrypted key from the text box and email the key to support@extrahop.com.
6. Click **Done**.

Enable the Atlas Remote UI account

The Atlas Remote UI account enables the ExtraHop Support team to provide remote analysis reports through Atlas Services (Discover appliance only).

1. In the Access Settings section, click **Support Account**.
2. Click **Atlas Remote UI Account**.
3. Click **Enable Atlas Remote UI Account**.
4. Copy the encrypted key from the text box and email the key to support@extrahop.com.
5. Click **Done**.

Users

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

Users and user groups

Users can access the ExtraHop appliance 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, Radius, and TACACS+.

If you are providing users access from an LDAP server, you can also import and manage the members of an existing user group.

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 appliances 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 on the Web UI, Admin UI, and Shell, which is the ExtraHop command-line interface (CLI). On physical appliances, the default password for this account is the service tag number on the front of the appliance. On virtual appliances, the default password is `default`.

shell

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

Note: The default ExtraHop password for either account when deployed in Amazon Web Services (AWS) is the string of numbers after the -i in the instance ID.

Next steps

- Add a local user account

Remote Authentication

ExtraHop appliances supports remote authentication for user authentication. Remote authentication enables organizations that have authentication systems such as LDAP (such as OpenLDAP or Active Directory), RADIUS, or TACACS+ to enable all or a subset of their users to log on to the appliance 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 LDAP 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 TACACS+
- Configure remote authentication through RADIUS

User groups

On Discover and Command appliances, the User Groups page provides controls to view, enable, and disable user groups that are imported from a configured LDAP server. User groups allow for easier sharing of dashboards to all members in the group. Only remote user accounts and groups can be members of remote user groups.

Remote user groups are automatically discovered in the distinguished name (DN) specified as part of the remote authentication settings. See the Remote Authentication section about configuring LDAP authentication.

After you enable LDAP user groups through the remote authentication settings, the following user group properties appear in the table:

Group Name

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

Members

Displays the number of users in the group that are associated with a dashboard and that have logged into the ExtraHop Discover or Command appliance.

Associations

Displays the number of dashboards that are shared with the group.

Status

Displays whether the group is enabled or disabled on the appliance. 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 a dashboard.

Last Refresh

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 selecting a specific user group and clicking **Refresh Users in Group**. You can refresh a group from the User Group page or from within the Member List page.
- A remote user logs into the ExtraHop Web UI or Admin UI for the first time.
- A user attempts to load a shared dashboard that they do not have access to.

Reset a user group

When you reset a user group, all shared dashboard associations are removed from the group. If the group no longer exists on the remote LDAP server, the group is removed from the user group list.

Select one or more user groups in the list and click **Reset User Groups**.

Enable or disable a user group

You can share custom dashboards with a remote user group so that every member of the group can view the associated dashboard. If a user group is disabled, no group member can view the associated dashboard, even if the dashboard is still shared with the group.

Select one or more user groups in the list and click **Disable User Groups**.

User privileges

Administrators determine the level of access and functionality users have with the ExtraHop Web and Admin UIs. In addition to setting the privilege level for the user, you can add certain options that can apply to any user privilege level.

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

Privilege Levels

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

	Unlimited	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	N
Save activity maps	Y	Y	Y	Y	N	N
Share activity maps	Y	Y	Y	N	N	N
Alerts						
View alert history	Y	Y	Y	Y	Y	N
Create and modify alerts	Y	Y	N	N	N	N
Custom Pages						
Create and modify	Y	Y	N	N	N	N

custom pages						
Dashboards						
View and organize dashboards	Y	Y	Y	Y	Y	Y
Create and modify dashboards	Y	Y	Y	Y	N	N
Share dashboards	Y	Y	Y	N	N	N
Detections	**Note:** Detections require a connection to the cloud-based ExtraHop Machine Learning Service.					
View detections and provide feedback	Y	Y	Y	Y	Y	N
Analysis Priorities						
View Analysis Priorities page	Y	Y	Y	Y	Y	N
Add and modify analysis levels for groups	Y	Y	N	N	N	N
Add devices to a watchlist	Y	Y	N	N	N	N
Transfer priorities management	Y	Y	N	N	N	N
Device Groups						
Create and modify device groups	Y	Y	N	N	N	N
Metrics						
View metrics	Y	Y	Y	Y	Y	N
Records (Explore appliance)						

View record queries	Y	Y	Y	Y	Y	N
View record formats	Y	Y	Y	Y	Y	N
Create, modify, and save record queries	Y	Y	N	N	N	N
Create, modify, and save record formats	Y	Y	N	N	N	N
Scheduled Reports (Command appliance)						
Create, view, and manage scheduled reports	Y	Y	Y	N	N	N
Triggers						
Create and modify triggers	Y	Y	N	N	N	N
Administrative Privileges						
Access the ExtraHop Admin UI	Y	N	N	N	N	N
Connect to other appliances	Y	N	N	N	N	N
Manage other appliances (Command appliance)	Y	N	N	N	N	N

Privilege Options

The following privilege options can be assigned to users with any privilege level.

- View and download packets
- View and download packets and session keys
- View connected appliances (Command appliance only)

Add a local user account

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

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

1. Log into the Admin UI on the ExtraHop appliance.
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 into their ExtraHop appliances 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, which must be a minimum of 5 characters.

   • Confirm Password**:** Re-type the password from the Password field.
5. In the User Type section, select the type of privileges for the user.
   - Unlimited privileges enables full read and write access to the Web and Admin UIs.
   - Limited privileges enable you to select from a subset of privileges and options.

   Note: For more information, see the User privileges section.
6. 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 appliance.

User Groups

User groups can be imported from LDAP servers and managed locally on Discover and Command appliances.

- Learn about ExtraHop Users and user groups.
- View the list of groups imported from your LDAP server.

Group Name

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

Members

Displays the number of users in the group that are associated with a dashboard and that have logged into the ExtraHop Discover or Command appliance.

Associations

Displays the number of dashboards that are shared with the group.

Status

Displays whether the group is enabled or disabled on the appliance. 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 a dashboard.

Last Refresh

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 into the ExtraHop Web UI or Admin UI for the first time.
- A user attempts to load a shared dashboard that they do not have access to.

- Manage imported LDAP user groups

Manage imported LDAP user groups

After you have imported your LDAP user groups, you can view and manage those groups on the User Groups page. The following topics provide information about how to enable, view, reset, and refresh the user groups imported to your ExtraHop Discover and Command appliances.

Before you begin

Configure remote authentication through LDAP and import your user groups.

View the members of a user group

The Member List page provides controls to view the members in a user group that are imported from a configured LDAP server. You can also reset, disable, and refresh the user group from within the Member List page.

1. In the Access Settings section, click **User Groups**.
2. Click the group name in the user groups list.

   Tip: You can find user groups quickly by typing a name in the Filter user groups field. You can also sort the user group list by clicking on a column title.

   The member list displays the full name, login ID, and enabled or disabled status of the members who have logged into the appliance and whose group is associated with a shared dashboard. Clicking on the full name of the member whose privileges are managed locally redirects you to the **Admin** > **Users** > **Edit User** page for that user. Users whose permissions are managed by the remote LDAP server are greyed out in the member list and cannot be clicked.

   Note: If a user belongs to a group, and that group is a member of a parent group (nested group) that is associated with a dashboard, then the user appears in the member list of the parent group. If a dashboard is shared with the child group, the user will also appear in the member list of the child group.

Enable or disable a user group

You can share custom dashboards with a remote user group so that every member of the group can view the associated dashboard. If a user group is disabled, no group member can view the associated dashboard, even if the dashboard is still shared with the group.

Tip: Select more than one user group to enable or disable multiple groups at one time.

1. In the Access Settings section, click **User Groups**.
2. Select the checkbox next to the name in the group list and click one of the following:
   - To enable a user group, click **Enable User Group**.
   - To disable a user group, click **Disable User Group**.

Reset a user group

When you reset a user group, all shared dashboard associations are removed from the group. If the group no longer exists on the remote LDAP server, the group is removed from the user group list.

Tip: Select more than one user group to reset multiple groups at one time.

1. In the Access Settings section, click **User Groups**.
2. Select the checkbox next to the group name in the list.

3. Click **Reset User Group**.
4. Click **Yes** to confirm the reset action.

Refresh users and user groups
You can manually refresh LDAP user groups (or all users within a specific group) to ensure that the users and groups are synchronized with the users and groups on the LDAP server.

Tip: Select more than one user group to refresh multiple users at one time.

1. In the Access Settings section, click **User Groups**.
2. Choose one of the following options:
   - To refresh all user groups, click **Refresh All User Groups**.
   - To refresh users in a user group, select the checkbox next to the group name and then click **Refresh Users in Group**.

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

ExtraHop appliances supports remote authentication for user authentication. Remote authentication enables organizations that have authentication systems such as LDAP (such as OpenLDAP or Active Directory), RADIUS, or TACACS+ to enable all or a subset of their users to log on to the appliance 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 LDAP 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 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 appliance 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 appliance, 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 appliance 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 into the Admin UI on the ExtraHop appliance.
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 appliance 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 appliance.
   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 appliance.
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 appliance. 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. To configure user group settings, select the **Import user groups from LDAP server** checkbox and configure the following 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 appliance. 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 appliance or configure and manage privileges through your LDAP server.

When assigning user privileges through LDAP, you must complete at least one of the available 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 a member of a group specified above will not have access. Groups that are not present are not authenticated on the ExtraHop appliance.

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

Here is some information about the available fields:

- **Full access DN:** Create and modify all objects and settings on the ExtraHop Web UI and Admin UI.

• **Read-write DN:** Create and modify objects on the ExtraHop Web UI.

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

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

• **Node connection privileges DN:** (Visible only on the Command appliance.): View a list of ExtraHop appliances that are connected to this Command appliance.

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

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

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

• **Packet and session key access full DN:** View and download packets and any associated SSL session keys captured through the ExtraHop Trace appliance.

1. Choose one of the following options from the Permission 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 distinguished name (DN) field. To enable a user to download packet captures and session keys, configure the Packet access full DN or Packet and session keys access full DN field.
   - **Remote users have full write access**

     This option allows remote users to have full write access to the ExtraHop Web UI.
   - **Remote users have full read-only access**

     This option allows remote users to have read-only privileges to the ExtraHop Web UI.
   - **Remote users can view connected appliances**

     This option, which only appears on the Command appliance, allows remote users to log into the Admin UI on the Command appliance and view any connected Discover, Explore, and Trace appliances.
2. Select one of the following options to allow remote users to download packet captures and SSL session keys.
   - **No access**
   - **Packets only**
   - **Packets and session keys**
3. Click **Save and Finish**.
4. Click **Done**.

Configure remote authentication through RADIUS

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

1. Log into the Admin UI on the ExtraHop appliance.
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 appliance is properly configured if you specify a hostname.

Secret

The shared secret between the ExtraHop appliance and the RADIUS server. Contact your RADIUS administrator to obtain the shared secret.

Timeout

The amount of time in seconds that the ExtraHop appliance 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 Permission assignment options drop-down list, choose one of the following options:
   - **Remote users have full write access**

     This option allows remote users to have full write access to the ExtraHop Web UI.
   - **Remote users have full read-only access**

     This option allows remote users to have read-only permissions to the ExtraHop Web UI.

     Note: You can add read-write permissions on a per-user basis later through the Users page in the Admin UI.
   - **Remote users can view connected appliances**

     This option, which only appears on the Command appliance, allows remote users to log into the Admin UI on the Command appliance and view any connected Discover, Explore, and Trace appliances.
9. Select one of the following options to allow remote users to download packet captures and SSL session keys.
   - **No access**
   - **Packets only**
   - **Packets and session keys**
10. Click **Save and Finish**.
11. Click **Done**.

Configure remote authentication through TACACS+

The ExtraHop appliance 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 into the Admin UI on the ExtraHop appliance.
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 appliance is properly configured if you are entering a hostname.

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

   • Timeout**:** The amount of time in seconds that the ExtraHop appliance 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 allows remote users to have full write access to the ExtraHop Web UI.
   - **Remote users have full read-only access**

     This option allows remote users to have read-only permissions to the ExtraHop Web UI.

     Note: You can add read-write privileges on a per-user basis later through the Users page in the Admin UI.
   - **Remote users can view connected appliances**

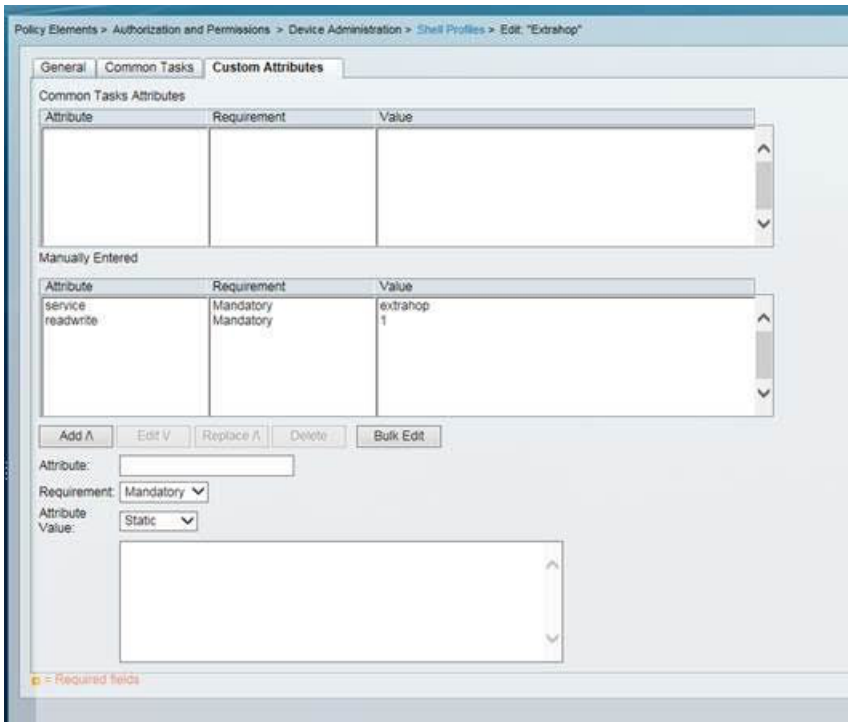
     This option, which only appears on the Command appliance, allows remote users to log into the Admin UI on the Command appliance and view any connected Discover, Explore, and Trace appliances.
9. Select one of the following options to allow remote users to download packet captures and SSL session keys.
   - **No access**
   - **Packets only**
   - **Packets and session keys**
10. Click **Save and Finish**.
11. Click **Done**.

Configure the TACACS+ server

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

1. Log into 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 permission level, such as `readwrite`.
5. For the second value, add `1`.

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



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

- `setup = 1`, which allows the user to create and modify all objects and settings on the ExtraHop Web UI and Admin UI
- `readwrite = 1`, which allows the user to create and modify all objects and settings on the ExtraHop Web UI
- `limited = 1`, which allows the user to create, modify, and share dashboards
- `readonly = 1`, which allows the user to view objects in the ExtraHop Web UI
- `personal = 1`, which allows the user to create dashboards for themselves and modify any dashboards that have been shared with them
- `limited_metrics = 1`, which allows the user to view shared dashboards

6. (Optional) If you have a Trace appliance, add a third attribute to allow users to download packet captures or packet captures with associated session keys.

   Here is a list of the available packet capture attributes and values:

   - `packetsfull = 1`, which allows users with any permission level to view and download packets
   - `packetsfullwithkeys = 1`, which allows users with any permission level to view and download packets and associated session keys stored on the Trace appliance

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 access

Users with unlimited 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. In the Access Settings section, click **API Access**.
2. In the Manage 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**

     Only users created on the appliance can generate API keys.
   - **No users can generate an API key**

     API keys cannot be generated. Selecting this option will delete any
3. Click **Save Settings**, then click **OK**, and then click **Done**.

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 administrative users with unlimited 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 system administrators with unlimited privileges. After you generate an API key, add the key to your request headers or the ExtraHop REST API Explorer.

1. In the Access Settings section, click **API Access**.
2. In the API Keys section, enter a description for the key, and then click **Generate**.

API privileges

The following REST API actions are allowed for each user privilege level.

Learn about ExtraHop Users and user groups or add a local user. Privileges can also be configured through remote authentication.

Privilege level	Actions allowed
Unlimited privileges	• Enable or disable API key generation for the ExtraHop appliance. • Generate an API key.

Privilege level	Actions allowed
	• 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. • Transfer ownership of any non-system dashboard to another user. • Perform any Admin UI task available through the REST API. • Perform any Web UI task available through the REST API.
Full write privileges	• Generate your own API key. • View or delete your own API key. • Change your own password, but you cannot perform any other Admin UI tasks through the REST API. • Perform any Web UI task available through the REST API.
Limited write privileges	• Generate an API key. • View or delete their own API key. • Change your own password, but you cannot perform any other Admin UI tasks through the REST API. • Perform all GET operations through the REST API. • Modify the sharing status of dashboards that you are allowed to edit. • Delete dashboards that you own. • Perform metric and record queries.
Personal write privileges Full read-only privileges	• Generate an API key. • View or delete your own API key. • Change your own password, but you cannot perform any other Admin UI tasks through the REST API. • Perform all GET operations through the REST API. • Delete dashboards that you own. • Perform metric and record queries.
View and download packets and session keys privileges	• View and download packets from an ExtraHop Discover appliance through the `GET/packetcaptures/{id}` operation. This additional privilege can be granted to a user with full write, limited write, personal write, or read-only privileges.

System Configuration

In the System Configuration section, you can modify ExtraHop appliance configuration settings for data capture and management.

Capture

Configure the network capture settings on the Discover appliance.

Datastore and Customizations

Reset the datastore and modify customizations. Datastore configuration settings are not available on the Command appliance.

Threat Intelligence (Reveal(x) Premium or Ultra only)

Manage threat intelligence data files.

Geomap Datasource

Modify the information in geomaps.

Open Data Streams

Send log data from the Discover appliance to another system such as a syslog system, MongoDB database, or HTTP server.

Trends

Reset all trends and trend-based alerts on the Discover appliance.

Threat Intelligence

Threat intelligence is a collection of information about malicious IP addresses, threat actor techniques, and other indicators of compromise that can help your organization detect attacks. You can upload STIX files as a threat intelligence collection to your ExtraHop Discover and Command appliances.

Note: This topic applies only to ExtraHop Reveal(x) Premium and Ultra.

Upload a threat intelligence collection to ExtraHop Reveal(x)

By uploading threat intelligence information in the form of the Structured Threat Information eXpression (STIX) file format to your Discover and Command appliances, you can find suspicious hosts, IP addresses, and URIs in the ExtraHop Web UI.

Before you begin

Learn about threat intelligence.

Note: This topic applies only to ExtraHop Reveal(x) Premium and Ultra.

Here are some important considerations about adding threat collections:

- ExtraHop currently supports STIX versions 1.0 - 1.2.
- The maximum number of observables that a threat collection can contain depends on your platform and license. Contact your ExtraHop representative for more information.

1. Log into the Admin UI on your Discover or Command appliance.

   Threat intelligence files are applied only to the local appliance and are not synced between appliances. If you manage your Reveal(x) system through a Command appliance, upload the threat collection to the Command appliance and to each connected Discover appliance.
2. In the System Configuration section, click **Threat Intelligence**.
3. Click **Upload New Collection**.

4. Type a unique collection ID in the Collection ID field. The ID can only contain alphanumeric characters. Spaces are not allowed.
5. Type a display name in the Display Name field.
6. Click **Choose file** and select a `.tar` or `.tgz` file that contains a STIX file.
7. Click **Upload**.

After the upload completes, the new threat collection appears in the table. You can now view threat intelligence metrics on the Security dashboard.

Update a threat collection

Because threat intelligence data is updated frequently (sometimes daily), you might need to update a threat collection with the latest data. When you update a threat collection with new data, the collection is deleted and replaced, and not appended to an existing collection.

Tip: The REST API offers a way to automate these updates across all appliances.

1. In the System Configuration section, click **Threat Intelligence**.
2. In the Actions column of the collection you want to update, click **Update**.
3. (Optional) If you want to only change the display name of the collection, type a new name in the Display Name field and then click **Update**.
4. Click **Choose file** and select a `.tar` or `.tar.gz` file that contains a STIX file.
5. Click **Update**.

After the upload completes, the threat collection is updated.

Capture

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

Exclude protocol modules

By default, all supported modules on the ExtraHop appliance 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 Discover appliance.

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 Discover appliance.

1. Go to the Configuration section and click **Capture**.
2. On the Capture Configuration page, click **Port Filters**.
3. Click **Add Filter**.
4. On the Port Address Filters page, enter the port you want to include.
   - To specify a source port you want to exclude, enter the port in the Source Port field.
   - To specify a destination port you want to exclude, enter the port in the Destination Port field.
5. From the **IP Protcol** 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 appliance.

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

Packet Dropped by	MAC address filter	IP address filter	Port filter	L2 dedup	L3 dedup
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 appliance 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.

Pseudo devices

Pseudo devices are deprecated as of ExtraHop version 6.0. If you have upgraded your system from a previous version with this functionality, you still can access the configuration page to migrate existing pseudo devices to custom devices. By default, all IP addresses outside of locally-monitored broadcast domains are aggregated at an incoming router. To identify the devices behind these routers for reporting, you can create custom devices. Unlike with pseudo devices, you do not need Admin UI privileges to configure a custom device.

Note: Any pseudo devices created on a previous version of ExtraHop firmware will remain on your Discover appliance until you migrate the pseudo device to a custom device.

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 that use TCP and UDP (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 appliance 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 Web UI or in reports based on any future data capture. The device will appear in reports that use 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 appliance recognizes most protocols on their standard ports. Exceptions include HTTP, SSH, and SSL, which are recognized on any port. In some cases, if a protocol is using a non-standard port, it is necessary to add the non-standard port in the Admin UI. 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 used when adding the custom port numbers in the Admin UI.

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

Canonical Name	Protocol Name	Transport	Default Source Port	Default Destination Port
DB2	DB2	TCP	0	50000, 60000
Diameter	AAA	TCP	0	3868
DHCP	DHCP	TCP	68	67
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
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
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

Canonical Name	Protocol Name	Transport	Default Source Port	Default Destination Port
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	TGCP	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
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
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

The name specified in the Protocol Name column in the table is used on the Protocol Classification page to classify a common protocol that uses non-standard ports.

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

DNS

The standard port for DNS is 53. DNS does not run on non-standard ports.

HTTP

The ExtraHop appliance classifies HTTP on all ports.

HTTP-AMF

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

SSL

The ExtraHop appliance classifies SSL on all ports.

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

FTP-DATA

The ExtraHop appliance 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 appliance looks for TDS traffic on TCP port 1533. 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 appliance 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 appliance 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.

Discover new devices by IP address

The ExtraHop Discover appliance automatically discovers devices that are communicating on the locally monitored network. This identification process is known as device discovery. After a device is discovered, you can search for the device and analyze device metrics in the Discover or Command appliances.

By default, Discover by IP is enabled, which means that devices are discovered when the ExtraHop system detects a response to an Address Resolution Protocol (ARP) request for an IP address. This method is also known as L3 discovery mode.

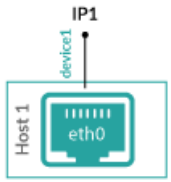
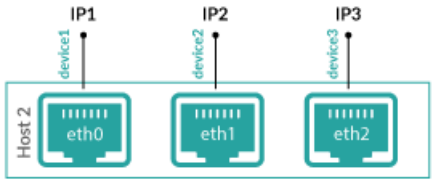
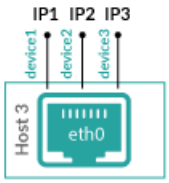
Note: Packet brokers can filter ARP requests. The ExtraHop system relies on ARP requests to associate L3 IP addresses with L2 MAC addresses.

If the ExtraHop system detects an IP address that does not have associated ARP traffic, that device is considered a remote device. Remote devices are not automatically discovered, but you can configure a remote range of IP addresses for discovery.

You can disable Discover by IP and only discover devices by unique MAC address. This method is known as L2 discovery mode. It is important to note that disabling Discover by IP changes the number of devices that are discovered by the ExtraHop system. The following table shows two Discover by IP scenarios, three common server NIC configurations, and the number of L3 devices (by IP address) and L2 devices (by MAC address) that are discovered for each scenario and configuration.

Note: Learn more about finding devices in the ExtraHop system.

Table 1: Discover by IP

Diagram	Enabled	Disabled
 Single NIC with single IP address	2 devices discovered: • eth0 device (L2) • IP1 device (L3)	1 device discovered: • eth0 device (L2)
 Multiple NICs, each with their own IP address	6 devices discovered: • eth0 device (L2) • IP1 device (L3) • eth1 device (L2) • IP2 device (L3) • eth2 device (L2) • IP3 device (L3)	3 devices discovered: • eth0 device (L2) • eth1 device (L2) • eth2 device (L2)
 Single NIC, multihomed with multiple IP addresses	4 devices discovered: • eth0 device (L2) • IP1 device (L3) • IP2 device (L3) • IP3 device (L3)	1 device discovered: • eth0 device (L2)

When Discover by IP is enabled, L2 devices are considered parents of their L3 devices. You can view metrics associated with each IP address by L3 device. When Discover by IP is disabled, only L2 devices are discovered, and metrics associated with those IP addresses are merged into the L2 device.

Remote discovery

The ExtraHop system automatically discovers local L3 devices based on observed ARP traffic that is associated with IP addresses. If the ExtraHop system detects an IP address that does not have ARP traffic, the ExtraHop system considers that IP address to be a remote device. Remote devices are not automatically discovered unless you configure a remote IP address range for remote discovery. When the ExtraHop system sees traffic associated with the range of remote IP addresses, it will discover those devices.

Note: If you have a proxy ARP configured in your network, the ExtraHop system might automatically discover remote devices. For more information, see this ExtraHop forum post.

Remote discovery is useful in the following scenarios:

- Your organization has a remote office without an on-site ExtraHop appliance but users at that site access central data center resources that are directly monitored by an ExtraHop appliance. The IP addresses at the remote site can be discovered as devices.
- A cloud service or other type of off-site service hosts your remote applications and has a known IP address range. The remote servers within this IP address range can be individually tracked.

Important: Devices discovered through remote discovery count towards your licensed device limit.

Add a remote IP address range

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

Important considerations about remote discovery:

- Only public-facing IP addresses are discovered and visible in the ExtraHop appliance. Private IP addresses, such as those on a private subnet, behind a router, or behind a NAT device, are not visible to the ExtraHop system.
- Additionally, 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 appliance. This information is not forwarded by routers, and therefore is not visible to the ExtraHop appliance.
- 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.

1. Log into the Admin UI on the Discover appliance.
2. In the System Configuration section, click **Capture**.
3. Click **Discover by IP**.
4. The Enable checkbox is selected by default. If the checkbox is deselected, select **Enable**.
5. In the Remote 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 appliance. Specifying wide subnet prefixes such as /16 might result in thousands of discovered devices, which might exceed your device limit.
6. 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 must be restarted when removing IP address ranges before the changes take effect. We recommend deleting all entries before restarting the capture. The capture does not need to be restarted when adding IP address ranges.

SSL decryption

The ExtraHop appliance supports real-time decryption of SSL traffic for analysis. Before you can decrypt your traffic, you must provide the private keys associated with the SSL server certificate. The server certificate and private keys are uploaded over an HTTPS connection from a web browser to the ExtraHop appliance.

Note: You must have a license for SSL decryption. If you do not have a license for SSL decryption, but you do have a license for MS SQL, you will see "For MS SQL Auth Only" in the ExtraHop Admin UI. This configuration only allows you to decrypt MS SQL traffic after you upload an SSL certificate.

You can decrypt SSL traffic that is encrypted with a supported ciphersuite by adding the following keys to the ExtraHop appliance to facilitate SSL traffic decryption. After you add a key, you can add the key to decrypt protocol traffic over a specified port. Port 0 represents all ports.

- Add PEM certificates and RSA private keys
- Add PKCS#12/PFX files with passwords
- Specify the protocols that handle decrypted SSL traffic

Tip: You can also decrypt SSL traffic that is encrypted with Perfect Forward Secrecy (PFS) ciphers when you configure session key forwarding. For more information, see Install the ExtraHop session key forwarder on a Windows server or Install the ExtraHop session key forwarder on a Linux server.

Configure the SSL decryption settings with a PEM certificate and private key

Before you can decrypt forwarded traffic, you must upload the private keys that are associated with your SSL server certificate. The certificate and keys are uploaded over an HTTPS connection from a web browser to the Discover appliance.

Before you begin

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

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

After upload, the private keys are stored on the internal USB flash media. All file systems on the internal USB flash media are obfuscated and cannot be mounted with standard tools. The private keys are stored in an encrypted format. To ensure that the keys are not transferable to other systems, they are encrypted with an internal key that is seeded with information specific to the system to which it was uploaded.

Separation of privileges is enforced such that only the SSL decryption process can access the private key material. The ExtraHop web administration utility can store new private keys and list the keys in the store for key management purposes, but cannot access the private key material after it is stored.

1. Click **System Configuration** > **Capture**.
2. Click **SSL Decryption**.
3. In the SSL Decryption Keys section, click **Add Keys**.
4. In the Add PEM Certificate and RSA Private Key section, enter the following information:

Name

A friendly name for the added key.

Enabled

Deselect this checkbox if you do not want to enable this SSL certificate.

Certificate

The public key certificate information.

Private Key

The RSA private key information.

5. Click **Add**.

Add PKCS#12/PFX files with passwords to the ExtraHop appliance

Before you begin
You can export a password-protected key to add to your ExtraHop appliance by running the following command on a program such as OpenSSL:

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

After upload, the private keys are stored on the internal USB flash media. All file systems on the internal USB flash media are obfuscated and cannot be mounted with standard tools. The private keys are stored in an encrypted format. To ensure that the keys are not transferable to other systems, they are encrypted with an internal key that is seeded with information specific to the system to which it was uploaded.

Separation of privileges is enforced such that only the SSL decryption process can access the private key material. The ExtraHop web administration utility can store new private keys and list the keys in the store for key management purposes, but cannot access the private key material after it is stored.

Note: The PKCS#12/PFX files are archived in a secure container that contains both public and private certificate pairs and requires a password to access.

1. Click **System Configuration** > **Capture**.
2. Click **SSL Decryption**.
3. In the SSL Decryption Keys section, click **Add Keys**.
4. In the Add PKCS#12/PFX File With Password section, enter the following information:

   Description

   A friendly name for the added key.

   Enabled

   Deselect this checkbox if you don't want to enable this SSL certificate.

   PKCS#12/PFX

   Click **Choose File** and browse to the file, select it, and click **Open**.

   Note: 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
   ```

   Password

   The password for the PKCS#12/PFX file.
5. Click **Add**.
6. Click **OK**.

Add encrypted protocols

1. Click **System Configuration** > **Capture**.
2. Click **SSL Decryption**.
3. In the Encrypted Protocols section, click **Add Protocol**.
4. On the Add Encrypted Protocol page, enter the following information:

   Protocol

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

Key

From the drop-down, select a previously set key.

Port

The source port for the protocol. By default this is set to 443, which specifies HTTP traffic.

5. Click **Add**.

Store SSL session keys on connected Trace appliances

This procedure shows you how to enable the storage of SSL session keys on connected Trace appliances. Keys are stored for all sessions that the Discover appliance can decrypt. These keys include SSL session keys derived from SSL decryption keys you upload on the SSL Decryption Keys page, and keys received from PFS session key forwarders.

Note: To ensure end to end security, the session keys are encrypted when moving between appliances as well as when the keys are stored on disk.

1. Log into the Admin UI on the Discover appliance.
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 Discover appliance. Note that this page only displays session key forwarders that have connected over the last few minutes, not all session key forwarders that are currently connected.

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

Import external data to your Discover appliance

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

After you enable the Open Data Context API on your Discover appliance, 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 Discover appliance. 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 appliance 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 Discover appliance before it can receive data from an external host.

Before you begin

- You must have unlimited privileges to access the Admin UI on your Discover appliance.
- 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 into the Admin UI on the Discover appliance.
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 appliance 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 Discover appliance, you must write a Python script that identifies your Discover appliance 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 Discover appliance 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 Discover appliance. 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 Discover appliance 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 into the Web UI on the ExtraHop Discover or Command appliance.
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 Discover appliance. 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 Web UI and add custom metrics
        //Note: The application is not displayed in the Web UI after the
  //initial request, but is displayed after subsequent requests.
        Application('DNSReputation').metricAddDetailCount('Bad DNS
 reputation', canonicalname + ':' + score, 1);
    }
}
```

Install the software tap on a Linux server

You must install the software tap on each server to be monitored in order to forward packets to the ExtraHop system. You can retrieve the commands from the procedures in this section or the ExtraHop Admin UI: `https://<discover_ip_address>/admin/capture/rpcapd/linux/`. The bottom of the ExtraHop Admin UI page contains links to automatically download the software tap.

Download and install on RPM-based systems

To download and install the software tap on RPM-based systems:

1. Download the software tap on the server by running on of the following commands:

   - ```
     wget --no-check-certificate 'https://<extrahop_ip_address>/tools/
     rpcapd-<extrahop_firmware_version>.x86_64.rpm'
     ```
   - ```
     curl -Ok 'https://<extrahop_ip_address>/tools/rpcapd-
     <extrahop_firmware_version>.x86_64.rpm'
     ```

   Where `<extrahop_ip_address>` is the IP address for interface 1 (management), and `<extrahop_firmware_version>` is the firmware version.

2. Install and run the software tap 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 Discover appliance, 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 software tap on the server by running one of the following commands:

   - ```
     wget --no-check-certificate 'https://<extrahop_ip_address>/tools/
     rpcapd-<extrahop_firmware_version>.tar.gz'
     ```
   - ```
     curl -Ok 'https://<extrahop_ip_address>/tools/rpcapd-
     <extrahop_firmware_version>.tar.gz'
     ```

   Where `<extrahop_ip_address>` is the IP address for Interface 1 (management), and `<extrahop_firmware_version>` is the firmware version.

2. Install and run the software tap on the server by running the following commands:

   a) Extract the software tap 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 tap 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 software tap on Debian-based systems:

1. Download the software tap on the server by running one of the following commands:

   - ```
     wget --no-check-certificate 'https://<extrahop_ip_address>/tools/
     rpcapd_<extrahop_firmware_version>_amd64.deb'
     ```
   - ```
     curl -Ok 'https://<discover_ip_address>/tools/
     rpcapd_<extrahop_firmware_version>_amd64.deb'
     ```

   Where `<extrahop_ip_address>` is the Interface 1 (management) IP address and `<extrahop_firmware_version>` is the firmware version.
2. Run the software tap on the server by running the following command:

   ```
   sudo dpkg -i rpcapd_<extrahop_firmware_version>_amd64.deb
   ```
3. At the prompt, enter the ExtraHop 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
   ```

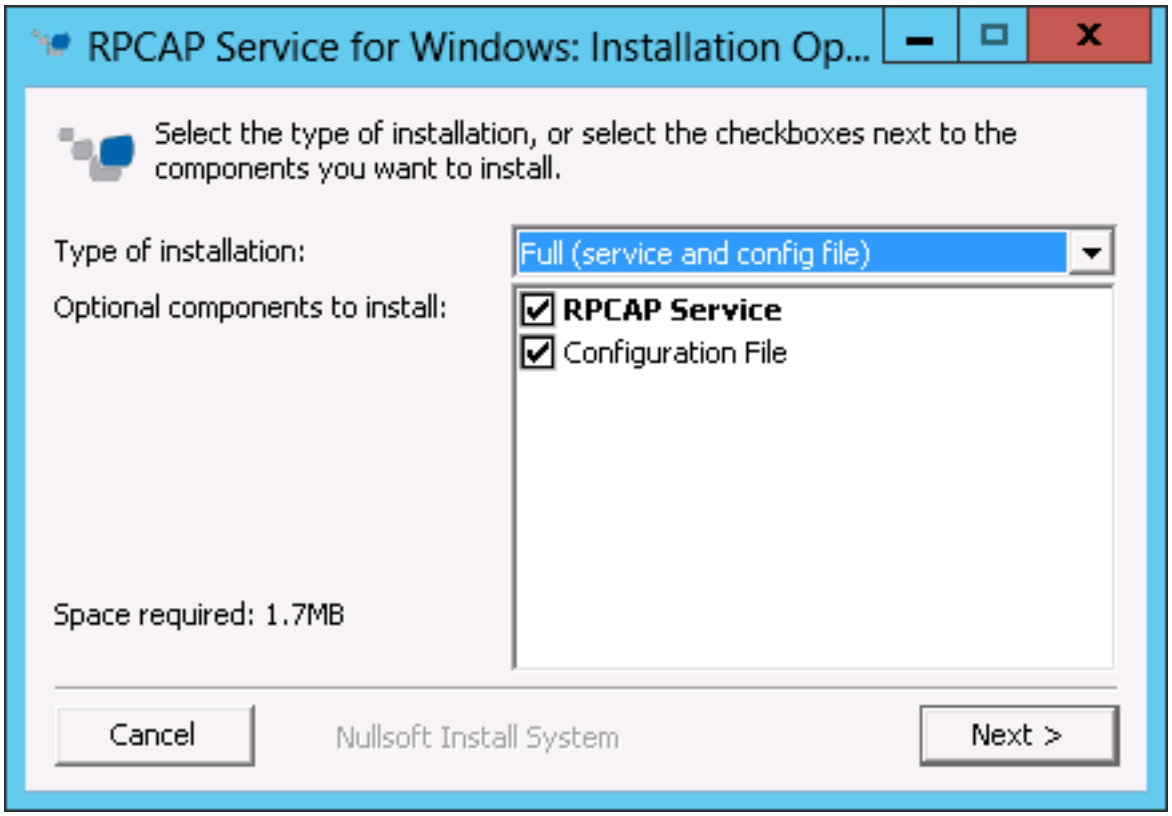
   ```
   sudo service rpcapd status
   ```
5. (Optional) To change the ExtraHop IP address, port number, or arguments to the service, run the following command.

   ```
   sudo dpkg-reconfigure rpcapd
   ```

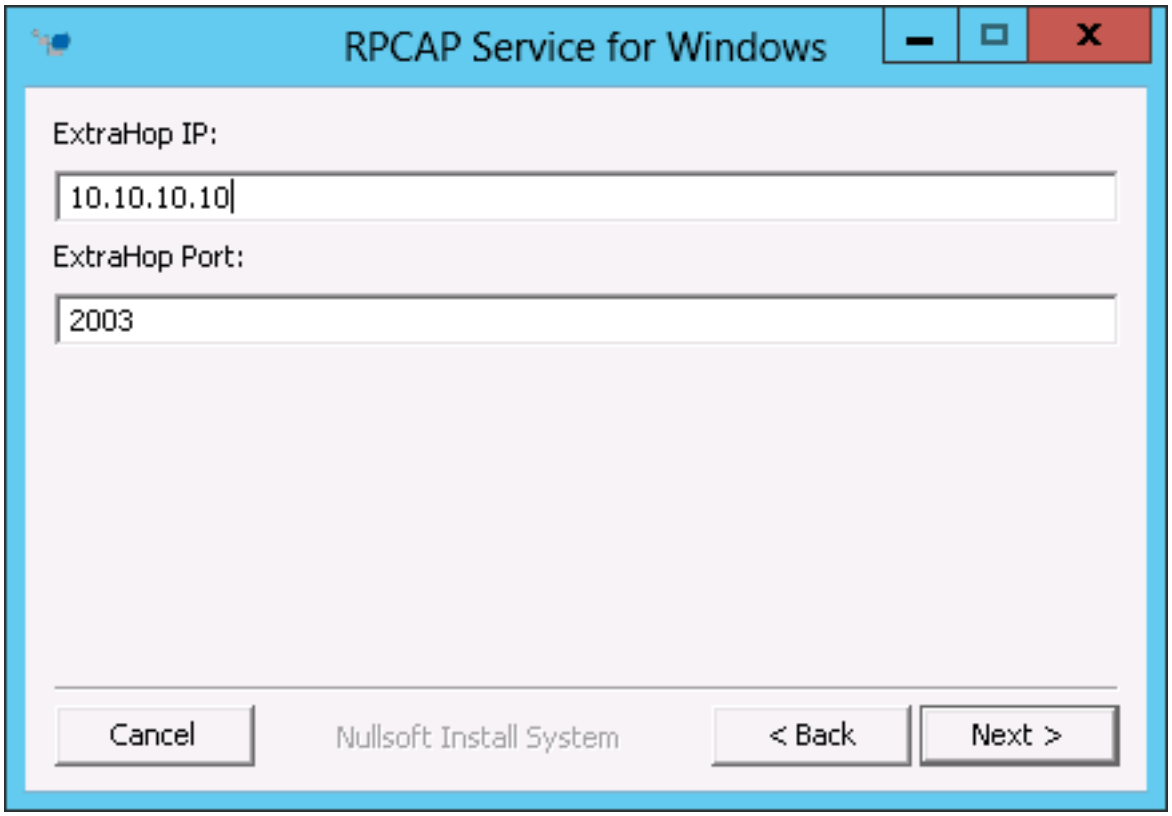
Install the software tap on a Windows server

You must install the software tap on each server to be monitored in order to forward packets to the ExtraHop system.

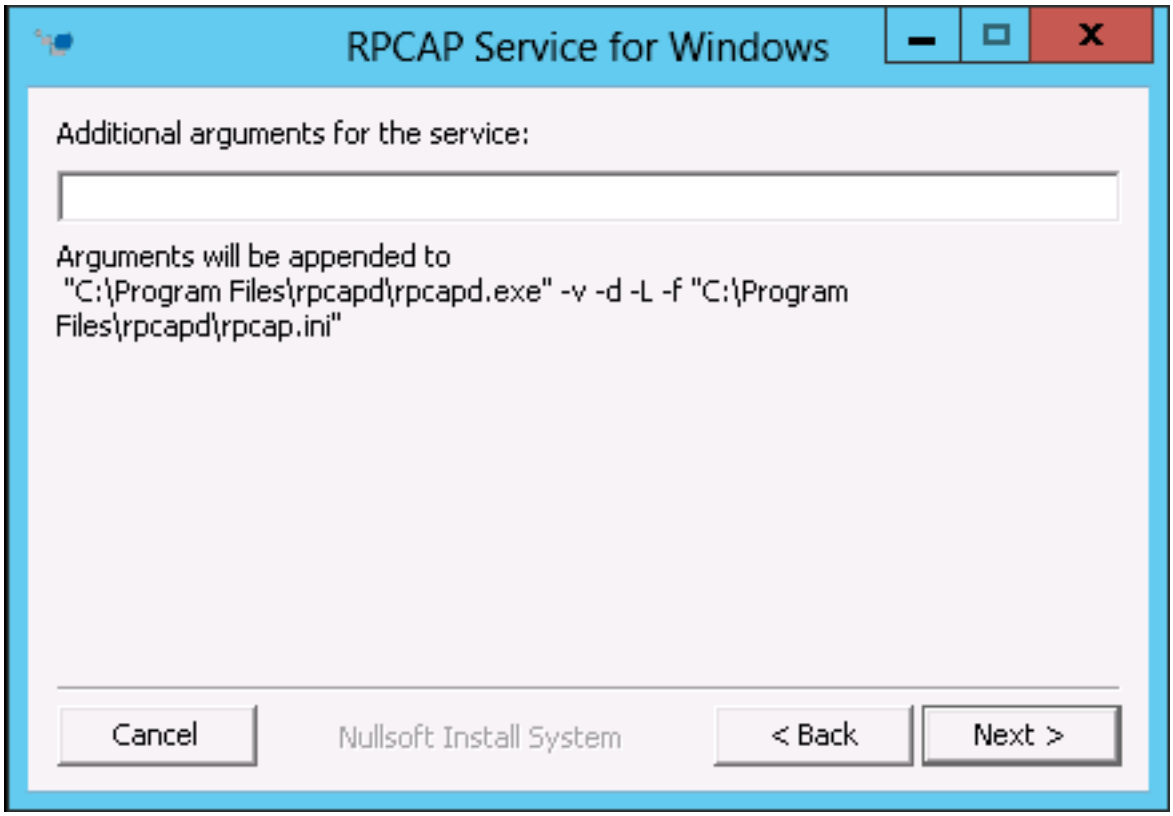
1. Go to `https://<extrahop_ip_address>/admin/capture/rpcapd/windows/` to download the RPCAP Service for Windows installer file.
2. When the file is finished downloading, double-click the file to start the installer.
3. In the wizard, select the components to install.



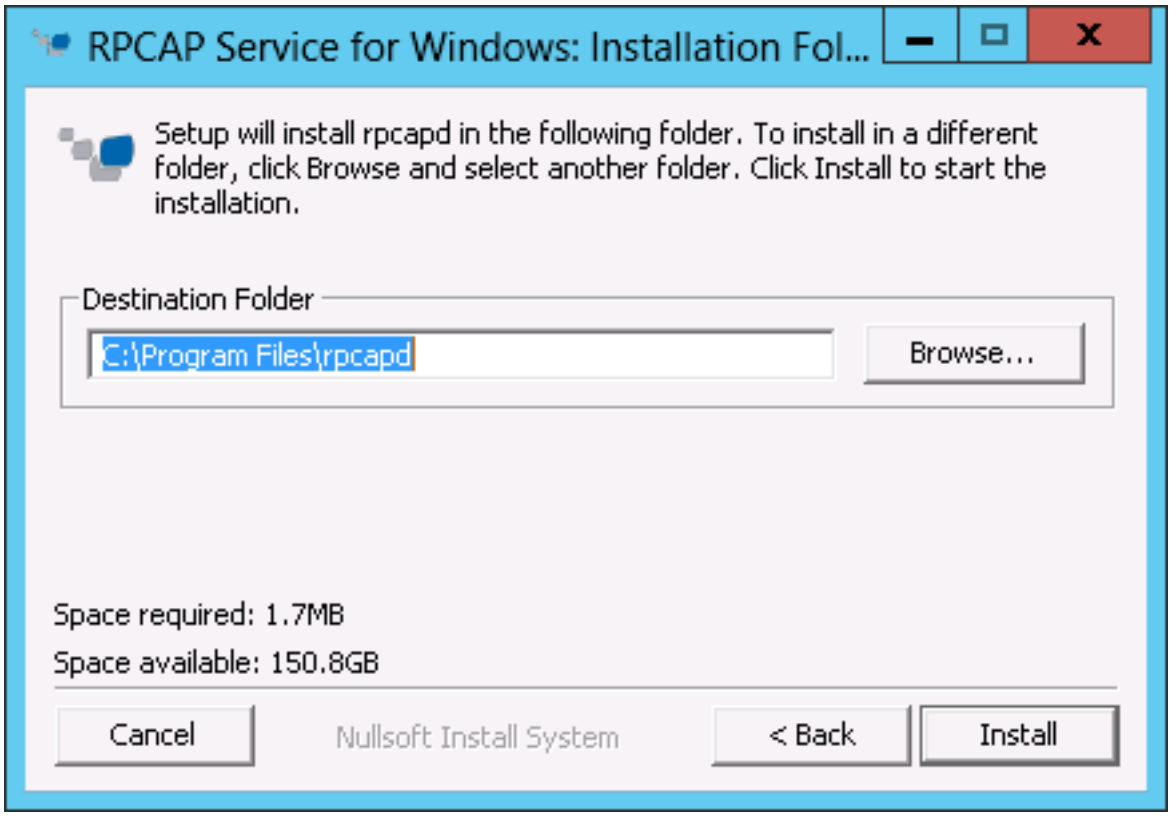
4. Complete the **ExtraHop IP** and **ExtraHop Port** fields and click **Next**. The default port is 2003.



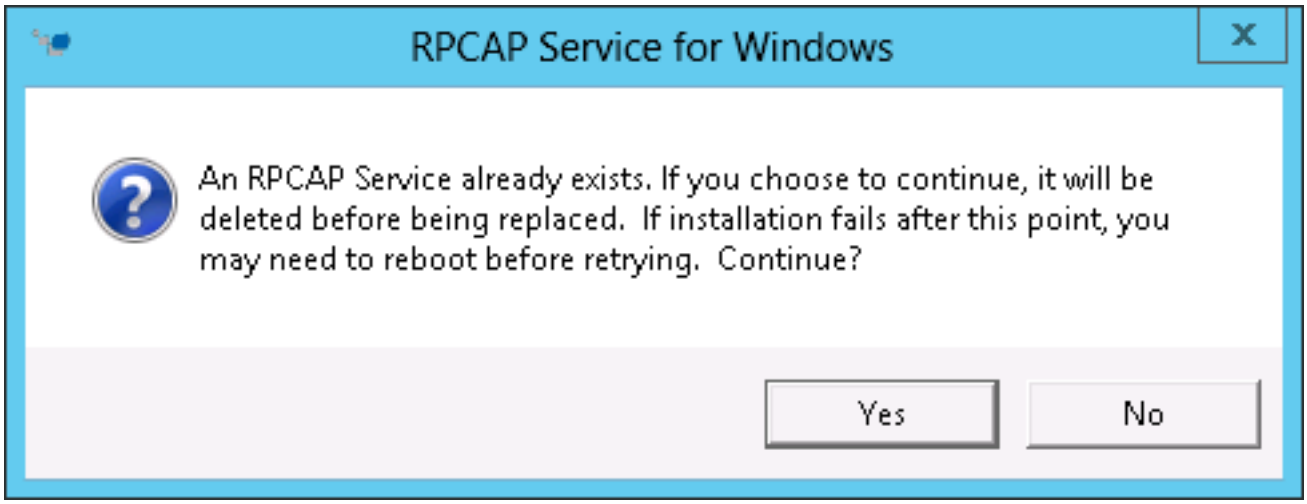
5. (Optional) Enter additional arguments in the text box and click **Next**.



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 software tap 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 software tap, 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 software tap 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 software tap by running the command:

```
sudo /etc/init.d/rpcapd restart
```

Note: To reinstall the software tap 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 software tap 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 software tap, 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 software tap by running the command:

```
restart-service rpcapd
```

Note: To reinstall the software tap 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 appliance to remove these outer encapsulating headers and then process the inner packets.

Note: Enabling NVGRE and VXLAN decapsulation on your ExtraHop appliance can increase your device count as virtual appliances 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 NVGRE decapsulation

1. Log into the Admin UI on the Discover appliance.
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**.
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.

1. Log into the Admin UI on the Discover appliance.
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**.

Analyze a packet capture file on the Discover appliance

The offline capture mode in the Discover appliance enables an ExtraHop administrator to upload a capture file recorded by packet analyzer software, such as Wireshark or tcpdump, to the ExtraHop datastore for analysis.

Here are some important considerations before enabling offline capture mode:

- When the capture is set to offline mode, the ExtraHop 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.

Set the offline capture mode

1. Log into the Admin UI on the Discover appliance.
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 Discover appliance displays the Offline Capture Results page when the capture file uploads successfully.
8. Click **View Results** to analyze the packet capture file in the Web UI as you would when the appliance is in live capture mode.

Return the appliance 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 Discover appliance removes the performance metrics collected from the previous capture file and prepares the datastore for real-time analysis from the capture interface.

Datastore

The Discover appliance 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 Discover appliance 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 Discover appliance as well as metrics for those devices. By storing this information on the Discover appliance, the ExtraHop system provides both quick access to the latest network capture and historic and trend-based information about selected devices.

Extended datastore

The Discover appliance can connect to an external storage device to expand your metric storage. By default, the Discover appliance 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 Discover appliance 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 Discover appliances.

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 a later ExtraHop appliance firmware version, the appliance with the older firmware cannot read those metrics.
- If an extended datastore becomes unreachable, the Discover appliance 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.

Related topics

Check out the following guides and resources that are designed to familiarize new users with our top features.

- Calculate the size you need for your extended datastore
- Configure an extended datastore

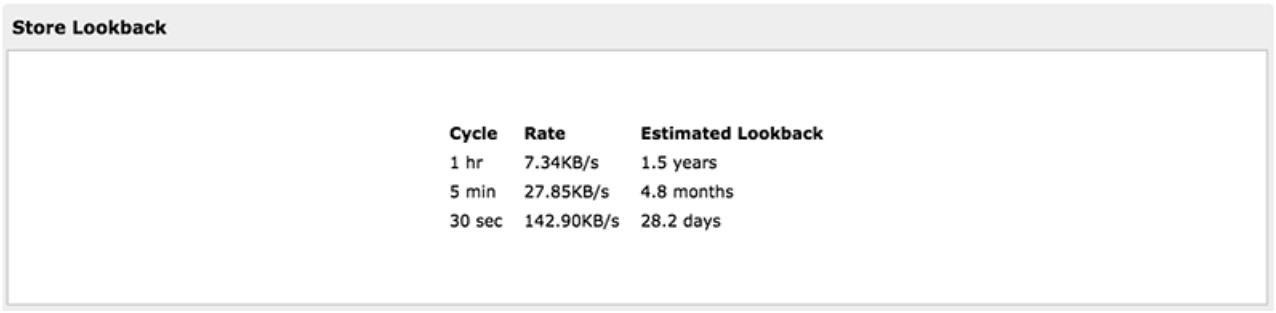
Calculate the size needed for your extended datastore

The extended datastore must have enough space to contain the amount of data generated by the Discover appliance. 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 into the Web UI of your Discover appliance.
2. Click the System Settings icon, and then click **System Health**.
3. Scroll down to the Datastore section.
4. In the Store Lookback chart, note the Rate and Estimated Lookback for each metric cycle (or time period) that you want to store on the external datastore. The rate for 5-minute metrics in our example figure below is 27.85 KB/s.



5. Calculate the amount of required space by applying the following formula: `<rate> x <lookback_time>`, and then convert the value to standard units.
   a) Convert the rate from seconds to days: `27.85 * 60 (seconds) * 60 (minutes) * 24 (hours) * 30 (days) = 72187200 KB` for 30 days of lookback.
   b) Convert the rate from kilobytes to megabytes: `72187200 / 1024 = 70495 MB` for 30 days of lookback.
   c) Convert the rate from megabytes to gigabytes:`70495 / 1024 = 68 GB` for 30 days of lookback.

   To store all of the 5 minute metrics from this appliance for 30 days, you need 68 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 Discover appliance.

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

SMB version 1.0 must be enabled on your SMB server where the share is located.

1. In the System Configuration section, click **Datastore and Customizations**.

2. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
3. Click **Add Mount**.
4. Click **Add CIFS Mount**.
5. 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
   ```

   Domain

   The site domain.
6. 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.
7. Click **Save**.

(Optional) Configure Kerberos for NFS

You must configure any desired Kerberos authentication before you add an NFS mount.

1. In the System Configuration section, click **Datastore and Customizations**.
2. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
3. 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.
4. In the Keytab File section, click **Choose File**, select a saved keytab file, and then click **Open**.
5. 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 the appliance to migrate any 5-minute and 1-hour metrics that the appliance collected from the local Discover appliance datastore 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. In the System Configuration section, click **Datastore and Customizations**.
2. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
3. From the Mount Name drop-down, select the name of the mount you want to specify as the extended datastore.
4. In the Datastore Directory field, type a name for the datastore directory. The directory is automatically created on the mount point by the Discover appliance.
5. From the Configure as options, select the **Active** radio button.
6. In the Datastore Size field, specify the maximum amount of data that can be stored on the datastore.
7. 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.
8. 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 Discover appliance 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
9. Select **Move existing**.
10. 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**.
11. Click **Configure**.
12. 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 a Discover appliance, you can create a read-only archive of the stored metrics data. Any number of Discover appliances can read from an archived datastore.

1. Log into the Admin UI on your Discover appliance.
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 appliance and marked for read-only access. Wait at least ten minutes before connecting any other Discover appliances to the archive.

Connect your Discover appliances to the archived datastore

Warning: To connect to an archived datastore, a Discover appliance 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. While the appliance is connecting to the archived datastore, the appliance 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. In the System Configuration, click **Datastore and Customizations**.
2. In the Extended Datastore Settings section, click **Configure Extended Datastore**.
3. Click the name of the mount that contains the archived datastore.
4. In the Datastore Directory field, type the path of the archived datastore directory.
5. Click **Archive (Read Only)**.
6. Click **Configure**.

Your extended database is now a read-only archive that can be accessed by multiple Discover appliances.

Import metrics from an extended datastore

If you stored metric data on an extended datastore that is connected to your Discover appliance, you can move that data to a new ExtraHop appliance as part of a system upgrade or if you plan to reset the datastore on an existing ExtraHop appliance.

Contact ExtraHop Support if you need to transfer metrics from an extended datastore.

Reset the local datastore and remove all device metrics from the Discover appliance

In certain circumstances, such as moving a Discover appliance 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 appliance.

Before you begin
Familiarize yourself with ExtraHop database concepts.

Customizations are changes that were made to the default settings on the appliance, such as triggers, dashboards, alerts, and custom metrics. These settings are stored in a file on the appliance, which 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 Discover appliance.

1. Log into the Admin UI on the Discover appliance.
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 into the Admin UI on your Discover appliance.
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 2: 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.

Status	Description	User Action
		• 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.
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 3: 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.

Ticket Tracking

ExtraHop detections identify when unusual behavior is discovered on your network. By configuring ticket tracking, you can create tickets in a third-party ticket tracking system and link them to your ExtraHop detections. Linked tickets display the associated ticket status and ticket assignee in the detection.

Before you begin
While you can enable ticket tracking and configure a URL template through the Admin UI, ticket tracking requires further configuration through ExtraHop Triggers and REST API.

Note: Detections require a connection to the cloud-based ExtraHop Machine Learning Service.

- To enable ticket tracking, select the Enable ticket tracking checkbox and then click **Save**.

  Note: You must enable ticket tracking on all connected Discover and Command appliances.
- To disable ticket tracking, clear the Enable ticket tracking checkbox. When ticket tracking is disabled, previously stored ticket information is preserved. However, users can no longer view ticket information from detections in the ExtraHop Web UI.
- 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.

Next steps
For more information about ticket tracking, see Configure ticket tracking for detections.

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 into the Admin UI on the Command or Discover appliance.
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. (Optional) In the Country-level Database section, select **Upload New Database**. The country-level database is subset of the city-level database.
7. (Optional) Click **Choose File** and navigate to the new country-level database file on your computer.
8. 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 Discover appliance to a remote HTTP server for long-term archiving and comparison with other sources.

1. Log into the Admin UI on the ExtraHop Discover appliance.
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. Select **Pipeline Requests** to enable HTTP pipelining, which can improve throughput speed.
10. 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.
11. (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.

12. (Optional) Click **Test** to establish a connection between the Discover appliance 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.
13. (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 Discover appliance 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.

14. 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 Discover appliance to any Kafka server for long-term archiving and comparison with other sources.

1. Log into the Admin UI on the ExtraHop Discover appliance.
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. 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.

9. (Optional) Click **Test** to establish a connection between the Discover appliance 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.
10. 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 Discover appliance to any system that receives MongoDB input for long-term archiving and comparison with other sources.

1. Log into the Admin UI on the ExtraHop Discover appliance.
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.
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 Discover appliance 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 Discover appliance 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 into the Admin UI on the ExtraHop Discover appliance.
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 Discover appliance 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 Discover appliance 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 into the Admin UI on the ExtraHop Discover appliance.
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**
9. Select **Local Time** to send syslog information with timestamps in the local time zone of the Discover appliance. If this option is not selected, timestamps are sent in GMT.
10. (Optional) Click **Test** to establish a connection between the Discover appliance 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.
11. 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.

Trends

Trend-based alerts are generated when a monitored metric deviates from the normal trends observed by the system. If needed, you can delete all configured trends and trend-based alerts from the appliance.

- Click **Reset Trends** to erase all trend data from the ExtraHop appliance.

Backup and Restore

The ExtraHop Discover and Command appliances have the ability to save user customizations and system resources. This feature gives you the ability to restore an existing appliance in case of a failure (a total appliance loss or any failure of the Discover or Command appliance firmware disk), or migrate the saved settings to a new appliance.

Back up a Discover or Command appliance

While daily backups are automatically saved on the local datastore, 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 appliance, for example). Then, download the backup file and save it to a secure location.

1. Log into the Admin UI on the Discover or Command appliance.
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 Discover or Command appliance 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.

1. Log into the Admin UI on the Discover or Command appliance.
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

Option	Description
	overwritten when the 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 the main Admin UI page.
   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 Discover or Command appliance from a backup file

You can restore the ExtraHop system from the user-saved or automatic backups stored on the system. You are able to perform two types of restore operations; you can choose to restore customizations (changes to alerts, dashboards, triggers, custom metrics, for example), or you can choose to restore customizations and system resources.

This procedure describes the steps required to restore a backup file to the same appliance that created the backup file. If you want to migrate the settings to a new appliance, see Migrate settings to a new Command or Discover appliance.

Before you begin
The target appliance must be running a firmware version that is the same major version as the firmware version that generated the backup file. For example, a backup created from an appliance running firmware 7.1.0 can be restored to an appliance running firmware 7.1.1, but the reverse is not allowed.

1. Log into the Admin UI on the Discover or Command appliance.
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 customizations and resources are restored.

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 the main Admin UI page.

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.

Migrate settings to a new Command or Discover appliance

If you are planning on replacing your ExtraHop Command or Discover appliance, you can migrate the settings from the source appliance to the target appliance.

Before you begin

- The target and source appliance cannot be active on the network at the same time.
- The target appliance must be the same size or larger (maximum throughput on the Discover appliance; CPU, RAM, and disk capacity on the Command appliance) as the source appliance.
- The target appliance must be running a firmware version that is the same major version as the firmware version that generated the backup file. For example, a backup created from an appliance running firmware 7.1.0 can be restored to an appliance running firmware 7.1.1, but the reverse is not allowed.
- The target appliance must be the same type of appliance, physical or virtual, as the source appliance.
- The target appliance requires an ExtraHop license.

In this procedure, you will backup your source appliance, disconnect the source appliance from the network, deploy the new appliance, and then restore the backup to the new appliance.

Note: When you restore from a backup that was created on a different appliance, the target appliance is disconnected from Atlas before restoring. You must manually reconnect to Atlas after the restore is complete.

1. Log into the source Command or Discover appliance that you are replacing.
2. Back up the appliance.
3. Shut down the source appliance and disconnect the management interfaces from the physical or virtual network where they are attached.

   Important: It is important that the source and target appliances with the same configuration are not active on the same network at the same time.
4. If you have not already done so, deploy the target appliance.
5. Log into the Admin UI on the target appliance.
6. In the System Configuration section, click **Backup and Restore**.
7. Click **Upload Backup File to Restore System**.
8. Select **Restore system customizations and resources**.
9. Click **Choose File**, navigate to the file you saved in step 2, and then click **Open**.
10. Click **Restore**.

    Warning: If the backup file is incompatible with the local datastore, the datastore must be reset. Resetting the datastore deletes all devices and metrics.

    After the restore is complete, you are logged out of the system.
11. Log into the Admin UI and verify that the target appliance has correctly restored your customizations.

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.

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:

Services
Enable or disable the Web Shell, management GUI, SNMP service, and SSH access. The Services page appears only on ExtraHop Discover and Command 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

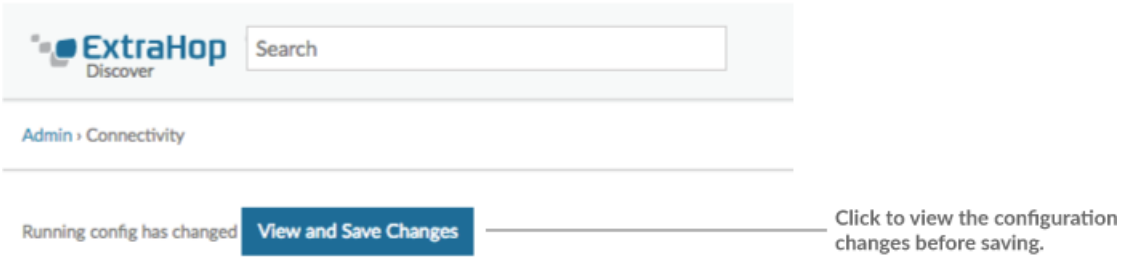
The running configuration file specifies the default system configuration. When you modify system settings, you must save the running configuration file to preserve those modifications after a system restart.

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 Admin UI.

Save system settings to the running config file

When you modify any of the system configuration settings on an ExtraHop appliance, you must confirm the updates by saving the running config file. If you do not save the settings, the changes are lost when your ExtraHop appliance restarts.

To remind you that the running configuration has changed, a red asterisk appears next to the Running Config link on the main Admin UI page, as well a **View and Save Changes** button on all Admin UI pages, as shown in the figure below.



1. Click **View and Save Changes**.
2. Review the comparison between the old running config and the current running config (not yet saved) 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 Admin UI provides an interface to view and modify the code that specifies the default system configuration. In addition to making changes to the running configuration through the settings pages in the Admin UI, 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 settings pages in the Admin UI.

Download the running config as a text file

You can download the Running Config settings to your workstation in text file format. 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 is downloaded as a text file to your default download location.

Disable ICMPv6 Destination Unreachable messages

You can prevent ExtraHop appliances 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 appliance to become unavailable or stop collecting data. You can contact ExtraHop Support at support@extrahop.com.

Disable specific ICMPv6 Echo Reply messages

You can prevent ExtraHop appliances 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. 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 appliance to become unavailable or stop collecting data. You can contact ExtraHop Support at support@extrahop.com.

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 Admin UI.

Enable or disable the Web Shell

The Web Shell provides access to the ExtraHop command-line interface (CLI). By default this service is enabled so that ExtraHop users can click the Launch Shell button in the upper right corner of the Admin UI screen and type commands. For more information, see the ExtraHop Command-line Reference.

Enable or disable the Management GUI

The Management GUI provides browser-based access to the ExtraHop appliance. By default, this service is enabled so that ExtraHop users can access the ExtraHop Web UI and Admin UI. 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 appliance when you want your network device monitoring software to collect information about the ExtraHop appliance. 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 into 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 appliance.

Enable or disable the SSL Session Key Receiver

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

Note: If you do not see this checkbox, and you have purchased the SSL Decryption license, contact ExtraHop Support to update your license.

Configure the SNMP service

Configure the SNMP service on your Extrahop appliance so that you can configure your network device monitoring software to collect information about your ExtraHop appliance 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 appliance and send an alert if the appliance is over 95% full. Import the ExtraHop SNMP MIB file into your monitoring software to monitor all ExtraHop-specific SNMP objects.

1. On the Services page, next to SNMP Service, click **Configure**.
2. On the SNMP Service Configuration page, complete the following steps:

Enabled

Select the checkbox to enable the SNMP 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 MIB file from the SNMP Service Configuration page.

Firmware

The Admin UI provides 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 appliance

The following procedure shows you how to upgrade your ExtraHop appliance 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.

Pre-upgrade checklist
Here are some important considerations and requirements about upgrading ExtraHop appliances.

- If you have multiple types of ExtraHop appliances, you must upgrade them in the following order:
  1. Command appliance
  2. Discover appliances
  3. Explore appliances
  4. Trace appliances
- If you have a Command appliance, apply the following guidance:
  - For large Command appliance deployments (managing 50,000 devices or more), reserve a minimum of one hour to perform the upgrade.
  - The Command appliance firmware version must be greater than or equal to the firmware version of all connected appliances.
- If you have Explore appliances, apply the following guidance:
  - You must halt the ingest of records from Command and Discover appliances before upgrading. If you are upgrading from a firmware version prior to 7.4, temporarily remove any connected Explore appliances, or alternatively, disable triggers that commit records and disable the automatic flow records setting.

    If you are upgrading from firmware version 7.4 or later, disable record ingest on the Explore cluster.

    You must re-enable these settings after all nodes in the Explore cluster are upgraded.
  - You must upgrade all Explore nodes in an Explore cluster. The cluster will not function correctly if nodes are on dissimilar firmware versions.

    After each node is upgraded, verify that the status of all cluster indices on the Explore Cluster Status page displays `Yellow` or `Green` before upgrading the next node.

Important: The message `Could not determine ingest status on some nodes` and `Error` appear on the Cluster Data Management page in the Admin UI of the upgraded nodes until all nodes in the cluster are upgraded. These errors are expected and can be ignored.

Upgrade the firmware

1. Download the firmware for the appliance from the ExtraHop Customer Portal to your computer.
2. Log into the Admin UI on the ExtraHop appliance.
3. In the Appliance Settings section, click **Firmware**.
4. Click **Upgrade**.
5. 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.
6. If you do not want to automatically restart the appliance after the firmware is installed, clear the **Automatically restart appliance after installation** checkbox.
7. Click **Upgrade**.
   The ExtraHop appliance 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.
8. 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 Admin UI.

   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 appliance 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 Admin UI on a Command appliance, view the appliance status on the Manage Connected Appliances page.
   - Connect to the appliance through the iDRAC interface.
9. If you disconnected any Explore appliances from Command and Discover appliances, make sure to reconnect them. If you disabled any triggers, automatic flow records, or disabled record ingest, make sure to re-enable those settings.

System Time

The System Time page displays the current configuration and the status of all configured NTP servers. When capturing data, it is helpful to have the time on the ExtraHop appliance match the local time of the router. The ExtraHop appliance can set time locally or synchronize time with a time server. By default, system time is set locally, but we recommend that you change this setting and set time through a time server.

- Configure the system time.
- View information about the appliance settings in the System Time section:

  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.

- View information for each configured NTP server in the NTP Status table:

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 reported time the server gave you. 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, ExtraHop appliances synchronize the system time through the *.extrahop.pool.ntp.org network time protocol (NTP) servers. If your network environment prevents the ExtraHop appliance from communicating with these time servers, you must configure an alternate time server source.

1. Log into the Admin UI on the ExtraHop appliance.
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 Discover appliances that are managed by a Command appliance.
   - 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 Admin UI provides an interface to halt, shutdown, and restart the ExtraHop appliance and its system components. For each ExtraHop appliance 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 appliance.
- Restart Bridge Status (Discover appliance only) to restart the ExtraHop bridge component.
- Restart Capture (Discover appliance only) to restart the ExtraHop capture component.
- Restart Portal Status to restart the ExtraHop web portal.
- Restart Scheduled Reports (Command appliance only) to restart the ExtraHop scheduled reports component.

License

The License Administration page enables you to view and manage licenses for your ExtraHop appliance. You must have an active license to access the ExtraHop Web UI, and your appliance 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 appliance

When you purchase an appliance, you will receive an email with a new product key that must be added to your appliance from the ExtraHop Admin UI. This guide provides instructions on how to apply the new product key and activate all of your purchased modules. You must have administrator privileges on the ExtraHop appliance to access the Admin UI.

Register the appliance

Before you begin

Note: If you are registering a Discover or Command appliance, you can optionally enter the product key from the ExtraHop Web UI, (`https://<extrahop_ip_address>/`) after you accept the EULA and log in.

1. In your browser, type the URL of the ExtraHop Admin UI, `https://<extrahop_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 a virtual appliance in AWS, type the instance ID, which is the string of characters that follow i- (but not i- itself).
- 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
Your ExtraHop appliance must be able to resolve the *.d.extrahop.com domain from the DNS server settings that you configured on your ExtraHop appliance. Communication with the licensing server through DNS is required for license updates and check-ins.

Open a terminal application on your Windows, Linux, or Mac OS client that is on the same network as your ExtraHop appliance and run the following command:

```
nslookup -type=NS d.extrahop.com
```

If the name resolution is successful, output similar to the following appears:

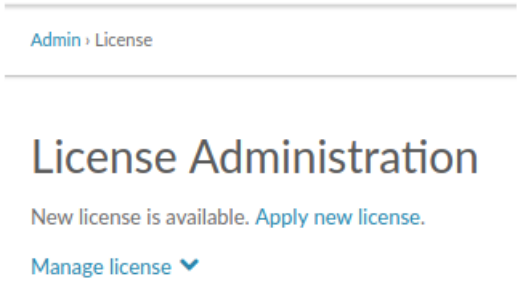
```
Non-authoritative answer:
d.extrahop.com  nameserver = ns0.use.d.extrahop.com.
d.extrahop.com  nameserver = ns0.usw.d.extrahop.com.
```

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, your updated license is automatically available on your appliance. However you must apply your updated license to your appliance through the Admin UI for the new changes to take effect.

1. Log into the Admin UI of your ExtraHop appliance.
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 appliance.

1. Log into the Admin UI on your ExtraHop appliance.
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 your ExtraHop appliance 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.

For information about configuring and repairing RAID10 functionality on the EH8000 and EDA 6100 appliances, 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 (EH2000/3000/5000/6000/8000)
- Packet Capture (EH3000/6000/8000)
- Firmware (EH3000/6000/8000)

Do not attempt to install or replace the drive in Slot 0 unless instructed by ExtraHop Support.

To ensure that system health checks and email notifications are running, mouse over the **Settings** button in the Web UI navigation bar.

- If the message "`System Health Checks Not Running`" appears, contact ExtraHop Support at support@extrahop.com for instructions. This message also appears at the top of the Settings page.
- If the message "System Health Notifications Not Configured" appears, refer to Email Notification Groups to set up email notifications for system health. Alternatively, click the **Settings** button, and then click **View Admin Notifications page for more details** at the top of the Settings page.

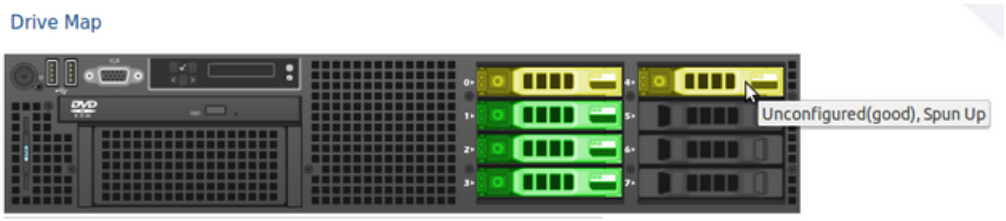
Note: Ensure that your device has a RAID controller before attempting the following procedure. If unsure, contact ExtraHop Support at support@extrahop.com. This procedure configures the EDA 5000 appliance as an example. A persistently damaged disk might not be replaceable with this procedure.

Replace a RAID 0 disk

1. In the system health email notification, note which machine has the problematic disk.
2. In the ExtraHop Web UI for the identified machine, click the **Settings** button in the navigation bar, and go to the Disk page by doing either of the following:
   - Click **Administration**. Then, under Appliance Settings, click **Disks**.
   - Click the **Disk Error** link at the top of the page.
3. Under the section for the disk type (for example, **Datastore**), find the problematic disk and note the Slot number.

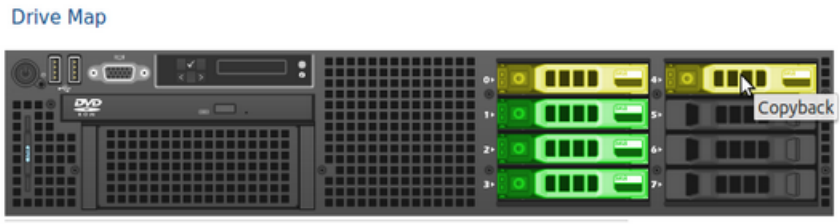
   Click **RAID Disk Details** to display more details.
4. Insert an identical disk into an available slot.

   The system detects the new disk and adds a new row (Disk Error Action) with a link to replace the bad disk.
5. 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`."



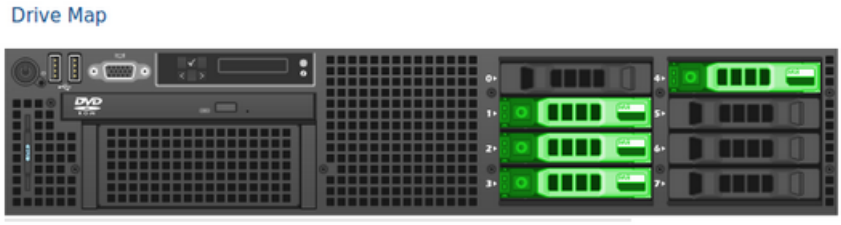
6. Under the section for the disk type, click **Replace with Disk in slot #n** in the Disk Error Action row.

   The data begins copying over. The Copy Status row displays the progress. Mousing over the disk in the Drive Map shows the status.



7. 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
8. Remove the old disk.

   The Drive Map now shows the new disk in green.

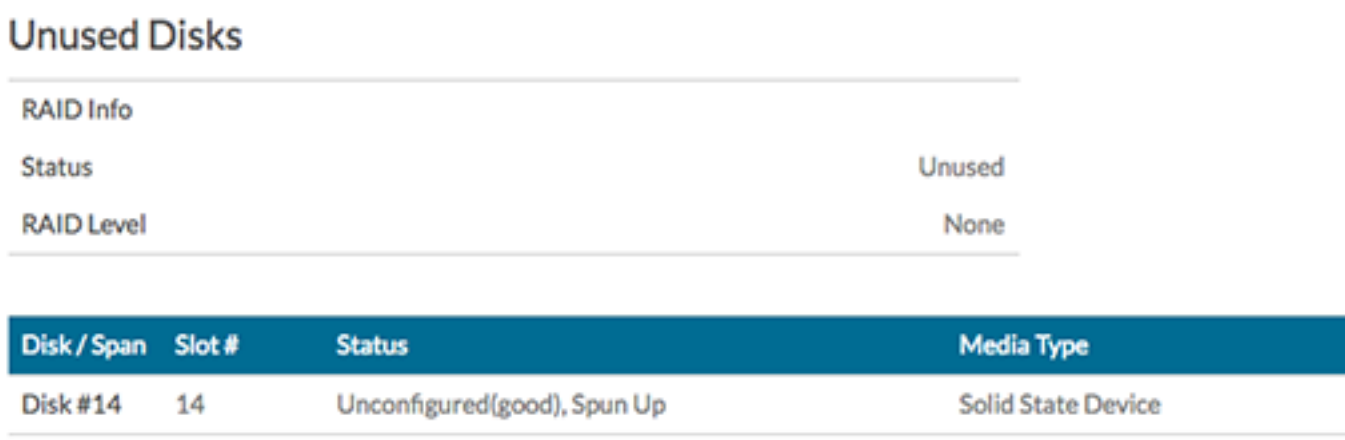


Install a new packet capture disk

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 Admin UI, refresh the browser.

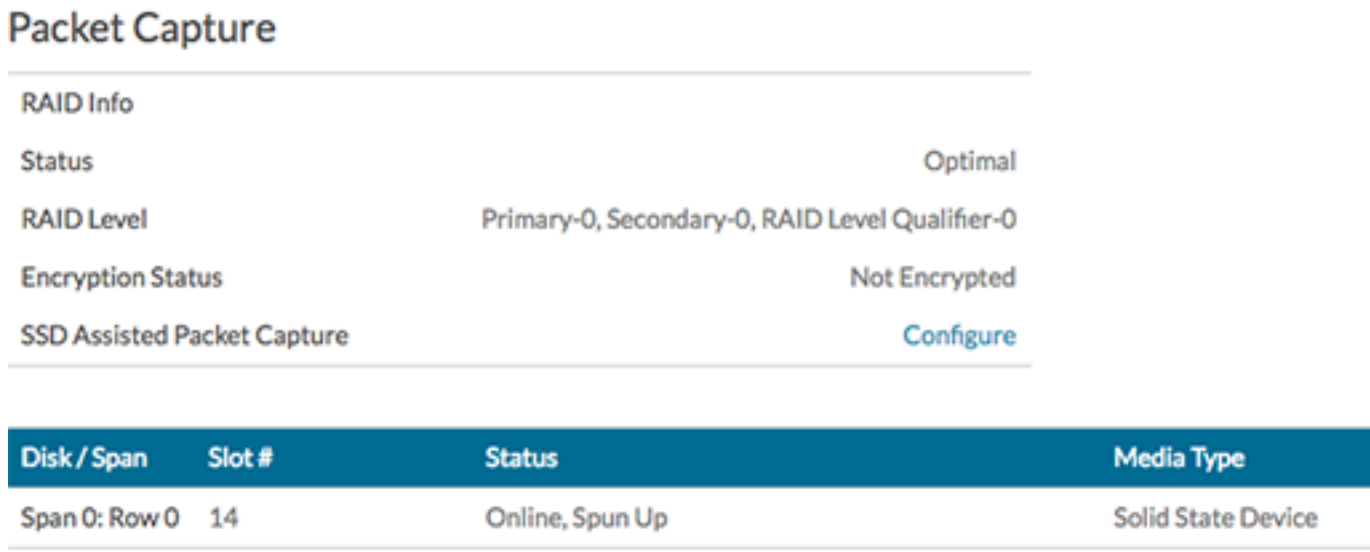
   The Drive Map shows the SSD slot in yellow because the drive is not configured.

4. Next to SSD Assisted Packet Capture, click **Enable**.



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`.



Tip: If the SSD drive is dislodged and reinserted, you can re-enable it. This process requires reformatting the disk, which erases all data.

Command Nickname

By default, your Command appliance is identified by its hostname on connected Discover appliances. However, you can optionally configure a custom name to identify your Command appliance.

Choose from the following options to configure the display name for your Command appliance:

- Select **Display custom nickname** and type the name in the field you want to display for this Command appliance.
- Select **Display hostname** to display the hostname configured for this Command appliance.

Packet Captures

When packet capture is enabled through the Admin UI, you can globally store every packet on every flow or write triggers to specify and deploy targeted packet captures from the ExtraHop Discover appliance to an SSD installed on your ExtraHop appliance or, in the case of a virtual machine, to a regular disk drive. You must have access to the ExtraHop Admin UI and write privileges to the ExtraHop Web UI to complete these steps.

Enable packet capture

Before you can perform packet captures through triggers, you must first ensure you are licensed for packet capture on your ExtraHop appliance and your SSD is installed if you are not using a virtual machine.

1. In the Appliance Settings section, click **License**.
2. In the Features section, verify that packet capture is enabled. If you do not see `Packet Capture` in the list or `Packet Capture` is not listed as `Enabled`, contact ExtraHop Customer Support.

   Note: On a Discover virtual machine, the packet capture license is labeled `Enabled (Unrestricted)`. This means the packet capture data will be written to a regular disk drive instead of an SSD.
3. Next, verify that the SSD is installed on your ExtraHop appliance. (This step is not applicable to virtual machines.)
4. In the Appliance Settings section, click **Disks**. If the Drive Map shows the last slot in red, refer to Disk to install and enable the drive.
5. If the Drive Map shows the SSD drive as green and the Status is `Online`, the disk is ready for packet capture.

   Note: If the SSD drive is dislodged and reinserted, you can re-enable it. This process requires reformatting the disk, which erases all data.

Identify metrics for packet capture

(Skip this section if you are doing a global packet capture.) The ExtraHop appliance uses Application Inspection Triggers to gather custom metrics. These metrics are stored internally and can be used by other features, such as packet capture. Triggers are user-specified scripts that perform additional actions during well-defined events.

For information about writing triggers, refer to the ExtraHop Trigger API Reference.

1. Click the System Settings icon and then click **Triggers**.
2. Click **New**.
3. Type a name for the trigger and select the events that will activate the trigger. Then click the **Editor** tab and write your trigger source code.

   Note: After you have tested the trigger to ensure it works, clear the **Enable Debugging** checkbox to avoid excessive debug messages in the runtime log.
4. Assign the trigger to a device or group of devices.
5. Click **Save**.

Configure global packet capture

When you enable the global packet capture feature on the Discover appliance, you start collecting packets for every flow to an SSD installed on your Discover appliance or, in the case of a virtual machine, to a regular disk drive.

Before you begin
Make sure you are licensed for the packet capture feature and that you have added the packet capture disk (an SSD on a physical appliance or an additional drive on a virtual machine). Note that the Packet Captures section in the Admin UI does not appear if your Discover appliance is not licensed for the feature. For information about adding an SSD drive, see Install an SSD for Packet Capture on the ExtraHop Discover Appliance.

For Discover virtual appliances, refer to your hypervisor manual for configuring an additional 500 GB disk.

1. Log into the Admin UI on the Discover appliance.
2. In the Packet Captures section, click **Global Packet Capture**.
3. In the Start Global Packet Capture section, type the following information:

   • **Name:** The name for the capture.

   • **Max Packets:** The maximum number of packets to capture. This value cannot be a negative number.

   • **Max Bytes:** The maximum number of bytes to captures. This value cannot be a negative number.

   • **Max Duration (milliseconds):** The maximum duration that the global capture should run. If this value is set to 0, this field is ignored and the duration runs for an unlimited time.

   • **Snaplen:** The maximum number of bytes copied per frame. By default, this value is 96 bytes, but you can set this value to a number between 1 and 65535.
4. Click **Start**.
5. Click **Stop** to stop the packet capture before any of the maximum limits are reached.

Download your packet capture from the View Packet Captures page and open the file in a packet analyzer such as Wireshark.

View and download packet captures

After you have written a trigger to specify the targeted packet capture and the trigger has collected data, you can view and download packet captures in the Admin UI.

1. In the Packet Captures section, click **View and Download Packet Captures**.
2. On the View Packet Captures page, select one or more packet captures, and then click **Download Selected Captures**. To filter packet captures, select the filter criteria from the Filter Packet Captures section. You can also filter by the date of capture.

   To sort packet captures, click a column heading in the table and click the arrow to the right of the heading to flip the sort order between ascending and descending order.
3. Open the downloaded packet captures in a packet analyzer such as Wireshark.

Configure automatic deletion of packet capture files

You can configure the Discover appliance to automatically delete packet capture (PCAP) files after a specified number of minutes to prevent the precision PCAP drive from filling to capacity and causing errors.

1. In the Packet Captures section, click **View and Download Packet Captures**.
2. Click **Configure packet capture settings**.

3. Type a value in the Automatically delete PCAP files (in minutes) field.
4. Click **Save**.

Encrypt the packet capture disk

You can encrypt the disk that packet captures are stored on for increased security. The disk is secured with 256-bit AES encryption.

Warning: You cannot decrypt a packet capture disk after it is encrypted. You can reformat an encrypted disk; however, all data stored on the disk will be lost. To perform a secure delete (secure wipe) of all system data, see the ExtraHop Rescue Media Guide.

1. In the Appliance Settings section, click **Disks**.
2. Navigate to the Packet Capture Disk Configuration page.

Option	Description
For virtual appliances	In the Direct Connected Disks table, in the row of a Packet Capture disk, click **Configure**.
For physical appliances	Under Packet Capture, next to SSD Assisted Packet Capture, click **Configure**.

3. Click **Encrypt Disk**.
4. Specify a disk encryption key.

Option	Description
To enter an encryption passphrase	Type a passphrase into the Passphrase and Confirm fields.
To select an encryption key file	Click **Choose File**, and then browse to an encryption key file.

5. Click **Encrypt**.

Remove the packet capture disk

You can remove the disk that packet captures are stored on if you are adding a higher capacity drive or you no longer wish to store packet capture data.

Warning: Removing the packet capture disk causes all data on the disk to be deleted.

1. In the Appliance Settings section, click **Disks**.
2. On the Disks page, choose one of the following options based on your appliance platform.

Option	Description
For virtual appliances	In the Actions column, next to Packet Capture Disk, click **Configure**.
For physical appliances	In the Packet Capture section, next to SSD Assisted Packet Capture, click **Configure**.

3. Click **Remove Disk**.
4. Select one of the following format options:
   - Quick Format
   - Secure Erase
5. Click **Remove**.

Next steps

After this procedure is complete, it is safe for you to remove the disk from the appliance.

Lock a packet capture disk

You can lock a packet capture disk to prevent read access to captured packets. Locking a packet capture disk disables packet capture until the disk is unlocked.

Warning: If you lock a packet capture disk, you will not be able to unlock the disk without the disk encryption key.

1. Under Appliance Settings, click **Disks**.
2. Navigate to the Packet Capture Disk Configuration page.

Option	Description
For virtual appliances	In the Direct Connected Disks table, in the row of a Packet Capture disk, click **Configure**.
For physical appliances	Under Packet Capture, next to SSD Assisted Packet Capture, click **Configure**.

3. Click **Lock Disk**.
4. Click **OK**.

Unlock a packet capture disk

1. Under Appliance Settings, click **Disks**.
2. Navigate to the Packet Capture Disk Configuration page.

Option	Description
For virtual appliances	In the Direct Connected Disks table, in the row of a Packet Capture disk, click **Configure**.
For physical appliances	Under Packet Capture, next to SSD Assisted Packet Capture, click **Configure**.

3. Click **Unlock Disk**.
4. Specify the disk encryption key.

Option	Description
If you entered an encryption passphrase	Type the passphrase into the Passphrase field.
If you entered an encryption key file	Click **Choose File**, and then browse to the encryption key file.

5. Click **Unlock**.

Clear the packet capture disk encryption

You can format the packet capture disk to delete all packet captures contained on the disk and return the disk to an unencrypted state.

Warning: This action is not reversible.

1. In the Appliance Settings section, click **Disks**.
2. Navigate to the Packet Capture Disk Configuration page.

Option	Description
For virtual appliances	In the Direct Connected Disks table, in the row of a Packet Capture disk, click **Configure**.
For physical appliances	Under Packet Capture, next to SSD Assisted Packet Capture, click **Configure**.

3. Click **Clear Disk Encryption**.
4. Click **Format**.

Change the packet capture disk encryption key

1. In the Appliance Settings, click **Disks**.
2. Navigate to the Packet Capture Disk Configuration page.

Option	Description
For virtual appliances	In the Direct Connected Disks table, in the row of a Packet Capture disk, click **Configure**.
For physical appliances	Under Packet Capture, next to SSD Assisted Packet Capture, click **Configure**.

3. Click **Change Disk Encryption Key**.
4. Specify a new disk encryption key.

Option	Description
If you entered an encryption passphrase	Type a passphrase into the Passphrase field.
If you selected an encryption key file	Click **Choose File**, and then browse to an encryption key file.

5. Click **Change Key**.

ExtraHop Command Settings

The ExtraHop Command Settings section on the Discover appliance enables you to connect the Discover appliance to a Command appliance. Depending on your network configuration, you can establish a connection from the Discover appliance (tunneled connection) or from the Command appliance (direct connection).

- We recommend that you log into the Admin UI on your Command appliance, and create a direct connection to the Discover appliance. Direct connections are made from the Command appliance over HTTPS on port 443 and do not require special access. For instructions, see Connect to a Discover appliance from a Command appliance.
- If your Discover appliance is behind a firewall, you can create an SSH tunnel connection from this Discover appliance to your Command appliance. For instructions, see Connect to a Command appliance from a Discover appliance.

Connect to a Command appliance from a Discover appliance

You can connect the Discover appliance to the Command appliance through an SSH tunnel.

We recommend that you always connect appliances directly through the Command appliance; however, a tunneled connection might be required in network environments where a direct connection from the Command appliance is not possible because of firewalls or other network restrictions. After you connect the appliances, you can view and edit the Discover appliance properties, assign a nickname, update firmware, check the license status, create a diagnostic support package, and connect to the ExtraHop Web Shell.

Before you begin

- You can connect a Discover appliance to multiple Command appliances.
- You can only establish a connection to a Command appliance that is licensed for the same system edition as the Discover appliance.

1. Log into the Admin UI on the Discover appliance.
2. In the ExtraHop Command Settings section, click **Connect Command Appliances**.
3. Click **Add Appliance** and then configure the following fields:

   • **Host:** The hostname or IP address of the Command appliance.

   Note: You cannot specify an IPv6 link-local address.

   • **Setup password:** The password for the setup user on the Command appliance.

   • **Discover nickname (Optional):** A friendly name for the node that appears on the Manage Connected Appliances page. If no friendly name is configured, the hostname for the Discover appliance appears instead.

   • **Reset configuration:** If you select the Reset Configuration checkbox, existing node customizations such as device groups, alerts, and triggers will be removed from the appliance. Gathered metrics such as captures and devices will not be removed.
4. Click **Pair**.

Connect a Command appliance to Discover appliances

You can manage multiple Discover appliances from a Command appliance. After you connect the appliances, you can view and edit the appliance properties, assign a nickname, upgrade firmware, check

the license status, create a diagnostic support package, and connect to the ExtraHop Web UI, Admin UI, and Web Shell.

The Command appliance connects directly to the Discover appliance 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 Command appliance through a tunneled connection from the Discover appliance.

Before you begin

- You can connect a Command appliance to multiple Discover appliances.
- You can only establish a connection to a Discover appliance that is licensed for the same system edition as the Command appliance.
- The Command appliance and Discover appliances must have the same version of ExtraHop firmware to function correctly together.

1. Log into the Admin UI on the Command appliance.
2. In the ExtraHop Discover Settings section, click **Manage Discover Appliances**.
3. In the Discover section, click **Connect Appliance**.
4. Configure the following settings:

   • Host**:** The hostname or IP address of the Discover appliance.

   • Setup Password**:** The `setup` user password for the Discover appliance.

   • Product Key (Optional)**:** The product key for the ExtraHop firmware.

   • Nickname (Optional)**:** A friendly name for the appliance. If no nickname is entered, the appliance is identified by the hostname.

   • Reset Configuration**:** If you select this checkbox, existing appliance customizations such as device groups, alerts, and triggers will be removed from the appliance. Gathered metrics such as captures and devices will not be removed.
5. Click **Pair**.

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 Explore Settings

This section contains the following configuration settings for the ExtraHop Explore appliance.

- Configure automatic flow records (Discover appliance only)
- Connect to an Explore appliance
- Manage an Explore appliance (Command appliance only)

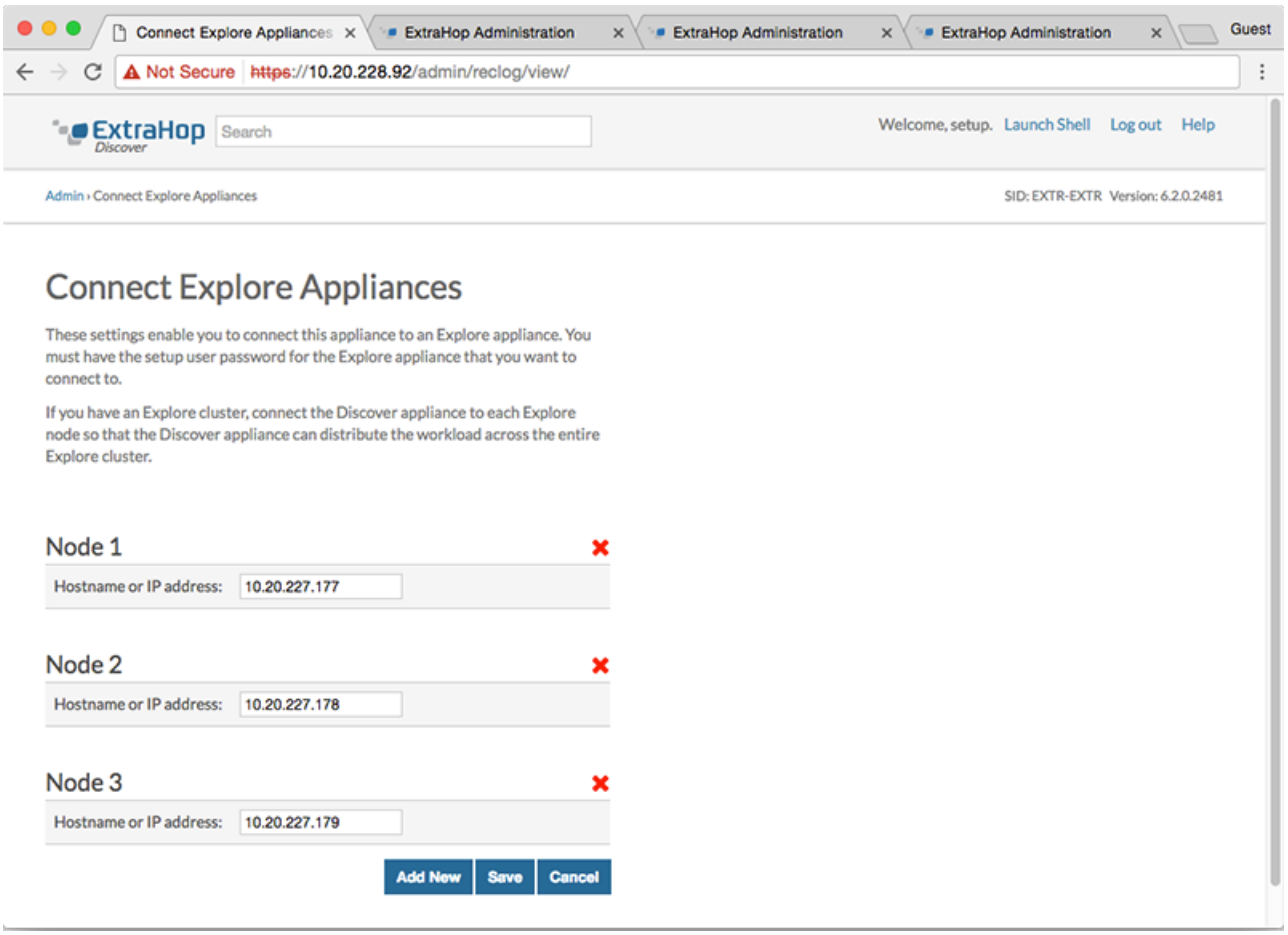
Connect the Discover and Command appliances to Explore appliances

After you deploy an Explore appliance, you must establish a connection from all ExtraHop Discover and Command appliances to the Explore appliance before you can query for stored records.

Important: If you have an Explore cluster of three or more Explore nodes, connect the Discover appliance to each Explore node so that the Discover appliance can distribute the workload across the entire Explore cluster.

Note: If the Explore appliance connections are managed from a Command appliance, you must perform this procedure from the Command appliance instead of from each Discover appliance.

1. Log into the Admin UI on the Discover or Command appliance.
2. In the ExtraHop Explore Settings section, click **Connect Explore Appliances**.
3. Click **Add New**.
4. In the Explore node field, type the hostname or IP address of any Explore appliance in the Explore cluster.
5. For each additional Explore appliance in the cluster, click **Add New** and enter the individual hostname or IP address in the corresponding Explore node field.



6. Click **Save**.
7. Confirm that the fingerprint on this page matches the fingerprint of Node 1 of the Explore cluster.
8. In the Explore Setup Password field, type the password for the Explore Node 1 `setup` user account and then click **Connect**.
9. When the Explore cluster settings are saved, click **Done**.

Next steps

Important: If you only deployed a single Explore appliance, after you connect to your Discover or Command appliance, you must log into the Admin UI on the Explore appliance and set the **Explore Cluster Settings** > **Cluster Data Management** > **Replication Level** to **0**.

Disconnect the Explore appliances

To halt the ingest of records to the Explore appliance, disconnect all Explore appliances from the Command and Discover appliances.

Note: If appliance connections are managed by a Command appliance, you can only perform this procedure on the Command appliance.

1. Log into the Admin UI on the Discover or Command appliance.
2. In the ExtraHop Explore Settings section, click **Connect Explore Appliances**.
3. Click the red **X** next to every node in the Explore 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 appliance to open the node properties. By clicking **Open Admin UI**, you can access the Admin UI 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 an Explore node or one or more connected Explore clusters. 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 Explore 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 Explore 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 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 all flow records, which are network-layer communications between two devices over an IP protocol. If you enable this feature, but do not add any IP addresses or port ranges, all detected flow records are captured.

Before you begin

- You must connect your Explore appliances to your Discover appliance before you can collect flow records. See Connect the Discover and Command appliances to Explore appliances.
- You must have unlimited privileges to configure automatic flow record collection.

Configuring flow records for automatic collection is fairly straight-forward and can be a good way to test that your appliances are connected.

1. Log into the Admin UI on your Discover appliance.
2. In the ExtraHop Explore Settings 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 Explore appliance. 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 connected Explore appliance. Wait a few minutes for records to be collected, and then verify that flow records are being collected in the next step.
8. Click **Records** from the top navigation to launch 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 Explore Status

If you have connected an Explore appliance to your Discover or Command appliances, you can access information about the Explore appliance.

The table on this page provides the following information about any connected Explore appliances.

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 Explore appliance from a Discover appliance.

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 Explore appliance.

ExtraHop Trace Settings

ExtraHop Trace appliances continuously collect and store raw packet data from your Discover appliance. Connect the appliances to begin storing packets on a Trace appliance.

Connect the Discover and Command appliances to the Trace appliance

After you deploy the Trace appliance, you must establish a connection from all ExtraHop Discover and Command appliances to the Trace appliance before you can query for packets.

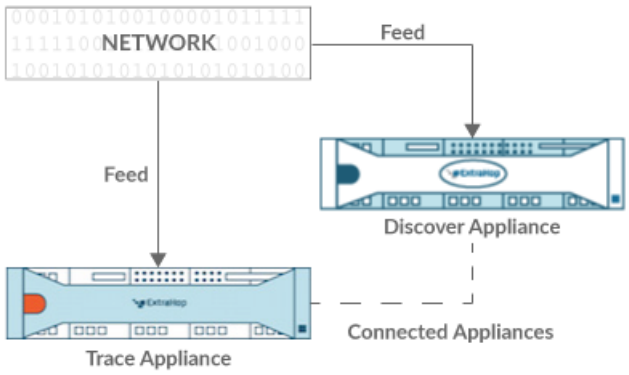


Figure 1: Connected to Discover Appliance

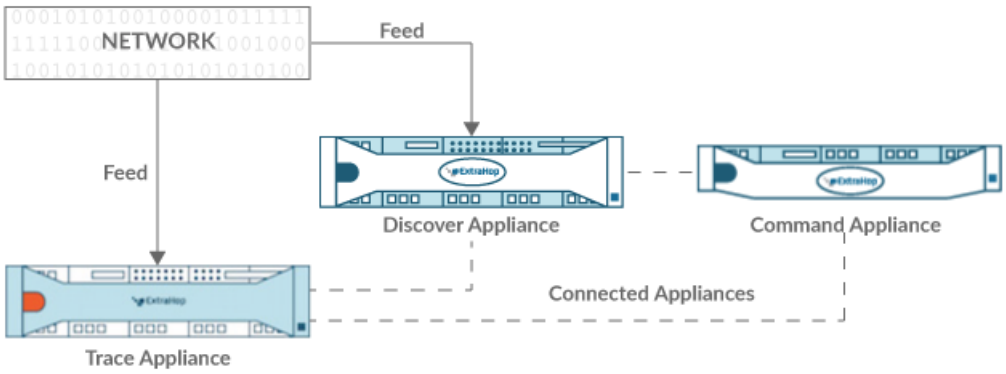


Figure 2: Connected to Discover and Command Appliance

1. Log into the Admin UI of the Discover appliance.
2. In the ExtraHop Trace Settings section, click **Connect Trace Appliances**.
3. Type the hostname or IP address of the Trace appliance in the Appliance hostname field.
4. Click **Pair**.
5. Note the information listed in the Fingerprint field. Verify that the fingerprint listed on this page matches the fingerprint of the Trace appliance listed on the Fingerprint page in the Admin UI of the Trace appliance.
6. Type the password of the Trace appliance `setup` user in the Trace Setup Password field.
7. Click **Connect**.
8. To connect additional Trace appliances, repeat steps 2 through 7.

Note: You can connect a Discover appliance to four or fewer Trace appliances. However, you can connect a Command appliance to an unlimited number of Trace appliances.

9. If you have a Command appliance, log into the Admin UI of the Command appliance and repeat steps 3 through 7 for all Trace appliances.

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 Admin UI 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

Decrypting SSL traffic

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

Implement the following recommendations to optimize security:

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

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

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

The following list includes some common cipher suites that support Perfect Forward Secrecy (PFS) and can be decrypted by the ExtraHop appliance when session key forwarding is configured. To configure session key forwarding, see Install the ExtraHop session key forwarder on a Windows server or Install the ExtraHop session key forwarder on a Linux server.

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

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

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

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

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
SMTP	Simple Message Transport Protocol

Acronym	Full Name
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 Discover appliance.

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 Discover appliance. 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 into 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 Port + Flow Target interface on the Discover appliance and <*udp-port*> is the configured collector UDP port number.