ExtraHop 7.0
Admin UI Guide

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

Published: 2018-10-27

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.

- 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.

Global navigation

This section describes the general layout of the ExtraHop Admin UI on the Discover and Command appliances.

The top toolbar includes the following controls.

Change default password

Opens the Change Password page where you can set a new Admin UI password. For more information about changing the default password, see the Change the default password for the setup user section.

Launch Shell

Opens the ExtraHop web shell, which enables users with administrative privileges to configure the ExtraHop appliance. For more information about the ExtraHop web shell, see the ExtraHop Command-line Reference.

Log out

Ends the ExtraHop Admin UI session. For more information about logging in and out, see the Log in and log out of the Admin UI section.

Help

Opens the ExtraHop Admin UI Guide

The main administration page has the following sections.

Search

Navigate to sections in the Admin UI quickly by typing a search term and clicking the search result link.

Status and Diagnostics

Verify how the ExtraHop appliance is functioning on the network

Network Settings

Configure the network settings for the ExtraHop appliance

Access Settings

Configure user access settings to the ExtraHop appliance.

ExtraHop Discover Settings

Manage connected Discover appliances from a Command appliance.

ExtraHop Command Settings

Connect to a Command appliance from a Discover appliance or manage connected appliances from a Command appliance.

ExtraHop Explore Settings

Connect an ExtraHop Discover or Command appliance to an ExtraHop Explore appliance.

ExtraHop Trace Settings

Connect an ExtraHop Discover or Command appliance to an ExtraHop Trace appliance.

System Configuration

Change the configuration settings of the ExtraHop appliance.

System Settings

Configure the system-level settings for the ExtraHop appliance.

Packet Captures

View and download packet captures.

Log in and log out of the Admin UI

The Admin UI on the ExtraHop appliance is a secure web page that requires a username and a password to access the interface.

1. In a web browser, navigate to the ExtraHop Admin UI by typing `https://<address>/admin`, where <*address*> is the hostname or IP address of your ExtraHop appliance.
2. To log into the Admin UI, type your username in the **Username** field and your password in the **Password** field, and then click **Log In**.

   Note: For physical appliances, the default Admin UI username is `setup` and the password is the service tag number on the pullout tab on the front of the appliance. For virtual appliances, excluding Amazon Web Services (AWS) deployments, the default password is `default`. The default ExtraHop password for Amazon Web Services (AWS) deployments is the string of numbers after the `-i` in the instance ID.
3. To log out of the Admin UI, click **Log out** on the toolbar.

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.

The Status and Diagnostics section includes the following pages:

Health

Provides metrics to view the operating efficiency of the Discover appliance.

Audit Log

Enables you to view event logging data and to change syslog settings

Exception Files

Enable or disable the creation Discover appliance exception files.

Support Packs

Upload and run Discover appliance support packages.

Health

The Health page provides a collection of metrics about the operation of the ExtraHop appliance.

If issues occur with the ExtraHop appliance, the metrics on the Health page can help you to troubleshoot the problem and determine why the ExtraHop appliance is not performing as expected.

The ExtraHop appliance system collects and reports metrics on the following operational activities that are performed by the ExtraHop appliance.

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 ExtraHop appliance audit log provides data about the operations of the system, broken down by component. The log lists all known events by timestamp, in reverse chronological order. In addition, you can configure where to send these logs in the **Syslog Settings**.

The ExtraHop appliance collects the following log data and reports the results on the audit log Activity page.

Time

The time at which the event occurred.

User

The ExtraHop appliance user who initiated the logged event.

Operation

The ExtraHop appliance operation that generated the logged event.

Details

The outcome of the event. Common results are Success, Modified, Execute, or Failure. Each log entry also identifies the originating IP address, if that address is known.

Component

The ExtraHop appliance component that is associated with the logged event.

View audit log activity

1. In the Status section, click **Audit Log**.
2. Click **View**.

Configure syslog settings

You can send audit logs to a remote syslog server for long-term storage, monitoring, and advanced analysis.

1. In the Status section, click **Audit Log**.
2. Click **Syslog Settings**.
3. Configure the following settings:

Destination:

Type the name of the remote syslog server.

Protocol:

Select UDP or TCP from the drop-down menu.

Port:

Type the port for the remote syslog server. The default value is 514.

4. 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
```

5. Click **Save**.
   The Audit Log page appears with the following message: `Running config has changed`.
6. Click **View and Save Changes** next to the message.
   The Running Config page appears with your changes highlighted.
7. Click **Save**.

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 Pack	• A default support pack is generated • A past support pack result is deleted • A support pack 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 • 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
Appliance user	• A user is added • User metadata is edited • A user is deleted • A user password is set • A user other than the `setup` user attempts to modify the password of another user • A user password is updated
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

Reports	• A scheduled report is created • A scheduled report is updated • A scheduled report is deleted.
Trends	A trend is reset
PCAP	• A packet capture (PCAP) file 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 • 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.

Enable writing to exception files

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

1. In the Status and Diagnostics section, click **Exception Files**.
2. Click **Enable Exception Files**.

Disable writing to exception files

1. In the **Status and Diagnostics** section, click **Exception Files**.
2. Click **Disable Exception Files**.

Support packs

When you receive assistance from ExtraHop Support, you might need to load an ExtraHop-provided support pack to apply a special setting, make a small adjustment to the system, or get help with remote support or enhanced settings. The Admin UI includes the following configuration settings to manage support packages:

View Support Pack results

View, download, or delete selected support packages.

Upload Support Pack

Upload diagnostic support packages on the ExtraHop system.

Run Default Support Pack

Create a diagnostic support package that can be downloaded and sent to the ExtraHop Support team.

View the diagnostic support packages

1. In the **Status and Diagnostics** section, click **Support Packs**.
2. Click **View Support Pack Results**.

Download a selected diagnostic support package

1. In the **Status and Diagnostics** section, click **Support Packs**.
2. Click **View Support Pack Results**.
3. Click the name of the diagnostic support package that you want to download. The file will download to your browser's default download location.

Delete a selected diagnostic support package

1. In the **Status and Diagnostics** section, click **Support Packs**.
2. Click **View Support Pack Results**.
3. Click the red **X** next to the support package you want to delete.
4. Click **OK**.

Upload a support pack

1. In the **Status and Diagnostics** section, click **Support Packs**.

2. Click **Upload Support Pack**.
3. Click **Choose File**, navigate to the diagnostic support package you want to upload, and then click **Open**.
4. Click **Upload** to add the file to the ExtraHop appliance.

System support pack

Some support packs only perform a function on the ExtraHop appliance, while other support packs gather information about the state of the system for analysis by the ExtraHop Support team. If the support pack generated a results package to send to the ExtraHop Support team, then the Admin UI redirects to the View Support Pack Results page.

To create a diagnostic support package that can be downloaded and sent to the ExtraHop Support team:

1. In the Diagnostics section, click **Support Packs**.
2. Click **Run Default Support Pack**.
3. Click **OK**.

Network Settings

The Network Settings section has the following configurable settings:

Atlas Services

Connect the Discover appliance to the ExtraHop Atlas service. See the Atlas Remote Analysis page on the ExtraHop website for more information about the Atlas service.

Connectivity

Configure the host name, DNS, proxy, and interface settings.

Flow Networks

Configure settings for flow network traffic sent to your Discover appliance.

Notifications

Configure email, SNMP, and syslog settings to receive notifications about your ExtraHop appliance.

SSL Certificate

View and manage SSL certificates.

For specifications, installation guides, and more information about your ExtraHop appliance, visit docs.extrahop.com.

ExtraHop Cloud Services

ExtraHop Cloud Services provides access to ExtraHop cloud-based services through an encrypted connection.

Addy is a cloud-based service from ExtraHop that detects anomalies by applying machine-learning techniques to wire data metrics.

To learn more, see the ExtraHop Addy User Guide.

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

Note: You can connect Discover, Explore, and Trace appliances to Atlas Services, but you cannot connect Command appliances to Atlas Services.

1. In the Network Settings section, click **Atlas Services**.
2. 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.
3. Return to the Connect to Atlas Services page and select the checkbox next to **Terms and Conditions**.
4. Click **Test Connectivity** to make sure the connection is successful. If you have problems connecting to the Atlas service, see the Troubleshoot an Atlas Connection for troubleshooting suggestions.
5. Click **Connect**.

Disconnect from Atlas services

If you no longer want to receive Atlas reports, you can disconnect from the subscription service.

1. In the Network Settings section, click **Atlas Services**.
2. Click **Disconnect**.

Connectivity

The Connectivity page provides options that enable you to view and modify your network settings.

Interface Status

In physical ExtraHop appliances, an Interface Status section appears on the Connectivity page. This section displays a diagram of the following interface connections on the back of the appliance:

Blue Ethernet Port:

Identifies the management port.

Black Ethernet Port:

Indicates that the port is licensed and enabled but down.

Green Ethernet Port:

Indicates that the licensed port has an active Ethernet cable connected.

Gray Ethernet Port:

Identifies a disabled or unlicensed port.

Network Settings

Hostname:

The name of the appliance on the network.

Primary DNS:

The IP address of the primary domain name server for the specified domain.

Secondary DNS:

(Optional) The IP address of the secondary domain name server for the specified domain.

Proxy Settings

Enable Global Proxy:

Provides the ability to enable proxy support for connection to the Command appliance.

Enable ExtraHop Cloud Proxy:

Provides the ability to enable proxy support for connection to ExtraHop Cloud services and the Atlas Remote UI.

Bond Interface Settings

Create Bond Interface:

Provides the ability to bond multiple interfaces together into a single logical interface that will use a single IP address for the combined bandwidth of the bond members. Only 1GbE ports are supported for bond interfaces. This is also known as link aggregation, port trunking, link bundling, Ethernet/network/NIC bonding, or NIC teaming.

Note: Creating bond interfaces will cause you to lose connectivity to your ExtraHop appliance. You must make changes to your network switch configuration to restore that connectivity. The changes required depend on which switch you are using. Contact ExtraHop Support for assistance before you create a bond interface.

Interfaces

Interface

Displays the interface number.

Mode

Displays whether the port is enabled or disabled and if enabled, the port assignment.

DHCPv4

Displays whether DHCPv4 is enabled or disabled.

IP address

Displays the static IP address of the ExtraHop appliance on the network.

Netmask

Displays the netmask configured to divide the IP address into subnets.

Gateway

Displays the IP address for the gateway node on the network.

Routes

Displays configured static route information.

MAC Address

Displays the MAC address of the ExtraHop appliance.

IPv6

Displays whether IPv6 is enabled or disabled.

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

Configure network settings

Set the hostname and DNS information for your ExtraHop appliance.

1. In the Network Settings section, click **Connectivity**.
2. In the Network Settings section, click **Change**.
3. On the Edit Hostname page, configure the following fields:

   • **Hostname:** The descriptive device name for the ExtraHop appliance on the network. Devices on the network can be identified by their IP address, MAC address, or by the descriptive name specified in this setting.

   • **Primary DNS:** The computer that stores the record of the network domain name, which is used to translate domain names specified in alpha-numeric characters into IP addresses. Each domain requires a primary domain name server and at least one secondary domain name server.

   • **Secondary DNS:** The backup server to the primary DNS.
4. Click **Save**.

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 Interface 2. These appliances cannot process NetFlow and wire data simultaneously.
Management Port + RPCAP/ERSPAN Target	Manages the ExtraHop appliance and captures traffic forwarded from a software tap or ERSPAN*.
High Performance ERSPAN Target	Captures traffic forwarded from ERSPAN*. 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.

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

Note: Interfaces 3 and 4 are disabled by default on the following appliances: EH2000, EDA 2000v, EH3000, EH5000, EH6000, EH6100, EH8000, EDA 8100, EDA 9100, and EDA 1100. Interfaces 5 and 6 are disabled by default on the following appliances: EH5000, EH6000, EDA 6100, EH8000, EDA 8100, and EDA 9100.

4. 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.
5. (Optional) Enable IPv6.

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

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

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**.

Change the RPCAP settings

After you configure an interface as an RPCAP target, configure the RPCAP settings.

Note: You must specify an interface address or an interface name. If you specify both, then both settings will apply.

1. In the Network Settings section, click **Connectivity**.
2. In the RPCAP Settings section, complete one of the following actions:
   - Click the port number in the Port field to edit an existing port definition.
   - Click **Add** to add a new port definition.
3. In the Add RPCAP Port Definition section, edit the following settings as needed:

   • **Port:** Specifies the listening port on the ExtraHop appliance. Each port must be unique for each interface subnet on the same server. You can configure different subnets across servers with the same port, which can be a TCP and UDP port. If you are configuring multiple software taps and multiple software tap listeners, the payload might traverse a range of UDP ports. The range consists of 16 ports, starting with the specified port.

   • **Interface Address:** Specifies the subnet on the software tap server. If the server has multiple interfaces that match the interface address, the first interface on the server sends traffic to the ExtraHop appliance unless the interface name is specified. By default, the interface address is set to `*`, which means the Discover appliance will accept packets from any IP address or CIDR range.

   For example, `10.10.0.0/24` forwards all traffic on the system that is part of that CIDR range, `*` is a wildcard that will match all traffic on the system, or `10.10.0.1` will send traffic that matches the local interface's netmask.

• **Interface Name:** Specifies the interface on the packet-forwarding server from which to forward packets. For example, `eth0` in a Linux environment or `\Device \NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}` in a Windows environment.

• **Filter:** Specifies the traffic to forward with Berkeley Packet Filter (BPF) syntax. For example, `tcp port 80` forwards only TCP traffic on port 80, and `not tcp port 80` forwards only non-TCP traffic on port 80. For more information about BPF syntax, see http://biot.com/capstats/bpf.html.

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.

Configure a global proxy server

1. In the Network Settings section, click **Connectivity**.
2. Click **Enable Global Proxy** or click on the name of an existing global proxy that you want to modify.
3. On the Global Proxy Settings page, type the following information:

   • **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.
4. Click **Save**.

Disable a global proxy server

1. In the Network Settings section, click **Connectivity**.
2. Click **Disable Global Proxy**.

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.

Configure an ExtraHop Cloud proxy server

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**.

Remove an ExtraHop Cloud proxy server

1. In the Network Settings section, click **Connectivity**.
2. Click **Change ExtraHop Cloud Proxy**.
3. Click **Delete**, and then click **OK**.

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 usable 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

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. In the Network Settings section, click **Connectivity**.
2. Click **Create Bond Interface**.
3. On the Bond Interface page, select from 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 are displayed.

• **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.

4. 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 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 **Mangement+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

Before you begin
You must have full system privileges to configure flow networks in the Admin UI.

First you will configure the interface on your Discover appliance.

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 you want to 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**.

Next, configure the flow type and the UDP port over which the 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**.

Finally, add the pending flow networks on the Discover appliance so the flow data can be seen in the ExtraHop Web UI.

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**.
8. The flow network appears in the Approved Flow Networks table. If you do not see the flow network, you might have to manually add it by clicking **Add Flow Network** in the Approved Flow Networks section.

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.
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 the 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.

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.
- The interface name of each interface on the SNMP agent. These identifiers are for each flow interface on the flow network.
- The interface speed of each interface on the SNMP agent.

1. Log into the Admin UI on your Discover appliance.
2. In the Actions column for the approved flow network, click **Poll**.

Notifications

The ExtraHop appliance can send alert notifications through email and SNMP traps. If SNMP is specified, then every alert is sent as an SNMP trap to the specified SNMP server. If an email notification group is specified, then emails are sent to the groups assigned to the alert.

In addition, you can send alerts to a remote server through a syslog export.

Configure email settings

You must configure an email server and sender before the ExtraHop appliance can send notifications about system alerts by email.

1. In the Network Settings section, click **Notifications**.
2. Click **Email Server and Sender**.
3. Type the IP address or hostname for the outgoing SMTP mail server in the SMTP Server field.

Note: 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 it needs to be an IP address.

4. Type the port number for SMTP communication in the SMTP Port field. The default port number is 25.
5. 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.
6. Type the email address for the notification sender in the Sender Address field.

   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.
7. Select Validate SSL Certificates 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. In addition, the host name specified in the certificate presented by the SMTP server must match the host name specified in your SMTP configuration or validation will fail. 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.
8. Type the email address for the report sender in the **Report Sender Address** field.
9. Select the Enable SMTP authentication checkbox and then type the SMTP server setup credentials in the Username and Password fields.
10. Click **Save**.

Configure an email notification group

Email notification groups are assigned to alerts to designate who should receive an email when that alert fires. 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. In the Network Settings section, click **Notifications**.
2. Click **Email Notification Groups**.
3. Click **Add Group**.
4. In the Group Info section, configure the following information:

   • **Name:** Define 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 sent 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 role is missing, such as firmware, datastore, or packet capture.
5. In the Email Addresses text box, enter the recipient email addresses for the team members that you want to 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.

Modify an email notification group

1. In the Network Settings section, click **Notifications**.
2. Click **Email Notification Groups**.
3. Click the name of the group that you want to modify.
4. In the Group Info section, modify the following information:

   • **Name:** Define 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 sent 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 role is missing, such as firmware, datastore, or packet capture.

5. In the Email Addresses text box, enter the recipient email addresses for the individuals that you want to receive the alert emails for this group. Email addresses can be entered one per line or separated by a comma, semicolon, or space.

Delete an email notification group

If you want to delete an existing email notification group, it is a best practice to first unassign it from any alerts it is assigned to.

Note: When you delete an email group, the group and all of its associated email addresses are deleted.

1. In the Network Settings section, click **Notifications**.
2. Click **Email Notification Groups**.
3. On the Email Groups page, click the red **X** to the left of the group name.
4. Click **OK**.

Configure SNMP notifications

Simple Network Management Protocol (SNMP) is used to monitor the state of the network. SNMP collects information both by polling devices on the network and when SNMP-enabled devices send alerts to SNMP management stations. SNMP communities specify 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. Click **SNMP**.
3. On the SNMP Settings page, type the following information:

   • **SNMP Monitor:** The hostname for the SNMP trap receiver. Multiple names can be entered, separated by commas.

   • **SNMP Community:** The SNMP community name.

   • **SNMP Port:** 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. By default, this value is set to 162.
4. 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.
5. Click **Save**.

Configure syslog notification settings

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

Note: To send syslog messages to your remote server, you must first configure the syslog notification settings. Only one remote syslog server can be configured for each ExtraHop appliance.

1. In the Network Settings section, click **Notifications**.
2. Click **Syslog**.
3. On the Syslog Notification Settings page, type the following information:

   • **Destination:** The IP address of the remote syslog server.

   • **Protocol:** From the drop-down, select which protocol to use to send information to your remote syslog server.

   • **Port:** The port number for your remote syslog server. By default, this is set to 514.
4. 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
   ```
5. Click **Save**.

SSL certificates

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

A self-signed certificate can be used in place of a certificate signed by a certificate authority. However, be aware that a self-signed certificate generates an error in the client browser and the browser reports that the signing certificate authority is unknown. The browser provides a set of confirmation pages to allow the use of the certificate, even though the certificate is self-signed.

Important: When replacing an SSL certificate, the webserver service is restarted. On a Command appliance, tunneled connections from Discover appliances are lost but are re-established automatically.

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`.

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**.

Add a trusted certificate to your ExtraHop appliance

Your ExtraHop appliance only trusts peers who present a TLS certificate that is signed by one of the built-in system certificates or any certificates that you upload. Only SMTP and LDAP connections are validated through these certificates.

Before you begin
You must be a user with full system privileges to add or remove trusted certificates.

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.
2. In the Network Settings section, click **Trusted Certificates**.
3. 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**.

Important: ExtraHop appliances only accept modern SSL configurations, which includes TLS 1.2 and the cipher suites listed below. Note that the ExtraHop Web UI will not display in Internet Explorer 11 unless TLS 1.0, TLS 1.1, and TLS 1.2 are turned on in the advanced settings for Internet Explorer 11.

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

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. The Access Settings section has the following configurable settings:

Password

Change the password for user accounts.

Support Account

Enable troubleshooting assistance from ExtraHop Support.

Users

Add and delete users, and modify user privileges.

Sessions

View and terminate user sessions on the Admin UI.

Remote Authentication

Enable users to log on to the Admin UI with their existing credentials.

API Access

Manage the settings that enable you to perform operations through the ExtraHop REST API.

User Groups

View and manage user groups imported from a configured LDAP server. The User Groups page appears only on ExtraHop Discover and Command appliances.

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 Change 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**.

Change a user password

Admin UI users may change their own passwords. Admin UI administrators may change the password for any local user accounts.

Note:
- You can only change passwords for local users, not for users authenticated with LDAP.
- The default password for Amazon Web Services (AWS) users is the string of numbers after the -i in the instance ID.

1. In the Access Settings section, click **Change Password**.

2. In the User field, select a user from the drop-down.
3. In the New password field, type the new password.
4. In the Confirm password field, type the same password again.
5. Click **Save**.
6. Click **OK**.

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

Support account

Support accounts provide access for the ExtraHop Support team to help customers troubleshoot issues with the ExtraHop appliance and to provide 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 a Command, Explore, and Trace appliance, 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 a Command, Explore, and Trace appliance, 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**.

Disable the Support account

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

   Note: On a Command, Explore, and Trace appliance, this step is unnecessary.
3. Click **Disable Support Account**.

Enable the Atlas Remote UI account

The Atlas Remote UI account enables the ExtraHop Support team to provide remote analysis reports through Atlas Services.

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**.

Disable the Atlas Remote UI account

1. In the Access Settings section, click **Support Account**.
2. Click **Atlas Remote UI Account**.
3. Click **Disable Atlas Remote UI Account**.

Users

Users can access the ExtraHop appliance through a set of pre-configured, default user accounts, and you can add local and remote user accounts with varying permission levels as needed.

User accounts can be authenticated locally or remotely. See the Remote Authentication section for information about configuring remote accounts.

The following default accounts are configured on the ExtraHop appliance:

setup

The `setup` 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 Amazon Web Services (AWS) users is the string of numbers after the -i in the instance ID.

Add a user account

1. In the Access Settings section, click **Users**.
2. Click **Add User**.
3. In the Personal Information section, type the following information:

   • Login ID**:** The username for the account. This is the name users will log in with and should not contain any spaces.

   • Full Name**:** A display name for the user.

   • Password**:** The new user password. The password must be a minimum of 5 characters

   • Confirm Password**:** Re-type the password from the previous field.
4. In the User Privileges section, select the desired permission for the user.

   Note: For more information, see the Permissions section.
5. Click **Save**.

Modify a user account

1. In the Access Settings section, click **Users**.
2. Click the name of the user that you want to modify.

3. On the Update User page, modify the privileges or change the full name of the user.
4. Click **Save**.

Delete a user account

Note: Remote user accounts must be deleted manually from the ExtraHop appliance.

1. In the Access Settings section, click **Users**.
2. Click the red **X** next to the user account you want to delete.

   Note: You cannot delete the account of the current user.

3. Click **OK**.

User privileges

An administrator can grant users the following privileges.

Privilege	Description
Full system privileges	• View dashboards and metrics. • Create, modify, and organize dashboards. • Create and modify objects such as alerts, triggers, device groups, and custom pages. • View and download packets captured through the Discover appliance and Trace appliance. • View and save record queries collected through the Explore appliance. • Access the ExtraHop Admin UI. • Connect a Command appliance to one or more Discover and Explore nodes. • Create, view, and manage scheduled reports.
Full write privileges	• View dashboards and metrics. • Create, modify, organize, and share dashboards. • Create and modify objects such as alerts, triggers, device groups and custom pages. • Create and edit record formats. • View and save record queries collected through the Explore appliance. • Create scheduled reports and view reports owned by the logged-in user.
Limited write privileges	• View dashboards and metrics. • Create, modify, organize, and share dashboards. • View record queries collected through the Explore appliance. • Create scheduled reports and view reports owned by the logged-in user.
Personal write privileges	• View dashboards and metrics.

Privilege	Description
	• Create, modify, and organize personal dashboards and modify dashboards shared with the logged-in user. • View record queries collected through the Explore appliance.
Full read-only privileges	• View dashboards and metrics. • View record queries collected through the Explore appliance.
Restricted read-only privileges	• View dashboards shared with the user.
No privileges (Admin UI)	• Cannot log into the Admin UI on a Command appliance.
No privileges (Web UI)	• Cannot log into the Web UI on a Command appliance.
View connected appliances	• View connected Discover, Explore, and Trace appliances on the Command appliance Admin UI.
View and download packets	• View and download packets captured through the Discover and Trace appliances. This privilege can be assigned to all users with access to the Web UI.

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.

Delete active sessions

When you delete an active session for a user, the user is logged out of the Admin UI. You can not delete the current user session.

1. In the Access Settings section, click **Sessions**.
2. Select the users that you want to delete.
   - To delete a specific user, in the sessions table, click the red **x** at the end of the row for the specific user.
   - To delete all active user sessions, click **Delete All** and then click **OK**.

Remote authentication

ExtraHop appliances supports remote authentication for user authentication. Remote authentication enables organizations that have authentication systems such as LDAP, RADIUS, or TACACS+ to allow 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.

To configure remote authentication, you must have a remote server with one of the following configurations:

- LDAP (such as OpenLDAP or Active Directory)

  Administrators can grant access to all known users or restrict access by applying LDAP filters.
- RADIUS
- TACACS+

LDAP

The ExtraHop system supports the Lightweight Directory Access Protocol (LDAP) for authentication and authorization. ExtraHop LDAP authentication only queries for user accounts; it does not use any other entities that might be in the LDAP directory.

Users whose credentials are not stored locally are authenticated against the remote LDAP server by their username and password when they attempt to log onto the ExtraHop system. When a user attempts to log onto the ExtraHop UI, the ExtraHop system:

- Attempts to authenticate the user locally.
- Attempts to authenticate the user through the LDAP server if the user does not exist locally and the ExtraHop system is configured to use LDAP for remote authentication.
- Logs the user on to the ExtraHop system if the user exists and the password is validated through LDAP. The LDAP password is not stored locally on the ExtraHop system.

If the user does not exist or an incorrect password is used, an error message appears with the login page.

Ensure that each user to be remotely authorized is in a permission-specific group on the LDAP server before beginning this procedure.

Configure LDAP authentication

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

1. In the Access Settings section, click **Remote Authentication**.
2. In the Methods section, select the **LDAP** option and click **Continue**.

   Note: Clicking the back button in your browser during this procedure could result in lost changes.
3. On the LDAP Settings page, complete the following server information fields:
   a) Type the hostname or IP address of the LDAP server in the Hostname field. Make sure that the DNS entry of the ExtraHop appliance is properly configured if you type a hostname.
   b) Type the port number on which the LDAP server is listening in the Port field. Port 389 is the standard cleartext LDAP server port. Port 636 is the standard port for secure LDAP (ldaps/tls ldap).
   c) Select the type of LDPA server from the Server Type drop-down list. Select **Posix** or **Active Direcrory**.
   d) Type the bind DN in the Bind DN field. 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.

Note: The standard login attribute for POSIX systems is `uid`. The standard login attribute for Active Directory systems is `sAMAccountName`.

e) Type the bind password in the Bind Password field. 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 setting 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) Select on of the following encryption options from the Encryption drop-down list.

- **None**. This options specifies the use of cleartext TCP sockets, typically port 389.

  Warning: All passwords are sent across the network in cleartext in this mode.

- **LDAPS**. This option specifies LDAP wrapped inside SSL, typically on port 636.
- **StartTLS**. This option specifies the use of TLS LDAP, typically on port 389. (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 certificate chains specified by the trusted certificates manager. In addition, the host name specified in the certificate presented by the LDAP server must match the host name specified in your LDAP configuration or validation will fail. 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.

4. 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.

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

- **Whole subtree**. This option looks recursively under the base DN for matching users. For example, with a Base DN value of `dc=example,dc=com`, the search would find the user `uid=jdoe,dc=example,dc=com` and `uid=jsmith,ou=seattle,dc=example,dc=com`.
- **Single level**. This option looks for users that exist in the base DN; not any subtrees. For example, with a Base DN value of `dc=example,dc=com`, the search would find a user `uid=jdoe,dc=example,dc=com`, but would not find `uid=jsmith,ou=seattle,dc=example,dc=com`.

5. 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.

c) Select one of the following options from the Search Scope drop-down list. 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.

6. 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.
7. Click **Save and Continue**.

Next steps
Continue to the Configure remote user permissions section.

Configure remote user permissions
Determine whether you want to allow local or remote authentication.

For information about user permissions, see the User privileges section.

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

     If you want to obtain a permissions level from a remote server, select the **Obtain permissions level from remote server** option and complete at least one of the following fields to specify the remote permissions:

     - Full access DN
     - Read-write DN
     - Limited DN
     - Personal DN
     - Node connection privileges DN

       Note: This field is visible only on the Command appliance.

     - Read-only DN
     - Read-limited DN
     - Packet access full DN

     These fields must be groups (not organizational units) that are pre-specified on the 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 that is a member of a group specified above will not have access. If the groups are not present, they will not be authenticated on the ExtraHop appliance.

     The ExtraHop appliance supports the following types of group membership:

     - Active Directory: `memberOf`
     - Posix: `posixGroups`, `groupofNames`, and `groupofuniqueNames`

   - **Remote users have full write access**

     This option allows remote users to have full write access to the ExtraHop Web UI. To allow remote users to view and download packet captures, select the Remote users can view and download packets checkbox.

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

     This option allows remote users to have read-only privileges to the ExtraHop Web UI. To allow remote users to view and download packet captures, select the Remote users can view and download packets checkbox.

     Note: You can add read-write permissions on a per-user basis later through the Users page in the Admin UI.

2. Click **Save and Finish**.
3. Click **Done**.

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.

Configure RADIUS authentication

1. In the Access Settings section, click **Remote Authentication**.
2. Select **RADIUS** from the Remote authentication method drop-down, then click **Continue**.
3. 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 the ExtraHop appliance waits for a response from the RADIUS server before attempting the connection again.
4. Click **Add Server**.
5. (Optional) Add additional servers as needed.
6. Click **Continue**.
7. By default, remote users have full write access. If you wish to grant all remote users read-only privileges by default, select **Remote users have Read Only access**.
8. (Optional) To allow remote users to view and download packet captures, select the Remote users can view and download packets checkbox.
9. Click **Save and Finish**.
10. Click **Done**.

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.

Configure TACACS+ authentication

1. In the Access Settings section, click **Remote Authentication**.
2. In the Methods section, select **TACACS+** from the Remote authentication method drop-down, then click **Continue**.
3. 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 the ExtraHop appliance waits for a response from the TACACS+ server before attempting to connect again.
4. Click **Add Server**.
5. (Optional) Add additional servers as needed.
6. Click **Save and Finish**.

7. Choose one of the following options from the Permission assignment options drop-down list:
   - **Obtain permissions level from remote server**

     This option allows remote users to obtain permission levels from the remote server.

     Note that you must also configure the TACACS+ server. Set up the ExtraHop service by adding the attribute `service = extrahop` and setting one of the following permission levels:

     - `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
     - `packetsfull = 1`, which allows the user to view and download packets for any of the above user permission levels

     For example:

     ```
     user = dave {
       ...
       service = extrahop {
       readonly = 1
       }
     }
     ```

   - **Remote users have full write access**

     This option allows remote users to have full write access to the ExtraHop Web UI.
   - **Remote users have 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.
8. (Optional) To allow remote users to view and download packet captures, select the Remote users can view and download packets checkbox.
9. Click **Save and Finish**.
10. Click **Done**.

API access

The API Access page provides controls to generate, view, and manage access for the API keys that are required to perform operations through the ExtraHop REST API. This page also provides a link to the REST API Explorer tool.

Administrators, or users with full system privileges, control whether users can generate API keys. For example, you can prevent remote users from generating keys or you can disable API key generation entirely. When this functionality is enabled, API keys are generated by users, listed in the Keys section, and can be viewed only by the user who generated the key.

You must generate an API key before you can perform operations through the ExtraHop REST API. API keys can be viewed only by the user who generated the key. After you generate an API key, you must append the key to your request headers.

Note: Administrators set up user accounts, and then users generate their own API key. Users can delete API keys for their own account, and users with full system privileges can delete API keys for any user. For more information, see the Users section.

Click the **REST API Explorer** link to open a web-based tool that enables you to try API calls directly on your ExtraHop appliance. The ExtraHop REST API Explorer tool also provides information about each resource and samples in cURL, Python 2.7, and Ruby.

See the ExtraHop REST API Guide for more information.

Manage API access

You can manage which users are able to generate API keys on the ExtraHop appliance.

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**.

Next steps
Save the changes to the running config file.

Enable CORS for the ExtraHop REST API

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 full system privileges can view and edit CORS settings.

Add an allowed origin

You can configure one or more allowed origins or you can allow access to the ExtraHop REST API from any origin.

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**.

Delete an allowed origin

You can delete a URL from the list of allowed origins or disable access from all origins.

1. In the Access Settings section, click **API Access**.
2. In the CORS Settings section, modify one of the following access configurations.
   - To delete a specific URL, click the delete (X) icon next to the origin you want to delete.

- To disable access from any URL, clear the **Allow API requests from any Origin** checkbox.

3. Click **Save Settings**.

Generate an API key

After you log into the ExtraHop appliance, if API key generation is enabled, you can generate an API key.

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**.

Delete an API key

1. In the Access Settings section, click **API Access**.
2. In the Keys section, click the **X** next to the API key you want to delete.
3. Click **OK**.

API permissions

The permission level that is set for a user dictates what that user can do through the REST API.

Permission level	Actions allowed
Full system privileges	• Enable or disable API key generation for the ExtraHop appliance. • Generate an API key. • View the last four digits and description for any API key on the system. • Delete API keys for any user. • View and edit cross-origin resource sharing. • 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 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.

Permission level	Actions allowed
	• Perform metric and record queries.
View and download packets 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.

User Groups

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 **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.

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 permissions 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**.

System Configuration

The System Configuration section contains ExtraHop appliance configuration settings that can be changed through the Admin UI.

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.

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.

Capture

The Admin UI provides an interface to manage the ExtraHop appliance network capture settings. For example, by default the ExtraHop appliance is configured to discover devices by their MAC address, maintaining a one-to-one correspondence between the MAC address and the discovered device. Using the Capture Configuration settings, this method of discovery can be changed so that devices are discovered by IP address.

The network capture settings give ExtraHop appliance administrators the ability to fine-tune the network capture so that the Discover appliance discovers devices in the best and most complete method possible, based on the host networking environment.

Note: Capture settings are not configurable through the Command appliance.

The ExtraHop Admin UI includes controls to manage the following network capture settings:

Excluded Protocol Modules:

Specify protocols and associated devices that should be excluded from the network capture.

MAC Address Filters

Determine which devices are discovered by MAC address.

IP Address Filters

Determine which devices are discovered by IP address.

Port Filters

Enable TCP and UDP ports.

Pseudo Devices

Identify individual devices (that have IP addresses outside the monitored domains) that normally are shown in the capture only as the router address.

Protocol Classification

Add custom protocols to the capture and associate these custom protocols with ExtraHop module protocols.

Discover by IP

Enable or disable the discovery of devices on the network capture by IP address rather than by MAC address.

SSL Decryption

Add and manage SSL decryption keys to decrypt SSL traffic on the network.

Open Data Context API

Access the session table with the ExtraHop system acting as a memcache server.

Software Tap

Capture traffic through a high-speed packet forwarder (RPCAP).

Network Overlay Decapsulation

Enable or disable the network overlay decapsulation for NVGRE and VXLAN protocols.

Excluded protocol modules

The Excluded Protocol Modules page provides an interface to manage the protocols that you want to include in the network capture. By default, all supported modules on the ExtraHop appliance are included in the capture unless you manually exclude them.

Note: Capture settings are not configurable through the Command appliance.

Exclude protocol modules

To exclude a protocol module from the network capture:

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**.

Re-include excluded protocol modules

To re-include a previously excluded protocol module:

1. Click **System Configuration** > **Capture**.
2. Click **Excluded Protocol Modules**.
3. On the Excluded Protocol Modules page, click **Delete** next to the module name for each module you want to re-include.
4. Click **Restart Capture**.
5. After the capture restarts, click **OK**.

MAC address filters

You can use filters to exclude specific MAC addresses or vendor device traffic from the network capture on the Discover appliance.

Note: Capture settings are not configurable through the Command appliance.

Exclude MAC addresses

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`

Re-include excluded MAC addresses

1. Click **System Configuration** > **Capture**.
2. Click **MAC Address Filters**.
3. On the MAC Address Filters page, click **Delete** next to the MAC address filter for each address you want to re-include.
4. Click **OK**.

IP address filters

You can use filters to exclude specific IP addresses and IP ranges from the network capture on the ExtraHop appliance.

Note: Capture settings are not configurable through the Command appliance.

Exclude an IP address or range

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**.

Re-include an excluded IP address or range

1. Click **System Configuration** > **Capture**.
2. Click **IP Address Filters**.
3. On the IP Address Filters page, click **Delete** next to the IP address filter for each address you want to re-include.
4. Click **OK**.

Port filters

You can use filters to exclude traffic from specific ports from the network capture on the Discover appliance.

Note: Capture settings are not configurable through the Command appliance.

Exclude a port

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**.

Re-include an excluded port

1. Click **System Configuration** > **Capture**.
2. Click **Port Filters**.
3. On the Port Address Filters page, click **Delete** next to the port you want to re-include.
4. Click **OK**.

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
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	--	--

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

Note: Capture settings are not configurable through the Command appliance.

Specify a pseudo device

Note: To monitor remote locations with multiple, non-contiguous subnets, specify the pseudo device multiple times with the same dummy MAC but with different IP subnets. For example, in the figure below, all traffic relating to any of the IP subnets assigned is attributed to the pseudo device with the MAC address 22:22:00:00:00:01.

1. Click **System Configuration** > **Capture**.
2. Click **Psuedo Devices**.
3. Click **Add Device**.
4. On the Add Pseudo Devices page, enter the following information:

IP Address

The IP address range for the device in CIDR notation.

```
IP Address/subnet prefix length
```

For example, `10.10.0.0/16` for IPv4 networks or `2001:db8::/32` for IPv6 networks.

MAC

A dummy MAC address for the device.

Remove pseudo devices

1. Click **System Configuration** > **Capture**.
2. Click **Psuedo Devices**.
3. On the Pseudo Devices page, click **Delete** next to the pseudo device you want to remove from the list.
4. Click **OK**.

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.
- 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 protocols on their standard ports (one exception is HTTP, which is 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 use 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).

Canonical Name	Protocol Name	Transport	Default Source Port	Default Destination Port
ActiveMQ	ActiveMQ	TCP	0	61616
AJP	AJP	TCP	0	8009
CIFS	CIFS	TCP	0	139, 445
DB2	DB2	TCP	0	50000, 60000
Diameter	AAA	TCP	0	3868
DICOM	DICOM	TCP	0	3868
DNS	DNS	TCP	0	53
DNS	DNS	UDP	0	53

Canonical Name	Protocol Name	Transport	Default Source Port	Default Destination Port
FIX	FIX	TCP	0	0
FTP	FTP	TCP	0	21
FTP-DATA	FTP-DATA	TCP	0	20
HL7	HL7	TCP	0	2575
HL7	HL7	UDP	0	2575
IBM MQ	IBMMQ	TCP	0	1414
IBM MQ	IBMMQ	UDP	0	1414
ICA	ICA	TCP	0	1494, 2598
Informix	Informix	TCP	0	1526, 1585
iSCSI	iSCSI	TCP	0	3260
Kerberos	Kerberos	TCP	0	88
Kerberos	Kerberos	UDP	0	88
LDAP	LDAP	TCP	0	389, 390, 3268
LLDP	LLDP	Link Level	N/A	N/A
Memcache	Memcache	TCP	0	11210, 11211
MongoDB	MongoDB	TCP	0	27017
MS SQL Server	TDS	TCP	0	1433
MSMQ	TDS	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
Oracle	TNS	TCP	0	1521
PCoIP	PCoIP	UDP	0	4172
PostgreSQL	PostgreSQL	TCP	0	5432
RADIUS	AAA	TCP	0	1812, 1813
RADIUS	AAA	UDP	0	1645, 1646, 1812, 1813
Redis	Redis	TCP	0	6397
SIP	SIP	TCP	0	5060, 5061
SMPP	SMPP	TCP	0	2775
SMTP	SMTP	TCP	0	25
SSH	SSH	TCP	0	22

Canonical Name	Protocol Name	Transport	Default Source Port	Default Destination Port
SSL	SSL	TCP	0	443
Sybase	Sybase	TCP	0	10200
SybaseIQ	SybaseIQ	TCP	0	2638
Telnet	Telnet	TCP	0	23
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 using 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:

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.

Remove a custom protocol classification

1. Click **System Configuration** > **Capture**.
2. Click **Protocol Classification**.
3. On the Protocol Classification page, click **Delete** next to the protocol that you want to remove from the list.
4. Click **OK**.
5. This change has been applied to the running config. When you save the change to the running config, it will be reapplied when the ExtraHop system restarts. Click **View and Save Changes** at the top of the screen.
6. Click **Save** to write the change to the default configuration.
7. After the configuration is saved, a confirmation message appears. Click **Done**.

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.

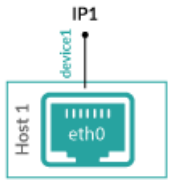
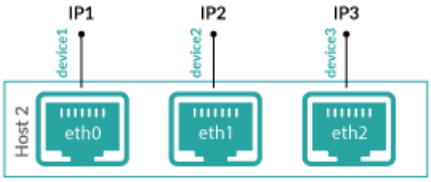
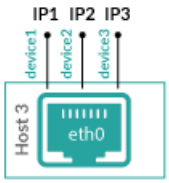
By default, Discover by IP is enabled, which means that devices are discovered when the ExtraHop system detects a response to an Address Resolution Protocol (ARP) request for an IP address. This method is also known as L3 discovery mode.

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.

Next steps

- Learn about remote discovery
- Add a remote IP address range

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 Enabled checkbox is selected by default. If the checkbox is deselected, select Enabled.
5. In the Remote Networks section, click Change.
6. In the Remote Discovery section, type the IP address in the IP address range 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.
7. 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.

Next steps

Important: The capture must be restarted when removing IP address ranges before the changes will take effect. ExtraHop recommends 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 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.

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.

- PEM certificates and RSA private keys
- PKCS#12/PFX files with passwords

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.

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.

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.

To export a password-protected key, run a program such as OpenSSL:

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

The Add Encrypted Protocol section specifies the protocols that handle decrypted SSL traffic. For example, for DNS traffic, you must create an entry for the DNS protocol on port 53. Port 0 represents any port.

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.

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

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

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**.

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**.

Open data context API

The Open Data Context API allows external access to the global session table. Clients can store and retrieve key-value pairs using the memcache protocol.

For example, a script running on an external host inserts CPU load information into the ExtraHop session table. Triggers commit this information and other HTTP transactions as custom metrics. The script running on the external host can use any memcache client, and then use memcache commands, such as `GET`, `SET`, and `INCREMENT`, to communicate with the ExtraHop appliance.

When using the Open Data Context API, remember the following:

- Committing large values to the session table causes performance degradation. Values can be almost unlimited in size. However, metrics committed to the datastore must be 4096 bytes or fewer.
- All data must be inserted as strings to be readable by the ExtraHop appliance.
- Keys expire at 30-second intervals. For example, if a key is set to expire in 50 seconds, it might take anywhere from 50 to 79 seconds to expire.
- All keys set in the Open Data Context API are exposed via the `SESSION_EXPIRE` trigger event as they expire. This behavior is in contrast to the Application Inspection Triggers API, where the default behavior is not to expose expiring keys via `SESSION_EXPIRE`.

Note: This connection is not encrypted and should not be used to exchange sensitive information.

Enable the open data context API

1. Click **System Configuration** > **Capture**.
2. Click **Open Data Context API**.
3. On the Open Data Context API page, enter the following information:

Enable Open Data Context API

Check this checkbox to enable the Open Data Context API.

TCP Port Enabled

Check this checkbox to enable the TCP port for Open Data Context.

TCP Port

The port number of the enabled TCP port. By default, this is set to 11211.

UDP Port Enabled

Check this checkbox to enable the UDP port for Open Data Context.

UDP Port

The port number of the enabled UDP port. By default, this is set to 11211.

4. Click **Save and Restart Capture**.
5. Click **OK**.

Note: Enabling the Open Data Context API opens TCP/UDP port 11211 by default, so ensure that the firewall rules allow access to these ports from any external host that will use the API.

Supported memcache client libraries

You can use any standard memcache client library with the Open Data Context API. The ExtraHop appliance acts as a memcache version 1.4 server.

All memcache commands are supported, but the following actions are not supported:

- Flush. Setting item expiration when adding or updating items is supported, but bulk expiration is not.
- Detailed statistics by item size or key prefix. Basic statistics reporting is supported.

Insert data as a string

Some memcache 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 using `Session.lookup` in triggers.

Incorrect

```
// python:
>>> mc.set("my_float", 1.5)
```

```
// triggers:
Session.lookup("my_float") // returns "F1.5\n."
```

Correct

```
// python:
>>> mc.set("my_float", str(1.5))
```

```
// triggers:
Session.lookup("my_float") // returns "1.5"
```

Change the session table size

The default session table size is 32768 entries. You can modify the running config to change the session table size, but increasing the session table size might impact memory consumption on the system and cause other issues. You must restart the capture to see these changes.

To change the session table size, add the following line to the "capture" section of the running config:

```
"jssession_table_size": 32768
```

For more information, see the Running Config section or contact ExtraHop Support.

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.

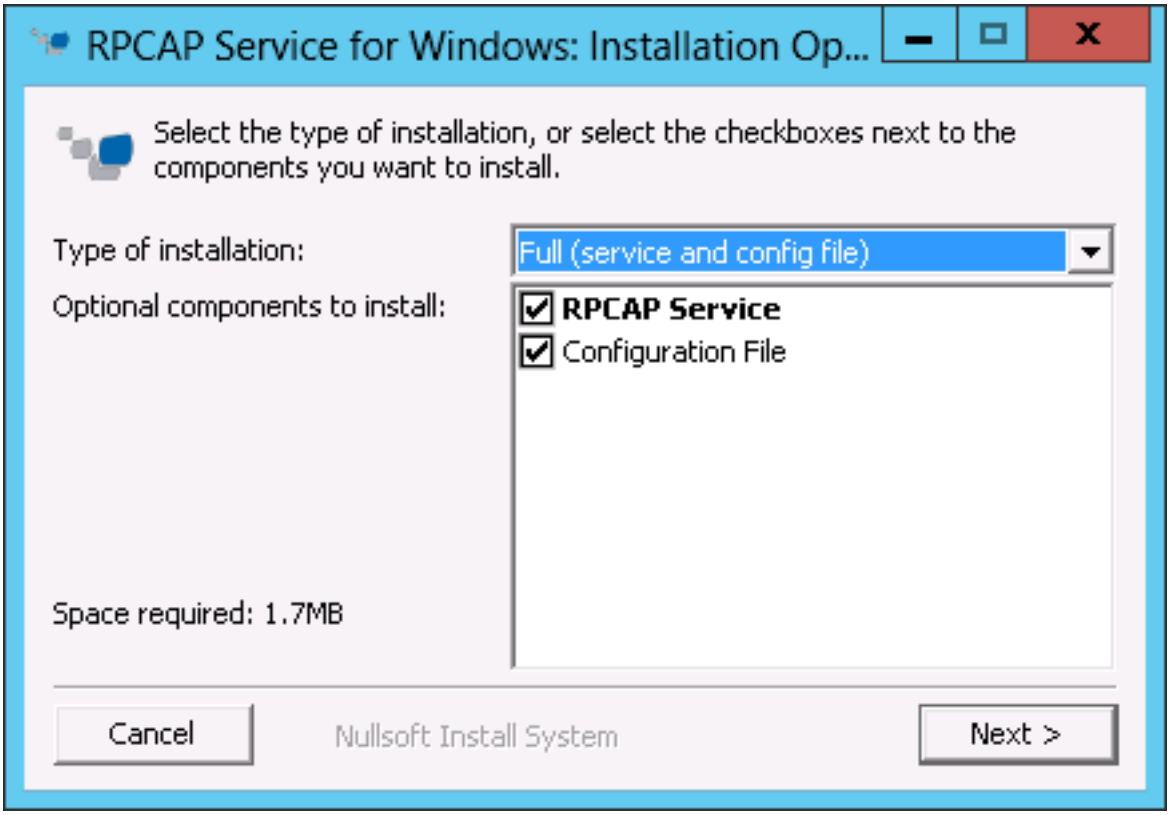
   ```
   sudo dpkg-reconfigure rpcapd
   ```

Install the software tap on a Windows server

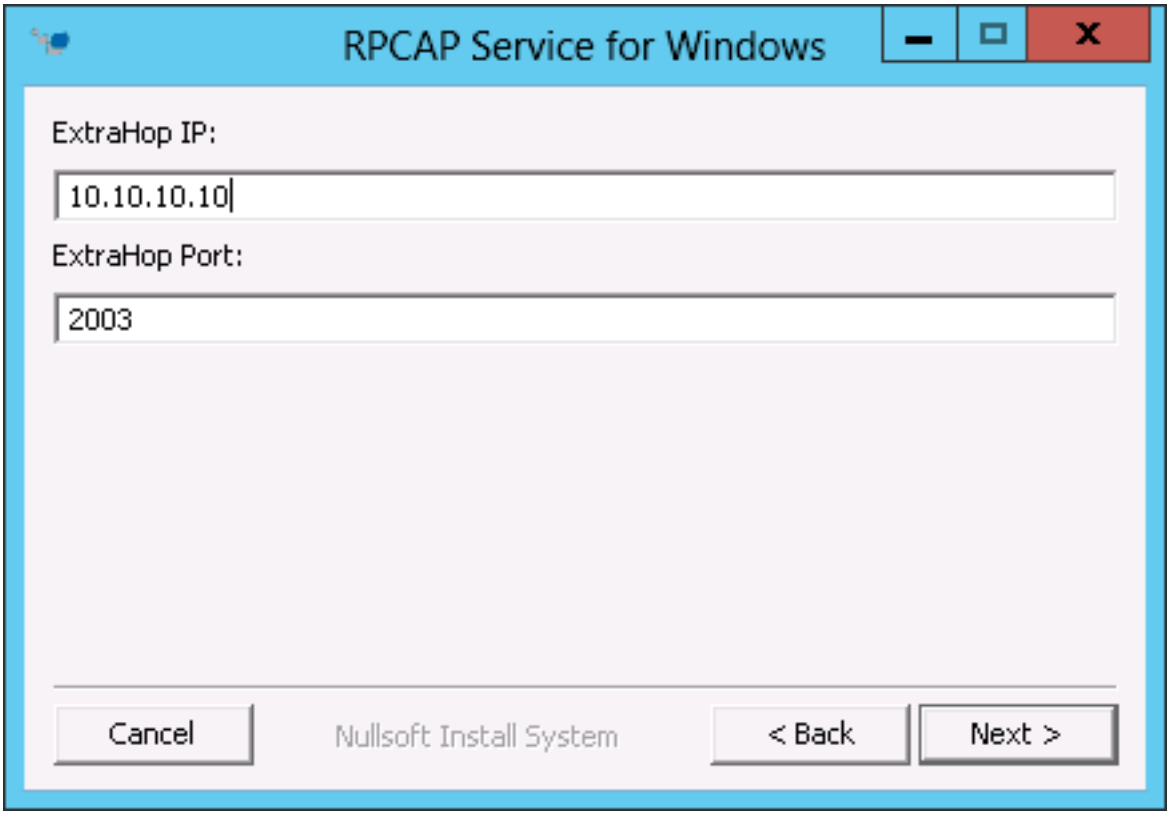
You must install the software tap on each server to be monitored in order to forward packets to the ExtraHop system.

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.

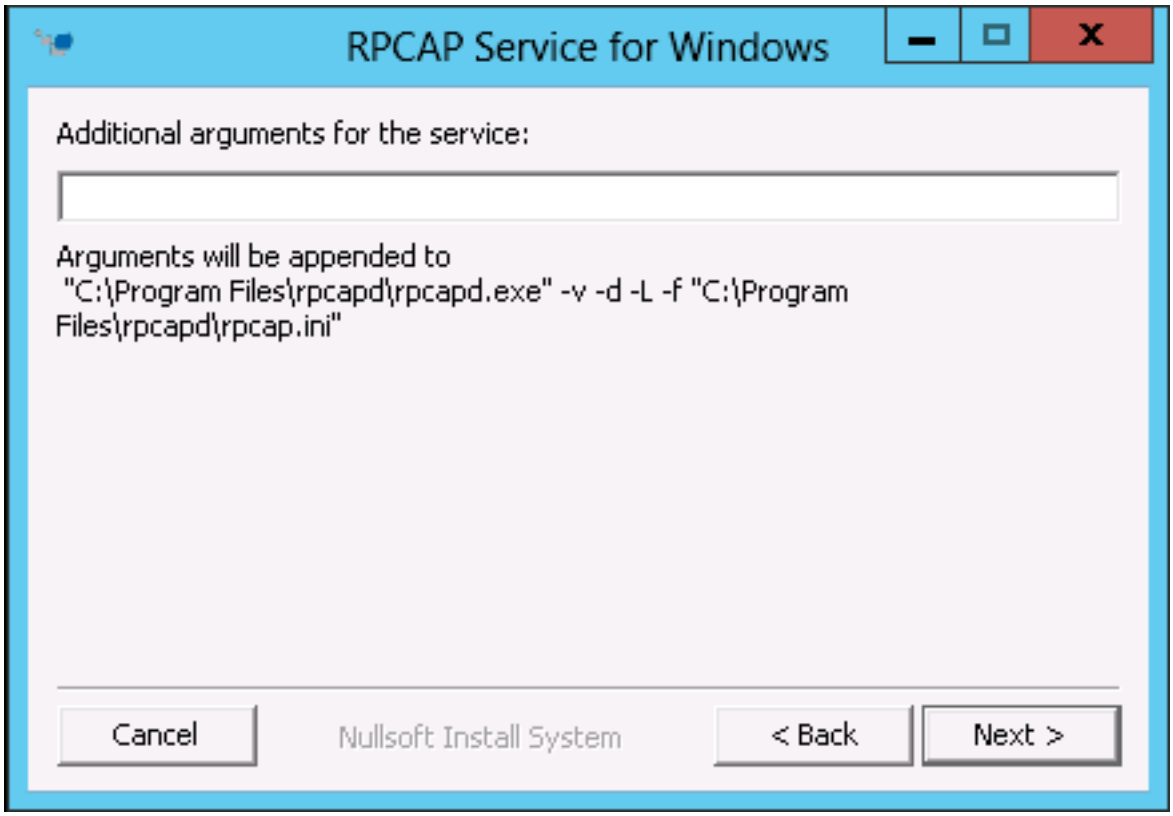
3. In the wizard, select the components to install.



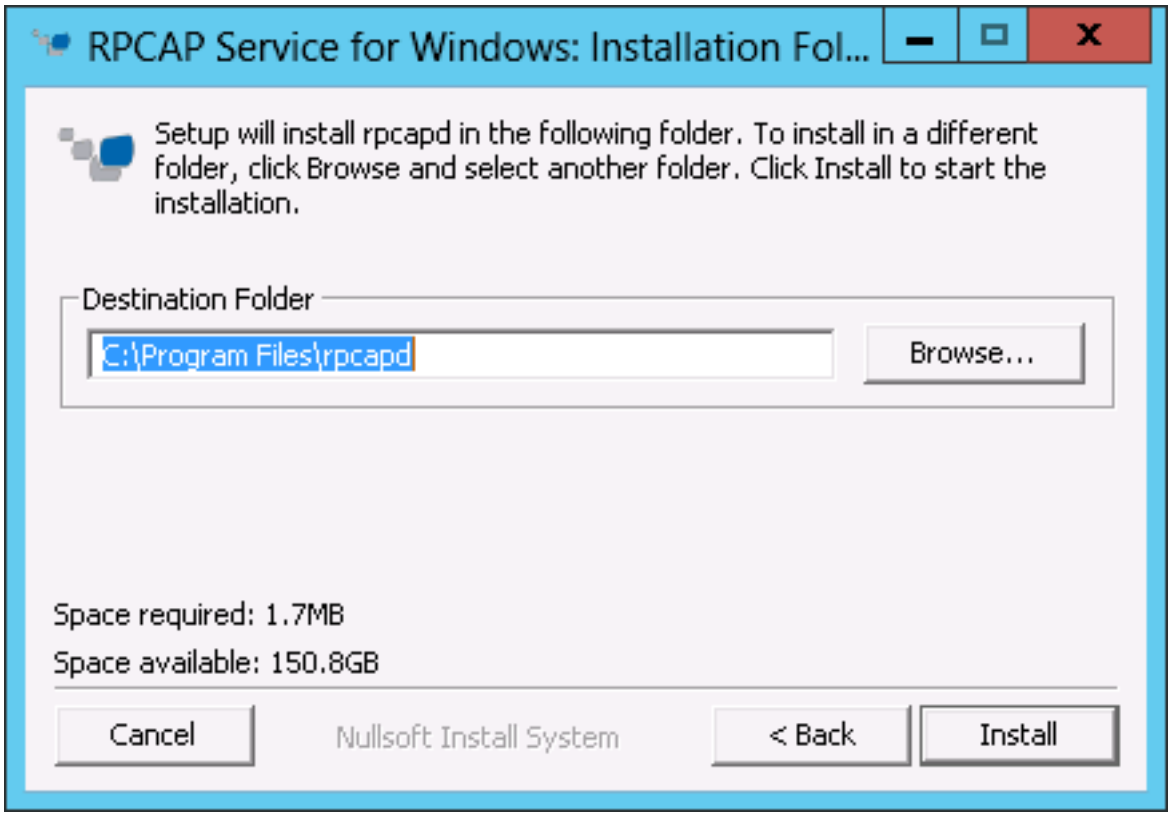
4. Complete the **ExtraHop IP** and **ExtraHop Port** fields and click **Next**. The default port is 2003.



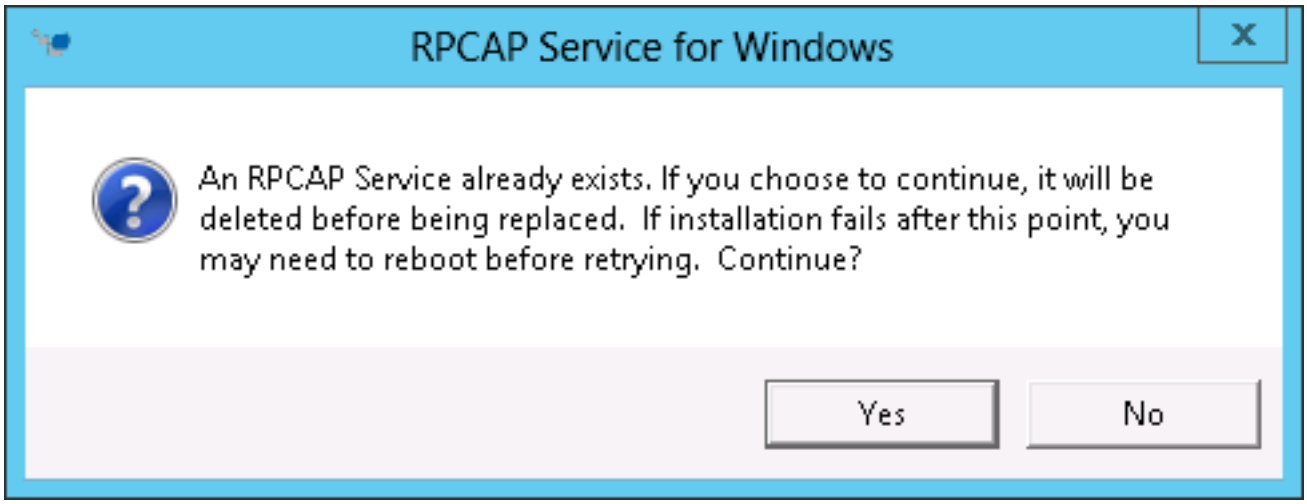
5. (Optional) Enter additional arguments in the text box and click **Next**.



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
```

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 cause you to exceed your licensed device limits 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. Click **System Configuration** > **Capture**.
2. Click **Network Overlay Decapsulation**.
3. In the Settings section, select the **Enabled** checkbox next to **NVGRE**.
4. Click **Save**.

Enable VXLAN decapsulation

VXLAN is a UDP tunneling protocol is 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. Click **System Configuration** > **Capture**.

2. Click **Network Overlay Decapsulation**.
3. In the Settings section, select the **Enabled** checkbox next to **VXLAN**.
4. In the **VXLAN UDP Destination Port** text box, 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.
5. Click **Save**.

Offline capture file

By default, the ExtraHop appliance is configured to obtain network data in Live Network Traffic (Online) Capture mode. You can turn off this setting if you want to capture data using an uploaded capture file.

The Offline Capture mode in the Discover appliance enables an ExtraHop administrator to upload a capture file (recorded by packet sniffers, such as Wireshark or tcpdump) to the ExtraHop datastore for analysis. When the system is set to Offline mode, the offline file upload feature is enabled, allowing a capture file to be uploaded to the datastore. In Offline mode, no metrics are collected from the capture interface until the system is set to online mode again.

When the capture is set to Offline mode, the ExtraHop datastore is reset. All previously recorded performance metrics are deleted from the datastore. When the system is set to online mode, the datastore is reset again.

Note: Offline Capture mode is not configurable when using the Command appliance.

Set the offline capture mode

1. Click **Diagnostics** > **Offline Capture File**.
2. Click the **Offline - Upload Capture File** radio button to turn on the setting to set the capture mode to offline.

   The capture process is stopped, the capture state is set to offline, and the datastore is cleared of all data.
3. Click **Save** to activate the new setting.

   When the system has set the capture to offline mode, the Upload a Capture File page is displayed.
4. To upload a capture file:
   a) Click **Choose File**, browse to the capture file that you want to upload, select the file and click **Open**.
   b) On the Offline Capture page, click **Upload**.

      The Discover appliance displays the Offline Capture Results page when the capture file uploads successfully.

To verify that the system is in offline mode, access the Health page in the Admin UI to see the `Capture Status` values. Each metric should have a value of `offline`. When you check the capture status, the status shown for VM RSS, VM Data, VM Size, and Start Time should indicate that the system is in offline mode.

For more information about the Health page, see the Health section.

Reset the online capture mode

The Capture mode settings in the Admin UI are also used to return the Discover appliance to online capture mode. When you choose to restart the ExtraHop online capture, the data loaded into the datastore from the offline capture file is deleted as soon as you save the online capture setting.

1. Click **Diagnostics** > **Offline Capture File**.
2. Click the **Online - Live Traffic** radio button.
3. Click **Save**.
4. At the prompt to restart the excap, click **OK**.

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 and customizations

The Discover appliance includes a self-contained, streaming datastore for recording and retrieving performance and health metrics in real time. The datastore bypasses the OS file system and accesses the underlying block devices directly, rather than using a conventional relational database.

The ExtraHop Admin UI includes the following datastore configuration settings:

Local Datastore Settings

Remove all devices and device metrics from the datastore.

Extended Datastore Settings

Configure an external NFS or CIFS mount for long term storage of 5-minute, 1-hour, and 24-hour metrics.

Customizations

View, save, upload, and restore customizations. Datastore configurations settings from one Discover appliance can be uploaded to another Discover appliance in multiple-appliance deployment for consistency. The Discover appliance stores the last three user-saved datastore configurations.

Resetting the local datastore

ExtraHop appliances maintain records for all devices discovered by the appliance on a local datastore. ExtraHop appliances also store device metrics in the local datastore to provide quick access to the latest network capture as well as historic and trend-based information about selected devices.

In certain circumstances, such as moving the ExtraHop appliance from one network to another, you might need to clear the metrics in the datastore. Resetting the datastore removes all metrics, baselines, trend analyses, and discovered devices. Alerts that have been configured are retained, but they must be reapplied to the correct network, device, or device group. System settings and user accounts are unaffected.

Before you reset the datastore, you might want to save your device and network customizations. Saved customizations are applied only to devices that have been discovered by the ExtraHop appliance, which typically takes a few minutes after resetting the datastore. For more information about saving customizations, see the Saving running config changes section.

Reset the datastore through the Admin UI

Warning: Resetting the ExtraHop datastore deletes device IDs and device metrics from the ExtraHop appliance. Do not perform this operation unless you want to erase all device information from the ExtraHop appliance.

1. Under System Configuration, click **Datastore and Customizations**.
2. Click **Reset Datastore**.
3. (Optional) 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 discard the current customizations after the datastore is reset, clear the **Save Customizations** checkbox and then type YES in the confirmation text box.
4. Click **Reset Datastore**.
5. Wait approximately one minute.
   When the datastore reset is complete, the browser will prompt you to restore customizations.

6. If you chose to restore customizations, the browser redirects to a detailed list of imported customizations.
7. Click **OK**.
8. Go to the Web UI to view the devices that were discovered after the datastore reset. Wait approximately one minute for the system to discover and display new devices.

Reset the datastore through the CLI

Warning: Resetting the ExtraHop datastore deletes device IDs and device metrics from the ExtraHop appliance. Do not perform this operation unless you want to erase all device information from the ExtraHop appliance.

1. Access the ExtraHop CLI using one of the following three methods:
   - From a USB keyboard and SVGA monitor directly connected to the ExtraHop appliance.
   - Using an RS-232 serial cable and a terminal-emulator program. The terminal emulator must be set to 115200 bps with 8 data bits, no parity, and 1 stop bit (8N1). Hardware flow control must be disabled.
   - Secure shell (SSH).
2. Connect to the ExtraHop appliance.

   The login is `shell` and the password is the service tag number on the pullout tab on the front panel of the ExtraHop appliance.
3. Enable the administration controls.

   The password is the service tag number on the rightfront bracket of the ExtraHop appliance.

   ```
   extrahop>enable
   ```
4. Reset the datastore.

   ```
   extrahop#reset datastore
   ```
5. Go to the Web UI to view the devices that were discovered after the datastore reset. Wait approximately one minute for the system to discover and display new devices.

Extended datastore

The ExtraHop appliance enables you to write and store metrics on an external storage device.

By default, ExtraHop appliances store fast (30-second), medium (5-minute), and slow (1-hour) metrics locally. However, you can also store 5-minute, 1-hour, and 24-hour metrics on an extended datastore.

To store metrics externally, you must mount an external datastore, and then configure the appliance to store data in the mounted directory. You can mount an external datastore through NFS v4 (with optional Kerberos authentication), and CIFS (with optional authentication).

You can configure only one active datastore at a time. The datastore contains all metric cycles that you collect. For example, if you configure your extended datastore to collect 1-hour, 5-minute, and 24-hour metrics, all three metrics are stored in the same datastore.

Extended datastore considerations

Before configuring an external datastore, note the following conditions:

- Only one ExtraHop appliance can write to an active extended datastore at a time. However, multiple appliances can read from an archived extended datastore simultaneously.
- If an extended datastore contains multiple files with overlapping time stamps, metrics will be incorrect.
- An ExtraHop appliance cannot read metrics committed to the extended datastore by a later ExtraHop appliance firmware version.
- If an extended datastore becomes unreachable, an ExtraHop appliance buffers metrics until the allocated memory is full. Once 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.
- Modifying datastore settings requires administrative access to the ExtraHop appliance.
- You can modify datastore settings only on licensed appliances.

Extended datastore performance guidelines

If you configure an extended datastore for an ExtraHop appliance, the device hosting the datastore must be able to support the processing requirements of the appliance. If the device is too slow to write all data sent from the appliance, system performance might be degraded.

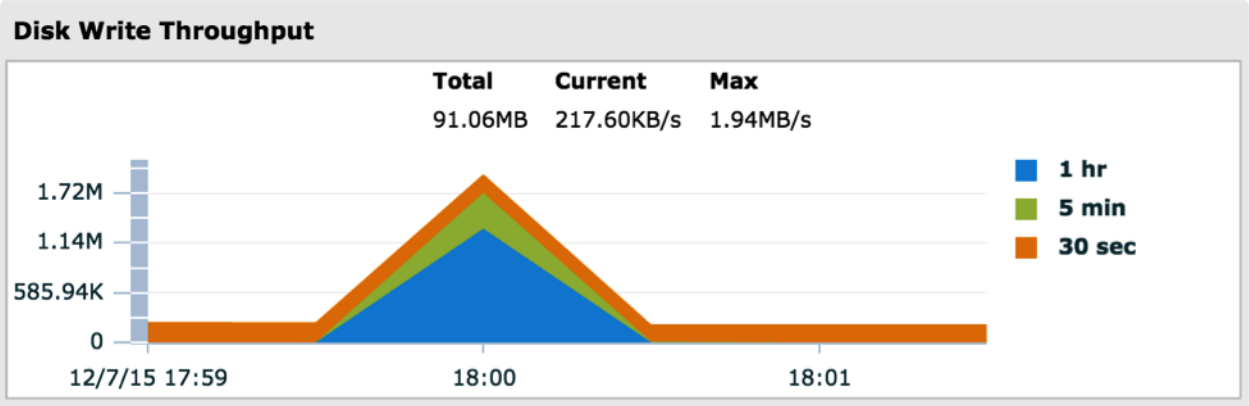
The following procedure shows you how to determine the write performance that will be required from the NAS device hosting the extended data store.

This procedure does not provide an estimate of the read performance required from the NAS device while users are accessing data on the datastore. Those needs vary based on how many users typically access the datastore at once and whether users are accessing newly written or archived data. However, we recommend that you minimize network latency between the external datastore and the Discover appliance; for example, you can place the extended datastore in the same data center as the appliance.

1. On an ExtraHop Discover or Command appliance, click the Settings icon.
2. Click **System Health**.
3. Scroll down to the Datastore section.
4. In the Disk Write Throughput chart, zoom in on a peak of blue and green.

   To zoom in on a time window, click and drag over the chart area.
5. Record the highest point of blue and green along with the amount of time it takes for activity to return to the baseline value.

   For example, in the following chart, the blue and green area peaks at 1.72 MB/sec and has returned to normal after 30 seconds:



6. The datastore must be able to write data at the highest rate for the amount of time it took for activity to return to normal.

   For example, in the previous example, the datastore would need to be able to write 1.7 MB/sec for 30 seconds.

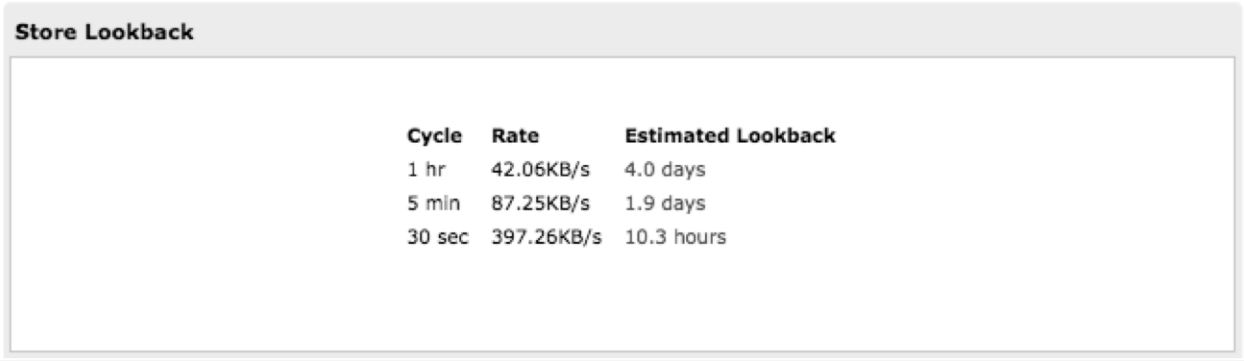
Extended datastore sizing guidelines

Before you store metric data in an external datastore, you must make sure that the datastore has enough space to contain the amount of data generated by the appliance. The following procedure explains how you can calculate approximately how much free space you need for the datastore.

1. On an ExtraHop Discover or Command appliance, click the Settings icon.
2. Click **System Health**.
3. Scroll down to the Datastore section.
4. From the Store Lookback chart, record the `Rate` and `Estimated Lookback` for each cycle (or time period) that you want to store on the external datastore.
5. Calculate the amount of required space by applying the following formula:

```
<rate> x <lookback_time>
```

For example, consider the following chart:



The following sequence shows how you can calculate the amount of space needed from the information in the chart:

```
87.25KB/sec * 1.9days
87.25KB/sec * 60sec * 60min * 24hr * 1.9days
14322960 KB
14 GB
```

To store all of the 5 minute metrics from this appliance, you need 14 GB of free space.

Adding mounts

Before you can store data on an external datastore, you must mount the share you want to store data in.

Add a CIFS mount

1. In the System Configuration section, click **Datastore and Customizations**.
2. Under Extended Datastore Settings, 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, enter the following information:
   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**.

Configure Kerberos authentication settings (NFS only)

Configure any applicable Kerberos authentication before you add an NFS mount.

1. Under System Configuration, click **Datastore and Customizations**.
2. Under Extended Datastore Settings, click **Configure Extended Datastore**.
3. Click **Add Kerberos Config**.
4. Enter the following information:

   Admin Server

   The IP address or hostname of the master Kerberos server that issues tickets.

   Key Distribution Center (KDC)

   The IP address or hostname of the server that holds the keys. (This server can be the same as the admin server.)

   Realm

   The name of the Kerberos realm for your configuration.

   Domain

   The name of the Kerberos domain for your configuration.
5. In the Keytab File section, click **Choose File**, select a saved keytab file, and then click **Open**.
6. Click **Upload**.

Add an NFS mount

Before you begin

Perform the following steps before configuring an NFS mount:

- Configure any applicable Kerberos authentication before you add an NFS mount. For more information, see Configure Kerberos authentication settings.
- Either allow read/write access for all users on the share or set assign the 'extrahop' user as the owner of the share and allow read/write access for the current user.

1. Under System Configuration, click **Datastore and Customizations**.
2. Under Extended Datastore Settings, click **Configure Extended Datastore**.
3. Click **Add NFSv4 Mount**.
4. On the Configure NFSv4 Mount page, enter the following information:

   Mount Name

   A name for the mount; for example, `EXDS`.

   Remote Share Point

   The path for the mount in the following format:

   ```
   host:/mountpoint
   ```

   For example, `herring:/mnt/extended-datastore`.
5. From the **Authentication** drop-down, select an authentication type:

   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**.

Create an active extended datastore

You can create an active extended datastore for a Discover appliance to store metrics on.

Before you begin

Before you can connect an active extended datastore, you must mount the share that contains the datastore.

1. Under System Configuration, click **Datastore and Customizations**.
2. Under Extended Datastore Settings, click **Configure Extended Datastore**.
3. On the Configure Extended Datastore page, click the name of the mount you want to create the extended datastore on.
4. In the Datastore Directory field, type a name for the datastore directory.

   The directory will be automatically created by the Discover appliance.
5. In the Datastore Size field, specify the maximum amount of data that can be stored on the datastore.
6. (Optional) To store 5-minute and 1-hour metrics on the extended datastore as well, select the **Include 5-minute and 1-hour metrics** checkbox.

   24-hour metrics are stored on the extended datastore regardless of whether you select this option.
7. (Optional) Specify whether to migrate existing metrics to the extended datastore.

   If you selected to store 5-minute and 1-hour metrics on the extended datastore, selecting this option will cause the appliance to migrate any 5-metrics and 1-hour metrics that the appliance had already collected from the local Discover appliance datastore to the extended datastore. Migrating 5-minute and 1-hour metrics to an extended datastore will leave more room to store 30-second metrics on the local datastore, which will increase the amount of high-resolution lookback available.

   Warning: While data is being migrated, the Discover appliance will not collect data and system performance will be degraded. The migration process will take 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

   - 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**.
8. Select the **Move existing** radio button.
9. Select whether to overwrite older data when the datastore becomes full.

   - 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**.
10. Click **Configure**.
    After the storage is added, the Status reads `Nominal`.

Monitoring storage space

When the datastore is almost full, a warning appears at the top of the Systems Settings page.

You can configure the system to send email messages based on the level of severity when the datastore space becomes limited. For more information, see the Notifications section.

Status messages
The `Status` row for each mount and external datastore displays status information about each device or connection.

Mounts

Status	Description	User Action
Mounted	The mount configuration was successful.	None required
NOT MOUNTED	The mount configuration was unsuccessful.	• Verify that the mount configuration information for accuracy and correct spelling. • Verify that the remote system is available. • Verify that the server is a supported type and version. • Verify credentials, if using authentication.
NOT READABLE	The mount has permissions or network-related issues that prevent reading.	• Verify that the correct permissions are set on the share. • Verify the network connection and availability.
NO SPACE AVAILABLE	The mount has no space remaining.	Detach the mount and create a new one.
INSUFFICIENT SPACE	• First appearance: The system anticipates that not enough space is available. • Second appearance: Less than 128MB of space is available.	Detach the mount and create a new one.
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.

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

Status	Description	User Action
		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.

Create an archive datastore
You can change an active datastore into an archive datastore by disconnecting an active datastore from a Discover appliance. Once you have disconnected an active datastore, the datastore becomes read-only, and you can connect any number of Discover appliances to the datastore. Disconnecting from an active datastore does not delete any of the data stored on the datastore.

1. Click **System Configuration** > **Datastore and Customizations**.
2. Click **Extended Datastore Settings** > **Configure Extended Datastore**.
3. On the Configure Extended Datastore page, click the name of the mount that contains the datastore you want to disconnect from.
4. In the row of the datastore you want to disconnect from, click **Disconnect Extended Datastare**.
5. Type YES to confirm and then click **OK**.

The datastore is disconnected from the appliance and the datastore is marked read-only.

Next steps
You can now connect to the datastore as an archive datastore. For more information, see Connect to an archive datastore.

Connect to an archive datastore
After you disconnect from an active extended datastore, you can connect to that datastore as an archive datastore. Archive datastores are read-only and can be accessed by multiple Discover appliances simultaneously.

Before you begin
To create an archive datastore, you must create an active extended datastore, collect data, and then disconnect from the active datastore.

Warning: To connect to an archive datastore, a Discover appliance must scan through the data contained in the datastore. Depending on the amount of data stored in the archive datastore, connecting to the archive datastore might take a long time. While the appliance is connecting to the archive datastore, the appliance will not collect data and system performance will be degraded. The connection process will take 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. Under System Configuration, click **Datastore and Customizations**.
2. Under Extended Datastore Settings, click **Configure Extended Datastore**.
3. On the Configure Extended Datastore page, click the name of the mount that contains the archive datastore.
4. In the Datastore Directory field, type the path of the archive datastore directory.

5. Click **Archive (Read Only)**.
6. Click **Configure**.

Upgrade your system
After you mount an NFS or CIFS share, you can update your ExtraHop appliance and import your existing metrics to that new ExtraHop appliance. To upgrade to a new ExtraHop appliance:

Note: If you are migrating 5-minute and 1-hour metrics from one ExtraHop appliance to another, you must perform a system reset on the target ExtraHop system. The internal datastore on the target ExtraHop system must be empty before data is imported from the external datastore.

1. On the old ExtraHop appliance (ExtraHop A), write the metrics to an external store using the previous procedure, **Add Storage Space**.
2. On ExtraHop A:
   a) Click **System Configuration** > **Datastores and Customizations**.
   b) Click **Extended Datastore Settings** > **Configure Extended Datastore**.
   c) Click **Disconnect Extended Datastore**.
   d) Type YES in the confirmation text box and click **OK**.
3. On the new ExtraHop appliance (ExtraHop B):
   a) Click **Configuration** > **Datastore and Customizations**.
   b) Click **Extended Datastore Settings** > **Import Metrics from External Datastore**.
   c) Click the name of the datastore directory that you configured for ExtraHop A, then click **Import Metrics**.
   d) Type YES in the confirmation text box and click **OK**.

Customizations

Extended datastore settings are saved in .json files. Datastore settings are automatically saved daily, but you can also save the current datastore setttings at any time.

You can download the .json files to save them locally or upload them to another appliance. You can apply the settings specified in a .json save file to undo saved changes or copy settings from one appliance to another.

Custom metrics that are auto-discovered are only saved in the customizations file if they meet one of the following conditions:

- The metric is referenced by a dashboard
- The custom metric has been edited in the Metric Catalog

View saved customizations

1. In the System Configuration section, click **Datastore and Customizations**.
2. In the Customizations section, click **Manage Customizations**.
3. In the Saved Customizations and Automatically Saved Customizations tables, view customizations.

Download datastore customizations
You can download the current datastore configuration settings into a .json archive file that can be stored on your workstation. This archive file can be used to restore the datastore settings on the originating ExtraHop appliance, if problems occur. In addition, these settings can be uploaded to specify the datastore configuration settings in a new ExtraHop appliance.

To download the ExtraHop datastore customization settings to an external file:

1. In the System Configuration section, click **Datastore and Customizations**.
2. In the Customizations section, click **Manage Customizations**.
3. Click on the name of the saved customization that you want to download.

The file is download to your browser's default download location.

Restore datastore customizations
Datastore configuration settings can be saved and, if necessary, saved settings can be used to restore the datastore to the last saved state.

Note: Restoring customizations does not create new devices; it associates the customized names to the devices found by the ExtraHop appliance. If a device has not been found, then the customized name is not restored. You can select **Restore Customizations** again to restore those same customizations. Restoring customizations does not overwrite any new customizations, but it overwrites any modified customized values.

1. In the System Configuration section, click **Datastore and Customizations**.
2. In the Customizations section, click **Manage Customizations**.
3. In either the **Saved Customizations** or the **Automatically Saved Customizations** table, click **Restore** next to the customization you want to restore.
4. Click **OK** to restore the datastore.
5. Click **OK** again.

Save the current datastore customizations
The ExtraHop appliance lets you save the current datastore configuration settings and store them in memory. These saved configuration settings can be used at a later date to restore the datastore to the saved state.e

1. In the System Configuration section, click **Datastore and Customizations**.
2. In the Customizations section, click **Save Customizations**.
3. Click **OK**.

Upload and restore datastore customizations
ExtraHop appliance datastore configuration can be exported and saved as a .json archive file. The datastore customization file can be uploaded to the ExtraHop appliance to restore customization settings on the original system or install datastore customization settings on a new ExtraHop appliance.

Note: Restoring customizations does not create new devices; it associates the customized names to the devices found by the ExtraHop appliance. If a device has not yet been found, then the customized name is not restored. Restoring customizations does not overwrite any new customizations, but it overwrites any modified customized values.

1. Click **System Configuration** > **Datastore and Customizations**.
2. Click **Customizations** > **Upload and Restore Customizations**.
3. On the Upload and Restore Customizations page, click **Choose File**, navigate to the datastore customization file that you want to upload and click **Open**.
4. Click **Restore**.
5. When the file is finished uploading, click **OK**.

Geomap data source

This section enables you to download specific settings related to geomaps.

GeoIP Database

Upload a user-specified database.

IP Location Override

Override missing or incorrect IPs in the database.

GeoIP database

The GeoIP Database specifies the current database being used by the ExtraHop appliance and enables you to choose between a default or user-uploaded database.

Change the GeoIP database

1. Click **System Configuration** > **Geomap Data Source**.
2. Click **GeoIP Database**.
3. In the Change Source section, select the **Upload New Database** radio button, then click **Choose File** to upload a database in `.dat` or `.mmdb` format from your workstation.
4. Navigate to the file you want to upload and click **Open**.
5. Click **Save**.

IP location override

The IP Location Override page enables you to override missing or incorrect IPs that are in the GeoIP database. You can type a comma-delimited list or copy and paste a tab or commadelimited 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 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**.

Override an IP location

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

The Open Data Streams page enables you to configure an interface through which you can send data to an external third-party system.

The following external systems are supported:

Syslog Systems

Send data to a specified syslog.

MongoDB

Send data to a MongoDB database.

HTTP

Send data to a remote HTTP server.

Kafka

Send data to a Kafka server.

Raw

Send raw data to an external server.

Note: You can configure up to 16 open data stream targets of each external system type.

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. For more information, see Open data stream classes in the ExtraHop Trigger API Reference.

Configure an open data stream for syslog

You can export data on ExtraHop Discover appliances to any system that receives syslog input (such as Splunk, ArcSight, or Q1 Labs) for long-term archiving and comparison with other sources.

1. In the System Configuration section, click **Open Data Streams**.
2. Click **Add Target**.
3. From the Target Type drop-down menu, select **Syslog**.
4. In the Name field, type a name to identify the target.
5. In the Host field, type the hostname or IP address of the remote syslog server.
6. In the Port field, type the port number of the remote syslog server.
7. In the Protocol field, select one of the following protocols over which to transmit data:
   - TCP
   - UDP
8. 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.
9. (Optional) Click **Test** to establish a connection between the Discover appliance and the remote syslog server and send a test message.
   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

After you configure a syslog target for an open data stream, you must create a trigger that initiates a `Remote.Syslog` class object that specifies what syslog message data to send through the stream. For more information, see the Remote.Syslog class in the ExtraHop Trigger API Reference.

Configure an open data stream for MongoDB

You can export data on ExtraHop Discover appliances to any system that receives MongoDB input for long-term archiving and comparison with other sources.

1. In the System Configuration section, click **Open Data Streams**.
2. Click **Add Target**.
3. From the Target Type drop-down menu, select **MongoDB**.
4. In the Name field, type a name to identify the target.

5. In the Host field, type the hostname or IP address of the remote MongoDB server.
6. In the Port field, type the port number of the remote MongoDB server.
7. Select **SSL/TLS Encryption** to encrypt transmitted data.
8. Select **Skip certificate verification** to bypass certificate verification of encrypted data.
9. (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.
10. (Optional) Click **Test** to establish a connection between the Discover appliance and the remote MongoDB server and send a test message.
    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
After you configure a MongoDB target for an open data stream, you must create a trigger that initiates a `Remote.MongoDB` class object that specifies what MongoDB message data to send through the stream. For more information, see the Remote.MongoDB class in the ExtraHop Trigger API Reference.

Configure an open data stream for HTTP

You can export data on ExtraHop Discover appliances to a remote HTTP server for long-term archiving and comparison with other sources.

HTTP requests from triggers are queued for processing by an open data stream HTTP client. Note that triggers do not receive results from requests sent to clients because the architecture of the trigger subsystem prevents clients from receiving the results of the requests from servers.

1. In the System Configuration section, click **Open Data Streams**.
2. Click **Add Target**.
3. From the Target Type drop-down menu, select **HTTP**.
4. In the Name field, type a name to identify the target.
5. In the Host field, type the hostname or IP address of the remote HTTP server.
6. In the Port field, type the port number of the remote HTTP server.
7. Select **Pipeline Requests** to enable HTTP pipelining, which can improve performance.
8. 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.
9. (Optional) In the Authentication field, 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.

10. (Optional) Provide a test configuration, in the form of an HTTP request, that is sent when the connection between the Discover appliance and the remote server is tested.

    The test configuration specifies an HTTP request for testing purposes only; it is not included in any trigger scripts.

    a) In the Method field, 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": "/"
}
```

    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.

11. (Optional) Click **Test** to establish a connection between the Discover appliance and the remote server and send a test message.

    If you provided a test configuration, the test message contains the specified content.

    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

After you configure an HTTP target for an open data stream, you must create a trigger that initiates a `Remote.HTTP` class object that specifies what HTTP message data to send through the stream. For more information, see the Remote.HTTP class in the ExtraHop Trigger API Reference.

Configure an open data stream for Kafka

You can export data on ExtraHop Discover appliances to any Kafka server for long-term archiving and comparison with other sources.

1. In the System Configuration section, click **Open Data Streams**.
2. Click **Add Target**.
3. From the Target Type drop-down menu, select **Kafka**.
4. In the Name field, type a name to identify the target.
5. In the Compression field, select one of the following compression methods that will be applied to the transmitted data:

- GZIP
- Snappy

6. In the Partition strategy field, select one of the following partitioning methods that will be applied to the transmitted data:
   - Hash Key (default)
   - Manual
   - Random
   - Round Robin
7. 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.
8. (Optional) Click **Test** to establish a connection between the Discover appliance and the remote Kafka server and send a test message.
   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.
9. Click **Save**.

Next steps
After you configure a Kafka target for an open data stream, you must create a trigger that initiates a `Remote.Kafka` class object that specifies what Kafka message data to send through the stream. For more information, see the Remote.Kafka class in the ExtraHop Trigger API Reference.

Configure an open data stream for raw data

You can export raw data on ExtraHop Discover appliances can be exported 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. In the System Configuration section, click **Open Data Streams**.
2. Click **Add Target**.
3. From the Target Type drop-down menu, select **Raw**.
4. In the Name field, type a name to identify the target.
5. In the Host field, type hostname or IP address of the remote server.
6. In the Port field, type the port number of the remote server.
7. In the Protocol field, select one of the following protocols over which to transmit data:
   - TCP
   - UDP
8. (Optional) Enable GZIP compression of the transmitted data.
   a) Select **GZIP compression**.
   b) Provide a value for one of the following fields:

   Number of bytes after which to refresh GZIP
   Default value is 64000 bytes.

   Number of seconds after which to refresh GZIP
   Default value is 300 seconds.

9. (Optional) Click **Test** to establish a connection between the Discover appliance and the remote server and send a test message.
   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
After you configure a raw data target for an open data stream, you must create a trigger that initiates a `Remote.Raw` class object that specifies what raw message data to send through the stream. For more information, see the Remote.Raw class in the ExtraHop Trigger API Reference.

Delete a data stream configuration

1. In the System Configuration section, click **Open Data Streams**.
2. In the row for the data stream configuration that you want to delete, click the delete (X) icon.

Next steps
After you delete an open data stream configuration, you should disable the trigger associated with the data stream to prevent unnecessary consumption of system resources. See *Delete a trigger* in the ExtraHop Web UI Guide.

View diagnostic information about open data streams

You can view diagnostic information about open data stream configurations.

1. In the System Configuration section, click **Open Data Streams**.
2. In the row for the data stream configuration, hover over the dot in the Status column to view diagnostic information.

Trends

This section enables you to reset all trends and trend-based alerts.

To reset trends:

1. Click **System Configuration** > **Trends**.
2. Click **Reset Trends** to erase all trend data from the ExtraHop appliance.

Appliance Settings

You can configure the following components of the ExtraHop Discover and Command appliance in the Appliance Settings section:

Running Config

View and modify the code that specifies the default system configuration.

Services

Enable management, SNMP, and SSH services.

Firmware

Update the ExtraHop appliance 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

View information about the disks in the ExtraHop appliance.

Command Nickname

Assign a nickname to the Command appliance. This setting is available only on the Command appliance.

Running config

The Running Config page provides an interface to view and modify the code that specifies the default system configuration and save changes to the current running configuration so the modified settings are preserved after a system restart.

The following controls are available to manage the default running system configuration settings:

Save config or Revert config

Save changes to the current default system configuration. The **Revert config** option appears when there are unsaved changes.

Edit config

View and edit the underlying code that specifies the default ExtraHop appliance configuration.

Download config as a file

Download the system configuration to your workstation.

Note: Making configuration changes to the code on the Edit page is not recommended. You can make most system modifications through other pages in the Admin UI.

Saving running config changes

When you modify any of the ExtraHop appliance default system configuration settings, you need to confirm the updates by saving the new settings. If you do not save the new settings, they will be lost when your ExtraHop appliance is rebooted.

The Save page includes a diff feature that displays the changes. This feature provides a final review step before you write the new configuration changes to the default system configuration settings.

When you make a change to the running configuration, either from the Edit Running Config page, or from another system settings page in the Admin UI, changes are saved in memory and take effect immediately, but they are not usually saved to disk. If the system is restarted before the running configuration changes are saved to disk, those changes will be lost.

As a reminder that the running configuration has changed, the Admin UI provides the following three notifications:

Save Configuration

The Admin UI displays a button on the specific page that you modified to remind you to save the change to disk. When you click **View and Save Changes**, the UI redirects to the Save page described above.

Running Config*

The Admin UI adds a red asterisk (*) next to the **Running Config** entry on the Admin UI main page. This asterisk indicates that the running configuration has been changed, but it has not been saved to disk.

Save*

The Admin UI adds a red asterisk (*) next to the **Save** entry on the Running Config page. This asterisk indicates that the running configuration has been changed, but it has not been saved to disk.

After you make changes to the running configuration, the Running Config page displays another entry through which you can revert the changes.

Save system configuration settings

To save any modified system configuration settings:

1. Click **Running Config**.
2. Click **Save config**.
3. Review the comparison between the old running config and the current (new) running config.
4. If the changes are correct, click **Save**.
5. Click **Done**.

Revert system configuration changes

To revert your changes without saving them to disk:

1. Click **Running Config**.
2. Click **Revert config**.
3. Click **Revert**.
4. Click **OK**.
5. Click **Done**.

Edit 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: Do not modify the code on the Running Config page unless instructed by ExtraHop Support.

Download 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 browser's 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

Services run in the background and perform functions that do not require user input. The Admin UI provides the following settings to manage the services used by the ExtraHop appliance. These services can be started and stopped through the Admin UI:

Web Shell

Enable or disable the Launch Shell button in the upper right corner of the Admin UI screen.

Management GUI

Enable or disable the ExtraHop GUI service. This service enables support for the browser-based ExtraHop Web UI and Admin UI interfaces.

SNMP Service

Enable or disable the ExtraHop system SNMP service.

SSH Access

Enable or disable SSH access. This service enables support for the ExtraHop command-line interface (CLI).

Management GUI

Management GUI setting controls the status of the Apache Web Server that runs the ExtraHop web interface application. By default, this service is enabled so that ExtraHop users have access to the ExtraHop Web UI and Admin UI. If this service is disabled, it terminates the Apache Web Server session, turning off web browser access to the ExtraHop UIs.

Warning: Do not disable this service unless you are an experienced ExtraHop administrator and you are familiar with the ExtraHop Command-Line Interface (CLI) commands to restart the Management GUI service.

To enable or disable the Management GUI service:

1. Click **Appliance Settings** > **Services**.
2. Select or clear the **Management GUI** checkbox.
3. Click **Save**.

SNMP service

The state of the network is monitored through the Simple Network Management Protocol (SNMP). SNMP collects information by polling devices on the network. SNMP agents can send alerts to SNMP managers. For example, you could configure an agent to determine how much free space is available on an ExtraHop appliance and send an alert if the appliance is over 95% full.

The SNMP service must be enabled for SNMP notification in the ExtraHop appliance. For more information about configuring SNMP notifications, see the Notifications section.

1. Enable or disable the SNMP service.
   a) In the Appliance Settings section, click **Services**.
   b) Select or clear the **SNMP Service** checkbox.
   c) Click **Save**.
2. Configure the SNMP service.

   The SNMP community string is an identifier that polls the SNMP service.
   a) On the Services page, next to SNMP Service, click **Configure**.
   b) On the SNMP Service Configuration page, enter the following information:

      Enabled

      Select the checkbox to enable the SNMP service.

      SNMP Community

      A friendly name for the SNMP community.

      SNMP System Contact

      A valid name or email address for the SNMP system contact.

      SNMP System Location

      A location for the SNMP system.
   c) Click **Save Settings**.

Download the ExtraHop SNMP MIB

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

To download the ExtraHop SNMP MIB:

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.

SSH access

The SSH Service setting controls the status of the Secure Shell protocol that manages the ExtraHop command-line interface (CLI). By default, this service is enabled so that ExtraHop users have access to the ExtraHop appliance functionality through the CLI. If this service is disabled, it terminates SSH, turning off CLI access to the ExtraHop appliance.

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 on the ExtraHop appliance at all times to provide interface functionality to the system.

To enable or disable the SSH:

1. Click **Appliance Settings** > **Services**.
2. Select or clear the **SSH Service** checkbox.
3. Click **Save**.

Web shell

The Admin UI provides access to the ExtraHop web shell by default. Click the Launch Shell button in the top right corner of the screen to launch the web shell.

To enable and disable the **Launch Shell** button:

1. Click **Appliance Settings** > **Services**.
2. Select or clear the **Web Shell** checkbox.
3. Click **Save**.

Firmware

The Admin UI provides an interface to upload and delete the firmware on ExtraHop appliances.

The Admin UI includes the following firmware configuration settings:

Upgrade

Upload and install new ExtraHop appliance firmware versions.

Delete

Select and delete installed firmware versions from the ExtraHop appliance.

You can download the latest firmware at the ExtraHop Customer Portal. A checksum of the uploaded firmware is usually available in the same download location as the .tar firmware file. If there is an error during firmware installation, ExtraHop Support might ask you to verify the checksum of the firmware file.

Firmware images that you want to upload must be accessible from the computer on which you are running the web browser.

Note: If you are upgrading the firmware on a Command appliance, first upgrade the Command appliance, next update all Discover nodes, and finally upgrade each Explore and Trace appliance individually. To function correctly, the Command appliance and Discover nodes must have the same minor version of ExtraHop firmware.

Upgrade to a new firmware version

Firmware images that you want to upload must be accessible from the computer on which you are running the web browser.

1. In the **Appliance Settings** section, click **Firmware**.
2. Click **Upgrade**.
3. On the Upgrade Firmware page, select from 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.

   If the ExtraHop appliance has less than 300MB of space remaining, a warning message displays with a link to clean up the disk. We recommend that you perform a disk cleanup before uploading new firmware to ensure continued device functionality.
4. (Optional) If you do not want to automatically restart the appliance after the firmware is installed, clear the **Automatically restart appliance after installation** checkbox.
5. Click **Upgrade**.

   The ExtraHop appliance initiates the firmware upgrade. You can monitor the progress of the upgrade with the Updating progress bar.
6. After the firmware update is installed successfully, the ExtraHop appliance displays the version number of the new firmware on the Admin UI. Click **Reboot** to restart the system.

Upload new firmware versions (Command appliance)

Firmware images that you want to upload must be accessible from the computer on which you are running the web browser.

Note: Make sure to upgrade the Command appliance first and then upgrade the connected appliances.

1. In the Appliance Settings section, click **Firmware**.
2. Click **Upgrade**.
3. On the Upgrade Firmware page, enter the following information:
   - 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 in the Firmware URL field, type the URL.

   If the ExtraHop appliance has less than 300MB of space remaining, a warning message appears with a link to clean up the disk. ExtraHop strongly recommends performing a disk cleanup before uploading new firmware to ensure continued device functionality.
4. (Optional) To not automatically restart after installing the new firmware, clear the **Automatically restart appliance after installation** checkbox.
5. Click **Upgrade**.

   The ExtraHop appliance initiates the firmware update. You can monitor the progress of the update with the Updating progress bar.
6. After the firmware upgrade is installed successfully, the ExtraHop appliance displays the version number of the new. Click **Reboot** to restart the system.
7. After restarting, on the Admin UI main page, view the firmware information at the top right of the page.
8. Verify that the firmware version number displayed matches the version that you downloaded from the URL.

Delete firmware versions

The ExtraHop appliance stores every firmware image that has been uploaded to the system. For maintenance purposes, these firmware images can be deleted from the system.

1. In the **Appliance Settings** section, click **Firmware**.
2. Click **Delete**.
3. On the Remove Version page, select the checkbox next to the firmware images that you want to delete or select the **Check all** checkbox.

   Selecting the **All** option does not allow you to select and delete the active firmware version.
4. Click **Delete Selected**.
5. Click **OK**.

System time

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.

The System Time page displays the current configuration and the status of all configured NTP servers.

In the System Time section, the following information appears:

- 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.

The following information for each configured NTP server appears 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

The default time server setting is `pool.ntp.org`. If you want to maintain the default setting, skip this procedure and go to the next section.

1. In the Appliance Settings section, click **System Time**.
2. Click **Configure Time**.
3. Click the Time Zone drop-down list and select a time zone.
4. 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 if the Discover appliance is managed by a Command appliance.
   - Set time with NTP server
6. Select the **Set time with NTP server** radio button, then click **Select**.

   The `pool.ntp.org` public time server appears in the Time Server #1 field by default.
7. Type the IP address or fully qualified domain name (FQDN) for the time servers in the Time Server fields. You can add a maximum of nine time servers.

   Tip: After adding the fifth time server, click **Add Server** to display up to four additional time server fields.
8. Click **Save**, and then 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. The ExtraHop Admin UI includes restart controls for the following system components:

System

Pause the operation of the ExtraHop appliance or shut down and restart the ExtraHop appliance.

Bridge Status

Shut down and restart the ExtraHop bridge component.

Capture

Shut down and restart the ExtraHop capture component.

Portal Status

Shut down and restart the ExtraHop web portal.

For each ExtraHop appliance component, the table includes a time stamp to show the start time.

Shutdown or restart the ExtraHop appliance

1. Click **Appliance Settings** > **Shutdown or Restart**.
2. Select whether to restart or shut down the system.
   - Click **Shutdown**, and then at the prompt, click **Shut down**.
   - Click **Restart**, and then at the prompt, click **Restart**.

Shut down and restart the ExtraHop bridge

1. Click **Appliance Settings** > **Shutdown or Restart**.
2. On the Shutdown or Restart page, under Bridge Status, click **Restart**.
3. At the prompt, click **OK**.
4. Click **Done**.

Shut down and restart the ExtraHop capture

1. Click **Appliance Settings** > **Shutdown or Restart**.
2. On the Shutdown or Restart page, under Capture Status, click **Restart**.
3. At the prompt, click **OK**.
4. Click **Done**.

Shut down and restart the ExtraHop web portal

1. In the **Appliance Settings** section, click **Shutdown or Restart**.
2. In the Actions column for Portal Status, click **Restart**.
3. Click **OK** to confirm.

License

The Admin UI provides an interface to add and update licenses for add-in modules and other features available in the ExtraHop appliance. The License Administration page includes the following licensing information and settings:

Manage license

Provides an interface to add and update licenses for ExtraHop appliance features and modules.

System Information

Displays the identification and expiration information about the ExtraHop appliance.

Features

Displays the list of licensed ExtraHop appliance features (such as Activity Mapping) and whether the licensed features are enabled or disabled.

Modules

Displays the list of modules on the ExtraHop appliance and whether they are enabled or disabled.

Interfaces

Displays the list of licensed Interfaces (such as 10G) and whether the specified interface is active.

View the licensing system information

To view the licensing system information and the status of licensed modules on the ExtraHop appliance:

1. In the Appliance Settings section, click **License**.
2. On the License Administration page, under Modules, check the status column to verify that the add-in modules are enabled.

Register an existing license

1. In the Appliance Settings, click **License**.
2. Click **Manage license**.
3. (Optional) Click **Test Connectivity** to ensure that the ExtraHop appliance can communicate with the licensing server.

   The ExtraHop license server determines whether a connection is possible through DNS records.

   If the test does not pass, open DNS server port 53 to make a connection or contact your network administrator.
4. Click **Register** and wait for the licensing server to finish processing.

   Note: **Register** is unavailable on Discover appliances that are managed by a Command appliance.
5. Click **Done**.

Update a module license or add new licenses

1. In the Appliance Settings section, click **License**.
2. Click Manage License.
3. Click **Update**.
4. In the Enter License text box, enter the licensing information for the module.

   License information must include the dossier and service tag number for the ExtraHop appliance as well as key-value pairs to enable the module licenses and other ExtraHop appliance features. In the license information, a key-value pair with a value of 1 enables the feature or module; a key-value pair with a value of 0 disables the feature or module. For example:

```
-----BEGIN EXTRAHOP LICENSE-----
serial=ABC123D;
dossier=1234567890abcdef1234567890abcdef;
mod_cifs=1;
mod_nfs=1;
mod_amf=0;
live_capture=1;
```

```
capture_upload=1;
10G=1;
triggers=0;
poc=0;
early_access_3.1=0;
activity_map=1;
ssl_acceleration=0;
ssl_decryption=0;
+++;
ABCabcDE/FGHIjklm12nopqrstuvwXYZAB12345678abcde901abCD;
12ABCDEFG1HIJklmnOP+1aA=;
=abcd;
-----END EXTRAHOP LICENSE-----
```

5. Click **Update**.

Disk

The Disk 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 appliance, refer to the guides on docs.extrahop.com.

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 uses 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.

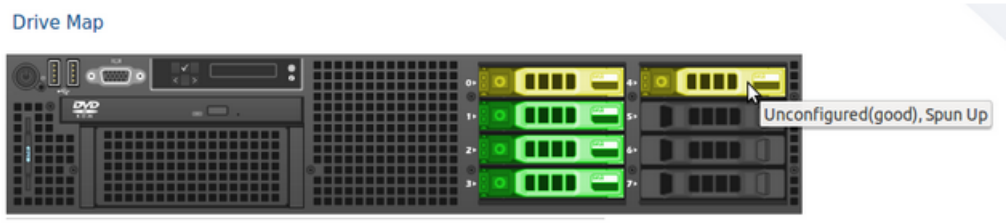
   Click **RAID Disk Details** to display more details.

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.

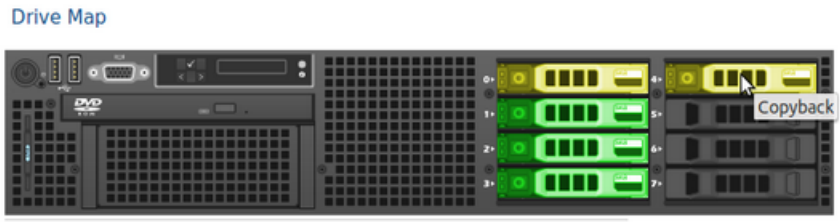
5. Verify the new disk information:

   - 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.

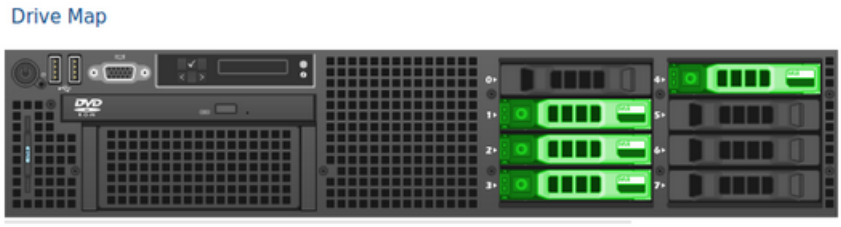


7. After copying is complete, make sure that the copy process was successful:

   - **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 SSD drive

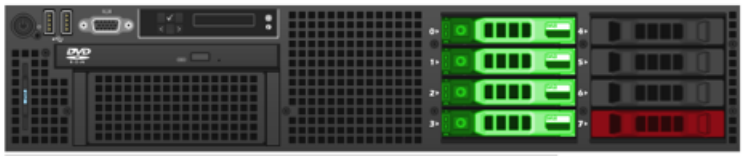
1. Ensure that your ExtraHop license has packet capture enabled.

   For more information, refer to Packet Captures.

2. In the Appliance Settings section, click **Disks**.

   If the Drive Map shows the last slot (Disk #5 on the EDA 2000, Disk #7 on the EDA 5000) in red, you must replace the SSD drive.

Drive Map



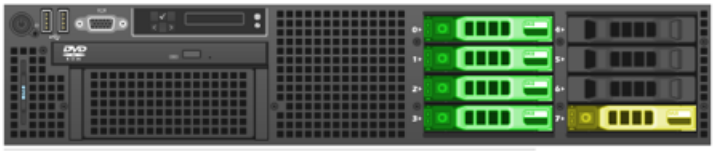
Physical Disk Info

Disk #0	
Status	Online
Media Type	Hard Disk Device
Disk #1	
Status	Online
Media Type	Hard Disk Device
Disk #2	
Status	Online
Media Type	Hard Disk Device
Disk #3	
Status	Online
Media Type	Hard Disk Device
Disk #7	No SSD Present
Status	Empty
Media Type	Empty

3. Insert the SSD drive into the last slot and wait for the LED on the drive to turn green.
4. In the Admin UI, refresh the browser.

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

Drive Map



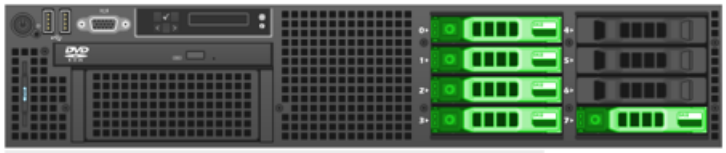
Physical Disk Info

Disk #0	
Status	Online
Media Type	Hard Disk Device
Disk #1	
Status	Online
Media Type	Hard Disk Device
Disk #2	
Status	Online
Media Type	Hard Disk Device
Disk #3	
Status	Online
Media Type	Hard Disk Device
Disk #7	
Status	Unconfigured(good), Spun Up
Media Type	Solid State Device
SSD Assisted Packet Capture	Enable

5. Next to SSD Assisted Packet Capture, click **Enable**.
6. Wait about 1 minute for the drive to be configured and brought online.
7. The browser automatically refreshes.

   The Drive Map shows the SSD drive as green and the Status changes to Online.

Drive Map



Physical Disk Info

Disk #0	
Status	Online
Media Type	Hard Disk Device
Disk #1	
Status	Online
Media Type	Hard Disk Device
Disk #2	
Status	Online
Media Type	Hard Disk Device
Disk #3	
Status	Online
Media Type	Hard Disk Device
Disk #7	
Status	Online
Media Type	Solid State Device

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

Packet Captures

When packet capture is enabled through the Admin UI, you can 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 permission 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

You can configure global packet capture through the Admin UI to save every packet on every flow.

Note: Global packet capture is limited to 96 bytes per packet.

1. In the Packet Captures section, click **Global Packet Capture**.
2. 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.
3. Click **Start**.
4. Click **Stop** to stop the packet capture before any of the maximum limits are reached.

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 128-bit AES keys.

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.

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

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

Next steps
After this procedure is complete, it is safe for you to remove the disk from the physical 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 will disable 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).

If your Discover appliance is behind a firewall, a tunneled connection can be made from the Discover appliance through an SSH tunnel. This configuration requires access privileges from your firewall.

Direct connections are made from the Command appliance over HTTPS on port 443 and do not require special access.

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.

Note: You can connect a Discover appliance to multiple Command appliances.

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**.

Remove a Discover appliance from a Command appliance

If you no longer want to have a Command appliance manage a Discover appliance, you can remove the Discover appliance from one or more Command appliances.

1. Log into the ExtraHop Admin UI on the Discover appliance.
2. Click **Connect Command Appliances** .
3. Click **Remove**.
4. Click **Yes** to confirm.

Set a nickname for a Command appliance

You can assign a custom name to the Command appliance. This custom name appears in the Web UI and Admin UI of connected appliances instead of displaying the Command appliance hostname.

1. Log into the Admin UI on the Command appliance.
2. In the Appliance Settings section, click **Command Nickname**.
3. Select Display custom nickname and then type a name in the field.
4. Click **Save**.

Manage connected appliances from a Command appliance

The Manage Connected Appliances page in the Command appliance enables you to perform administrative tasks on multiple Discover, Explore, and Trace appliances.

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.

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**.

View connected Discover appliances

After you connect a Discover appliance from a Command appliance, the Discover appliance is listed in a table that displays the following information:

Name

The following entries appear in the Name field:

- The IP address or hostname of the Discover appliance. Click the hostname link to open the Properties window.
- The appliance nickname if the Nickname field in the node Properties window is configured. If a nickname is not configured, only the hostname appears. To assign a nickname, click the appliance hostname or IP address link, type a name in the Nickname field and then click **Save**.

- The connection type. Displays `Direct` if the connection to the managed appliance is established from the Command appliance or `Tunneled` if the connection to the Command appliance is established from the Discover appliance.
- The ExtraHop license key.

ID

Displays a numeric number which identifies the Discover appliance.

Version

Displays the ExtraHop firmware version number.

Date Added

Displays the date and time the Discover appliance was added.

Status

Displays one of the following connection states:

Online

Connection to the appliance is active.

Disabled

Connection to the appliance is disabled.

Offline

Connection to the appliance has timed out.

License

Displays one of the following license states:

Valid

The license is valid.

Expiring Soon

The license will expire shortly. Read access to the appliance will be lost if the license is not renewed.

License Check Pending

The node cannot connect to the ExtraHop license server.

Disconnected

The node cannot connect to the ExtraHop license server, and the capture has stopped.

Invalid

The license is invalid or has expired.

Reset

All configuration, software, and data has been deleted from this appliance.

NTP

Displays one of the following time states:

Time Synced

The time on the Discover appliance is synced to the configured time server.

Large Time Delta

The time on the Discover appliance does not match the time of the Command appliance.

Not Configured

NTP is not configured on the Discover appliance.

Actions

Displays a drop-down menu with links to open the Web UI, Admin UI, and Web Shell of the connected Discover appliance. The drop-down menu also includes the following appliance actions: **Check License**, **Run Support Pack**, **Upgrade Firmware**, **Disable**, and **Remove Appliance**.

Tip: You can search for specific Discover appliance by typing in the filter appliances field.

Check the license status of managed Discover appliances

1. Log into the ExtraHop Admin UI on the Command appliance.
2. In the ExtraHop Discover Settings section, click **Manage Discover Appliances**.
3. On the Discover tab, select the checkbox next to each Discover appliance that you want to verify.
4. Click **Check License**. The License field displays `Pending` until the status check is complete.

Generate or upload a support pack

You can run a support pack on any ExtraHop appliance that is managed by a Command appliance.

For more information about support packs, see the Support packs section.

1. Log into the Admin UI on the Command appliance.
2. In the ExtraHop Discover Settings section, click **Manage Discover Appliances**.
3. On the **Discover**, **Explore**, or **Trace** tab, select the appliance in the table and then click **Run Support Pack**.

   Tip: You can select multiple Discover appliances to run the support pack action on each selected node.
4. In the Support Pack section, select from the following options:
   - Select **Default Support Pack** to generate diagnostics from the system.
   - Select **Upload Support Pack**, click **Choose File**, and navigate to a saved support pack file on your workstation.
5. Click **Run**.

Upgrade Discover appliance firmware from a Command appliance

You can upgrade the firmware on any Discover appliance that is connected to a Command appliance.

Note: You should always update Command appliances first, and then update the Discover appliances.

1. Log into the Admin UI on the Command appliance.
2. In the ExtraHop Discover Settings section, click **Manage Discover Appliances**.
3. On the Discover tab, select the checkbox next to the nodes you want to update and then click **Upgrade Firmware**.
4. Select from the following options:
   - Click **Retrieve from URL** and type the HTTP or FTP firmware URL in the field.
   - Click **Upload firmware image**, click **Choose File** to navigate to the firmware file saved on your workstation, and then click **Open**.
5. Click **Upgrade**.

   The Job column displays `Firmware Update Pending` until the firmware installation is complete.

After the firmware update successfully completes, a `Firmware Update Completed` confirmation message appears on the right-hand side of the Manage Connected Appliance page.

Disable a Discover appliance

You can disable the connection to a Discover appliance from the Command appliance. When you disable a Discover appliance, the Discover appliance is removed from theCommand appliance and you can no longer view data from that node in the ExtraHop Web UI on the Command appliance.

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

2. In the ExtraHop Discover Settings section, click **Manage Discover Appliances**.
3. On the Discover tab, select the checkbox next to each Discover appliance that you want to disable.
4. Click **Disable**.

Enable a Discover appliance

You can enable the connection to a Discover appliance in the Command appliance if the Discover appliance is disabled for administrative purposes. When the status returns to `Online`, you can view the data from the Discover appliance in the ExtraHop Web UI on the Command appliance.

1. Log into the Admin UI on the Command appliance.
2. In the ExtraHop Discover Settings section, click **Manage Discover Appliances**.
3. On the Discover tab, select the checkbox next to each Discover appliance that you want to enable.
4. Click **Enable**.

Remove a managed Discover appliance from a Command appliance

If you no longer want to manage an Discover Appliance through a Command appliance, remove the node through the Manage Connected Appliances page.

1. Log into the Admin UI on the Command appliance.
2. In the ExtraHop Discover Settings section, click **Manage Discover Appliances**.
3. Select the checkbox next to the Discover appliance you want to delete.
4. Click **Remove Appliance**.

   Tip: To remove multiple Discover appliances at once, select the checkbox next to each appliance you want to remove and then click **Remove Appliances**.
5. Click **Yes** to confirm.

Add an Explore appliance to a Command appliance

You can manage multiple Explore appliances from a Command appliance. After you connect the Explore appliances, you can view the Explore appliance properties, assign a nickname, create a diagnostic support package, and connect to the Admin UI on the Explore appliance though the Command appliance.

Note: A managed node only enables you to perform administrative tasks. To enable record queries from the Command appliance, see the ExtraHop Explore Settings section.

1. Log into the ExtraHop Admin UI on the Command appliance.
2. In the ExtraHop Explore Settings section, click **Manage Explore Appliances**.
3. Click **Add Appliance**.
4. Type the hostname or IP address of the Explore appliance in the Host field.
5. Click **Confirm Fingerprint**.
6. Note the information listed for Fingerprint. Verify that the fingerprint listed on this page matches the fingerprint of the Explore appliance listed on the **Status** > **Fingerprint** page in the Admin UI on the Explore appliance.
7. Type the password for the Explore appliance `setup` user in the Setup Password field.
8. Click **Connect**.
9. Repeat steps 2 through 8 for each additional Explore appliance (including multiple appliances that are members of a single Explore cluster) that you want to manage.

View Explore node information

After you add an Explore node, the node is listed in a table that has the following information:

Name

The following entries appear in the Name field:

- The unique Explore cluster ID. Click the link to open the Cluster Properties window and add or modify the cluster nickname.
- The IP address or hostname of the Explore node. Click the link to open the Properties window.
- The Explore cluster nickname if the Nickname field in the Properties window is configured. If a nickname is not configured, only the hostname appears. To assign a nickname, click the cluster ID link, type a name in the Nickname field and then click **Save**.
- The connection type. Displays `Direct` when the connection to the Explore appliance is established from the Command appliance or `Tunneled` when the connection is established from the Explore appliance.

Date Added

Displays the date and time the node was added as a managed appliance.

License

Displays one of the following license states:

Valid

The license is valid.

Expiring Soon

The license will expire shortly. Read access to the appliance will be lost if the license is not renewed.

License Check Pending

The node cannot connect to the ExtraHop license server.

Disconnected

The node cannot connect to the ExtraHop license server, and the capture has stopped. ExtraHop ExtraHop Discover and Command appliances cannot query any stored records.

Invalid

The license is invalid or has expired. ExtraHop ExtraHop Discover and Command appliances cannot query any stored records.

Reset

All configuration, software, and data has been deleted from this appliance.

Actions

Displays a list of actions that you can perform on the Explore cluster.

Job

Displays the status of any currently running support pack job.

Generate or upload a support pack for the Explore appliance

You can run a support pack on any Explore node that is managed by a Command appliance.

For more information about support packs, see the Support packs section.

1. Log into the Admin UI on the Command appliance.
2. In the ExtraHop Explore Settings section, click **Manage Explore Appliances**.
3. Select the Explore node in the table and then click **Run Support Pack**.
4. In the Support Pack section, select from the following options:
   - Select **Default Support Pack** to generate diagnostics from the system.
   - Select **Upload Support Pack**, click **Choose File**, and navigate to a saved support pack file on your workstation.
5. Click **Run**.

Remove an Explore cluster from a Command appliance

You can remove a connected Explore cluster from the list of managed Explore clusters on a Command appliance. The cluster will remain connected, collecting record data, but you will no longer be able to manage administrative functions for the Explore cluster through the Command appliance.

1. In the ExtraHop Explore Settings section, click **Manage Explore Appliances**.
2. Click a blank area in the table next to the Explore cluster that you want to remove
3. Click **Remove Cluster**.

   Note: If there are multiple Explore nodes in a single Explore cluster, all nodes in the cluster are removed.
4. Click **Yes** to confirm.

Add a Trace appliance to a Command appliance

You can manage multiple Trace appliances from a Command appliance. After you add the nodes, you can view the Trace appliance properties, assign a nickname, create a diagnostic support package, and connect to the Admin UI on the Trace appliance.

Note: A managed node only enables you to perform administrative tasks. To enable packet queries from the Command appliance, see the ExtraHop Trace Settings section.

1. Log into the ExtraHop Admin UI on the Command appliance.
2. In the ExtraHop Trace Settings section, click **Manage Trace Appliances**.
3. Click **Add Appliance**.
4. Type the hostname or IP address of the Trace appliance.
5. Click **Confirm Fingerprint**.
6. Note the information listed for Fingerprint. Verify that the fingerprint listed on this page matches the fingerprint of the Trace appliance listed on the **Status** > **Fingerprint** page in the Admin UI on the Trace appliance.
7. Type the password for the Trace appliance `setup` user in the Setup Password field
8. Click **Connect**.

View Trace appliance information

After you add a Trace appliance, the appliance is listed in a table that has the following information:

Name

The following entries appear in the Name field:

- The unique Trace cluster ID. Click the link to open the Properties window and add or modify the cluster nickname.
- The IP address or hostname of the Trace appliance. Click the link to open the Properties window.
- The Trace appliance nickname if the Nickname field in the Properties window is configured. If a nickname is not configured, only the hostname appears. To assign a nickname, click the cluster ID link, type a name in the Nickname field and then click Save.
- The connection type. Displays **Direct** if the connection is established from the Command appliance or **Tunneled** if the connection to the Command appliance is established from the Trace appliance.

Date Added

Displays the date and time the node was added as a managed appliance.

License

Displays one of the following license states:

Valid

The license is valid.

Expiring Soon

The license will expire shortly. Read access to the appliance will be lost if the license is not renewed.

License Check Pending

The node cannot connect to the ExtraHop license server.

Disconnected

The node cannot connect to the ExtraHop license server, and the capture has stopped.

Invalid

The license is invalid or has expired.

Reset

All configuration, software, and data has been deleted from this appliance.

Remote Interfaces

Displays a link to the Admin UI on the Trace appliance. Click the link to open the Admin UI in a new browser window.

Job

Displays the status of any currently running support pack job.

Generate or upload a support pack for the Trace appliance

You can run a support pack on any Trace appliance that is managed by a Command appliance.

For more information about support packs, see the Support packs section.

1. Log into the Admin UI on the Command appliance.
2. In the ExtraHop Explore Settings section, click **Manage Trace Appliances**.
3. Select the Trace node in the table and then click **Run Support Pack**.
4. In the Support Pack section, select from the following options:
   - Select **Default Support Pack** to generate diagnostics from the system.
   - Select **Upload Support Pack**, click **Choose File**, and navigate to a saved support pack file on your workstation.
5. Click **Run**.

Upgrade Trace appliance firmware

You can upgrade the firmware on any Trace appliance that is managed by a Command appliance. You can only upgrade nodes that are connected from the Command appliance (direct connection). Firmware upgrades through tunneled connections are not supported.

Note: You should always upgrade firmware on the Command appliance first, and then upgrade the Trace appliance.

1. Log into the Admin UI on the Command appliance.
2. In the ExtraHop Trace Settings section, click **Manage Trace Appliances**.
3. Select the node you want to upgrade and then click **upgrade Firmware**.
4. Select from the following options:
   - Click **Retrieve from URL** and type the HTTP or FTP firmware URL in the field.
   - Click **Upload firmware image**, click **Choose File** to navigate to the firmware file saved on your workstation, and then click **Open**.
5. Click **Install**.

   The Job column displays `Firmware Update Pending` until the firmware installation is complete.

After the firmware upgrade successfully completes, a `Firmware Update Completed` confirmation message appears on the right-hand side of the Manage Connected Appliance page.

Remove a Trace appliance from a Command appliance

You can remove a connected Trace appliance from the list of managed Trace appliances on a Command appliance. The Trace appliance will remain connected, collecting packet capture data, but you will no longer be able to manage administrative functions for the Trace appliance through the Command appliance.

1. In the ExtraHop Trace Settings section, click **Manage Trace Appliances**.
2. Click a blank area in the table next to the Trace appliance you want to remove.
3. Click **Remove Appliance**.

   Note: You can remove only one Trace appliance at a time.

4. Click **Yes** to confirm.

View cluster history

You can view a list of the five most recent firmware updates and support packs that were run on the system.

1. Log into the Admin UI on the Command appliance.
2. In the ExtraHop Command Settings section, click **Manage Discover Appliances**.
3. Click **History**.

   The following entries appear in the History table:

   Time

   Displays the time the action started.

   Name

   Displays the name of the action.

   Status

   Displays the completed status of the action.

   Result

   Displays a **Download** link that enables you to download the support pack to your computer.

ExtraHop Explore Settings

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

Automatic Flow Records

Specify the automatic flow record settings.

Connect Explore Appliances

Specify Explore appliances to store and retrieve records.

Manage Explore Appliances

View the properties of managed Explore cluster nodes.

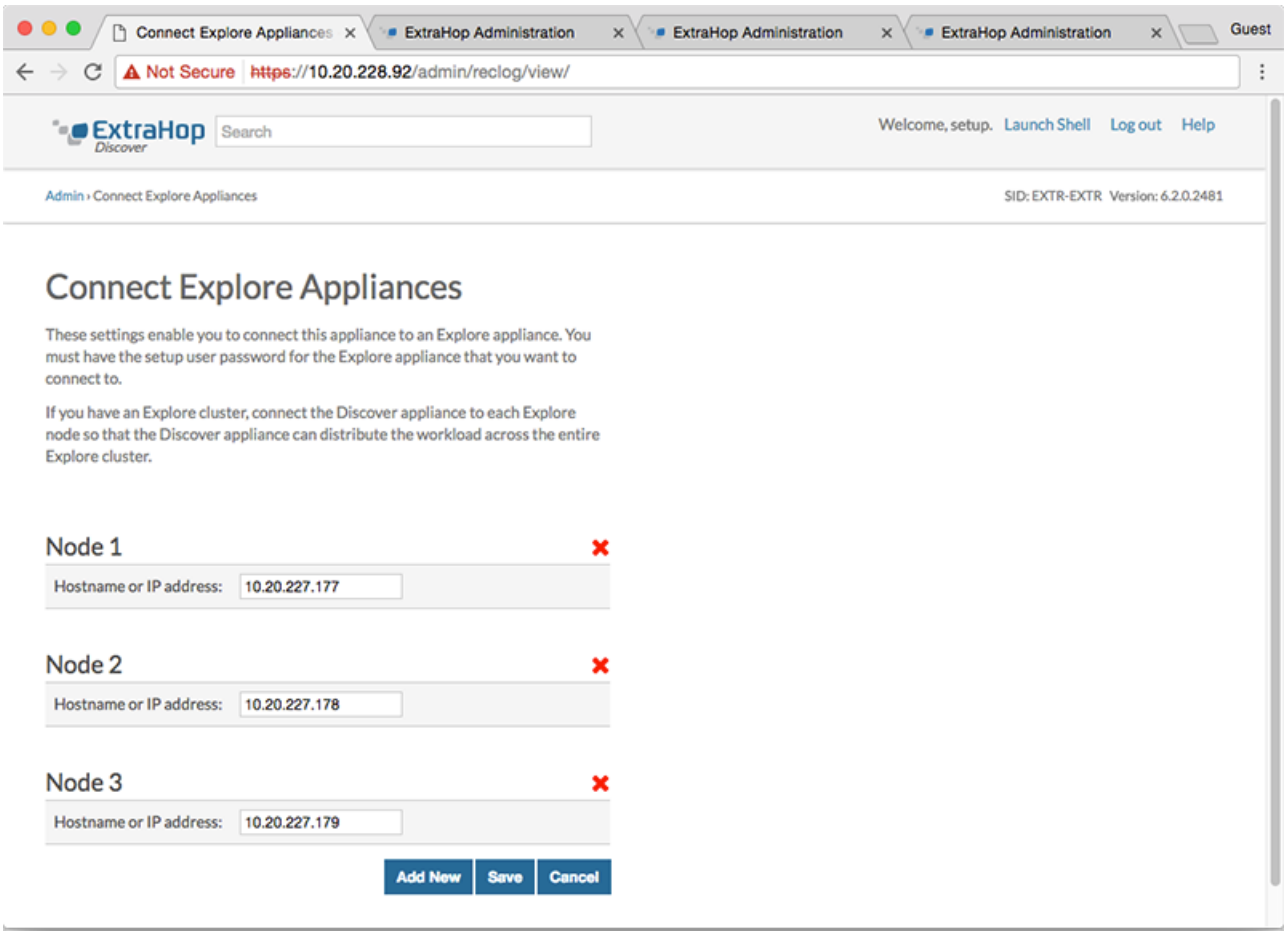
Connect to Explore appliances

When you deploy an ExtraHop Explore appliance in your environment, you must establish a connection from an ExtraHop Discover appliance to the Explore appliance before you can query records. For optimal performance, we recommend that you set up three or more Explore appliances in a cluster to take advantage of data redundancy.

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

Note: If your Discover appliance is managed by an ExtraHop Command appliance, you must perform this procedure from the Admin UI on the Command appliance.

1. In the ExtraHop Explore Settings section, click **Connect Explore Appliances**.
2. Click **Add New**.
3. Type the hostname or IP address of any Explore appliance in the Node 1 field.
4. For each additional Explore appliance in the cluster, click **Add New** and enter the unique hostname or IP address in the corresponding Node field. Your Connect Explore Appliances page should look similar to the following figure.



5. Click **Save**.
6. Note the information listed for **Fingerprint**. Verify that the fingerprint listed on this page matches the fingerprint of the Explore appliance (**Node 1**) as it appears on the **Status** > **Fingerprint** page in the Explore Admin UI.
7. Type the password for the Explore appliance `setup` user in the Explore Setup Password field.
8. Click **Connect**, and then click **Done**.

Configure automatic flow record settings

Flow records show communication between two devices over an (L3) IP protocol. Automatic flow records are sent when a flow terminates, or periodically for flows that remain active for an extended period of time.

Flow records are captured across all IP addresses and port ranges when Enabled is selected. You can restrict capture activity to specific devices or traffic by adding IP addresses or ports in the settings below. If you add both IP addresses and ports, capture activity is restricted to the ports for the IP addresses that you specify.

1. Log into the Admin UI on the Discover appliance.
2. In the ExtraHop Explore Settings section, click **Automatic Flow Records**.
3. Select the Enabled checkbox.
4. Type the number of seconds after which a flow record is sent to the Explore appliance if the flow is still active in the Publish Interval field. The minimum value is `60` and the maximum value is `21600`.
5. Type a single IP address or a range of IP addresses in the IP Addresses field and then click the green plus (+) icon. IP address ranges need to be separated by a hyphen (-). To remove an IP address, click the red delete (x) icon next to the IP address.

6. Type a single port number or a range of port numbers in the Port Ranges field and then click the green plus (+) icon. Port ranges need to be separated by a hyphen (-). To remove port ranges, click the red delete (x) icon next to the port .
7. Click **Save**.

ExtraHop Explore appliance status

The ExtraHop Explore Status section displays the following status information for the Explore appliance:

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

Specify ExtraHop Trace appliances to continuously collect and store raw packet data.

Connect a Trace appliance

When you deploy a Trace appliance in your environment, you must establish a connection from an ExtraHop Discover appliance and Command appliance to the Trace appliance before you can query packets.

Note: A Discover appliance can only be connected to four or fewer Trace appliances, whereas a Command appliance can be connected to more than four Trace appliances.

To connect a Discover appliance or Command appliance to a Trace appliance:

1. Log into the Admin UI on the Discover or Command appliance.
2. In the ExtraHop Trace Settings section, click **Connect Trace Appliances**.
3. Type the hostname of the Trace appliance in the Appliance hostname field.
4. Click **Connect**.
5. Note the information listed for **Fingerprint**. Verify that the fingerprint listed on this page matches the fingerprint of the Trace appliance listed on the **Status** > **Fingerprint** page in the Admin UI on the Trace appliance.
6. Type the password for the Trace appliance `setup` user in the Trace Setup Password field
7. Click **Connect**.
8. Repeat steps 3-7 for each additional Trace appliance.

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.

- DHE_RSA_WITH_3DES_EDE_CBC_SHA
- DHE_RSA_WITH_AES_128_CBC_SHA
- DHE_RSA_WITH_AES_256_CBC_SHA
- DHE_RSA_WITH_AES_128_CBC_SHA256
- DHE_RSA_WITH_AES_256_CBC_SHA256
- DHE_RSA_WITH_AES_128_GCM_SHA256
- DHE_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_RSA_WITH_RC4_128_SHA
- ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- ECDHE_RSA_WITH_AES_128_CBC_SHA
- ECDHE_RSA_WITH_AES_256_CBC_SHA
- ECDHE_RSA_WITH_AES_128_SHA256
- ECDHE_RSA_WITH_AES_256_SHA384
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 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.