ExtraHop 5.3
Admin UI Guide

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

Published: 2017-09-01

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 ExtraHop Discover or Command appliance, see the ExtraHop Post-deployment Checklist.

Global navigation

This section describes the general layout of the ExtraHop Admin UI. It focuses on navigating to the top level sections in the user interface, changing the password, logging on and off, and other page-level toolbar controls.

The ExtraHop Admin UI is a web application that uses the features of an Internet browser to create the graphical user interface. When the ExtraHop Admin UI opens in the browser window, the main frame contains a fixed toolbar at the top of the UI page to display application-level controls and links that are relevant to all interface pages.

The application-level toolbar contains the following controls or links:

- Change default password: Opens the Change Password page to specify a new Admin UI password. For more information about changing the default password, see the Change Password section.
- Launch Shell: Opens the ExtraHop web shell for entering admin commands to configure the ExtraHop appliance. For more information about using the ExtraHop web shell, see the Shell Commands section.
- Log out: Ends the ExtraHop Admin UI session. For more information about logging out, see the Login/Logout section.
- Help: Opens the ExtraHop Admin UI Guide.

The main administration page includes the following sections for configuring the ExtraHop appliance:

- Status: Verify how the ExtraHop appliance is functioning on the network.
- Network Settings: Configure the network settings for the ExtraHop appliance.
- Packet Captures: View and download packet captures.
- Cluster Settings: Add nodes to a Command appliance. Not available on a node.
- ExtraHop Command Memberships: Join a Command appliance cluster. Not available on a Command appliance.
- Access Settings: Configure access settings to the ExtraHop appliance.
- System Configuration: Change the configuration settings of the ExtraHop appliance.
- ExtraHop Explore Settings: Change the configuration settings of the Explore appliance.
- System Settings: Configure the system-level settings for the ExtraHop appliance.
- Diagnostics: Troubleshoot ExtraHop appliance issues.

Log into the ExtraHop Admin UI

The ExtraHop appliance prompts you for a username and a password when you access the interface through your web browser.

The default user name for ExtraHop appliances is `setup` and the default password is the service tag number of the appliance, which is located on the pullout tab on the front of the appliance.

1. In a web browser, navigate to the ExtraHop Admin UI by typing https://[IP address]/admin, where [IP address] is the IP address of your ExtraHop appliance.

2. On the Login page, enter the following information:

   Username

   Type your ExtraHop administrator username.

   Password

   Type your ExtraHop administrator password.

Log out of the ExtraHop Admin UI

From the top right of the page, click **Log out**.

Browser compatibility

The following browsers are compatible with all ExtraHop appliances.

- Chrome 45
- Firefox 41
- Internet Explorer 10 and 11
- Safari 9

Status

The Status section provides metrics about the overall health of the ExtraHop appliance.

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. (Optional) Click **Test Settings** to make sure the settings are correct.
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 messages

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

Category	Event

Login	• A login succeeds • A login fails
Running Config	The running config changes
Support/Diag Pack	• A default support pack is generated • A past diagnostic pack result is deleted • A support pack is uploaded and applied
System and Service Status	• The system starts up • The system shuts down • The system is restarted • The bridge/capture/portal process is restarted • A system service is enabled (SNMP/web shell/ management/SSH) • A system service is disabled (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
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 • “Sync time now” 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 from license server is applied
ECA Cluster	• An ECA cluster is joined • An ECA cluster is left • ECA info is set • A node’s nickname is set • A cluster node is enabled • A node is added to a cluster • A node is removed from an ECA cluster • A node is enabled

	• A node is disabled • A node UI is remotely viewed • An license for a node is checked by an ECA • An license for a node is set by an ECA
Agreements	A EULA or POC agreement is agreed to
SSL Decryption	An SSL decryption key is saved
Appliance user	• A user is added • A user's metadata is edited • A user is deleted • A user's password is set • A user's 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
Trends	A trend is reset
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
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
EXA Cluster	• A new EXA node is initialized • A node is added to an EXA cluster • A node is removed from an EXA cluster • A node joins an EXA cluster • A node leaves an EXA cluster • An ECA/EDA is paired to an EXA • An ECA/EDA is unpaired from an EXA

	• An EXA node is removed or missing, but not via a supported interface
EXA Records	All EXA records are deleted

Network settings

The ExtraHop appliance has four 10/100/1000baseT network ports. The Gb1 port is used for management and requires an IP setting. The Gb2 port is used for monitoring network traffic and connects to the network tap or mirror port on your network switch.

You also monitor through the Gb3 and Gb4 ports, if permitted by your license. Some appliances have two 10GbE SFP+ ports with the accompanying SFP+ SR-fiber modules.

Before you begin configuring the network settings of the ExtraHop appliance, verify that a network patch cable connects the Gb1 port on the ExtraHop appliance to the management network.

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

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 appliance nodes that are part of a Command cluster to Atlas Services, but you cannot connect the Command appliance to Atlas Services.

1. In the Network Settings section, click **Connect to Atlas Services**.
2. In the Connect to Atlas Services dialog box, click **Terms and Conditions** to read about the service agreement.
   The Atlas subscription services agreement opens in a new browser tab.
3. Return to the previous tab and select the checkbox next to **Terms and Conditions**.
4. (Optional) Click **Test Connectivity** to make sure the connection is functional.
5. Click **Yes**.

Disconnect from Atlas services

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

1. In the Network Settings section, click **Disconnect from Atlas Services**.
2. In the confirmation dialog box, click **OK**.

Connectivity

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

(Optional) 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

Host Name:

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

Global Proxy:

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

Atlas Proxy:

Provides the ability to enable proxy support for connection to 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 modes

The EDA 5000, EDA 6000, EDA 6100, EDA 8000, and EDA 8100 have two 10GbE interfaces and three 1GbE interfaces. The 1GbE interfaces are disabled by default, and the ExtraHop appliance operates in the standard throughput mode. Enabling one or more of the 1GbE interfaces puts the ExtraHop appliance into the reduced throughput mode. Before changing the interface settings, refer to the following table to determine which throughput mode you want to use.

ExtraHop Appliance	Throughput Mode	Definition
EDA 9100	Standard 40Gbps throughput mode	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 9100	Reduced 23Gbps throughput mode for use of 1GbE ports	If the non-management 1GbE interfaces are enabled, the maximum total combined throughput is 23Gbps.
EDA 8000/8100	Standard 20Gbps throughput mode	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 8000/8100	Reduced 13Gbps throughput mode for use of 1GbE ports	If the non-management 1GbE interfaces are enabled, the maximum total combined throughput is 13Gbps.
EDA 5000/6000/6100	Standard 10Gbps throughput mode	If the non-management 1GbE interfaces are disabled, the maximum total combined throughput is 10Gbps.
EDA 5000/6000/6100	Reduced 8Gbps throughput mode	If the non-management 1GbE interfaces are enabled, the maximum total combined throughput is 8Gbps.
EDA 5000/6000/6100	Reduced 3Gbps throughput mode with 10GbE ports disabled	If the 10GbE interfaces are disabled, the maximum total combined throughput is 3Gbps.

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 + NetFlow 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.

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: EDA 2000, EDA 2000v, EDA 3000, EDA 5000, EDA 6000, EDA 6100, EDA 8000, EDA 8100, EDA 9100, and EDA 1100. Interfaces 5 and 6 are disabled by default on the following appliances: EDA 5000, EDA 6000, EDA 6100, EDA 8000, EDA 8100, and EDA 9100.

4. DHCPv4 is enabled by default. If your network does not support DHCP, you can deselect 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

If you do not have DHCP enabled, you can manually set a route to determine the traffic goes.

1. In the Network Settings section, click **Connectivity**.
2. In the Interfaces section, click the interface you want to set a manual route for.
3. On the Network Settings for Interface <interface number> page, ensure that the **IP Address** and **Netmask** fields are complete and saved, and then click **Edit Routes**.
4. In the Add Route section, complete the **Network** and **Via IP** fields, and then click **Add**.
5. Repeat the previous step for each route you want to add.
6. Click **Save**.

Change RPCAP settings

If you do not have DHCP enabled, you can manually set a route to determine the traffic goes.

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

1. Click **RPCAP Settings**.
2. On the Add RPCAP Port Definition page, 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.

   • **Interface Name:** Specifies the interface on the packet-forwarding server from which to forward packets.

   • **Filter:** Specifies the traffic to forward with Berkeley Packet Filter 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.
3. 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**.

Atlas 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 Atlas connectivity. Only one Atlas proxy can be configured per ExtraHop appliance.

Note: If no Atlas 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 use a direct HTTP proxy to enable Atlas services.

Configure an Atlas proxy server

1. In the Network Settings section, click **Connectivity**.
2. Click **Enable Atlas Proxy** or click on the name of an existing Atlas proxy that you want to modify.
3. On the Atlas Proxy Settings page, type the following information:
   - **Hostname:** The hostname or IP address for your Atlas proxy server.
   - **Port:** The port number for your Atlas proxy server.
   - **Username:** The name of a user that has for access to your Atlas proxy server.
   - **Password:** The password for the user specified above.
4. Click **Save**.

Disable an Atlas proxy server

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

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, 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.
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 membership can be **Management** or **Mangement+RPCAP/ERSPAN Target** only.

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

NetFlow

Configure port and network settings to send flow network traffic to your ExtraHop appliance.

Add a flow network

Configure the interface mode of the Discover management port to **Management Port + NetFlow Target**.

Before you begin
For more information see the Configure an interface section.

Note: The EDA 1100 and EDA 1000v must be configured for either NetFlow or wire data because these appliances cannot process NetFlow and wire data simultaneously. If these appliances are configured for NetFlow, you must set the monitoring port to **Disabled**.

1. In the Network Settings section, click **Flow Networks**.
2. In the Ports section, type `2055` in the port field and then click the plus (**+**) icon.

   Note: UDP port 2055 is the default port for NetFlow. You can add additional ports as needed for your environment.
3. In the Flow Networks section, click **Add Flow Network**.
4. Enter the following information:

Name

Type a name to identify this flow network.

IP address

Type the IP address of the flow network device in IPv4 or IPv6 format.

Automatic records

(Optional) Select this checkbox to send records to a paired Explore appliance.

Enable SNMP polling

(Optional) Select this checkbox to enable SNMP polling.

SNMP Polling type

Select **v1/v2c** or **v3** from the drop-down list and then configure the remaining settings for the specific polling type.

5. Click **Save**.

Next steps

Configure your network devices to export flow records to the ExtraHop appliance. For sample Cisco configurations, see Configure Cisco NetFlow devices in the appendix.

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. On the Email Settings page, enter the following information:
   - **SMTP Server:** The IP address for the outgoing SMTP mail server.

     Note: The SMTP server should be the 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.

   - **Sender Address:** The email address for the notification sender.
   - **Report Sender Address:** The email address for the report sender.
4. 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 will fire 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 a 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 th 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 will fire 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 a 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. (Optional) Click **Test Settings** to verify that your SNMP settings are functioning properly.
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 (e.g., Splunk, ArcSight, Q1 Labs, etc.) 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. (Optional) Click **Test Settings** to verify that your syslog settings are functioning properly.
5. Click **Save**.

SSL certificates

SSL is used to provide secure authentication to the Web UI and Admin UI of the ExtraHop appliance. To use SSL, a SSL certificate must be 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.

Generate a self-signed certificate

If you plan to use a self-signed certificate for your ExtraHop appliance, you must first generate the 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 regenerate the SSL self-signed certificate based on the hostname.

   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**.

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 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 use triggers to perform packet captures, 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. Click the System Settings icon, and then click **License**.
2. In the Features section, verify that packet capture is enabled. If you do not see Packet Capture on the list or it is not listed as Enabled, contact ExtraHop Customer Support.

   Note: If you are using a 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 System Settings section, click **Disk**. 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, it is ready to use 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 following related documentation:

- ExtraHop Trigger API Quick Start Guide
- Trigger API Reference

and the .

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 0 and 65536.
3. Click **Start**.
4. (Optional) Click **Stop** to stop the packet capture before any of the maximum limits are reached.

Encrypt packet capture disk

You can encrypt the disk that packet captures are stored on for increased security.

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. Under System Settings, click **Disk**.
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 field.
To enter an encryption key file	Click **Choose File**, and then browse to an encryption key file.

5. Click **Encrypt**.

Remove 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. Under System Settings, click **Disk**.
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 **Remove Disk**.

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 System Settings, click **Disk**.
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 System Settings, click **Disk**.
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**.

Format packet capture disk

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. After a disk is reformatted

1. Under System Settings, click **Disk**.
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 **Format Disk**.
4. Click **OK**.

Change packet capture disk encryption key

1. Under System Settings, click **Disk**.
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 entered an encryption key file	Click **Choose File**, and then browse to an encryption key file.

5. Click **Change Key**.

ExtraHop Command settings

You can manage multiple Discover nodes that are joined to an ExtraHop Command appliance.

Set a name for your Command appliance

This name identifies the cluster to Discover appliances that are added as nodes.

1. In the ExtraHop Command Settings section, click **Set ECA Name**.
2. In the Set ECA Name dialog box, type a name, and then click **Save**.

Join a Command cluster

Each Discover appliance can belong to multiple Command clusters; however, a Command appliance cannot be a node in another Command cluster.

1. In the ExtraHop Command Memberships section, click **Join a Cluster**.
2. In the Join a Command Cluster window, configure the following information:
   - Command hostname**:** The hostname or IP address of the Command appliance.

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

   - Command setup password**:** The setup password for the Discover node.
   - Discover node nickname**:** A friendly name for the node. If no friendly name is entered, the host name will be used instead.
   - (Optional) Reset configuration**:** If you select this checkbox, existing node customizations such as device groups, alerts, and triggers will be removed. Gathered metrics such as captures and devices will not be removed.
3. Click **Save**.

Nodes

You can manage Discover nodes that are joined to the Command cluster.

View cluster history

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Activity section, click **History**.
   The five most recent actions appear.

Update node firmware

You can update the firmware on any node that is joined to a Command cluster.

Note: You should always first upgrade the Command appliance and then upgrade any Discover nodes.

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Activity section, click **Update Firmware**.
3. In the Firmware Image section, select from the following options:
   - To select firmware saved on your workstation, navigate to the firmware file and click **Open**.

- To enter a URL that you received from ExtraHop support, click **retrieve from URL instead**.

4. In the Apply to section, select from the following options:
   - To update the firmware on all Discover nodes, select **All nodes**.
   - To update only the Discover nodes that match specific criteria, select **Matching nodes** and then type your search criteria, such as hostname or IP address.
5. Click **Upload**.

Run support packs on nodes

You can run a support pack on any node that is joined to a Command cluster.

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Activity section, click **Run Support Pack**.
3. In the Support Pack section, select from the following options:
   - To generate diagnostics from the system, select **Default Support Pack**.
   - To upload a support pack file, select **Upload Support Pack**, click **Choose File**, and navigate to a file.
4. In the Apply to section, select from the following options:
   - To apply your support pack selection to all Discover nodes, select **All nodes**.
   - To apply your support pack selection to only the Discover nodes that match specific criteria, select **Matching nodes** and then type your search criteria, such as hostname or IP address.
5. Click **Submit**.

View node information

1. View the following information about each node in the table:

   • **Host:** Hover over the node name to see more information about the node.

   • **Added:** Mouse over the date to see the full date and time the node was added to the cluster.

   • **Status:** Hover over the status symbol to see the current status and the date and time the node was last synced. The available statuses are: Online, Warning, Disabled, and Offline.

   • **License:** Hover over the status symbol to see the license status of the node. The available statuses are: Nominal, Expiring soon, License check pending, and Invalid.

   • **Time:** Hover over the time symbol to see the node time delta compared to the time of the Command appliance. The available deltas are: NTP synced, Large time delta from ECA, and NTP not configured.
2. Hover over the settings icon to edit the cluster node settings for that node, launch the shell, view the node in the Web UI, or view the node in the Admin UI.

Add a single node to a Command cluster

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Nodes section, click **Add Node**.
3. In the Add Cluster Node window, configure the following information:

   • Host**:** The name of the node.

   • Setup Password**:** The setup password for the node.

   • Product Key**:** The optional product key for the node firmware.

   • Nickname**:** A friendly name for the node. If no friendly name is entered, the host name will be used instead.

• (Optional) Reset Configuration**:** If you select this checkbox, existing node customizations such as device groups, alerts, and triggers will be removed. Gathered metrics such as captures and devices will not be removed.

4. Click **Save**.

Add multiple nodes to a Command cluster

1. Create a text file with the information on the nodes that you want to add to the cluster, one node per line, in the following format:

   ```
   <Host> <Password> <Product-key> <Nickname>
   ```

   Note: The `<Product-Key>` and `<Nickname>` values are optional.

2. In the ExtraHop Command Settings section, click **Nodes**.
3. In the Cluster Nodes section, click **Add Node**.
4. In the Add Cluster Node window, click **Add multiple nodes**.
5. In the Add Multiple Cluster Nodes window, perform one of the following steps:
   - Paste the contents of your text file into the Paste text file box.
   - Click **Upload text file**, then click **Choose File**. Navigate to your saved text file and click **Open**.
6. (Optional) Select or de-select Reset Configuration. If you select this checkbox, existing node customizations such as device groups, alerts, and triggers will be removed. Gathered metrics such as captures and devices will not be removed.
7. Click **Add Nodes**.

Delete a node from a Command cluster

You can delete one or more nodes from the cluster at a time.

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Nodes section, select the checkbox next to each node you want to delete.
3. Click the **Delete** button.
4. In the Delete Cluster Nodes dialog box, click **OK**.

Create a tag

You can add tags to your Command appliance to categorize your nodes. There are eight tag colors available and each color can be used multiple times with different labels. You must create a tag before you can apply it to a node.

For example, you might label all nodes on one datacenter by location, and then apply a tag with a single color to indicate the datacenter.

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Nodes section, click **Tags**.
3. Click **Add New Tag**.
4. In the Add Tag window, type the following information:

   • **Name:** The label you want displayed with the tag color.

   • **Color:** Click the radio button next to the color you want to use for this tag.

5. Click **Save**.

Edit a tag

You can edit both the text and color of an existing tag. The tag will remain applied to any nodes it was previously assigned to, but the color and label will be updated.

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Nodes section, click **Tags**.
3. Click **Edit Tag** next to the tag you want to edit.
4. In the Edit Tag window, rename the tag or select a different color.
5. Click **Save**.

Delete a tag

You can delete a tag at any time. It will be deleted from the tag list and removed from any nodes it had been applied to as soon as it is deleted.

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Nodes section, click **Tags** and click the **X** next to each tag that you want to delete.
3. Click **OK**.

Add a tag to a node

You can apply one or many tags to a node. You can also apply tags to multiple nodes at a time.

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Nodes section, select the checkbox next to each node that you want to tag.
3. Click **Tags** and select the checkbox next to each of the tags you want to apply to the selected nodes.
4. Click **Apply**.

License nodes through the Command appliance

1. In the Cluster Settings section, click **Nodes**.
2. In the Cluster Nodes section, select the checkbox next to each Discover node that you want to license.
3. Click **More**, and then select **License Register**.
4. In the Nodes License Registration dialog box, click **OK**.

Enable a node

Enabled nodes display a green status icon in the Cluster Nodes list.

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Nodes section, select the checkbox next to each node that you want to enable.
3. Click **More**, and then select **Enable Nodes**.
4. Click **OK**.

Disable a node

Disabled nodes display a blue status icon in the Cluster Nodes list.

1. In the ExtraHop Command Settings section, click **Nodes**.
2. In the Cluster Nodes section, select the checkbox next to each node that you want to disable.
3. Click **More**, and then select **Disable Nodes**.
4. Click **OK**.

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.

Change the default password

It is recommended that you change the default password on the ExtraHop appliance after you log in for the first time.

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

1. Log in to the ExtraHop Admin UI with the default login name and password.
2. Click **Change default password**, which is located at the top of the page.
3. In the New password field, type the new password.
4. In the Confirm password field, type the same password again.
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 Discover appliance and to provide Atlas Services remote analysis reports.

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 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 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 appliance, this step is unnecessary.
3. Click **Disable Support Account**.

Enable the Atlas Remote UI account

This account enables the ExtraHop support team to provide Atlas Services remote analysis reports.

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. For more information, see the Remote Authentication section.

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

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). The default password for this account is the service tag number on the right-front bracket of the ExtraHop appliance.

shell

The `shell` account provides full system read and write privileges on the Web UI, Admin UI, and Shell, which is the ExtraHop command-line interface (CLI). This account only permits access to non-administrative shell commands. When accessing the privileged system configuration shell commands, the user types in enable and authenticates with the setup user password. The default password for this account is the service tag number on the right-front bracket of the ExtraHop appliance.

admin

The `admin` account provides full system read and write privileges on the ExtraHop Web UI. The default password for this account is `admin`.

operator

The `operator` account provides limited system write privileges on the ExtraHop Web UI. This account is disabled by default and is not configured with a password. But you can enable this account, assign a password, and select the appropriate privileges for this user.

readonly

The `readonly` account provides limited system read-only privileges on the ExtraHop Web UI. This account does not have a preset password, so a password needs to be set manually prior to use.

Add a user account

1. In the Access Settings section, click **Users**.
2. Click **Add User**.
3. On the Add New User page, 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**:**

   • Confirm Password**:** Re-type the password from the previous field.
4. In the Permissions section, select the desired permission for the user, and then select **Enabled**.

   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 user name that you want to modify.
3. On the Update User page, modify the permissions or change the full name of the user.

   Note: On a Command appliance, select **Cluster Node UI Privileges** to grant the user access to specific clusters and nodes as permitted by LDAP settings.
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.

User permissions

An administrator can grant users the following permissions.

Permission	Description
Full System Privileges	• Create and modify objects such as alerts, triggers, device groups, and custom pages. • Create, modify, organize, and share dashboards. • View dashboards and metrics. • 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. • Access system configuration commands in the ExtraHop command-line interface (CLI) by securing the `enable` command.
Full Write Privileges	• View dashboards and metrics. • Create and modify objects such as alerts, triggers, device groups and custom pages. • Create, modify, organize, and share dashboards.
Limited Write Privileges	• View dashboards and metrics. • Create, modify, organize, and share dashboards.
Read-Only Privileges	• View dashboards and metrics.
No privileges (Admin UI)	• Cannot log into the Command applianceAdmin UI.
No privileges (Web UI)	• Cannot log into the Web UI on the Command appliance.
Cluster Node UI Privileges	• View connected Discover appliances in the Command appliance Admin 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.

View active sessions

In the Access Settings section, click **Sessions**.

Delete an active session

You can delete active sessions individually or all at once. When you delete an active session, the session is terminated for the user and they must log in again to access the web interface.

1. In the Access Settings section, click **Sessions**.
2. Click the red **X** next to the session you want to delete, or click **Delete All** to delete all active sessions.
3. Click **OK**.

Remote authentication

ExtraHop appliances supports remote authentication for user authentication. It 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 using 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 use remote authentication, you must have a remote server with one of the following configurations:

- LDAP (such as OpenLDAP or Active Directory)
- RADIUS
- TACACS+

Administrators can grant access to all known users or restrict access by using LDAP filters.

LDAP

The ExtraHop appliance supports the Lightweight Directory Access Protocol (LDAP) for authentication and authorization. Users whose credentials are not stored locally can be authenticated against a remote LDAP server through their username and password.

You can assign privileges to LDAP users based on their group memberships on the LDAP server; you can also automatically assign Read-only or Full Write access to all users that exist on the LDAP server. When a user attempts to log onto the Web UI, the ExtraHop appliance processes the request through the following methods:

1. Authenticate the user locally.
2. If the user does not exist locally, authenticate the user through the LDAP server with the specified username and password. The LDAP password is not stored locally on the ExtraHop appliance.

Next, if the appliance is configured to assign privileges from the LDAP server, the appliance assigns privileges to the user based on the groups that the user belongs to on the LDAP server, such as Read-only or Full Write.

Note: Any user that exists both locally and on a remote LDAP server cannot authenticate until one of the two entries is deleted.

Configure LDAP authentication

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, type the following information:

Hostname

Specifies the hostname or IP address of the LDAP server. Make sure that the DNS of the ExtraHop appliance is properly configured if you use a hostname.

Port

Specifies the port on which the LDAP server is listening. Port 389 is the standard cleartext LDAP server port. Port 636 is the standard port for secure LDAP (ldaps/tls ldap).

Base DN

Specifies the base of the LDAP search used to find 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. Consult your LDAP administrator to learn what your organization uses.

- Active directory canonical name: `example.com/people`
- LDAP base DN: `ou=people,dc=example,dc=com`

Server Type

Specifies the type of LDAP server. Select **Posix** or **Active Direcrory**.

Search Filter

Specifies the criteria used when searching the LDAP directory for user accounts. Examples include:

```
objectclass=person
objectclass=*
&(objectclass=person)(ou=webadmins)
```

A search filter of `objectclass=*` matches all entities and is the default wildcard.

Search Scope

Specifies the scope of the directory search when looking for user entities. Select one of the following options:

- **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`.
- **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`.

Bind DN

Specifies the Distinguished Name (DN) used by the ExtraHop appliance 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. To verify whether anonymous binds are enabled, contact your LDAP administrator. Using the active directory canonical name `example.com/people`, Bind DN examples include: `cn=admin, ou=users, dc=example,dc=com` `uid=nobody,ou=people,dc=example,dc=com`

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

Bind Password

Specifies the password used when authenticating with the LDAP server as the bind DN specified above. If you are using 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.

Encryption

Specifies if encryption should be used when making LDAP requests. Options include:

- **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.)

4. 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.
5. Click **Save and Continue**.
6. Determine whether you want to do local or remote authentication.
   a) Local authorization: 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**. You can add read-write permissions on a per-user basis later through the Users page in the Admin UI.
   b) Remote authorization: You might also choose to obtain a permissions level from a remote server. When you select the **Obtain permissions level from remote server** option, you must complete at least one of the following fields to specify the remote permissions:

      - Full Access DN
      - Read-Write DN
      - Limited DN
      - Read-Only 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`
7. Click **Save and Finish**.
8. Click **Done**.

For example, given the base DN:

```
ou=seattle,ou=washington,dc=usa,dc=example,dc=com
```

and the bind DN:

```
cn=ehaccess,ou=admins,ou=seattle,ou=Washington,dc=usa,dc=example,dc=com
```

and the Search Scope set to `Whole Subtree`, any user account in the `usa.example.com` domain that is a member of:

```
cn=extrahop-
readonly,ou=groups,ou=seattle,ou=washington,dc=usa,dc=example,dc=com
```

and is nested within:

```
ou=seattle,ou=washington,dc=usa,dc=example,dc=com
```

would have read-only access on the ExtraHop appliance.

The following example shows accounts with access:

```
cn=JDoe,ou=users,ou=seattle,ou=Washington,dc=usa,dc=example,dc=com
                cn=admin,ou=seattle,ou=washington,dc=usa,dc=example,dc=com
```

The following example shows accounts without access:

```
cn=JaneD,ou=users,dc=usa,dc=example,dc=com
                cn=Administrator,dc=usa,dc=example,dc=com
```

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. In the Methods section, 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 use 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 will wait for a response from the RADIUS server before it attempts to connect again.
4. Click **Add Server**.
5. Repeat steps 2, 3, and 4 to add multiple servers, if 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. Click **Save and Finish**.
9. 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 use 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 will wait for a response from the TACACS+ server before it attempts to connect again.

4. Click **Add Server**.
5. Repeat steps 2, 3, and 4 to add multiple servers, if needed.
6. Click **Continue**.
7. Determine whether you want to do local or remote authentication.
   a) Local Authorization: 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**.
   b) Remote Authorization: On the TACACS+ server, set up the ExtraHop service by adding the `attributeservice=extrahop` and setting one of the following permissions.

- `readonly=1`
- `readwrite=1`
- `limited=1`
- `setup=1`

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

8. Click **Save and Finish**.
9. 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 Discover 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 User Generated API Keys**: Local and remote users can generate API keys.
   - **Local Users Only**: Only local users can generate API keys.
   - **No API Keys Allowed**: API keys cannot be generated.
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

You can delete an API key from the ExtraHop appliance.

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	Functionality
Full System Privileges	• Users can enable or disable API key generation for the ExtraHop appliance • Users can delete API keys for any user • Users can perform any operation available through the REST API • Users can view the last four digits and description for any API key on the system
Full Write Privileges	• Users can generate an API key • Users can view or delete their own API key • Users can perform any configuration task through the REST API that is available for the ExtraHop Web UI • Users cannot perform any administration task through the REST API that is available for the ExtraHop Admin UI
Limited Write Privileges	• Users can generate an API key • Users can view or delete their own API key • Users can modify personal customizations (such as a personal dashboard) through the REST API that is available for the ExtraHop Web UI • Users cannot perform any configuration task that might affect other users in the system

Permission level	Functionality
	• Users cannot perform any administration task through the REST API that is available for the ExtraHop Admin UI
Read-Only Privileges	• Users can generate an API key • Users can view or delete their own API key • Users can perform limited GET operations through the REST API for the ExtraHop Web UI

System configuration

This section contains ExtraHop appliance configuration settings that can be changed through the Admin UI.

Running Config

Download and modify the running configuration file.

Geomap Datasource

Modify the information in geomaps.

Datastore and Customizations

Reset the datastore and modify customizations.

Open Data Streams

Send log data to another system.

Capture

Configure the network capture settings.

Trends

Reset all trends and trend-based alerts.

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.

For example, if you make a change to a protocol classification setting on the Protocol Classification page, the change (in memory) takes effect immediately, but it does not permanently change the running

configuration until you save the changes. 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 **System Configuration** > **Running Config**.
2. Click **Running Config** > **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 **System Configuration** > **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.

To download the current running configuration settings as a text file:

1. Click **System Configuration** > **Running Config**.
2. Click **Download config as a File**.

The current running configuration will be downloaded as a text file to your browser's default download location.

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** rado button, then click **Choose File** to upload a database in .dat 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.

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.

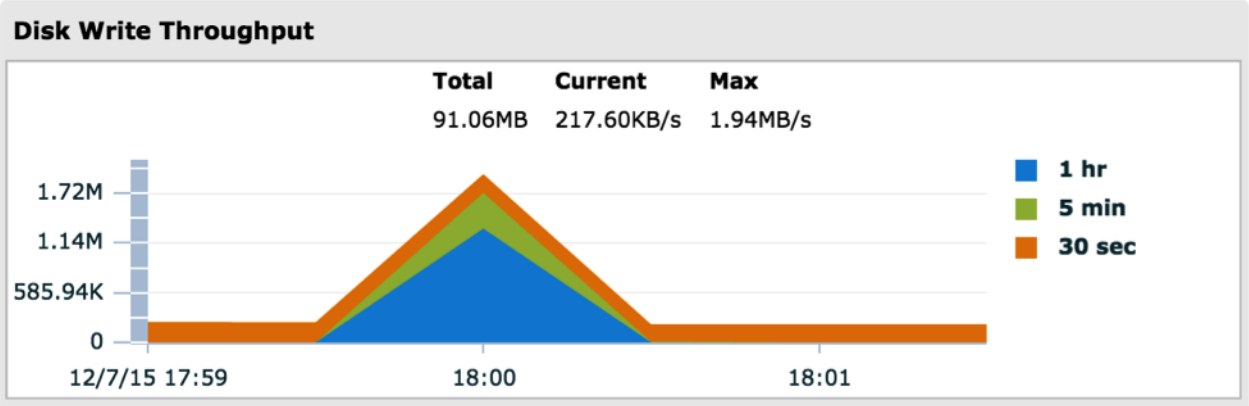
The following procedure shows you how to determine the write performance that will be required from the NAS device hosting the extended data store.

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.

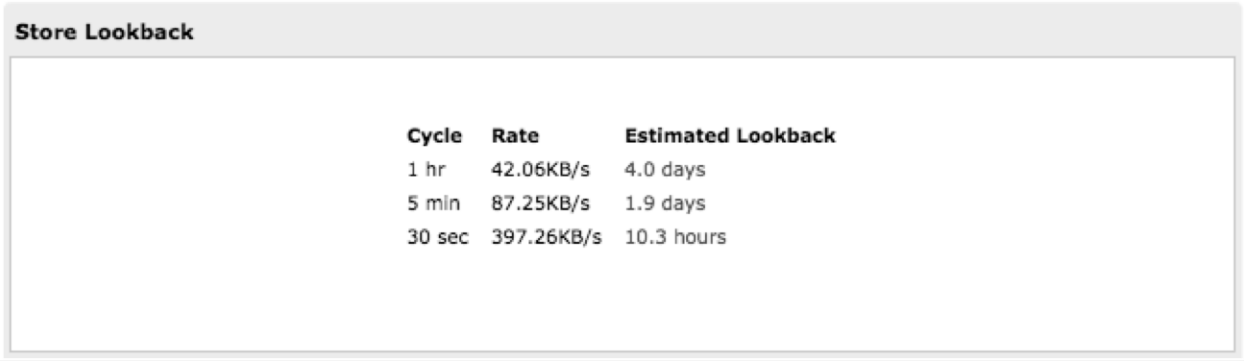
Extended datastore sizing guidelines

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. Under System Configuration, 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.

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**.

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: The first target of each type is named `default`; you cannot change this setting. 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 the ExtraHop Trigger API Reference.

Configure 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. Enter the following information:

   Name

   A name to identify this configuration.

   Note: The configuration you create is automatically titled `default` and cannot be renamed.

   Host

   The hostname or IP address of your syslog server.

   Port

   The port number to connect to on your syslog server. By default, the port is set to `514`.

   Protocol

   From the drop-down, select the protocol you want to send syslog information through.

   Local Time

   Select this checkbox if you want to send syslog information with timestamps in the local time zone of the ExtraHop appliance. If this option is not selected, timestamps are sent in GMT.
5. Click **Save**.

Next steps

After you configure an ODS for Syslog, 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* section of the ExtraHop Trigger API Reference.

Configure 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. Enter the following information:

   Name

   A name to identify this configuration.

   Note: The configuration you create is automatically titled `default` and cannot be renamed.

Host

The hostname or IP address of the remote MongoDB server.

Port

The port number of your remote MongoDB server. By default, the port is set to `27017`.

SSL/TLS Encryption

Specifies whether data is encrypted.

5. (Optional) In the User Details section, enter the following information for a user who has permissions to write to the MongoDB server and click **Add User**:

Database

The name of the MongoDB database to send data to.

Username

The MongoDB username that will write to the database.

Password

The password of the MongoDB user.

6. Click **Save**.

Next steps

After you configure an ODS for MongoDB, 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.MongDB* section of the ExtraHop Trigger API Reference.

Configure 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. Enter the following information:

Name

A name to identify this configuration.

Note: The configuration you create is automatically titled `default` and cannot be renamed.

Host

The hostname or IP address of the remote server.

Port

The port number of your server.

Type

The type of protocol to send information through.

Pipeline Requests

Specifies whether HTTP pipelining to improve performance is enabled.

Additional HTTP Header

An additional HTTP header to include.

5. (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 AWS.
Microsoft Azure	Authenticates through Microsoft Azure.

6. (Optional) Specify the test configuration.

   You can configure the HTTP requests that the Discover appliance will send to the HTTP server to test the connection between the appliance and the server.

   Method

   The HTTP method.

   Options

   path

   The path that the HTTP request will be applied to.

   payload

   The payload of the HTTP request.

   headers

   The headers of the HTTP request.

   Note: You must specify headers as an array, even if you specify only one header. For example:

   ```
   "headers": {"content-type":["application/json"]},
   ```

7. Click **Save**.

Next steps

After you configure an ODS for HTTP, 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* section of the ExtraHop Trigger API Reference.

Configure 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. Enter the following information:

   Name

   A name to identify this configuration.

   Note: The configuration you create is automatically titled `default` and cannot be renamed.

   Compression

   A compression method.

   Partition Strategy

   A partition strategy.

   Brokers

   Kafka brokers.

Note: You must add at least one broker but 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.

Host

The hostname or IP address of your Kafka broker.

Port

The port of your Kafka broker.

5. Click **Save**.

Next steps

After you configure an ODS for Kafka, 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* section of the ExtraHop Trigger API Reference.

Configure 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 Data Stream Configuration section, configure the following information:

Name

A name to identify this configuration.

Note: The configuration you create is automatically titled `default` and cannot be renamed.

Host

The hostname or IP address of the remote server.

Port

The port number for the remote server.

Protocol

TCP or UDP.

5. To enable gzip compression, select the **GZIP** checkbox and type one of the following values to specify when the data is compressed and sent to the target server.

Option	Description
Number of bytes after which to refresh gzip	Type the number of bytes.
Number of seconds after which to refresh gzip	Type the number of seconds.

6. Click **Save**.

Next steps

After you configure an ODS for raw data, 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* section of 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.

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 when using 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 using 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 when using 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 when using the Command appliance.

Exclude MAC addresses

1. Click **System Configuration** > **Capture**.
2. Click **MAC Address Filters**.
3. Click **Add Filter**.
4. On the MAC Address Filters page, enter the following information for the MAC address or set of addresses you want to exclude:

   Note: You cannot use both filters at the same time. Use `MAC Address` to provide a specific MAC address to match and filter. Use `Mask` to provide a MAC address mask to filter ranges or sets of MAC addresses.

MAC Address

The MAC address to exclude. Enter an individual MAC address here if you want to filter an exact match.

Mask

The mask to use to filter non-exact match addresses.

5. Click **Add**.

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 when using 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 when using 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 reinclude.
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 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

By default, all IP addresses outside the locally-monitored broadcast domains are aggregated at one of the incoming routers. To identify the devices behind these routers, you can use the pseudo devices settings in the capture to enable reporting on these devices.

Note: Custom devices in version 4.0 and later take the place of pseudo devices. Unlike pseudo devices, you do not need Administrator privileges to configure custom devices. If you have previously created pseudo devices, they will remain on your ExtraHop appliance until you migrate them to custom devices. For more information, go to the ExtraHop Web UI, click **Help**, and refer to the ExtraHop Web UI Guide.

Note: Capture settings are not configurable when using 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 that use 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
CIFS	CIFS	TCP	0	139, 445
DB2	DB2	TCP	0	50000, 60000
Diameter	AAA	TCP	0	3868
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
LDAP	LDAP	TCP	0	389, 390
LLDP	LLDP	Link Level	N/A	N/A
Memcache	Memcache	TCP	0	11210, 11211

Canonical Name	Protocol Name	Transport	Default Source Port	Default Destination Port
MongoDB	MongoDB	TCP	0	27017
MS SQL Server	TDS	TCP	0	1433
MSRPC	MSRPC	TCP	0	135
MySQL	MySQL	TCP	0	3306
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
SIP	SIP	TCP	0	5060, 5061
SMPP	SMPP	TCP	0	2775
SMTP	SMTP	TCP	0	25
Sybase	Sybase	TCP	0	10200
SybaseIQ	SybaseIQ	TCP	0	2638

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. Click **System Configuration** > **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

   Check this checkbox if you want the classifier to attempt to categorize the connection without seeing the connection open. ExtraHop recommends using 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 by IP address

The ExtraHop appliance analyzes its incoming data feed to identify the devices that are communicating on the monitored network. This identification process is known as device discovery.

You can configure the ExtraHop appliance to approach device discovery in one of two ways:

- Discovery by L3, or IP address (Default)
- Discovery by L2, or MAC address

L3 discovery mode

In the default L3 discovery mode, the ExtraHop appliance recognizes a new device for each observed IP address that meets the following criteria:

- A device responds to an Address Resolution Protocol (ARP) request for the IP address, allowing the ExtraHop appliance to associate the IP address with an L2 (MAC) address.
- The associated MAC address is not the MAC address of an L3-routing device. The ExtraHop appliance uses heuristics for determining whether traffic having a particular MAC is a routing device.

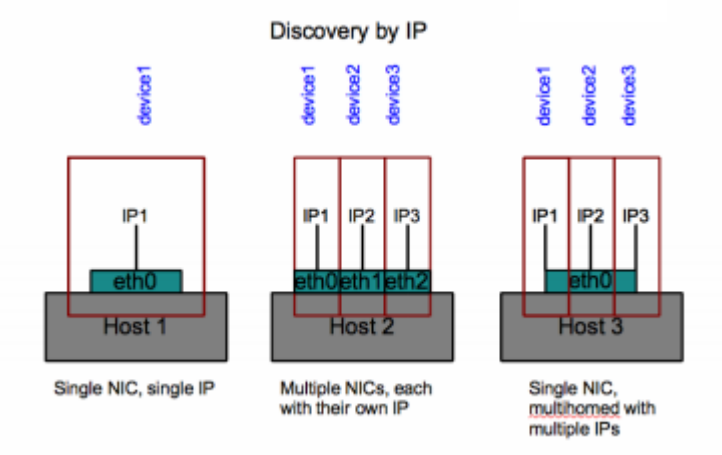
In cases where multiple IP addresses meet the above criteria while sharing a MAC address (e.g., multi-homed NICs), each IP is discovered as a separate device.

When L3 discovery mode is used, in addition to the discovered =L3 Devices, the ExtraHop appliance also creates L2 Devices for each unique MAC address. The following characteristics apply to these L2 devices:

- When an L2 and L3 address are associated with the same device, a parent-child relationship is shown in the detail page for each device.
- Any L2 traffic metrics that cannot be associated with a particular child L3 device (for example, L2 broadcast traffic) are associated with the parent L2 device.
- In the device list view, you can filter the full device list for L2 devices only, L3 devices only, or all devices.
- L2 devices that exist solely as parents to L3 devices do not count against licensed device count limits.

IP addresses in the data feed that do not appear to have an associated MAC address are generally located remotely beyond an L3-routing device and are not auto-discovered. However, discovery of a new device can be forced in the Remote Networkssection.

The following diagram shows L3 device discovery in three common server NIC configurations.



L3 discovery on remote networks

Remote networks are subnets visible to ExtraHop only via L3-routing devices. By default, the ExtraHop appliance does not discover and monitor devices on these networks. Adding these networks in the Remote Networks section configures the ExtraHop appliance to treat individual devices on remote networks as if they were part of the local network.

The following scenarios use the remote networks setting to discover devices:

- An organization has a remote office without an on-site ExtraHop appliance but users at that site access central datacenter 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 remote applications and has a known IP address range. The remote servers within this IP range can be individually tracked.

In the ExtraHop Administration UI, remote networks are designated by network addresses specified in CIDR notation (network IP address / subnet prefix length). For example, for IPv4 networks, the network identifier is written as `192.168.0.0/16`. For IPv6 networks, the network identifier is written as `2001:db8::/32`.

The following characteristics apply to remote network discovery:

- The **Local Network** checkbox must be checked on the Discover by IP page to make remote networks available.
- Remote networks are configured manually so the ExtraHop appliance does not require ARP traffic for their discovery.
- Every actively communicating remote IP that matches a remote network's CIDR block will result in the discovery of one device in the ExtraHop appliance. Specifying wide subnet prefixes such as /16 might result in the discovery of a large number of devices. A /32 subnet prefix might be used to match a single remote IP.
- Devices discovered by remote networks discovery count against licensed device count limits.

The following limitations apply to remote network discovery:

- Private IP addresses, such as those on a private subnet (behind a router) or those that are behind a NAT device, are not visible. Only the public-facing IP addresses are discovered and visible in the ExtraHop appliance.
- L2 information, such as the device's 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 it is not visible to the ExtraHop appliance.

L2 discovery mode
You can also configure the ExtraHop appliance to discover devices using L2 discovery mode. In this mode, instead of an IP address acting as the basis for defining a new device, a MAC address is used. All IP addresses associated with a given MAC address are aggregated into a single device.

L2 discovery mode was once the default, but it is no longer common. If you feel that your ExtraHop deployment might benefit from the use of L2 discovery mode, contact ExtraHop Support at support@extrahop.com for further assistance.

Configure the Discovery mode
To select the discovery mode and optionally configure remote network discovery:

1. Click **System Configuration** > **Capture**.
2. Click **Discover by IP**.
3. On the Discover by IP page, in the Local Network section, do one of the following:
   - Check the **Enable** checkbox to turn on device discovery by IP address (L3 discovery).
   - Deselect the **Enable** checkbox to turn on device discovery by MAC address (L2 discovery).
4. To configure remote network discovery, in the Remote Networks field, specify the remote network address in CIDR format and click **Add**.
5. Click **Save and Restart Capture**.
6. Click **Done**.

   ExtraHop recommends performing a datastore reset after enabling or disabling Discover by IP. Clearing the datastore protects against potential problems, such as redundant data.

SSL decryption

The ExtraHop appliance supports real-time decryption of SSL traffic for analysis. To use this feature, private keys associated with the SSL server certificate must be provided. 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 with a ciphersuite, or you can add 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.

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 using 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, use a utility 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.

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.

For a list of client libraries, refer to http://code.google.com/p/memcached/wiki/Clients.

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
   ```

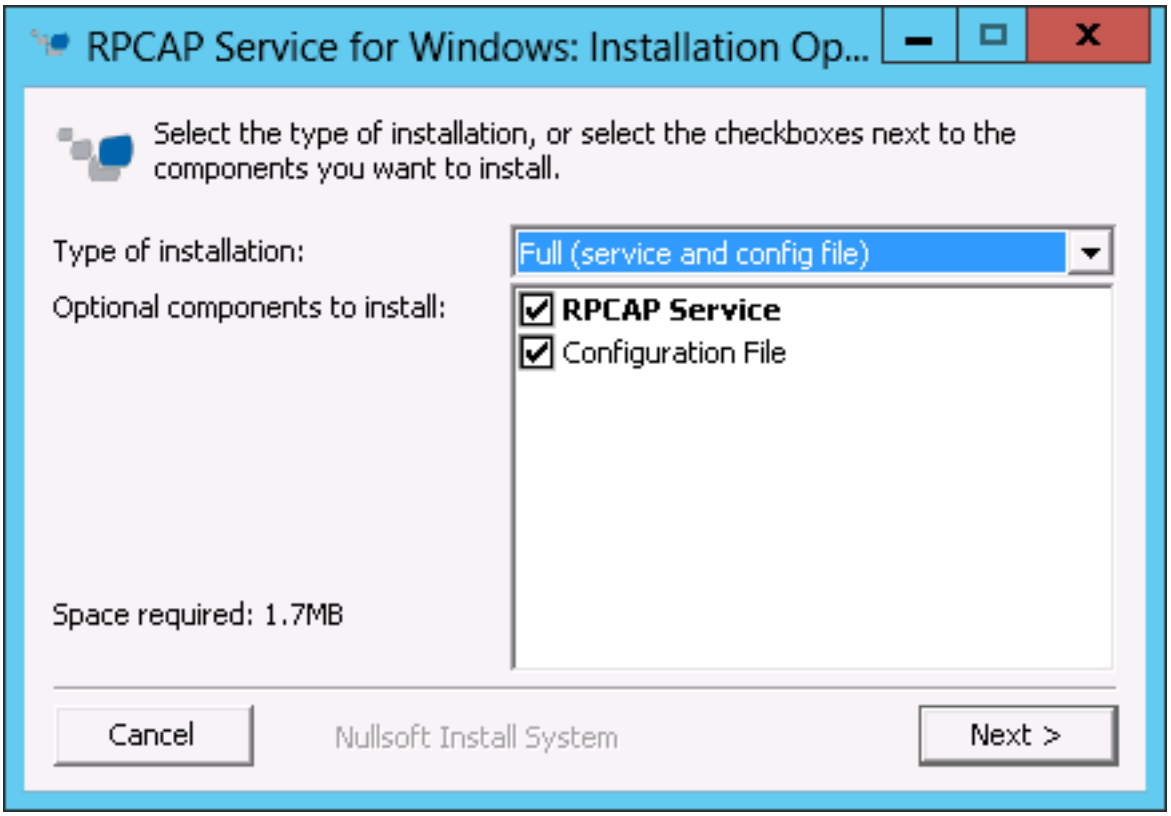
5. (Optional) To change the ExtraHop IP address, port number, or arguments to the service, run the following command.

```
sudo dpkg-reconfigure rpcapd
```

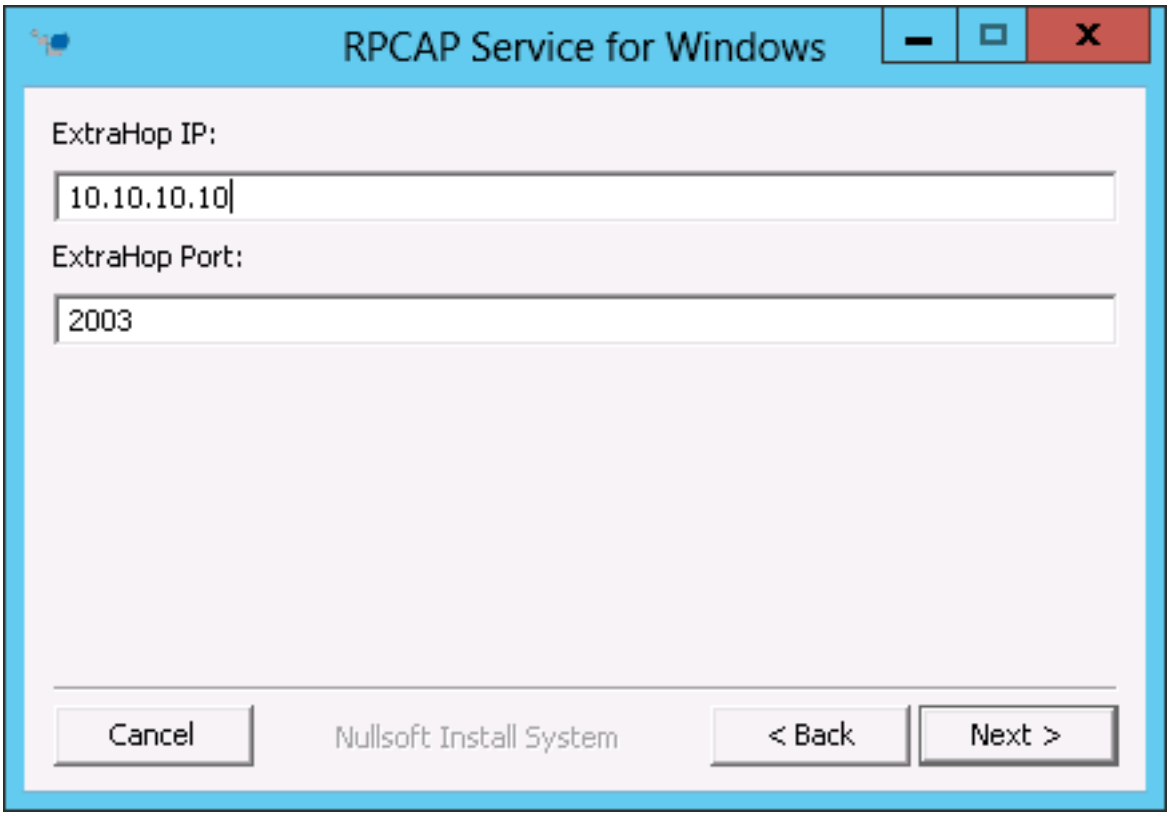
Install the software tap on a Windows server

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

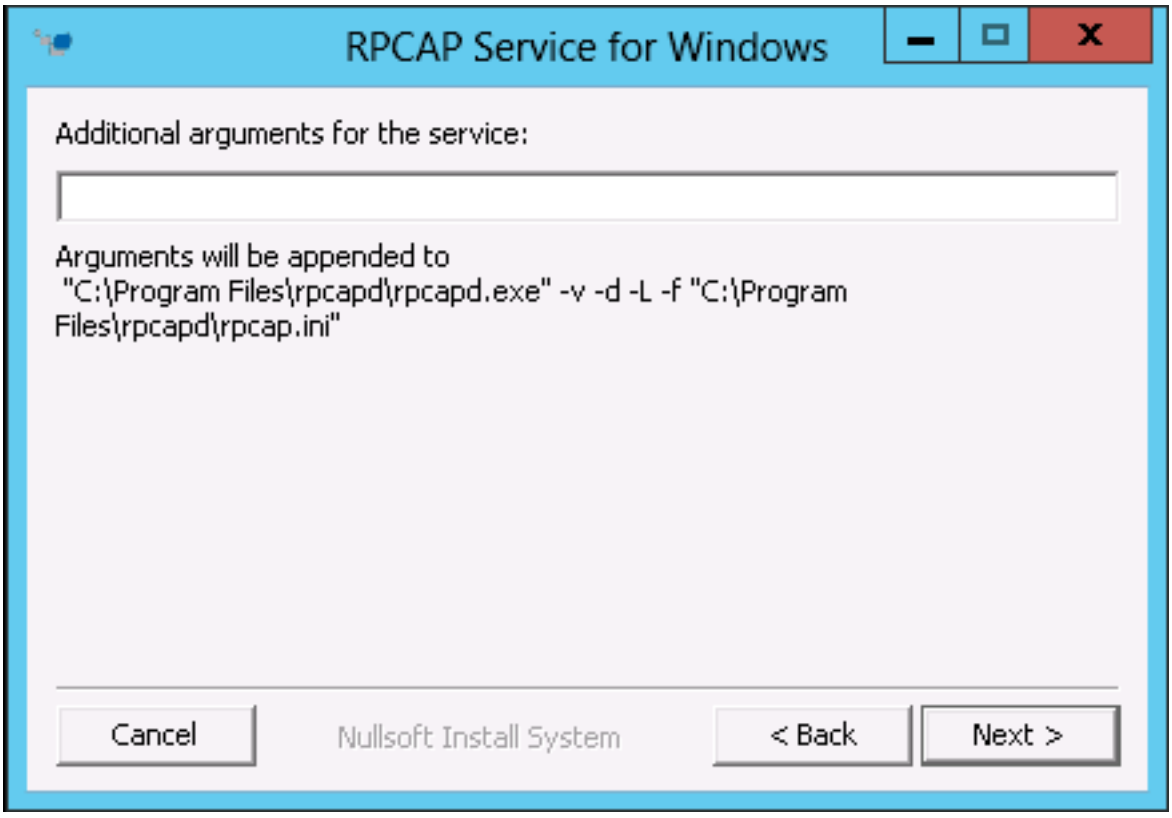
1. Go to `https://<extrahop_ip_address>/admin/capture/rpcapd/windows/` to download the RPCAP Service for Windows installer file.
2. When the file is finished downloading, double-click the file to start the installer.
3. In the wizard, select the components to install.



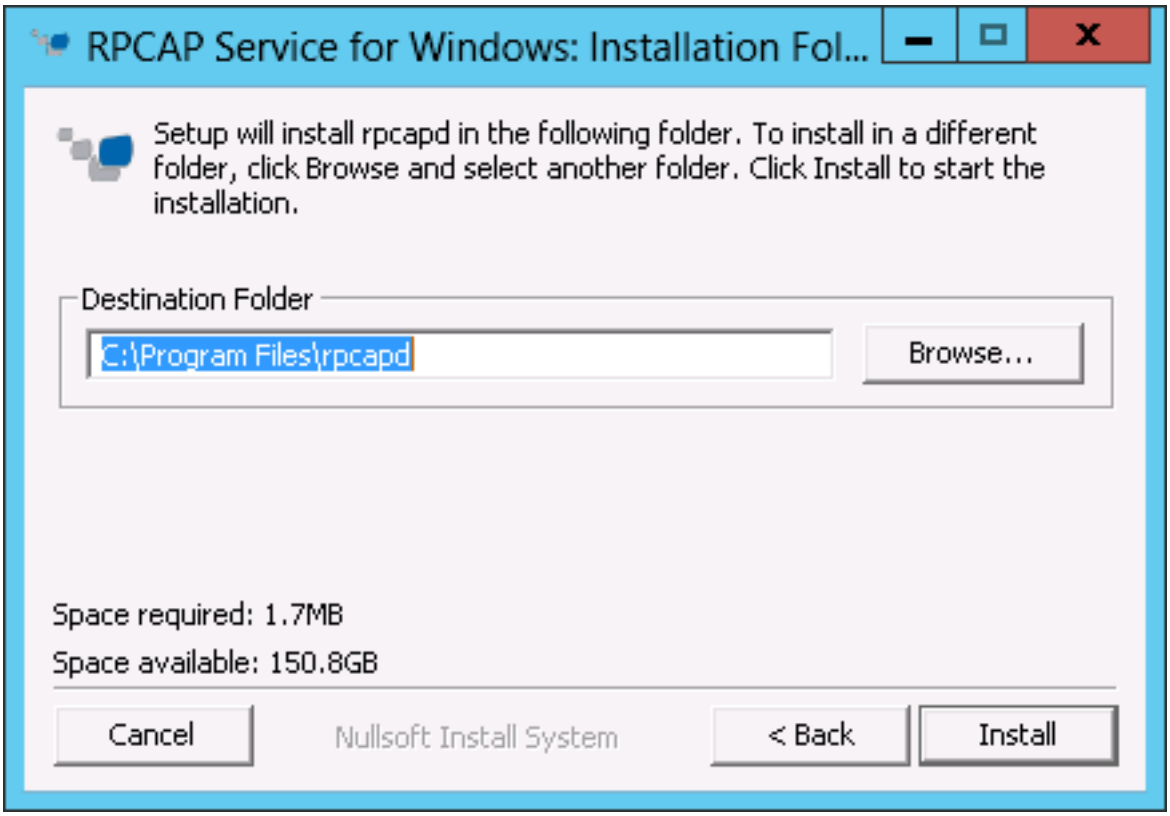
4. Complete the **ExtraHop IP** and **ExtraHop Port** fields and click **Next**. The default port is 2003.



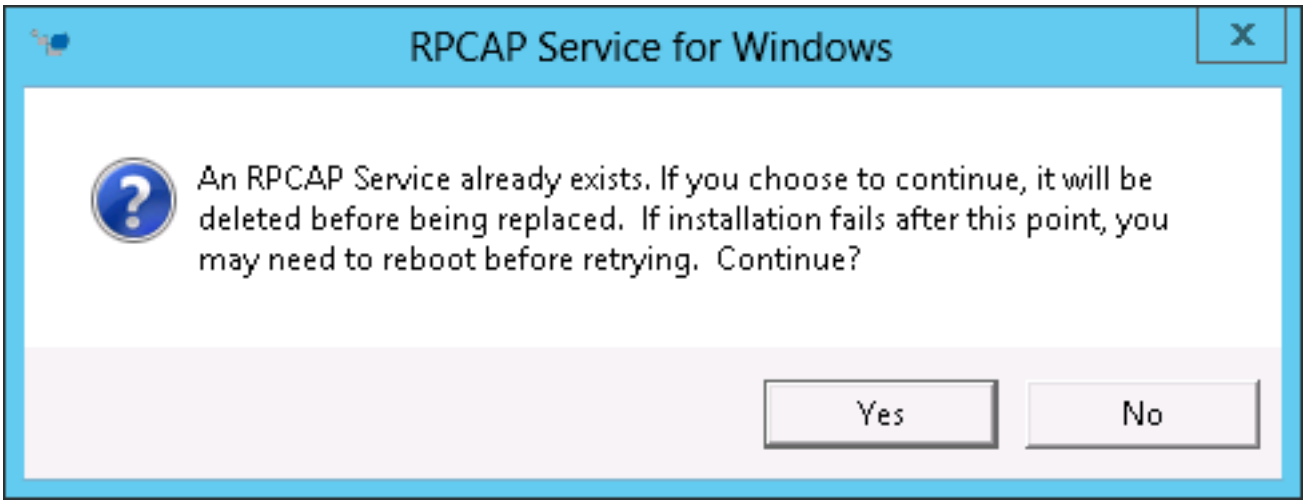
5. (Optional) Enter additional arguments in the text box and click **Next**.



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**.

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.

ExtraHop Explore settings

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

Configure Explore Cluster

Specify an Explore appliance to store flow and transaction records.

Automatic Flow Record Settings:

Specify the automatic flow record settings.

ExtraHop Explore Status

View information about the Explore cluster status.

Configure an Explore cluster

When you deploy an Explore cluster in your environment, you must establish a connection from an ExtraHop Discover appliance or Command appliance to the Explore cluster before you can query records.

To pair a Discover appliance or Command appliance to an Explore cluster:

1. Click on **ExtraHop Explore Settings** > **Configure Explore Cluster**.
2. Click **Add New**.
3. In the Host #1 Host field, type the hostname or IP address of any Explore appliance in the Explore cluster.
4. For each additional Explore appliance in the cluster, click **Add New** and enter the unique hostname or IP address in the corresponding Host field.
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 (**Host #1**) listed on the **Status** > **Fingerprint** page in the Explore Admin UI.
7. In the Explore Setup Password field, type the password of the Explore appliance.
8. Click **Join**, and then click **Done**.

Automatic flow records

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.

Enabled

Enable or disable the generation of flow records.

Publish Interval (in seconds)

Specify the number of seconds after which a flow record is sent to the Explore appliance if the flow is still active. The minimum value is 60 and the maximum value is 21600.

IP Addresses

Add IP addresses to restrict flow record generation to specific devices.

Port Ranges

Add port numbers to restrict flow record generation to a single port or range of ports.

ExtraHop Explore appliance status

This 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.

System settings

You can configure the following components of the ExtraHop appliance in the System Settings section:

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 status times.

License

Update the license to enable add-on modules.

Schedule Reports

View a list of scheduled reports that are in the process of being generated.

Disk

View information about the disks in the ExtraHop appliance.

Note: If you are using the Command appliance, `Scheduled Reports` appears instead of `Disk`. The scheduled reports functionality allows you to view reports for troubleshooting purposes.

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 UI web 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 **System Settings** > **Services**.
2. Select or deselect 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 System Settings section, click **Services**.
   b) Select or deselect 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**.

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 **System Settings** > **Services**.
2. Select or deselect 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 **System Settings** > **Services**.

2. Select or deselect the **Web Shell** checkbox.
3. Click **Save**.

Firmware

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

The ExtraHop Admin UI includes the following firmware configuration settings:

Update

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.

Note: If you are upgrading an Command appliance, make sure to upgrade the Command appliance first and then upgrade the nodes. To function correctly, the Command appliance and nodes must use the same minor version of ExtraHop firmware.

Upload new firmware versions

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

1. Click **System Settings** > **Firmware**.
2. Click **Update**.
3. On the Update 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, deselect the **Automatically Restart** checkbox.
5. Click **Update**.

   The ExtraHop appliance initiates the firmware update. You can monitor the progress of the update with the Updating progress bar.
6. After the firmware update is installed successfully, the ExtraHop appliance displays the version number of the new firmware image. 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.

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 nodes.

1. Click **System Settings** > **Firmware**.
2. Click **Update**.
3. On the Update 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, deselect the **Automatically Restart** checkbox.
5. Click **Update**.

   The ExtraHop appliance initiates the firmware update. You can monitor the progress of the update with the Updating progress bar.
6. After the firmware update is installed successfully, the ExtraHop appliance displays the version number of the new firmware image. 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.
9. Update node firmware from a command appliance.
   a) On the Command appliance, click **Cluster Settings** > **Nodes**.
   b) Click **Update Firmware**.
   c) Upload firmware.
      - To select the `.tar` file on your workstation, click **Choose File**.
      - If you received a URL from ExtraHop Support, click the **Retrieve from URL** link.
   d) Click the **All nodes** radio button to update the firmware on all nodes, or click the **Matching nodes** radio button and enter search criteria to update specific nodes at a time.
   e) Click **Upload**.

Delete firmware versions

The ExtraHop appliance makes available every installed firmware image that has been uploaded on the system. For maintenance purposes, these uploaded firmware images can be deleted from the system to reduce the number of available versions.

To delete firmware images from the ExtraHop appliance:

1. Click **System Settings** > **Firmware**.
2. Click **Delete**.
3. On the Installed Firmware Images page, select the checkbox next to the firmware image that you want to delete.

   Note: You can select multiple versions.
4. If you want to delete all installed firmware images, select the **Check all** checkbox.

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

Update the firmware through the command-line interface

Follow these steps to update the firmware for the ExtraHop appliance through the ExtraHop command-line interface (CLI).

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 should be disabled.
   - Secure shell (SSH)

     Note: When changing the network settings, it is recommended that you use a serial cable or directly connected keyboard and monitor. This approach ensures that access to the ExtraHop appliance will not be disrupted if the settings are configured improperly.
2. Connect to the ExtraHop appliance.

   The `login` is shell and the password is the service tag number on the right-front bracket of the ExtraHop appliance.
3. Enable the administration controls.

   The password is the same as above.

   ```
   extrahop>enable
   ```
4. Enter configuration mode.

   ```
   extrahop#configure term
   ```
5. Download the firmware update using the FTP account credentials that you received from ExtraHop Support.

   ```
   extrahop(config)#download ftp://[login]:[password]@[FTP IP address]:/
   [firmware image]
   ```
6. The ExtraHop appliance downloads and applies the upgrade.

   ```
   Connecting to ipaddr ... connected.
   Logging in as login ... Logged in!
   ==> SYST ... done. ==> PWD ... done.
   ==> TYPE I ... done. ==> CWD not needed.
   ==> PASV ... done. ==> LIST ... done.
   [ <=> ] 1,591 --.-K/s in 0s
   ==> CWD not required.
   ==> PASV ... done. ==> RETR firmware-image-version ... done.
   Length: 10045440 (9.6M)
   100%[====================>] 10,045,440 --.-K/s in 0.09s
   FINISHED --2009-03-10 12:28:59--
   Downloaded: 2 files, 9.6M in 0.09s (112 MB/s)
   Applying update. Please wait...
   Update succeeded. Would you like to reboot now [Y/n]?:
   ```
7. Restart the ExtraHop appliance.
8. After the ExtraHop appliance restarts, verify the version by connecting to the CLI and running the show version command.

   ```
   extrahop>show version
   extrahop-1.0.7238
   ```

Note: The version number displayed should match the version of the firmware image you downloaded when you updated the Command appliance.

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 rely on setting time locally, or it can keep the system time accurate by using time servers. You can use the default time server setting, `pool.ntp.org`, or you can configure the system time manually.

To configure the system time:

1. Click **System Settings** > **System Time**.
2. Click **Configure Time**.
3. From the **Select time zone drop-down**, a time zone.
4. Click **Save and Continue**.
5. Select the **Use NTP server to set time** radio button, the click **Select**.
6. To set the NTP servers, enter the IP addresses for the time servers and click **Save**.
7. Click **Done**.

The default time server setting is `pool.ntp.org`.

The NTP Status table displays a list of NTP servers that are used to keep the system clock in sync. To sync a remote server to the current system time, 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 **System 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 **System 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 **System 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. Click **System Settings** > **Shutdown or Restart**.
2. On the Shutdown or Restart page, under Portal Status, click the **Restart**.
3. At the prompt, click **OK**.
4. Click **Done**.

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.

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.

Features

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

View the licensing system information

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

1. Click **System Settings** > **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. Click **System Settings** > **License**.
2. Click **Manage license**.
3. Click **Register** and wait for the licensing server to finish processing.
4. Click **Done**.

Update a module license or add new licenses

1. Click **System Settings** > **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 EDA 8000 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 (EDA 2000/3000/5000/6000/8000)
- Packet Capture (EDA 3000/6000/8000)
- Firmware (EDA 3000/6000/8000)

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

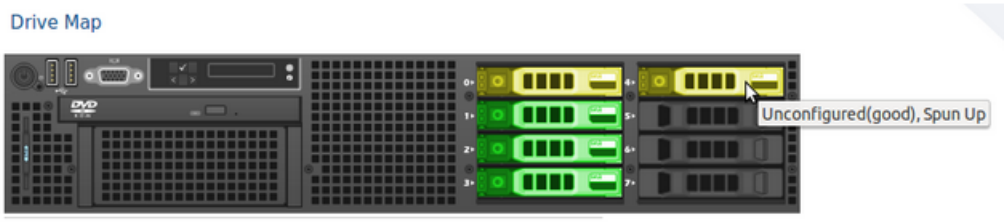
5000 appliance as an example. A persistently damaged disk might not be replaceable with this procedure.

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 System Settings, click **Disk**.
   - 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.

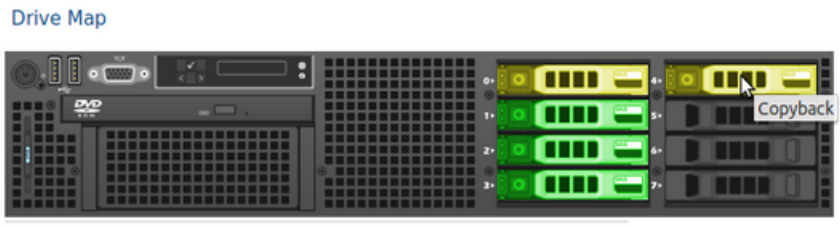
   Click **RAID Disk Details** to display more details.
4. Insert an identical disk into an available slot.

   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.

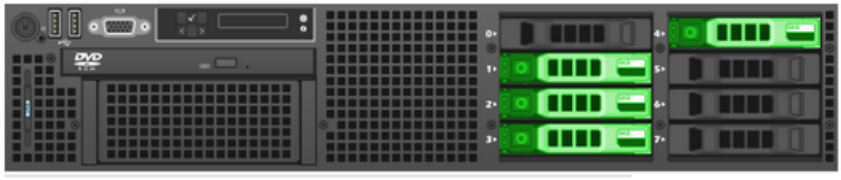
   The data begins copying over. The Copy Status row displays the progress. Mousing over the disk in the Drive Map shows the status.



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.

Drive Map



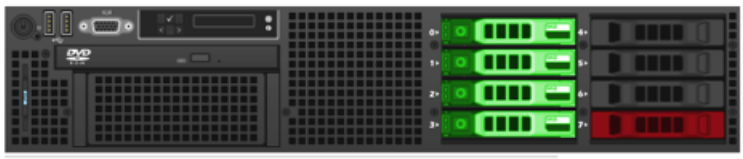
Install a new SSD drive

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

   For more information, refer to Packet Captures.
2. Go to the System Settings section and click **Disk**.

   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



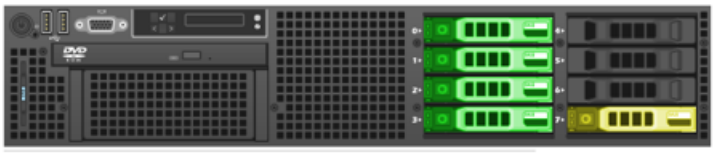
Physical Disk Info

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



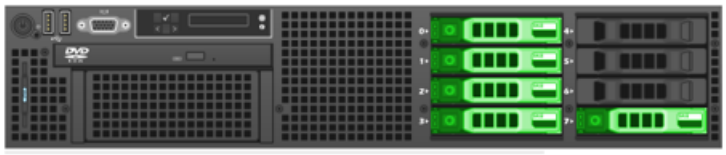
Physical Disk Info

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.

Scheduled reports (Command appliance)

This page displays a list of scheduled reports are in the process of being generated by the Command appliance. This list contains only reports that are presently being processed or were halted during generation due to an error, not reports to be processed in the future. Refer to this page if you stop receiving the scheduled reports that you created in the Reports section of the ExtraHop Web UI.

For more information about creating a report, refer to the Reports section of the ExtraHop Web UI Guide.

For more information about configuring email server settings and creating email groups, see the Notifications section.

To view scheduled reports:

1. In the ExtraHop Web UI, click **Settings**, click **Reports**, click a report, and click the **Email Schedule** tab to ensure the report has been scheduled.
2. In the Admin UI, click **System Settings** > **Scheduled Reports**.
3. View the list of reports.

   If the report was scheduled to be sent less than 10 minutes in the past, it might be in the process of generating. If the first report was scheduled to be sent more than 10 minutes in the past, an error might have occurred while generating the report and is delaying subsequent reports from being sent.
4. Click the red delete symbol next to the report to remove it from the list.

Note: If all reports are generating without errors, reports remain in the queue while they are generating and then leave the queue when sent. Reports typically remain in the queue for less than 1 minute.

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.

Diagnostics

The Diagnostics section includes the following pages:

Exception Files

Enable or disable the ExtraHop appliance exception files.

Support Packs

Upload and execute ExtraHop appliance support packages.

Offline Capture File

Configure the Discover appliance live (online) or offline capture mode. (Not available on a Command appliance.)

Enable writing to exception files

1. Click **Diagnostics** > **Exception Files**.
2. On the Enable/Disable Exception Files page, click **Enable Exception Files**.

Disable writing to exception files

1. Click **Diagnostics** > **Exception Files**.
2. On the Enable/Disable Exception Files page, 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.

View the diagnostic support packages

1. Click **Diagnostics** > **Support Packs**.
2. Click **View Support Pack Results**.

Download a selected diagnostic support package

1. Click **Diagnostics** > **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. Click **Diagnostics** > **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 support pack

1. Click **Diagnostics** > **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. Click **Diagnostics** > **Support Packs**.
2. Click **Run Default Support Pack**.
3. Click **OK**.

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.

Shell

The ExtraHop shell provides a command-line interface (CLI) for managing configuration settings in the ExtraHop appliance. The CLI can be used as a stand-alone interface, or as an supplemental interface that is accessible through the Admin UI.

Note: The CLI is used as the primary management interface when using the appliance's USB connection to attach a keyboard and monitor to the appliance itself, or when using the IDRAC interface that is available on the latest ExtraHop appliance models.

When the Admin UI is enabled and you are logged on, you can open the ExtraHop shell from the Admin UI application toolbar.

To open a shell window from the Admin UI, go to the top-level toolbar, click **Launch Shell**. The ExtraHop Web Shell opens in a separate browser window.

The command syntax includes the ExtraHop appliance hostname to specify the appliance that will process the commands. For example, the following enable command is executed on the ExtraHop appliance on the network that has a hostname of extrahop.

```
extrahop>enable
```

You can type a question mark (?) at any prompt to generate a list of available commands. For example, if you type `show ?` at the prompt, the CLI will list all supported show commands and provide a brief description of each command.

Note: The question mark (?) does not print in the CLI display, and you do not have to press the ENTER key after typing the question mark. The CLI displays the sub-commands (or parameters) associated with the current command.

Privileged and non-privileged modes

The CLI distinguishes between two user modes to determine the access privileges to specific commands:

Privileged

Has read-write privileges which provides access to all commands. In privileged mode, the elevated-privileged prompt is a hash symbol (#) instead of a greater than symbol (>).

Non-Privileged

Has read-only privileges which provides access to a limited set of commands. In non-privileged mode, the prompt is a greater than symbol (>).

Users that log on in non-privileged mode have access to the following four commands and their sub-commands:

enable

Enables privileged mode. When this command is executed, it prompts for a password to authorize privileged mode.

ping

Sends a ping request to a specified device.

show

Shows the ExtraHop appliance configuration settings in view-only mode.

traceroute

Sends a traceroute request to a specified device.

Users that enable privileged mode are granted access to all the CLI commands. The top-level commands that are enabled in privileged mode are:

configure
Enables configuration mode.

delete
Allows delete operations.

disable
Disables privileged mode.

enable
Enables privileged mode.

ping
Sends a ping request.

reload
Allows reload services operations.

reset
Allows reset services operations.

restart
Allows restart services operations.

show
Shows the current system configuration settings.

shutdown
Shuts down the ExtraHop appliance.

stop
Stops ExtraHop services.

support
Enables (or disables) the ExtraHop Support account.

traceroute
Sends a traceroute request.

Shell commands

The following shell commands are supported by the ExtraHop appliance. Note that you need to be in Privileged mode to execute commands that change ExtraHop appliance configuration settings.

configure

Puts the ExtraHop appliance into Configuration mode. After the configure command executes and the system is in Configuration mode, you can pass in any of the sub-commands listed below.

Syntax

```
extrahop#configure
```

Example

The following command sequence opens Configuration mode, enables the interface subcommands, sets a static IP address, DNS servers, and hostname for interface 2 on the ExtraHop appliance, and then exits Configuration mode:

```
extrahop#configure
extrahop(config)#interface 2
extrahop(config-if)#ip ipaddr <ipaddr> <netmask> <gateway>
extrahop(config-if)#ip dnsservers <ipaddr> <ipaddr 2>
extrahop(config-if)#ip hostname <name>
extrahop(config-if)#exit
extrahop(config)#exit
```

The configure command supports the following sub-commands:

current
Enables the user to change the firmware version to any version that is installed on the system. After specifying a new firmware version, the CLI will prompt you to reboot the ExtraHop appliance.

Syntax

```
extrahop#configure
extrahop(config)#current <version>
```

Parameters

version

Specifies the version number of the ExtraHop firmware that you want to upload as the current firmware on the ExtraHop appliance.

URI

Specifies the URI of a downloaded diagnostic script from ExtraHop Support to run on the ExtraHop appliance.

diagnostics
Downloads and executes a signed diagnostics script.

Syntax

```
extrahop#configure
extrahop(config)#diagnostics <URI>
```

Parameters

URI

URI. Specifies the URI of a downloaded diagnostic script from ExtraHop Support to run on the ExtraHop appliance.

disk_cleanup
Frees disk space by compressing and deleting large ExtraHop log files. It is not necessary to run this command unless instructed to do so by ExtraHop support. However, you can run this command at any time.

Syntax

```
extrahop#configure
```

```
extrahop(config)#disk_cleanup
```

dnsservers
Shows the DNS server configuration settings for the ExtraHop appliance.

Syntax

```
extrahop#show dnsservers
```

eula_reset
Reset the POC and EUSL/TOS license agreements. Note that this command is intended for use by ExtraHop Support only.

Syntax

```
extrahop#configure
extrahop(config)#eula_reset
```

hostname
Shows the system hostname for the ExtraHop appliance.

Syntax

```
extrahop#show hostname
```

install
Retrieves and uploads a firmware update from ExtraHop.

Syntax

```
extrahop#configure
extrahop(config)#install <uri>
```

Parameters

URI

Specifies the URI of a firmware update from ExtraHop Support that is uploaded to the ExtraHop appliance.

interface
Puts the CLI in Interface mode and provides sub-commands to specify how the ExtraHop appliance acquires an IP address and the hostname for the ExtraHop appliance.

Syntax

```
extrahop#configure
extrahop(config)#interface <interface-number>
extrahop(config-if)#ip ipaddr <addr> <netmask> <gateway>
Parameters
```

Note: You can specify the interface you want to configure by entering the interface number when running the `interface` command. If you do not specify an interface, the command will configure the primary management interface.

The `interface` command includes the following sub-commands and parameters:

ip dhcp

Configures the ExtraHop appliance to use the DHCP option.

ip dnsserver

Configures the system DHCP servers. This parameter requires the following values:

primary addr

Specifies the primary IP address of the DNS Server.

secondary addr

Specifies the secondary IP address of the DNS server. This parameter is optional.

ip hostname

Specifies the system hostname.

name

Specifies the hostname for the ExtraHop appliance.

ip ipaddr

Specifies the hostname for the ExtraHop appliance.

addr

A static IP address.

netmask

An address that specifies the subnet mask.

gateway

The IP address of the computer that is used by devices on the network to access another network or a public network.

ip6 dhcp

Enables IPv6 and configures the ExtraHop appliance to use the DHCPv6 option with IPv6.

Note: If enabled, DHCPv6 will be used to configure DNS settings.

ip6 disable

Disables IPv6.

ip6 ipaddr

Enables IPv6 and sets a static IPv6 address. If specified without an IPv6 address, clears all previously configured static IPv6 addresses.

ip6 ra_dns

Enables the appliance to configure Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) information according to router advertisements,

ip6 slaac

Enables IPv6 and configures Stateless Address Autoconfiguration for IPv6.

disabled

Disables Stateless Address Autoconfiguration.

hwaddr

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

stable_private

Configures the appliance to automatically assign private IPv6 addresses that are not based on hardware addresses. This method is described in RFC 7217.

license

Provides sub-commands to enter the license string to update the ExtraHop license. The license key text is sent by ExtraHop Support, and it is pasted into the CLI at the Enter license text prompt.

Syntax

```
extrahop#configure
extrahop(config)#license update
Enter license text: <license>
```

Parameters

The license command includes the following sub-commands and parameters:

update

Updates the ExtraHop appliance license. This parameter requires the following parameter values:

license

Specifies the license key.

reformat

Provides sub-commands to schedule or cancel a reformat.

Syntax

```
extrahop#configure
extrahop(config)#reformat
```

Parameters

The reformat command performs a reformat on the next boot and includes the following subcommand:

reformat cancel

Cancels the scheduled reformat.

remote_auth

Provides sub-commands to enable or disable remote authentication of users on the ExtraHop appliance. Note that the sub-commands `ldap`, `radius`, and `tacacs` put the CLI in the specific mode to accept parameters for the specified remote authentication method.

Syntax

```
extrahop#configure
extrahop(config)#remote_auth disabled
```

Parameters

The `remote_auth` command includes the following sub-commands and parameters:

disabled

Disables remote authentication.

ldap

Specifies configuration parameters to enable the LDAP remote authentication method. This command puts the CLI in `ldap` mode and requires the following parameter values:

basedn

Specifies the base of the LDAP search used to find users.

binddn

Specifies the Distinguished Name (DN) used by the ExtraHop appliance to authenticate with the LDAP server.

port

Specifies the listening port number of the LDAP server.

search

Specifies the search filter used when searching the LDAP directory for user accounts.

server

Specifies the hostname or IP address of the LDAP server (or servers).

show

Displays the current LDAP settings.

radius

Specifies configuration parameters to enable the RADIUS remote authentication method. This command puts the CLI in radius mode and requires requires the following parameter values:

delete_server

Deletes a specified RADIUS server host.

server

Specifies the hostname or IP address of the RADIUS server (or servers), the shared secret password, and an optional timeout value.

show

Displays the current RADIUS settings.

tacacs

Specifies configuration parameters to enable the TACACS remote authentication method. This command puts the CLI in tacacs mode and requires requires the following parameter values:

delete_server

Deletes a specified TACACS server host.

server

Specifies the hostname or IP address of the TACACS server (or servers), the shared secret password, and an optional timeout value.

show

Displays the current TACACS settings.

running_config

Provides commands to update the running configuration settings and save changes made to the running configuration to disk. The update command generates a prompt in the CLI to provide the updated configuration text. For more information about modifying the running config code, see the Running Config section.

Syntax

```
extrahop#configure
extrahop(config)#running_config edit
Enter configuration:
```

Parameters

The running_config command includes the following sub-commands and parameters:

edit

Provides an interface to make changes to sections of the running configuration.

update

Provides an interface to make changes to the entire running configuration. You are prompted to enter the running config text by the CLI.

save

Saves the changes made to the running configuration to disk.

revert

Reverts to the saved running configuration.

services

Provides commands to enable or disable the Admin UI, enable or disable the SSH service that supports the CLI interface, and enable or disable SNMP services.

Syntax

```
extrahop#configure
extrahop(config)#services gui <enable/disable>
```

The `services` command includes the following sub-commands and parameters:

gui

Enables or disables the web service that supports the Admin UI. This command supports the parameter values `enable` to turn on the service and `disable` to turn off the service.

snmp

Enables or disables the SNMP service that supports SNMP monitoring. This command supports the parameter values `enable` to turn on the service and `disable` to turn off the service.

ssh

Enables or disables the SSH service that supports the command-line interface. This command supports the parameter values `enable` to turn on the service and `disable` to turn off the service.

systemsettings

Provides commands to work with core files.

Syntax

```
extrahop#configure
extrahop(config)#systemsettings corefiles lifetime <value>
```

The `systemsettings` command includes the following sub-commands and parameters:

corefiles enable

Enables the core files.

corefiles disable

Disables the core files.

lifetime

Sets the value for the core files lifetime.

value

Specifies the lifetime value.

time

Provides commands to set the ExtraHop appliance time, specified using the following datetime syntax: `<MMM DD YYYY H:M:S>`.

Syntax

```
extrahop#configure
extrahop(config-time)#time <time>
```

Parameters

time

Specifies the time in the following format: `MMM DD YYYY H:M:S`.

delete

Puts the ExtraHop appliance into Delete mode. After the delete command executes and the system is in delete mode, you can pass in any of the sub-commands listed below to remove files from the system.

Syntax

```
extrahop#delete
```

Example

The following command sequence opens delete mode and removes a specified firmware version from the system:

```
extrahop#delete firmware <version>
```

The `delete` command supports the following sub-commands:

core
Provides commands to delete core files from the ExtraHop appliance. This command requires that you specify at least one core file name.

Syntax

```
extrahop#delete core <file>
```

Parameters

file

Specifies the name of the core file to delete.

firmware
Provides commands to delete firmware versions from the ExtraHop appliance. This command requires that you specify at least one firmware version name.

Syntax

```
extrahop#delete firmware <version>
```

Parameters

version

Specifies the firmware version that you want to delete from the ExtraHop appliance.

disable

Removes the ExtraHop appliance from Enable mode. After the `disable` command executes and the system is disabled, you will need to execute the `enable` command to perform any operations that modify settings using the command-line interface.

Syntax

```
extrahop#disable
```

Example

The following command sequence disables the command-line interface:

```
extrahop#disable
```

enable

Puts the ExtraHop appliance in Privileged mode. After the `enable` command executes and the system is fully enabled, you can enter and execute other commands to perform operations using the command-line interface. At the start of a session, this command is usually the first command issued. If you are prompted to enter a username and password, use the following credentials:

- Type `shell` as the logon user name.
- Type the number displayed on the service tag

Note: The service tag is on a pullout tab located on the front of the ExtraHop appliance, below the video connector on the 610 and below the power button on the 710.

Syntax

```
extrahop>enable
```

Example

The following command sequence enables the command-line interface and prompts for the appliance password:

```
extrahop>enable
password:
```

ping

Executes a command to ping a selected target to verify the ability to contact the specified host. Ping results specify the response packets received and the round-trip time.

Syntax

```
extrahop#ping <addr>
```

Parameters

addr.

Specifies the IP address of the device to ping.

Example

The following command sequence pings a device at the specified IP address:

```
extrahop#ping 192.164.111.10
```

reload

Executes a reload operation for the specified ExtraHop appliance component. After the reload command is invoked, you can reload any of the supported components identified by their subcommands.

Syntax

```
extrahop#reload
```

Example

The following command sequence activates Reload mode and reloads the ExtraHop bridge service:

```
extrahop#reload exbridge
```

The `reload` command supports the following sub-commands:

exbridge
Specifies the ExtraHop bridge as the component service to reload.

Syntax

```
extrahop#reload exbridge
```

excap
Specifies the ExtraHop capture as the component service to reload.

Syntax

```
extrahop#reload excap
```

reset

Executes a reset operation for the specified ExtraHop appliance component. After the `reset` command is invoked, you can reset the ExtraHop Datastore, which clears all current data from the Datastore.

Syntax

```
extrahop#reset
```

Example

The following command sequence activates Reset mode and clears data from the ExtraHop datastore:

```
extrahop#reset datastore
```

The `reset` command supports the following sub-commands:

datastore
Clears the saved data from the ExtraHop Datastore.

Syntax

```
extrahop#reset datastore
```

restart

Executes a restart operation for the specified ExtraHop appliance component. After the `restart` command is invoked, you can restart the ExtraHop component services identified by the following sub-commands.

Syntax

```
extrahop#restart
```

Example

The following command sequence activates Restart mode and restarts the ExtraHop bridge service:

```
extrahop#restart exbridge
```

The `restart` command supports the following sub-commands:

exbridge
Specifies the ExtraHop bridge as the component service to restart.

Syntax

```
extrahop#restart exbridge
```

excap
Specifies the ExtraHop capture as the component service to restart.

Syntax

```
extrahop#restart excap
```

exportal
Specifies the ExtraHop web portal as the component service to restart.

Syntax

```
extrahop#restart exportal
```

webserver
Specifies the ExtraHop web server as the component service to restart.

Syntax

```
extrahop#restart webserver
```

show

Puts the CLI in View mode so that you can see the settings and parameter values associated with the ExtraHop appliance components. After the `show` command executes and the system is in View mode, you can look at the settings associated with every aspect of the ExtraHop appliance.

Syntax

```
extrahop#show
```

Example

The following command sequence puts the interface in View mode and shows the ExtraHop appliance time:

```
extrahop#show clock
```

The `show` command supports the following sub-commands:

clock
Specifies the ExtraHop computer current clock time as the setting to show.

Syntax

```
extrahop#show clock
```

controllers
Shows the settings for all the ExtraHop appliance active interfaces.

Syntax

```
extrahop#show controllers
```

cores
Shows the settings for the ExtraHop appliance core files.

Syntax

```
extrahop#show cores
```

dhcp
Shows whether DHCP is enabled or disabled on the primary management interface of the ExtraHop appliance.

Syntax

```
extrahop#show dhcp
```

diskmon
Shows the hard disk monitor statistics for the hard drive on the ExtraHop appliance appliance.

Syntax

```
extrahop#show diskmon
```

dnsservers
Shows the DNS server configuration settings for the ExtraHop appliance.

Syntax

```
extrahop#show dnsservers
```

eula_accepted
Shows whether the EUSL/TOS and POC agreements have been accepted for the ExtraHop appliance.

Syntax

```
extrahop#show eula_accepted
```

firmware
Shows the firmware versions installed on the ExtraHop appliance. Executing this command on a Discover appliance will result in each firmware version being prefaced with "ExtraHop". Executing this command on a Command appliance will result in each firmware version listed being prefaced with "ECA".

Syntax

```
extrahop#show firmware
```

flash
Shows the content of the flash key for the ExtraHop appliance.

Syntax

```
extrahop#show flash
```

gateway
Shows the gateway configuration settings for the ExtraHop appliance.

Syntax

```
extrahop#show gateway
```

history
Shows the session command history for the current CLI session.

Syntax

```
extrahop#show history
```

hostname
Shows the system hostname for the ExtraHop appliance.

Syntax

```
extrahop#show hostname
```

interface
Displays information about a specific interface of the ExtraHop appliance.

Syntax

```
extrahop#show interface <interface-number> <sub-command>
```

The `interface` command includes the following sub-commands:

dhcp

Shows whether DHCP is enabled or disabled on the interface.

ipaddr

Shows the IP address and netmask for the ExtraHop appliance management port on the interface.

macaddr

Shows the MAC address for the interface.

inventory

Shows the firmware version, service tag, dossier ID, and hostname for the ExtraHop appliance.

Syntax

```
extrahop#show inventory
```

ip

Provides sub-commands to show IP address configuration settings for the ExtraHop appliance.

Syntax

```
extrahop#show ip arp
```

Parameters

The `ip` command includes the following parameters:

arp

Shows ARP resolution for the device and any computers connected to the device.

interface

Shows information for every IP interface on the connected computer.

sockets

Shows all active Internet connections for the device.

traffic

Shows the IP, ICMP, ICMP msg, TCP, UDP, UDP lite, TCP Ext, and IP Ext traffic for the device.

ipaddr

Shows the IP address and netmask for the ExtraHop appliance management port on the primary management interface.

Syntax

```
extrahop#show ipaddr
```

ldap

Shows the LDAP configuration settings for the ExtraHop appliance.

Syntax

```
extrahop#show ldap
```

license

Shows the licensed modules for the ExtraHop appliance and which ones are enabled or disabled.

Syntax

```
extrahop#show license
```

log
Provides sub-commands to show the logs for the ExtraHop appliance.

Syntax

```
extrahop#show log
```

Parameters

The `log` command includes the following parameters:

exbridge
Shows the ExtraHop appliance bridge component logs.

excap
Shows the ExtraHop appliance capture logs.

exportal
Shows the ExtraHop appliance web portal logs.

macaddr
Shows the MAC address for the primary management interface of the ExtraHop appliance.

Syntax

```
extrahop#show macaddr
```

memory
Shows the total, used, free, shared, buffers, and cached memory as well as Swap information for the ExtraHop appliance.

Syntax

```
extrahop#show memory
```

nics
Shows all NICs (network interface controllers) as well as their link status and link speed for the ExtraHop appliance.

Syntax

```
extrahop#show nics
```

processes
Shows the status of all ExtraHop appliance processes.

Syntax

```
extrahop#show processes
```

radius
Shows the RADIUS configuration settings for the ExtraHop appliance.

Syntax

```
extrahop#show radius
```

remote_auth
Shows the remote authentication configuration settings for the ExtraHop appliance.

Syntax

```
extrahop#show remote_auth
```

running_config
Shows the running configuration settings for the ExtraHop appliance.

Syntax

```
extrahop#show running_config
```

systemsettings
Shows whether the core files are enabled and if the offline capture setting is enabled for the ExtraHop appliance.

Syntax

```
extrahop#show systemsettings
```

tacacs
Shows the TACACS configuration settings for the ExtraHop appliance.

Syntax

```
extrahop#show tacacs
```

users
Shows the user accounts for the ExtraHop appliance.

Syntax

```
extrahop#show users
```

version
Shows the base firmware version and the currently running firmware version on the ExtraHop appliance.

Syntax

```
extrahop#show version
```

shutdown

Initiates the system shutdown operation for the ExtraHop appliance.

Syntax

```
extrahop#shutdown
```

Example

The following command sequence initiated the ExtraHop appliance shutdown:

```
extrahop#shutdown
```

stop

Stops the specified ExtraHop appliance components. After the stop command is invoked, you can halt the operation of specific system component services without shutting down the entire ExtraHop appliance.

Syntax

```
extrahop#stop
```

Example

The following command sequence puts the interface in Stop mode and halts the operation of the ExtraHop bridge component service:

```
extrahop#stop exbridge
```

The `stop` command supports the following sub-commands:

exbridge
Specifies the ExtraHop bridge as the system component service to stop.

Syntax

```
extrahop#stop exbridge
```

excap
Specifies the ExtraHop capture as the system component service to stop.

Syntax

```
extrahop#stop excap
```

exportal
Specifies the ExtraHop web portal as the system component service to stop.

Syntax

```
extrahop#stop exportal
```

webserver
Specifies the ExtraHop web server as the system component service to stop.

Syntax

```
extrahop#stop webserver
```

support

Provides commands to enable or disable the ExtraHop appliance support account. After the `support` command is invoked, you can enable or disable the support account.

Syntax

```
extrahop#support
```

Example

The following command sequence puts the interface in Support mode and it activates the support account:

```
extrahop#support enable
```

The `support` command includes the following sub-commands:

enable
Turns on the ExtraHop appliance support account.

Syntax

```
extrahop#support enable
```

disable
Turns off the ExtraHop appliance support account.

Syntax

```
extrahop#support disable
```

traceroute

Executes the traceroute command on the ExtraHop appliance to measure packet delays across the network.

Syntax

```
extrahop#traceroute <addr>
```

Parameters

addr.

Specifies the IP address of a network device.

Example

The following command executes the traceroute command to measure network packet loss for the route to and from the specified IP address:

```
extrahop#traceroute <addr>
```

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 ciphersuites 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 ciphersuite in order of the server preference.

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

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

The following list includes some common ciphersuites that support Perfect Forward Secrecy, and can not be decrypted by the ExtraHop appliance:

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

The following sample configuration is for Apache 2.4 environments:

```
SSLProtocol all -SSLv3
SSLHonorCipherOrder on
SSLCompression off
SSLSessionTickets off
SSLCipherSuite AES256-GCM-SHA384:
AES128-GCM-SHA256:
AES256-SHA256:
AES128-SHA256:
AES256-SHA:
AES128-SHA:
DES-CBC3-SHA:
ECDHE-ECDSA-AES256-GCM-SHA384:
ECDHE-RSA-AES256-GCM-SHA384:
ECDHE-ECDSA-AES128-GCM-SHA256:
```

```
ECDHE-RSA-AES128-GCM-SHA256:
ECDHE-ECDSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA384:
ECDHE-ECDSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA256
```

For additional information, see the following websites:

- https://www.ssllabs.com/ssltest/
- https://www.ssllabs.com/projects/best-practices/index.html
- https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Server_Protocol_and_Cipher_Configuration
- https://wiki.mozilla.org/Security/Server_Side_TLS
- https://mozilla.github.io/server-side-tls/ssl-config-generator/

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

Acronym	Full Name
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
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 you Cisco router documentation or the Cisco website at www.cisco.com.

Configure an exporter on Cisco Nexus switch

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

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

a) Enter global configuration mode:

```
config t
```

b) Create a flow exporter and enter flow exporter configuration mode.

```
flow exporter <name>
```

For example:

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

c) (Optional) Enter a description:

```
description <string>
```

For example:

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

d) Set the destination IPv4 or IPv6 address for the exporter.

```
destination <eda_mgmt_ip_address>
```

For example:

```
destination 192.168.11.2
```

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

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

For example:

```
source ethernet 2/2
```

f) Specify the NetFlow export version:

```
version 9
```

Configure Cisco switches through Cisco IOS CLI

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

```
config t
```

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

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

     For example:

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

   - Cisco 7200 series routers:

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

For example:

```
interface fastethernet 0/1
```

4. Enable NetFlow:

```
ip route-cache flow
```

5. Export NetFlow statistics:

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

Where <*ip-address*> is the Management Port + NetFlow Target interface on the Discover appliance and <*udp-port*> is the configured collector UDP port number.