



ExtraHop 8.9

ExtraHop Trace Admin UI Guide

© 2022 ExtraHop Networks, Inc. All rights reserved.

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

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

Published: 2022-07-22

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 Trace Admin UI | 6 |
| Supported browsers | 6 |
| Status and Diagnostics | 7 |
| Health | 7 |
| Audit Log | 8 |
| Fingerprint | 8 |
| Support Scripts | 9 |
| Run the default support script | 9 |
| Run a custom support script | 9 |
| Exception Files | 9 |
| Network Settings | 10 |
| Connect to ExtraHop Cloud Services | 10 |
| Configure your firewall rules | 11 |
| Connect to ExtraHop Cloud Services through a proxy | 11 |
| Bypass certificate validation | 12 |
| Connectivity | 12 |
| Configure an interface | 12 |
| Interface throughput | 14 |
| Set a static route | 14 |
| Enable IPv6 for an interface | 15 |
| Global proxy server | 15 |
| ExtraHop Cloud proxy | 15 |
| Bond interfaces | 16 |
| Create a bond interface | 16 |
| Modify bond interface settings | 16 |
| Destroy a bond interface | 17 |
| Notifications | 17 |
| Configure email settings for notifications | 17 |
| Add a new notification email address on an Explore or Trace appliance | 18 |
| Configure settings to send notifications to an SNMP manager | 18 |
| Download the ExtraHop SNMP MIB | 19 |
| Send system notifications to a remote syslog server | 19 |
| SSL Certificate | 20 |
| Upload an SSL certificate | 20 |
| Generate a self-signed certificate | 20 |
| Create a certificate signing request from your ExtraHop system | 20 |
| Trusted Certificates | 21 |
| Add a trusted certificate to your ExtraHop system | 21 |
| Access Settings | 23 |
| Passwords | 23 |
| Change the default password for the setup user | 23 |
| Support Access | 23 |
| Generate SSH key | 23 |
| Regenerate or revoke the SSH key | 24 |
| Users | 24 |
| Add a local user account | 24 |

| | |
|---|-----------|
| Users and user groups | 25 |
| Local users | 25 |
| Remote Authentication | 25 |
| Remote users | 25 |
| User groups | 26 |
| User privileges | 26 |
| Sessions | 30 |
| Remote Authentication | 31 |
| Configure remote authentication through LDAP | 31 |
| Configure user privileges for remote authentication | 33 |
| Configure remote authentication through RADIUS | 34 |
| Configure remote authentication through TACACS+ | 35 |
| Configure the TACACS+ server | 36 |
| API Access | 37 |
| Manage API key access | 37 |
| Configure cross-origin resource sharing (CORS) | 37 |
| Generate an API key | 38 |
| Privilege levels | 38 |
| Appliance Settings | 41 |
| Running Config | 41 |
| Save system settings to the running config file | 41 |
| Edit the running config | 42 |
| Download the running config as a text file | 42 |
| Disable ICMPv6 Destination Unreachable messages | 42 |
| Disable specific ICMPv6 Echo Reply messages | 42 |
| Services | 43 |
| Configure the SNMP service | 43 |
| Firmware | 44 |
| Upgrade the firmware on your ExtraHop system | 44 |
| Pre-upgrade checklist | 44 |
| Upgrade the firmware on a console and sensor | 45 |
| Upgrade the firmware on recordstores | 45 |
| Upgrade the firmware on packetstores | 46 |
| Upgrade connected sensors in Reveal(x) 360 | 46 |
| System Time | 47 |
| Configure the system time | 48 |
| Shutdown or restart | 48 |
| License | 48 |
| Register your ExtraHop system | 49 |
| Register the appliance | 49 |
| Troubleshoot license server connectivity | 49 |
| Apply an updated license | 50 |
| Update a license | 50 |
| Disks | 51 |
| Encrypt the packetstore disk | 51 |
| Change the packet capture disk encryption key | 52 |
| Add storage capacity to the ETA 6150 or 8250 | 52 |
| Compatibility | 52 |
| Installation prerequisites | 53 |
| Set up the extended storage unit | 53 |
| Shut down the packetstore | 53 |
| Connect the extended storage unit | 53 |
| Attach the extended storage unit | 54 |
| Managing extended storage units with a foreign packetstore status | 55 |

| | |
|--|-----------|
| For extended storage units disconnected and then reconnected to the same Trace appliance | 56 |
| For extended storage units configured on a device other than the Trace appliance | 56 |
| Reset Packetstore | 56 |
| Trace Cluster Settings | 57 |
| Manager | 57 |
| Packet Query Status | 57 |
| Remove packet queries | 58 |
| Manage with a console | 58 |

Introduction to the ExtraHop Trace Admin UI

The ExtraHop Trace Admin UI Guide provides detailed information about the administrator features and functionality of the ExtraHop Trace appliance.

In addition, this guide provides an overview of the global navigation and information about the controls, fields, and options available throughout the Trace Administration settings.


After you have deployed your Trace appliance, see the [Trace Post-deployment Checklist](#).

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

Supported browsers

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

- Firefox
- Google Chrome
- Microsoft Edge
- Safari

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

Status and Diagnostics

The Status and Diagnostics section includes metrics and logging data about the current state of the ExtraHop packetstore and enables system administrators to view the overall system health.

Health

Provides metrics about the operating efficiency of the ExtraHop packetstore.

Audit Log

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

Fingerprint

Provides the unique hardware fingerprint for the ExtraHop packetstore.

Support Scripts

Enables you to upload and run support scripts.

Exception Files

Enable or disable the ExtraHop packetstore exception files.

Health

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

The metrics on this page can help you troubleshoot problems and determine why the ExtraHop appliance is not performing as expected.

System

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

CPU User

Displays the percentage of CPU usage associated with the Trace appliance user.

CPU System

Displays the percentage of CPU usage associated with the Trace appliance.

CPU Idle

Displays the CPU idle percentage associated with the Trace appliance.

CPU IO

Displays the percentage of CPU usage associated with the Trace appliance IO functions.

Service Status

Reports the status of ExtraHop packetstore system services.

exadmin

Displays the time the ExtraHop packetstore web portal service started.

exconfig

Displays the time the ExtraHop packetstore config service started.

excap

Displays the time the ExtraHop packetstore capture service started.

Interfaces

Reports the status of ExtraHop packetstore network interfaces.

RX packets

Displays the number of packets received by the ExtraHop packetstore on the specified interface.

RX Errors

Displays the number of received packet errors on the specified interface.

RX Drops

Displays the number of received packets dropped on the specified interface.

TX Packets

Displays the number of packets transmitted by the ExtraHop packetstore on the specified interface.

TX Errors

Displays the number of transmitted packet errors on the specified interface.

TX Drops

Displays the number of transmitted packets dropped on the specified interface.

RX Bytes

Displays the number of bytes received by the ExtraHop packetstore on the specified interface.

TX Bytes

Displays the number of bytes transmitted by the ExtraHop packetstore on the specified interface.

Partitions

Reports the status and usage of ExtraHop packetstore components. The configuration settings for these components are stored on disk and retained even when the power to the packetstore is turned off.

Name

Displays the ExtraHop packetstore settings that are stored on disk.

Options

Displays the read-write options for the settings stored on disk.

Size

Displays the size in gigabytes for the identified component.

Utilization

Displays the amount of memory usage for each of the components as a quantity and as percentage of total disk space.

Audit Log

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

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

Fingerprint

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

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

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

Support Scripts

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

Run the default support script

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

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

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

Run a custom support script

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

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

Exception Files

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

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

Network Settings

The Network Settings section provides the following configurable network connectivity settings.

Connectivity

Configure network connections.

SSL Certificate

Generate and upload a self-signed certificate.

Notifications

Set up alert notifications through email and SNMP traps.

The Trace appliance has two 10/100/1000baseT network ports and four 10 GbE SFP+ network ports. By default, the Gb3 port is configured as the management port and requires an IP address. Port 5 is the default monitor (or capture) interface.

Before you begin configuring the network settings, verify that a network patch cable connects the Gb3 port on the Trace appliance to the management network. For more information about installing a Trace appliance, see the [ExtraHop Trace appliance deployment guide](#) or contact [ExtraHop Support](#) for assistance.

For specifications, installation guides, and more information about your appliance, see the complete ExtraHop documentation set at docs.extrahop.com.

Connect to ExtraHop Cloud Services

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

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

- ExtraHop Machine Learning Service enables detections for your ExtraHop system. In Reveal(x) Enterprise, you can enable security-only or security and performance detections. In addition, you can allow the ExtraHop Machine Learning Service to access pre-filtered, plaintext external IP addresses as well as plaintext domains and hostnames. These settings enable the system to identify new categories of detections and improve the accuracy of existing detections. See the [Collective Threat Analysis FAQ](#) for more information.
- ExtraHop Update Service enables automatic updates of resources to the ExtraHop system, such as ransomware packages.
- ExtraHop Remote Access enables you to allow ExtraHop account team members, ExtraHop Atlas analysts, and ExtraHop Support to connect to your ExtraHop system for configuration help. If you have signed up for the Atlas Remote Analysis service, ExtraHop analysts can perform an unbiased analysis of your network data and report on areas in your IT infrastructure where improvements can be made. See the [Remote Access FAQ](#) for more information about remote access users.

Before you begin

- Reveal(x) 360 systems are automatically connected to ExtraHop Cloud Services, however, you might need to allow access through network firewalls.
 - You must apply the relevant license on the ExtraHop system before you can connect to ExtraHop Cloud Services. See the [License FAQ](#) for more information.
 - You must have [unlimited privileges](#) to access Administration settings.
1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
 2. In the Network Settings section, click **ExtraHop Cloud Services**.

3. Click **Terms and Conditions** to read the content.
4. Read the terms and conditions, and then select the checkbox.
5. Click **Connect to ExtraHop Cloud Services**.
After you are connected, the page updates to show status and connection information for each service.
6. (Optional) In the Machine Learning Service section, select the checkbox for **Contribute to the Machine Learning Service for collective threat analysis** and then select one of the following options:
 - External IP addresses
 - External IP addresses, domains, and hostnames

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

Configure your firewall rules

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

Open access to Cloud Services

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

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

Open access to Cloud Recordstore

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

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

You can also review the public guidance from Google about [computing possible IP address ranges](#) for googleapis.com.

In addition to configuring access to these domains, you must also configure the [global proxy server settings](#).

Connect to ExtraHop Cloud Services through a proxy


If you do not have a direct internet connection, you can try connecting to ExtraHop Cloud Services through an explicit proxy. If your proxy acts as a "man-in-the-middle", ensure that CONNECT requests are allowed over port 22.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Connectivity**.
3. Click **Enable ExtraHop Cloud Proxy**.
4. Type the hostname for your proxy server, such as `proxyhost`.
5. Type the port for your proxy server, such as `8080`.
6. (Optional) If required, type a user name and password for your proxy server.
7. Click **Save**.

Bypass certificate validation

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

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

 **Note:** The following procedure requires familiarity with modifying the ExtraHop Running Configuration file.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **Running Config**.
3. Click **Edit config**.
4. Add the following line to the end of the Running Config file:

```
"hopcloud": { "verify_outer_tunnel_cert": false }
```
5. Click **Update**.
6. Click **View and Save Changes**.
7. Review the changes and click **Save**.
8. Click **Done**.

Connectivity

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

Interface Status

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

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

Network Settings

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

Proxy Settings



- Enable a [global proxy](#) to connect to an ExtraHop Command appliance
- Enable a [cloud proxy](#) to connect to ExtraHop Cloud Services

Bond Interface Settings

- Create a [bond interface](#) to bond multiple interfaces together into one logical interface with a single IP address.

Interfaces

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


- [Collect traffic from NetFlow and sFlow devices](#) 
- [Packet Forwarding with RPCAP](#) 

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.


- 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. |
| Management Port | Manages the ExtraHop sensor. |
| Management Port + Flow Target | Manages the ExtraHop sensor 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 sensors cannot process NetFlow and wire data simultaneously.

| | |
|---|--|
| Management Port + RPCAP/ERSPAN/VXLAN Target | Manages the ExtraHop sensor and captures traffic forwarded from a packet forwarder, ERSPAN*, or VXLAN**. |
|---|--|

While 10 GbE management + capture interfaces on the EDA 10200, EDA 9200, and ETA 8250 can conduct management functions at 10 Gbps speeds, processing traffic such as ERSPAN is limited to 1 Gbps.


 **Tip:** In environments with asymmetric routing adjacent to the high-performance interfaces, ping replies might not get back to the sender.

| | |
|--------------------------------------|--|
| High-Performance ERSPAN/VXLAN Target | Captures traffic forwarded from ERSPAN* or VXLAN**. This interface mode enables the port to handle more than 1 Gbps. Set this interface mode if the ExtraHop sensor has a 10 GbE port. This interface mode only requires that you configure an IPv4 address. |
|--------------------------------------|--|

*The ExtraHop system supports the following ERSPAN implementations:

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

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

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

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

- 40 Gbps
- 100 Gbps

Important: When you change the interface speed to **Auto-negotiate**, you might need to restart the sensor before the change takes effect.

5. DHCPv4 is enabled by default. If your network does not support DHCP, you can clear the DHCPv4 checkbox to disable DHCP and then type a static IP address, netmask, and default gateway.

Note: Only one interface should be configured with a default gateway. [Configure static routes](#) if your network requires routing through multiple gateways.

6. (Optional) Enable IPv6.

For more information about configuring IPv6, see [Enable IPv6 for an interface](#).

7. (Optional) Manually add routes.
8. Click **Save**.

Interface throughput

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

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

Note: EDA 4200, EDA 6200, EDA 8200, EDA 9200, and EDA 10200 sensors are not susceptible to reduced throughput if you enable 1GbE interfaces for monitoring traffic.

| ExtraHop Sensor | Throughput | Details |
|-----------------|----------------------------|---|
| EDA 9100 | Standard 40Gbps throughput | If the non-management 1GbE interfaces are disabled, you can use up to four of the 10GbE interfaces for a combined throughput of up to 40Gbps. |
| EDA 8100 | Standard 20Gbps throughput | If the non-management 1GbE interfaces are disabled, you can use either one or both of the 10GbE interfaces for a combined throughput of up to 20Gbps. |
| EDA 6100 | Standard 10Gbps throughput | If the non-management 1GbE interfaces are disabled, the maximum total combined throughput is 10Gbps. |
| EDA 3100 | Standard 3Gbps throughput | No 10GbE interface |
| EDA 1100 | Standard 1Gbps throughput | No 10GbE interface |

Set a static route


Before you begin

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

1. On the Edit Interface page, ensure that the **IPv4 Address** and **Netmask** fields are complete and saved, and click **Edit Routes**.
2. In the Add Route section, type a network address range in CIDR notation in the **Network** field and IPv4 address in the **Via IP** field and then click **Add**.


3. Repeat the previous step for each route you want to add.
4. Click **Save**.

Enable IPv6 for an interface

1. In the Network Settings section, click **Connectivity**.
2. In the Interfaces section, click the name of the interface you want to configure.
3. On the Network Settings for Interface <interface number> page, select **Enable IPv6**. IPv6 configuration options appear below **Enable IPv6**.
4. (Optional) Configure IPv6 addresses for the interface.
 - To automatically assign IPv6 addresses through DHCPv6, select **Enable DHCPv6**.
 -  **Note:** If enabled, DHCPv6 will be used to configure DNS settings.
 - To automatically assign IPv6 addresses through stateless address autoconfiguration, select one of the following options from the Stateless Address Autoconfiguration list:
 - Use MAC address**
Configures the appliance to automatically assign IPv6 addresses based on the MAC address of the appliance.
 - Use stable private address**
Configures the appliance to automatically assign private IPv6 addresses that are not based on hardware addresses. This method is described in RFC 7217.
 - To manually assign one or more static IPv6 addresses, type the addresses in the Static IPv6 Addresses field.
5. To enable the appliance to configure Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) information according to router advertisements, select **RDNSS/DNSSL**.
6. Click **Save**.

Global proxy server

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

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

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

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

ExtraHop Cloud proxy

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

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

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

- **Password:** The password for the user specified above.

Bond interfaces

You can bond multiple 1 GbE interfaces on your ExtraHop system together into a single logical interface that has one IP address for the combined bandwidth of the member interfaces. Bonding interfaces enable a larger throughput with a single IP address. This configuration is also known as link aggregation, port channeling, link bundling, Ethernet/network/NIC bonding, or NIC teaming. 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 system. You must make changes to your network switch configuration to restore connectivity. The changes required are dependent on your switch. Contact ExtraHop Support for assistance before you create a bond interface.

- Bonding is only configurable on 1 GbE Management or Management+RPCAP/ERSPAN interfaces.
- [Port channeling](#) on traffic monitoring ports is supported on the ExtraHop sensors.

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

- [Create a bond interface](#)
- [Modify a bond interface](#)
- [Destroy a bond interface](#)

Create a bond interface

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

1. Click **Create Bond Interface**.
2. Configure the following options:
 - **Members:** Select the checkbox next to each interface you want to include in the bonding. Only ports that are currently available for bond membership appear.
 - **Take Settings From:** Select the interface that has the settings you want to apply to the bond interface. Settings for all non-selected interfaces will be lost.
 - **Bond Type:** Specify whether to create a static bond or a dynamic bond through IEEE 802.3ad Link Aggregation (LACP).
 - **Hash Policy:** Specify the hash policy. The **Layer 3+4** policy balances the distribution of traffic more evenly across interfaces; however, this policy is not fully compliant with 802.3ad standards. The **Layer 2+3** policy balances traffic less evenly and is compliant with 802.3ad standards.
3. Click **Create**.

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

Modify bond interface settings

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

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

- **Members:** The interface members of the bond interface. Members cannot be changed after a bond interface is created. If you need to change the members, you must destroy and recreate the bond interface.
- **Bond Mode:** Specify whether to create a static bond or a dynamic bond through IEEE 802.3ad Link Aggregation (LACP).
- **Interface Mode:** The mode of the bond membership. A bond interface can be **Management** or **Management+RPCAP/ERSPAN Target** only.
- **Enable DHCPv4:** If DHCP is enabled, an IP address for the bond interface is automatically obtained.
- **Hash Policy:** Specify the hash policy. The **Layer 3+4** policy balances the distribution of traffic more evenly across interfaces; however, it is not fully compliant with 802.3ad standards. The **Layer 2+3** policy balances traffic less evenly; however, it is compliant with 802.3ad standards.
- **IPv4 Address:** The static IP address of the bond interface. This setting is unavailable if DHCP is enabled.
- **Netmask:** The network netmask for the bond interface.
- **Gateway:** The IP address of the network gateway.
- **Routes:** The static routes for the bond interface. This setting is unavailable if DHCP is enabled.
- **Enable IPv6:** Enable configuration options for IPv6.

4. Click **Save**.

Destroy a bond interface

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

1. In the Network Settings section, click **Connectivity**.
2. In the Bond Interfaces section, click the red **X** next to the interface you want to destroy.
3. On the Destroy Bond Interface <interface number> page, select the member interface to move the bond interface settings to. Only the member interface selected to retain the bond interface settings remains active, and all other member interfaces are disabled.
4. Click **Destroy**.

Notifications


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

Configure email settings for notifications

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

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Notifications**.
3. Click **Email Server and Sender**.
4. In the SMTP Server field, type the IP address or hostname for the outgoing SMTP mail server. The SMTP server should be the fully qualified domain name (FQDN) or IP address of an outgoing mail server that is accessible from the ExtraHop system. If the DNS server is set, then the SMTP server can be a FQDN, otherwise you must type an IP address.

5. In the SMTP Port field, type the port number for SMTP communication. Port 25 is the default value for SMTP and port 465 is the default value for SSL/TLS encrypted SMTP.
6. Select one of the following encryption methods from the Encryption drop-down list:
 - **None.** SMTP communication is not encrypted.
 - **SSL/TLS.** SMTP communication is encrypted through the Secure Socket Layer/Transport Layer Security protocol.
 - **STARTTLS.** SMTP communication is encrypted through STARTTLS.
7. In the Alert Sender Address field, type the email address for the notification sender.



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

Next steps

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


Add a new notification email address on an Explore or Trace appliance

You can send system storage alerts to individual recipients. Alerts are sent under the following conditions:

- A physical disk is in a degraded state.
 - A physical disk has an increasing error count.
 - (Explore appliance only) A virtual disk is in a degraded state.
 - (Explore appliance only) A registered Explore node is missing from the cluster. The node might have failed, or it is powered off.
1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
 2. In the Network Settings section, click **Notifications**.
 3. Under Notifications, click **Email Addresses**.
 4. In the **Email address** text box, type the recipient email address.
 5. Click **Save**.

Configure settings to send notifications to an SNMP manager

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

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

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Notifications**.
3. Under Notifications, click **SNMP**.
4. On the SNMP Settings page, in the **SNMP Monitor** field, type the hostname for the SNMP trap receiver. Multiple names can be entered, separated by commas.
5. In the **SNMP Community** field, enter the SNMP community name.
6. In the **SNMP Port** field, type the SNMP port number for your network that is used by the SNMP agent to respond back to the source port on the SNMP manager. The default response port is 162.
7. Click **Test Settings** to verify that your SNMP settings are correct. If the settings are correct, you should see an entry in the SNMP log file on the SNMP server similar to the following:

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

Where 192.0.2.0 is the IP address of your ExtraHop system and 192.0.2.255 is the IP address of the SNMP server.

8. Click **Save**.

Download the ExtraHop SNMP MIB

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

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. Go to the Network Settings section and click **Notifications**.
3. Under Notifications, click **SNMP**.
4. Under SNMP MIB, click the **Download ExtraHop SNMP MIB**. The file is typically saved to the default download location for your browser.

Send system notifications to a remote syslog server

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

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

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

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

7. Click **Save**.


Next steps

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

SSL Certificate


SSL certificates provide secure authentication to the ExtraHop system.

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

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

Upload an SSL certificate

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


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

 **Note:** You can also [automate this task through the REST API](#).

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

Generate a self-signed certificate

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

 **Note:** The default hostname is `extrahop`.

Create a certificate signing request from your ExtraHop system

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

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **SSL Certificate**.
3. Click **Manage certificates** and then click **Export a Certificate Signing Request (CSR)**.

- In the Subject Alternative Names section, type the DNS name of the ExtraHop system. You can add multiple DNS names and IP addresses to be protected by a single SSL Certificate.
- In the Subject section, complete the following fields. Only the **Common Name** field is required.

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

- Click **Export**. The CSR file is automatically downloaded to your computer.

Next steps

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



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

Trusted Certificates

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


Add a trusted certificate to your ExtraHop system

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

Before you begin

You must log in as a user with unlimited privileges to add or remove trusted certificates.

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

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

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Trusted Certificates**.
3. (Optional) The ExtraHop system ships with a set of built-in certificates. Select **Trust System Certificates** if you want to trust these certificates, and then click **Save**.
4. To add your own certificate, click **Add Certificate** and then paste the contents of the PEM-encoded certificate chain into the Certificate field
5. Type a name into the Name field and click **Add**.

Access Settings

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

Passwords


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

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

For more information about privileges for specific Administration page users and groups, see the [Users](#) section.

Change the default password for the setup user

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

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

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

Support Access

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

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

Generate SSH key

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

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

Regenerate or revoke the SSH key

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

1. In the Access Settings section, click **Support Access**.
2. Click **Generate SSH Key**.
3. Choose one of the following options:
 - Click **Regenerate SSH Key** and then click **Regenerate**.
Copy the encrypted key from the text box and email the key to support@extrahop.com and then click **Done**.
 - Click **Revoke SSH Key** to prevent SSH access to the system with the current key.

Users


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

Add a local user account


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

To learn about default system user accounts, see [Local users](#).


1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Users**.
3. Click **Add User**.
4. In the Personal Information section, type the following information:
 - **Login ID:** The username that users will log in to the sensor with, which cannot contain any spaces. For example, `adalovelace`.
 - **Full Name:** A display name for the user, which can contain spaces. For example, `Ada Lovelace`.
 - **Password:** The password for this account.

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

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

 **Note:** For more information, see the [User privileges](#) section.

7. Click **Save**.

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

Users and user groups

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

Local users

This topic is about default and local accounts. See [Remote Authentication](#) to learn how to configure remote accounts.

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

setup

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

shell

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



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

Next steps

- [Add a local user account](#)

Remote Authentication

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

Centralized authentication provides the following benefits:

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

Next steps

- [Configure remote authentication through LDAP](#)
- [Configure remote authentication through SAML](#)
- [Configure remote authentication through TACACS+](#)
- [Configure remote authentication through RADIUS](#)

Remote users

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

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

Next steps

- [Add an account for a remote user](#)

User groups

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

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

Group Name

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

Type

Displays Local or Remote as the type of user group.

Members

Displays the number of users in the group.

Shared Content

Displays the number of user-created dashboards and activity maps that are shared with the group.

Status

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

Members Refreshed (LDAP only)

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

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

User privileges

Administrators determine the level of access and functionality users have with the ExtraHop system. In addition to setting the privilege level for local users, you can enable options for any user privilege level.

For information about user privileges for the REST API, see the [REST API Guide](#).

For information about remote user privileges, see the configuration guides for [LDAP](#), [RADIUS](#), [SAML](#), and [TACACS+](#).

Privilege Levels

Set the privilege level for your user to determine which areas of the ExtraHop system they can access. Users with unlimited or System Administration privileges can access all areas of the ExtraHop system, including packets, session keys, and detections.

| | Unlimited | System and Access Administration (Reveal(x) 360 only) | System Administration (Reveal(x) 360 only) | Full Write | Limited Write | Personal Write | Full Read-Only | Restricted Read-Only |
|---|-----------|---|--|------------|---------------|----------------|----------------|----------------------|
| Activity Maps | | | | | | | | |
| Create, view, and load shared activity maps | Y | Y | Y | Y | Y | Y | Y | N |
| Save activity maps | Y | Y | Y | Y | Y | Y | N | N |
| Share activity maps | Y | Y | Y | Y | Y | N | N | N |
| Alerts | | | | | | | | |
| View alerts | Y | Y | Y | Y | Y | Y | Y | Y |
| Create and modify alerts | Y | Y | Y | Y | N | N | N | N |
| Bundles | | | | | | | | |
| Create a bundle | Y | Y | Y | Y | N | N | N | N |
| Upload and apply a bundle | Y | Y | Y | Y | N | N | N | N |
| View list of bundles | Y | Y | Y | Y | Y | Y | Y | N |
| Dashboards | | | | | | | | |
| View and organize dashboards | Y | Y | Y | Y | Y | Y | Y | Y |
| Create and | Y | Y | Y | Y | Y | Y | N | N |

modify
dashboards

| | | | | | | | | |
|------------------|---|---|---|---|---|---|---|---|
| Share dashboards | Y | Y | Y | Y | Y | N | N | N |
|------------------|---|---|---|---|---|---|---|---|

Detections  **Note:** Machine learning detections require a [connection to ExtraHop Cloud Services](#).

Administrators can configure the [Detections Access Control global policy](#) to specify whether all users, or only specified users can access detections. The privilege level of the user determines the level of access to detections.

| | | | | | | | | |
|-----------------|---|---|---|---|---|---|---|---|
| View detections | Y | Y | Y | Y | Y | Y | Y | Y |
|-----------------|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|------------------------|--|---|---|---|---|---|---|---|
| Acknowledge Detections | | Y | Y | Y | Y | Y | N | N |
|------------------------|--|---|---|---|---|---|---|---|

| | | | | | | | | |
|-----------------------------------|---|---|---|---|---|---|---|---|
| Modify detection status and notes | Y | Y | Y | Y | Y | N | N | N |
|-----------------------------------|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|----------------------------------|---|---|---|---|---|---|---|---|
| Create and modify investigations | Y | Y | Y | Y | Y | N | N | N |
|----------------------------------|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|--------------------------------|---|---|---|---|---|---|---|---|
| Create and modify tuning rules | Y | Y | Y | Y | N | N | N | N |
|--------------------------------|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|--------------------------------------|---|---|---|---|---|---|---|---|
| Create and modify notification rules | Y | Y | Y | Y | N | N | N | N |
|--------------------------------------|---|---|---|---|---|---|---|---|

Analysis
Priorities

| | | | | | | | | |
|-------------------------------|---|---|---|---|---|---|---|---|
| View Analysis Priorities page | Y | Y | Y | Y | Y | Y | Y | N |
|-------------------------------|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Add and modify analysis levels for groups | Y | Y | Y | Y | N | N | N | N |
|---|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|----------------------------|---|---|---|---|---|---|---|---|
| Add devices to a watchlist | Y | Y | Y | Y | N | N | N | N |
|----------------------------|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|--|---|---|---|---|---|---|---|---|
| Transfer priorities management | Y | Y | Y | Y | N | N | N | N |
| Device Groups | | | | | | | | |
| Create and modify device groups | Y | Y | Y | Y | N | N | N | N |
| Metrics | | | | | | | | |
| View metrics | Y | Y | Y | Y | Y | Y | Y | N |
| Records (Explore appliance) | | | | | | | | |
| View record queries | Y | Y | Y | Y | Y | Y | Y | N |
| View record formats | Y | Y | Y | Y | Y | Y | Y | N |
| Create, modify, and save record queries | Y | Y | Y | Y | N | N | N | N |
| Create, modify, and save record formats | Y | Y | Y | Y | N | N | N | N |
| Scheduled Reports (Command appliance) | | | | | | | | |
| Create, view, and manage scheduled reports | Y | Y | Y | Y | Y | N | N | N |
| Threat Intelligence | | | | | | | | |
| Manage threat collections | Y | Y | Y | N | N | N | N | N |
| View threat | Y | Y | Y | Y | Y | Y | Y | N |

intelligence information

Triggers

| | | | | | | | | |
|----------------------------|---|---|---|---|---|---|---|---|
| Create and modify triggers | Y | Y | Y | Y | N | N | N | N |
|----------------------------|---|---|---|---|---|---|---|---|

Administrative Privileges

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Access the ExtraHop Administration settings | Y | Y | Y | N | N | N | N | N |
|---|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|-----------------------------|---|---|---|---|---|---|---|---|
| Connect to other appliances | Y | Y | Y | N | N | N | N | N |
|-----------------------------|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Manage other appliances (Command appliance) | Y | Y | Y | N | N | N | N | N |
|---|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|-----------------------------|---|---|---|---|---|---|---|---|
| Manage users and API access | Y | Y | N | N | N | N | N | N |
|-----------------------------|---|---|---|---|---|---|---|---|

Privilege options

The following privilege options can be assigned to users with limited Web UI and API privileges.

Packet and Session Key Access

- View and download packets
- View and download packets and session keys

Detections Access

- No access
- Full access
 - Full access to detections is determined by your privilege level. See the Privilege Levels table to see what level of detections each privilege level can access.



Note: (Reveal(x) Enterprise only) The Detections Access settings appear only if the global privilege policy for [detections access control](#) is set to **Only specified users can access detections**.

Sessions

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

Remote Authentication

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

Centralized authentication provides the following benefits:

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

Next steps

- [Configure remote authentication through LDAP](#)
- [Configure remote authentication through SAML](#)
- [Configure remote authentication through TACACS+](#)
- [Configure remote authentication through RADIUS](#)

Configure remote authentication through LDAP


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

Before you begin

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

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

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


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

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


- a) In the Hostname field, type the hostname or IP address of the LDAP server. If you are configuring a hostname, make sure that the DNS entry of the ExtraHop system is properly configured.
 - b) In the Port field, type the port number on which the LDAP server is listening.
 - c) From the Server Type drop-down list, select **Posix** or **Active Directory**.
 - d) (Optional) In the Bind DN field, type the bind DN. The bind DN is the user credentials that allow you to authenticate with the LDAP server to perform the user search. The bind DN must have list access to the base DN and any OU, groups, or user account required for LDAP authentication. If this value is not set, then an anonymous bind is performed. Note that anonymous binds are not enabled on all LDAP servers.
 - e) (Optional) In the Bind Password field, type the bind password. The bind password is the password required when authenticating with the LDAP server as the bind DN specified above. If you are configuring an anonymous bind, leave this field blank. In some cases, an unauthenticated bind is possible, where you supply a Bind DN value but no bind password. Consult your LDAP administrator for the proper settings.
 - f) From the Encryption drop-down list, select one of the following encryption options.
 - **None:** This options specifies cleartext TCP sockets. All passwords are sent across the network in cleartext in this mode.
 - **LDAPS:** This option specifies LDAP wrapped inside SSL.
 - **StartTLS:** This option specifies TLS LDAP. (SSL is negotiated before any passwords are sent.)
 - g) Select **Validate SSL Certificates** to enable certificate validation. If you select this option, the certificate on the remote endpoint is validated against the root certificates as specified by the trusted certificates manager. You must configure which certificates you want to trust on the Trusted Certificates page. For more information, see [Add a trusted certificate to your ExtraHop system](#).
 - h) Type a time value in the Refresh Interval field or leave the default setting of 1 hour. The refresh interval ensures that any changes made to user or group access on the LDAP server are updated on the ExtraHop system.
5. Configure the following user settings:
- a) Type the base DN in the Base DN field. The Base DN is the point from where a server will search for users. The base DN must contain all user accounts that will have access to the ExtraHop system. The users can be direct members of the base DN or nested within an OU within the base DN if the **Whole Subtree** option is selected for the Search Scope specified below.
 - b) Type a search filter in the Search Filter field. Search filters enable you to define search criteria when searching the LDAP directory for user accounts.
 - ❗ **Important:** The ExtraHop system automatically adds parentheses to wrap the filter and will not parse this parameter correctly if you add parentheses manually. Add your search filters in this step and in step 5b, similar to the following example:

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

In addition, if your group names include the asterisk (*) character, the asterisk must be escaped as \2a. For example, if your group has a CN called test*group, type cn=test\2agroup in the Search Filter field.
 - c) From the Search Scope drop-down list, select one of the following options. Search scope specifies the scope of the directory search when looking for user entities.
 - **Whole subtree:** This option looks recursively under the group DN for matching users.
 - **Single level:** This option looks for users that exist in the base DN only; not any subtrees.
6. (Optional) Import user groups. Select the **Import user groups from LDAP server** checkbox and configure the following settings.

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

- a) Type the base DN in the Base DN field. The Base DN is the point from where a server will search for user groups. The base DN must contain all user groups that will have access to the ExtraHop system. The user groups can be direct members of the base DN or nested within an OU within the base DN if the **Whole Subtree** option is selected for the Search Scope specified below.
- b) Type a search filter in the Search Filter field. Search filters enable you to define search criteria when searching the LDAP directory for user groups.

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

- c) From the Search Scope drop-down list, select one of the following options. Search scope specifies the scope of the directory search when looking for user group entities.
 - **Whole subtree:** This option looks recursively under the base DN for matching user groups.
 - **Single level:** This option looks for user groups that exist in the base DN; not any subtrees.
7. Click **Test Settings**. If the test succeeds, a status message appears near the bottom of the page. If the test fails, click **Show details** to see a list of errors. You must resolve any errors before you continue.
8. Click **Save and Continue**.

Next steps

[Configure user privileges for remote authentication](#)

Configure user privileges for remote authentication

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

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

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

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

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

 - **Unlimited DN:** Create and modify all objects and settings on the ExtraHop system, including Administration settings.
 - **Full Write DN:** Create and modify objects on the ExtraHop system, not including Administration settings.
 - **Limited Write DN:** Create, modify, and share dashboards.
 - **Personal Write DN:** Create personal dashboards and modify dashboards shared with the logged-in user.
 - **Full read-only DN:** View objects in the ExtraHop system.
 - **Restricted Read-only DN:** View dashboards shared with the logged-in user.
 - **Packet Access DN:** View and download packets captured through the ExtraHop Trace appliance.
 - **Packet and Session Keys Access DN:** View and download packets and any associated SSL session keys captured through the ExtraHop Trace appliance.

- **Detections Access DN:** View, acknowledge, and hide detections that appear in the ExtraHop system.
 - **Remote users have full write access**
This option grants remote users full write access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, and detections.
 - **Remote users have full read-only access**
This option grants remote users read-only access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, and detections.
2. (Optional) Configure packet and session key access. Select one of the following options to allow remote users to download packet captures and SSL session keys.
 - **No access**
 - **Packets only**
 - **Packets and session keys**
 3. (Optional) Configure detections access. Select one of the following options to allow remote users to view detections. This setting is visible only when the global privilege policy for detections access control is set to **Only specified users can view detections**.
 - **No access**
 - **Full access**
 4. Click **Save and Finish**.
 5. Click **Done**.

Configure remote authentication through RADIUS

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

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

Host

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

Secret

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

Timeout

The amount of time in seconds that the ExtraHop system waits for a response from the RADIUS server before attempting the connection again.

5. Click **Add Server**.
6. (Optional) Add additional servers as needed.
7. Click **Save and Finish**.
8. From the Privilege assignment options drop-down list, choose one of the following options:

- **Remote users have full write access**

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


- **Remote users have full read-only access**
This option grants remote users read-only access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, and detections.
9. (Optional) Configure packet and session key access. Select one of the following options to allow remote users to download packet captures and SSL session keys.
 - **No access**
 - **Packets only**
 - **Packets and session keys**
 10. (Optional) Configure detections access. Select one of the following options to allow remote users to view detections. This setting is visible only when the global privilege policy for detections access control is set to **Only specified users can view detections**.
 - **No access**
 - **Full access**
 11. Click **Save and Finish**.
 12. Click **Done**.

Configure remote authentication through TACACS+

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

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

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Remote Authentication**.
3. From the Remote authentication method drop-down list, select **TACACS+**, and then click **Continue**.
4. On the Add TACACS+ Server page, type the following information:
 - **Host:** The hostname or IP address of the TACACS+ server. Make sure that the DNS of the ExtraHop system is properly configured if you are entering a hostname.
 - **Secret:** The shared secret between the ExtraHop system and the TACACS+ server. Contact your TACACS+ administrator to obtain the shared secret.

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

- **Timeout:** The amount of time in seconds that the ExtraHop system waits for a response from the TACACS+ server before attempting to connect again.
5. Click **Add Server**.
 6. (Optional) Add additional servers as needed.
 7. Click **Save and Finish**.
 8. From the Permission assignment options drop-down list, choose one of the following options:
 - **Obtain privileges level from remote server**
This option allows remote users to obtain privilege levels from the remote server. You must also configure permissions on the TACACS+ server.
 - **Remote users have full write access**
This option grants remote users full write access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, and detections.
 - **Remote users have full read-only access**

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

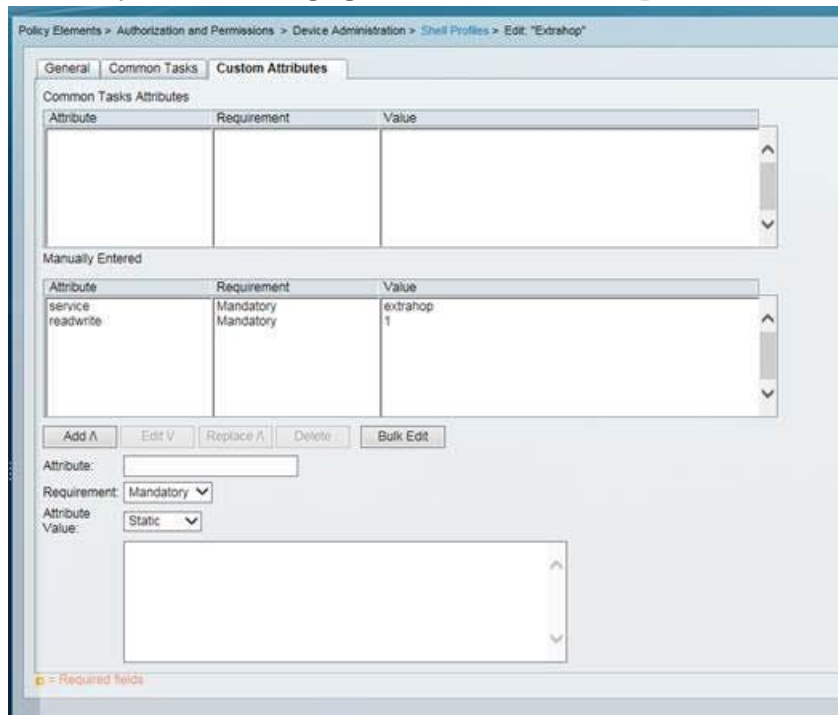
9. (Optional) Configure packet and session key access. Select one of the following options to allow remote users to download packet captures and SSL session keys.
 - **No access**
 - **Packets only**
 - **Packets and session keys**
10. (Optional) Configure detections access. Select one of the following options to allow remote users to view detections. This setting is visible only when the global privilege policy for detections access control is set to **Only specified users can view detections**.
 - **No access**
 - **Full access**
11. Click **Save and Finish**.
12. Click **Done**.

Configure the TACACS+ server

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

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

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



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

- `setup = 1`, which allows the user to create and modify all objects and settings on the ExtraHop system, including Administration settings
 - `readwrite = 1`, which allows the user to create and modify all objects and settings on the ExtraHop system, not including Administration settings
 - `limited = 1`, which allows the user to create, modify, and share dashboards
 - `readonly = 1`, which allows the user to view objects in the ExtraHop system
 - `personal = 1`, which allows the user to create dashboards for themselves and modify any dashboards that have been shared with them
 - `limited_metrics = 1`, which allows the user to view shared dashboards
6. (Optional) Add the following attribute to allow users to view, acknowledge, and hide detections that appear in the ExtraHop system.
 - `detectionsaccessfull = 1`
 7. (Optional) If you have an ExtraHop packetstore, add an attribute to allow users to download packet captures or packet captures with associated session keys.
Here is a list of the available packet capture attributes and values:
 - `packetsfull = 1`, which allows users with any privilege level to view and download packets
 - `packetsfullwithkeys = 1`, which allows users with any privilege level to view and download packets and associated session keys stored on the packetstore

API Access

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

Manage API key access

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

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

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

Configure cross-origin resource sharing (CORS)

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

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

1. In the **Access Settings** section, click **API Access**.
2. In the CORS Settings section, specify one of the following access configurations.

- To add a specific URL, type an origin URL in the text box, and then click the plus (+) icon or press ENTER.

The URL must include a scheme, such as HTTP or HTTPS, and the exact domain name. You cannot append a path; however, you can provide a port number.

- To allow access from any URL, select the Allow API requests from any Origin checkbox.



Note: Allowing REST API access from any origin is less secure than providing a list of explicit origins.

3. Click **Save Settings** and then click **Done**.

Generate an API key

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

Before you begin

Make sure the ExtraHop system is [configured to allow API key generation](#).

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

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

Privilege levels

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

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

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

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

The `granted_roles` and `effective_roles` properties support the following privilege levels. Note that the type of tasks for each ExtraHop system vary by the available [resources](#) listed in the REST API Explorer.

| Privilege level | Actions allowed |
|------------------|--|
| "system": "full" | <ul style="list-style-type: none"> • Enable or disable API key generation for the ExtraHop system. • Generate an API key. • View the last four digits and description for any API key on the system. • Delete API keys for any user. • View and edit cross-origin resource sharing. • Transfer ownership of any non-system dashboard to another user. • Perform any administration task available through the REST API. • Perform any ExtraHop system task available through the REST API. |

| Privilege level | Actions allowed |
|-------------------------|--|
| "write": "full" | <ul style="list-style-type: none"> • Generate your own API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform any ExtraHop system task available through the REST API. |
| "write": "limited" | <ul style="list-style-type: none"> • Generate an API key. • View or delete their own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform all GET operations through the REST API. • Modify the sharing status of dashboards that you are allowed to edit. • Delete dashboards and activity maps that you own. • Perform metric and record queries. |
| "write": "personal" | <ul style="list-style-type: none"> • Generate an API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform all GET operations through the REST API. • Delete dashboards and activity maps that you own. • Perform metric and record queries. |
| "metrics": "full" | <ul style="list-style-type: none"> • Generate an API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • View dashboards and activity maps shared with you. • Perform metric and record queries. |
| "metrics": "restricted" | <ul style="list-style-type: none"> • Generate an API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • View dashboards and activity maps shared with you. |
| "packets": "full" | <ul style="list-style-type: none"> • View and download packets from an ExtraHop system through the <code>GET/packetcaptures/{id}</code> operation. <p>This is an add-on privilege that can be granted to a user with one of the following privilege levels:</p> <ul style="list-style-type: none"> • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted" |

| Privilege level | Actions allowed |
|------------------------------------|--|
| <p>"packets": "full_with_keys"</p> | <ul style="list-style-type: none"> • View and download packets from an ExtraHop system through the <code>GET/packetcaptures/{id}</code> operation. <p>This is an add-on privilege that can be granted to a user with one of the following privilege levels:</p> <ul style="list-style-type: none"> • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted" |
| <p>"detections": "full"</p> | <ul style="list-style-type: none"> • View detections in the ExtraHop system. <p>This is an add-on privilege that can be granted to a user with one of the following privilege levels:</p> <ul style="list-style-type: none"> • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted" |
| <p>"detections": "none"</p> | <ul style="list-style-type: none"> • No access to detections. <p>This is an add-on privilege that can be granted to a user with one of the following privilege levels:</p> <ul style="list-style-type: none"> • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted" |

Appliance Settings

You can configure the following components of the ExtraHop appliance in the Appliance Settings section.

All appliances have the following components:

Running Config

Download and modify the running configuration file.

Services

Enable or disable the Web Shell, management GUI, SNMP service, SSH access, and SSL session key receiver. The SSL Session Key Receiver option appears only on the Discover appliance.

Firmware

Upgrade the ExtraHop system firmware.

System Time

Configure the system time.

Shutdown or Restart

Halt and restart system services.

License

Update the license to enable add-on modules.

Disks

Provides information about the disks in the appliance.

The following components only appear on the specified appliances:

Command Nickname


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

Reset Packetstore

Delete all packets stored on the ExtraHop Trace appliance. The Reset Packetstore page appears only on the Trace appliance.

Running Config

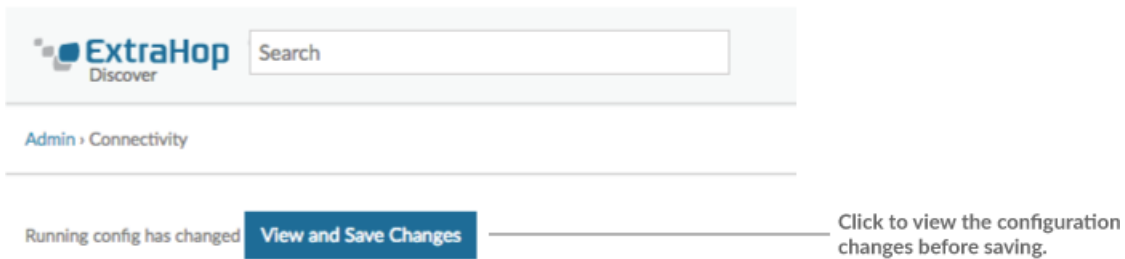
The running configuration file specifies the default system configuration. When you modify system settings, you must save the running configuration file to preserve those modifications after a system restart.

 **Note:** Making configuration changes to the code from the Edit page is not recommended. You can make most system modifications through other pages in the Administration settings.

Save system settings to the running config file

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

To remind you that the running configuration has changed, (Unsaved changes) appears next to the Running Config link on the main Administration settings page, as well as a **View and Save Changes** button on all Administration settings pages, as shown in the figure below.



1. Click **View and Save Changes**.
2. Review the comparison between the old running config and the current running config (not yet saved) and then select from the following options:
 - If the changes are correct, click **Save**.
 - If the changes are not correct, click **Cancel** and then revert the changes by clicking **Revert config**.

Edit the running config

The ExtraHop Administration settings provide an interface to view and modify the code that specifies the default system configuration. In addition to making changes to the running configuration through the Administration settings, changes can also be made on the Running Config page.



Note: Making configuration changes to the code from the Edit page is not recommended. You can make most system modifications through other Administration settings.

Download the running config as a text file

You can download the Running Config settings to your workstation in text file format. You can open this text file and make changes to it locally, before copying those changes into the Running Config window.

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

The current running configuration is downloaded as a text file to your default download location.

Disable ICMPv6 Destination Unreachable messages

You can prevent the ExtraHop system from generating ICMPv6 Destination Unreachable messages. You might want to disable ICMPv6 Destination Unreachable messages for security reasons per RFC 4443.

To disable ICMPv6 Destination Unreachable messages, you must edit the Running Configuration. However, we recommend that you do not manually edit the Running Configuration file without direction from ExtraHop Support. Manually editing the running config file incorrectly might cause the system to become unavailable or stop collecting data. You can contact ExtraHop Support at support@extrahop.com.

Disable specific ICMPv6 Echo Reply messages

You can prevent the ExtraHop system from generating Echo Reply messages in response to ICMPv6 Echo Request messages that are sent to an IPv6 multicast or anycast address. You might want to disable these messages to reduce unnecessary network traffic.

To disable specific ICMPv6 Echo Reply messages, you must edit the Running Configuration. However, we recommend that you do not manually edit the Running Configuration file without direction from ExtraHop Support. Manually editing the running config file incorrectly might cause the system to become unavailable or stop collecting data. You can contact ExtraHop Support at support@extrahop.com.

Services


These services run in the background and perform functions that do not require user input. These services can be started and stopped through the Administration settings.

Enable or disable the Web Shell

The Web Shell provides access to the ExtraHop command-line interface (CLI). By default this service is enabled so that ExtraHop users can click the **Launch Shell** link in the upper right corner of the Administration settings and type commands. For more information, see the [ExtraHop Command-line Reference](#).

Enable or disable the Management GUI

The Management GUI provides browser-based access to the ExtraHop system. By default, this service is enabled so that ExtraHop users can access the ExtraHop system through a web browser. If this service is disabled, the Apache Web Server session is terminated and all browser-based access is disabled.

 **Warning:** Do not disable this service unless you are an experienced ExtraHop administrator and you are familiar with the ExtraHop CLI.


Enable or disable the SNMP Service

Enable the SNMP service on the ExtraHop system when you want your network device monitoring software to collect information about the ExtraHop system. This service is disabled by default.

- Enable the SNMP service from the Services page by selecting the Disabled checkbox and then clicking **Save**. After the page refreshes, the Enabled checkbox appears.
- [Configure the SNMP service](#) and download the ExtraHop MIB file


Enable or disable SSH Access

SSH access is enabled by default to enable users to securely log in to the ExtraHop command-line interface (CLI).

 **Note:** The SSH Service and the Management GUI Service cannot be disabled at the same time. At least one of these services must be enabled to provide access to the system.

Enable or disable the SSL Session Key Receiver (Sensor only)

You must enable the session key receiver service through the Administration settings before the ExtraHop system can receive and decrypt session keys from the session key forwarder. By default, this service is disabled.

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

Configure the SNMP service

Configure the SNMP service on your ExtraHop system so that you can configure your network device monitoring software to collect information about your ExtraHop system through the Simple Network Management Protocol (SNMP). For example, you can configure your monitoring software to determine how much free space is available on an ExtraHop system and send an alert if the system is over 95% full. Import the ExtraHop SNMP MIB file into your monitoring software to monitor all ExtraHop-specific SNMP objects.

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

Enabled

Select the checkbox to enable the SNMP service.

SNMP Community

Type a friendly name for the SNMP community.

SNMP System Contact

Type a valid name or email address for the SNMP system contact.

SNMP System Location

Type a location for the SNMP system.

3. Click **Save Settings**.

Next steps

Download the ExtraHop MIB file from the SNMP Service Configuration page.

Firmware

The Administration settings provide an interface to upload and delete the firmware on ExtraHop appliances. The firmware file must be accessible from the computer where you will perform the upgrade.

Before you begin

Be sure to read the [release notes](#) for the firmware version that you want to install. Release notes contain upgrade guidance as well as known issues that might affect critical workflows in your organization.


Upgrade the firmware on your ExtraHop system

The following procedure shows you how to upgrade your ExtraHop system to the latest firmware release. While the firmware upgrade process is similar across all ExtraHop appliances, some appliances have additional considerations or steps that you must address before you install the firmware in your environment. If you need assistance with your upgrade, contact ExtraHop Support.

Pre-upgrade checklist

Here are some important considerations and requirements about upgrading ExtraHop appliances.

- A system notice appears on consoles and sensors connected to ExtraHop Cloud Services when a new firmware version is available.
- Verify that your Reveal(x) 360 system has been upgraded to version 8.9 before upgrading your self-managed sensors.
- If you are upgrading from firmware version 8.7 or earlier, contact ExtraHop Support for additional upgrade guidance.
- If you have multiple types of ExtraHop appliances, you must upgrade them in the following order:
 1. Console
 2. Sensors (EDA and Ultra)
 3. Recordstores
 4. Packetstores
- If you are upgrading a console, apply the following guidance:
 - For large console deployments (managing 50,000 devices or more), reserve a minimum of one hour to perform the upgrade.
 - The console firmware version must be greater than or equal to the firmware version of all connected appliances. To ensure feature compatibility, all connected appliances should be running firmware version 8.7 or later.
- If you are upgrading recordstores, apply the following guidance:
 - Do not upgrade recordstores to a firmware version that is newer than the version installed on connected consoles and sensors.
 - After upgrading the console and sensors, [disable record ingest on the recordstore](#) before upgrading the recordstore.
 - You must upgrade all recordstore nodes in a recordstore cluster. The cluster will not function correctly if nodes are on dissimilar firmware versions.

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

- You must enable record ingest and shard reallocation from the Cluster Data Management page after all nodes in the recordstore cluster are upgraded.
- If you are upgrading packetstores, apply the following guidance:
 - Do not upgrade packetstores to a firmware version that is newer than the version installed on connected consoles and sensors.



Note: Your browser might time out after 5 minutes of inactivity. Refresh the browser page if the update appears incomplete.

If the browser session times out before the ExtraHop system is able to complete the update process, you can try the following connectivity tests to confirm the status up the upgrade process:

- Ping the appliance from the command line of another appliance or client workstation.
- From the Administration settings on a console, view the appliance status on the Manage Connected Appliances page.
- Connect to the appliance through the iDRAC interface.

Upgrade the firmware on a console and sensor

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **Firmware**.
3. From the **Available Firmware** drop-down list, select the version of firmware that you want to install. The recommended version is selected by default.
4. Click **Download and Install**.

After the firmware upgrade installs successfully, the ExtraHop appliance restarts.

Upgrade the firmware on recordstores

1. Download the firmware for the appliance from the [ExtraHop Customer Portal](#) to your computer.
2. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
3. Click **Cluster Data Management**.
4. Click **Disable Record Ingest**.
5. Click **Admin** to return to the main Administration page.
6. Click **Firmware**.
7. Click **Upgrade**.
8. On the Upgrade Firmware page, select one of the following options:
 - To upload firmware from a file, click **Choose File**, navigate to the `.tar` file you want to upload, and click **Open**.
 - To upload firmware from a URL, click **retrieve from URL** instead and then type the URL in the Firmware URL field.
9. Click **Upgrade**.
The ExtraHop system initiates the firmware upgrade. You can monitor the progress of the upgrade with the Updating progress bar. The appliance restarts after the firmware is installed.
10. Repeat steps 6-9 on all remaining recordstore cluster nodes.

Next steps

After all nodes in the recordstore cluster are upgraded, re-enable record ingest and shard reallocation on the cluster. You only need to perform these steps on one recordstore node.

1. In the Explore Cluster Settings section, click **Cluster Data Management**.
2. Click **Enable Record Ingest**.
3. Click **Enable Shard Reallocation**.

Upgrade the firmware on packetstores

1. Download the firmware for the appliance from the [ExtraHop Customer Portal](#) to your computer.
2. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
3. Click **Upgrade**.
4. On the Upgrade Firmware page, select one of the following options:
 - To upload firmware from a file, click **Choose File**, navigate to the `.tar` file you want to upload, and click **Open**.
 - To upload firmware from a URL, click **retrieve from URL** instead and then type the URL in the Firmware URL field.
5. (Optional) If you do not want to automatically restart the appliance after the firmware is installed, clear the **Automatically restart appliance after installation** checkbox.
6. Click **Upgrade**.
The ExtraHop system initiates the firmware upgrade. You can monitor the progress of the upgrade with the Updating progress bar. The appliance restarts after the firmware is installed.
7. If you did not choose to automatically restart the appliance, click **Reboot** to restart the system.
After the firmware update is installed successfully, the ExtraHop appliance displays the version number of the new firmware on the Administration settings.

Upgrade connected sensors in Reveal(x) 360

Administrators can upgrade sensors that are connected to Reveal(x) 360.

Before you begin

- Your user account must have privileges on Reveal(x) 360 for System and Access Administration or System Administration.

Here are some considerations about upgrading sensors:

- Sensors must be connected to ExtraHop Cloud Services
- Notifications appear when a new firmware version is available
- You can upgrade multiple sensors at the same time

1. Log in to Reveal(x) 360.
2. Click the System Settings icon and then click **Sensors**.

Sensors that are eligible for upgrade display an up arrow in the Sensor Version field.

| Reveal(x) 360 Sensors | | | | | | |
|-------------------------------------|----------|--------------|--------|----------------------------|----------------|---------------------|
| Name <input type="text"/> | | 7 results | | New firmware is available. | | |
| <input type="checkbox"/> | Name | Sensor Model | Status | License | Sensor Version | Date Added |
| <input checked="" type="checkbox"/> | sensor-1 | EDA1100V | Online | Valid | ↑ 8.8.0.1362 | 2022-03-16 10:15:53 |
| <input checked="" type="checkbox"/> | sensor-2 | EDA1100V | Online | Valid | ↑ 8.8.0.1414 | 2022-03-11 08:43:58 |

3. Select the checkbox next to each sensor that you want to upgrade.
4. In the Sensor Details pane, select the firmware version from the **Available Firmware** drop-down list.
The drop-down list only displays versions that are compatible with the selected sensors.
Only the selected sensors that have a firmware upgrade available appear in the Sensor Details pane.

5. Click **Install Firmware**.

When the upgrade completes, the Sensor Version field is updated with the new firmware version.

System Time

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

- [Configure the system time.](#)
- View information about the appliance settings in the System Time section:

Time Zone

Displays the currently selected time zone

System Time

Displays the current system time.

Time Servers

Displays a comma-separated list of configured time servers.

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

remote

The host name or IP address of the remote NTP server you have configured to synchronize with.

st

The stratum level, 0 through 16.

t

The type of connection. This value can be `u` for unicast or manycast, `b` for broadcast or multicast, `l` for local reference clock, `s` for symmetric peer, `A` for a manycast server, `B` for a broadcast server, or `M` for a multicast server.

when

The last time when the server was queried for the time. The default value is seconds, or `m` is displayed for minutes, `h` for hours, and `d` for days.

poll

How often the server is queried for the time, with a minimum of 16 seconds to a maximum of 36 hours.

reach

Value that shows the success and failure rate of communicating with the remote server. Success means the bit is set, failure means the bit is not set. 377 is the highest value.

delay

The round trip time (RTT) of the ExtraHop appliance communicating with the remote server, in milliseconds.

offset

Indicates how far off the ExtraHop appliance clock is from the reported time the server gave you. The value can be positive or negative, displayed in milliseconds.

jitter

Indicates the difference, in milliseconds, between two samples.

Configure the system time

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

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the **Appliance Settings** section, click **System Time**.
3. Click **Configure Time**.
4. Select your time zone from the drop-down list then click **Save and Continue**.
5. On the Time Setup page, select one of the following options:

- Set time manually



Note: You cannot manually set the time for systems that are managed by a Command appliance or Reveal(x) 360.

- Set time with NTP server

6. Select **Set time with NTP server** and then click **Select**.

The ExtraHop time servers, `0.extrahop.pool.ntp.org`, `1.extrahop.pool.ntp.org`, `2.extrahop.pool.ntp.org`, and `3.extrahop.pool.ntp.org` appear in the first four Time Server fields by default.

7. Type the IP address or fully qualified domain name (FQDN) for the time servers in the Time Server fields. You can have up to nine time servers.



Tip: After adding the fifth time server, click **Add Server** to display up to four additional timer server fields.

8. Click **Done**.

The NTP Status table displays a list of NTP servers that keep the system clock in sync. To sync the current system time a remote server, click the **Sync Now** button.

Shutdown or restart

You can shut down or restart the Trace appliance in the Administration settings.

1. In the Appliance Settings section, click **Shutdown or Restart**.
2. In the Actions column, select one of the following options:
 - Click **Restart** and then on the confirmation page, click **Restart** to restart the appliance.
 - Click **Shutdown**, and then on the confirmation page, click **Shut down** to shut down the system and power off the appliance.

License

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

Manage license

Provides an interface to add and update the ExtraHop system

System Information

Displays the identification and expiration information about the ExtraHop system.

Features

Displays the list of licensed features and whether the licensed features are enabled or disabled.

Register your ExtraHop system

This guide provides instructions on how to apply a new product key and activate all of your purchased modules. You must have privileges on the ExtraHop system to access the Administration settings.

Register the appliance

Before you begin



Note: If you are registering a sensor or a console, you can optionally enter the product key after you accept the EULA and log in to the ExtraHop system (`https://<extrahop-ip-address>/`).

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. Review the license agreement, select **I Agree**, and then click **Submit**.
3. On the login screen, type `setup` for the username.
4. For the password, select from the following options:
 - For 1U and 2U appliances, type the serial number printed on the label on the back of the appliance. The serial number can also be found on the LCD display on the front of the appliance in the `Info` section.
 - For the EDA 1100, type the serial number displayed in the `Appliance info` section of the LCD menu. The serial number is also printed on the bottom of the appliance.
 - For the EDA 1200, type the serial number printed on the back of the appliance.
 - For a virtual appliance in AWS, type the instance ID, which is the string of characters that follow `i-` (but not `i-` itself).
 - For a virtual appliance in GCP, type the instance ID.
 - For all other virtual appliances, type `default`.
5. Click **Log In**.
6. In the Appliance Settings section, click **License**.
7. Click **Manage License**.
8. If you have a product key, click **Register** and type your product key into the field.



Note: If you received a license file from ExtraHop Support, click **Manage License**, click **Update**, then paste the contents of the file into the Enter License field. Click **Update**.

9. Click **Register**.

Next steps

Have more questions about ExtraHop licensing works? See the [License FAQ](#).

Troubleshoot license server connectivity

For ExtraHop systems licensed and configured to connect to ExtraHop Cloud Services, registration and verification is performed through an HTTPS request to ExtraHop Cloud Services.

If your ExtraHop system is not licensed for ExtraHop Cloud Services or is not yet licensed, the system attempts to register the system through a DNS TXT request for `regions.hopcloud.extrahop.com` and an HTTPS request to all [ExtraHop Cloud Services regions](#). If this request fails, the system tries to connect to the ExtraHop licensing server through DNS server port 53. The following procedure is useful to verify that the ExtraHop system can communicate with the licensing server through DNS.

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

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

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

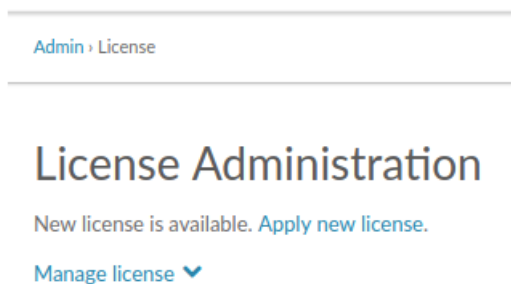
```
Non-authoritative answer:
d.extrahop.com nameserver = ns0.use.d.extrahop.com.
d.extrahop.com nameserver = ns0.usw.d.extrahop.com.
```

If the name resolution is not successful, make sure that your DNS server is properly configured to lookup the `extrahop.com` domain.

Apply an updated license

When you purchase a new protocol module, service, or feature, the updated license is automatically available on the ExtraHop system. However you must apply the updated license to the system through the Administration settings for the new changes to take effect.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **License**. A message appears about the availability of your new license, as shown in the following figure.



3. Click **Apply new license**. The capture process restarts, which might take a few minutes.



Note: If your license is not automatically updated, [troubleshoot licensing server connectivity](#) or contact ExtraHop Support.

Update a license

If ExtraHop Support provides you with a license file, you can install this file on your appliance to update the license.



Note: If you want to update the product key for your appliance, you must [register your ExtraHop system](#).

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **License**.
3. Click Manage License.
4. Click **Update**.
5. In the Enter License text box, enter the licensing information for the module.
Paste the license text provided to you by ExtraHop Support. Be sure to include all of the text, including the `BEGIN` and `END` lines, as shown in the example below:

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

```


mod_amf=0;
live_capture=1;
capture_upload=1;
...
ssl_decryption=0;
+++;
ABCabcDE/FGHIjklm12nopqrstuvwxyzXYZAB12345678abcde901abCD;
12ABCDEFGH1HIJklmnOP+1aA=;
=abcd;
-----END EXTRAHOP LICENSE-----

```

6. Click **Update**.

Disks

The Disks page provides information about the configuration and status of the disks in your Trace appliance as well the disks in any attached storage units.

 **Note:** We recommend that you configure the settings to receive [email notifications](#) about your system health. If a disk is beginning to experience problems, you will be alerted.

The following information displays on the page:

Drive Map

Provides a visual representation of the front of the Trace appliance. The drive map does not appear in the Administration settings on the virtual Trace appliance.

RAID Disk Details

Provides access to detailed information about all the disks in the node.

Packetstore

Displays information about disks reserved for packet storage and the option to encrypt the packetstore disk. For more information, see the [Encrypt the packetstore disk](#) section.

Direct Connected Disks

Displays information about the SD memory cards. The memory cards have the following roles:

Firmware

Displays information about disks reserved for the firmware.

Utility


Displays information about disks reserved for system files.


Extended Storage Units

Displays information about ExtraHop extended storage units.

Encrypt the packetstore disk

You can encrypt the disk, including attached extended storage units that packet captures are stored on for increased security. The packetstore disk is secured with 256-bit AES encryption.

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

 **Important:** The packetsore is locked when the Trace appliance is restarted. Before packets can written to disk, you must unlock the disk from the Packetstore Encryption Settings page.

1. In the Appliance Settings section, click **Disks**.
2. Navigate to the Packetstore Encryption Settings page.

- | Option | Description |
|-------------------------|---|
| For virtual appliances | In the Direct Connected Disks table, click Settings . |
| For physical appliances | In the Packetstore section, next to Packetstore Encryption, click Settings . |
3. Click **Encrypt Packetstore**.
 4. Specify a disk encryption key by choosing one of the following options.
 - To encrypt the disk with a passphrase, type a passphrase of at least 8 characters into the Passphrase and Confirm fields. The passphrase must contain a combination of uppercase letters, lowercase letters, numbers, and special characters.
 - To encrypt the disk with a key file, click **Choose File**, and then browse to an encryption key file.
 5. Click **Encrypt**.

Change the packet capture disk encryption key

1. In the Status section, click **Disks**.
2. In the Datastore section, click **Packetstore Encryption Settings**.
3. Click **Change Packetstore Encryption Key**.
4. Specify the existing encryption key.

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

5. Specify a new disk encryption key.

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

6. Click **Change Key**.

Add storage capacity to the ETA 6150 or 8250

Adding additional storage capacity to your ExtraHop packetstore enables you to store more packets and extend the amount of lookback available when running packet queries. You can safely add ExtraHop Extended Storage Units to a packetstore and retain all packets currently stored on the packetstore.

Compatibility

The ExtraHop Extended Storage Unit (ESU) is available in two models, the 72 TB ESU and the 96 TB ESU.

| ExtraHop Packetstore | Extended Storage Unit |
|----------------------|---|
| ETA 6150 | <ul style="list-style-type: none"> • 72 TB ESU • 96 TB ESU <p>You can attach a mix of 72 TB and 96 TB ESUs to the ETA 6150.</p> |
| ETA 8250 | <ul style="list-style-type: none"> • 96 TB ESU |

You can attach up to four ESUs to a packetstore.

Installation prerequisites

Before connecting your ESU, make sure you have the following items available:

- ExtraHop packetstore with firmware 7.2 or later. Firmware 7.4 is required to encrypt the ESU. If you have not deployed the packetstore, follow the instructions in the [Deploy the ETA 6150 packetstore](#) and [Deploy the ETA 8250 packetstore](#) guides.
- ExtraHop license for the extended packetstore feature
- ExtraHop extended storage unit
- 2U of rack space and electrical connections for 2 x 600 W power supplies.
- Power cables
- SAS cables
- Rail kit

Set up the extended storage unit

1. Install the extended storage unit in your data center with the included rack-mounting kit. The mounting kit supports most four-post racks with either round or square holes.
2. Connect the power cables to the power supply units (PSUs).

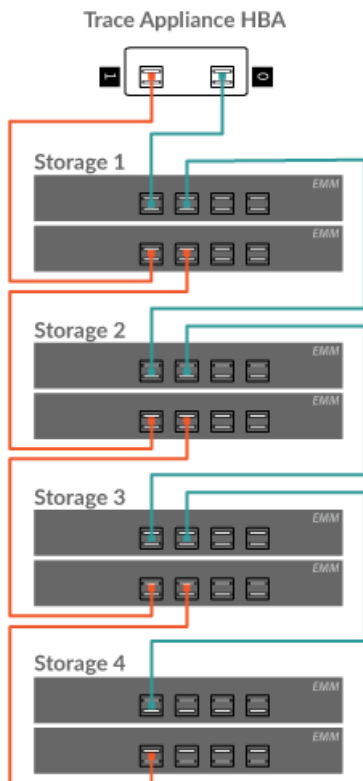
Shut down the packetstore

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **Shutdown or Restart**.
3. In the Actions column, click **Shutdown**.
4. On the confirmation page, click **Shut down**.

Connect the extended storage unit

The extended storage unit connects to the packetstore through both of the two enclosure management modules (EMMs). Each EMM has four ports for connecting the SAS cables.

In a redundant configuration, the storage units are linked together in a series, with one of the extended storage units connected to both host bus adapter (HBA) ports on the packetstore, as shown in the following figure.



1. Connect the SAS cables to the EMM SAS connectors on the extended storage unit and to the HBA ports on the packetstore. Connect the SAS cable as follows for the first storage unit:
 - HBA port 0 (on the right) to upper EMM port 1
 - HBA port 1 (on the left) to lower EMM port 1

Push the cable into the connector until it clicks into place. Green link lights will appear next to the ports when the ESU and packetstore are both powered on.

- Note:**
- Connectors on both ends of the SAS cable are universally keyed. You can connect either end of the cable to the EMM or the HBA on the packetstore.
 - Attach the SAS cable to the EMM with the blue pull-tab oriented on the top of the connector.
 - Attach the SAS cable to the HBA on the packetstore with the blue pull-tab oriented on the bottom of the connector.
 - To remove the SAS cable, pull the pull-tab to release the cable from the connector on the EMM and the packetstore.

2. Cable any additional storage units as illustrated above.
3. Make sure that the power switch on both PSUs is turned off and then connect the PSUs to the power source.
4. Power on the PSUs on each ESU and then wait 60 seconds before powering on the Trace appliance.

Attach the extended storage unit

1. Power on the packetstore.
2. Log in to the Administration settings.

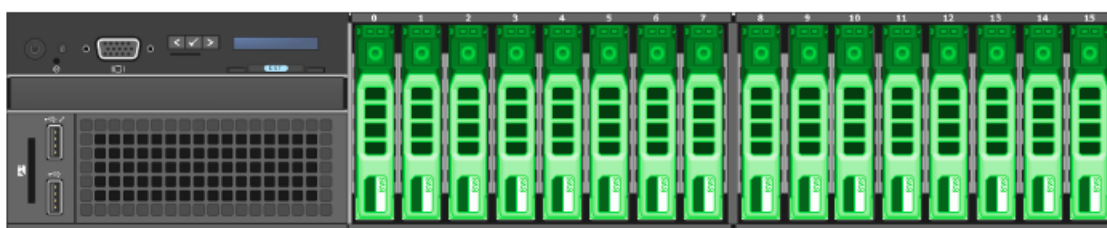
- Note:** If the packetstore was previously encrypted, it will be locked when it is powered on. An encrypted packetstore must be unlocked before you can attach the ESU.

Appliance Settings

- Running Config
- Firmware
- System Time
- Shutdown or Restart
- License
- Disks *(Locked)*
- Reset Packetstore

3. In the Appliance Settings section, click **Disks**.
4. Confirm that all drives in the Drive Map section are colored green, indicating they are healthy. If any disk is unhealthy, contact [ExtraHop Support](#).

Drive Map



5. At the bottom of the Disks page, click **Extended Storage Units**.
6. In the Unused Disks section for the extended storage unit, click **Attach**, and then click **OK**.

| | |
|-------------------------|------------------------|
| RAID Status | Unused |
| RAID Level | None |
| Extended Storage Status | Unconfigured |
| Manage Extended Storage | Attach |

7. After the configuration is complete, confirm that all drives in the extended storage unit are colored green, indicating they are healthy. If any disk is unhealthy (yellow), contact [ExtraHop Support](#).

Extended Storage Unit 0



8. Repeat steps 6 and 7 for any additional extended storage units.
9. (Optional) If the packetstore is locked, you must unlock it from the Packetstore Encryption Settings page before the ESU can be encrypted and new packets can be stored.

Managing extended storage units with a foreign packetstore status

When an extended storage unit with an existing RAID configuration is connected to a RAID controller on the Trace appliance, the extended storage unit is designated as “foreign”. This status can occur when an extended storage unit was previously connected and then disconnected from the RAID controller on the

Trace appliance and when the extended storage unit was configured on a RAID controller other than the Trace appliance it was originally connected to.

For extended storage units disconnected and then reconnected to the same Trace appliance


1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **Disks**.
3. Click **Extended Storage Units**.
4. Click **Import foreign packetstore disks**.
The extended storage unit is automatically configured and ready to store packets.

For extended storage units configured on a device other than the Trace appliance

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **Disks**.
3. Click **Extended Storage Units**.
4. Click **Import foreign packetstore disks**, and then click **OK**.
5. In the RAID Info section, click **Unconfigure**, and then click **OK**.
6. After the packetstore disk is deleted, click **Attach** and then click **OK**.
The extended storage unit is automatically configured and ready to store packets.

Reset Packetstore

In certain circumstances, you might want to reset the packetstore. For example, if you accidentally collected packets with sensitive data or from the wrong data feed, you can reset the datastore so the packets do not appear in any packet queries.

 **Warning:** If you reset the packetstore, all existing packets will be inaccessible to packet queries.

1. In the Appliance Settings section, click **Reset Packetstore**.
2. Type **YES** in the confirmation field and then click **Reset Packetstore**.

It typically takes less than a minute to reset the packetstore.

Trace Cluster Settings

The Trace Cluster Settings section includes the following sections:

Connect to Reveal(x) 360

This option only appears when the packetstore is licensed for Reveal(x) 360.

Manager

Enable a console to remotely run support scripts and upgrade firmware on the packetstore.

View the hostname of the console that is configured to manage the packetstore as well as a list of all sensors and consoles connected to the packetstore.

Packet Query Status

View a list of all packet queries generated from a connected console and connected sensors.

Manager

The Manager page contains the following information and controls:

Manager

Displays the hostname of the console that is configured to manage the packetstore. To connect a console through a tunneled connection, click **Manage with a Command Appliance**. A tunneled connection might be required if a direct connection cannot be established through the Command appliance.

Click **Remove Manager** to remove the console as the manager.



Note: The packetstore can be managed by only one console.

Connected Appliances

Displays a table of all sensors and consoles connected to the packetstore. The table includes the hostname, product key and IP address of the connected ExtraHop system.

Packet Query Status

The Packet Query Status page provides a collection of metrics about the packetstore.

The metrics on this page can help you troubleshoot problems and determine why the packetstore is not performing as expected.

Packet Query Status

Displays statistics about packet queries run from the Packets page.

If the number of simultaneous packet queries exceeds the maximum allotted system memory, errors might occur and you must delete in-progress or completed queries by clicking the **Remove** or **Remove All** button before you can create new queries. Queries are cached until you navigate away from the Packets page.

Packetstore Disks

Displays statistics about packet storage disks.

SSL Session Key Storage

Displays statistics about session keys stored on the packetstore. For information about session key storage, see [Store SSL session keys on connected packetstores](#).

Remove packet queries

You can remove one or more packet queries to clear query memory and disk cache.


1. In the Trace Cluster Settings section, click **Packet Query Status**.
2. Do one of the following:
 - To remove a single query, click **Remove** in the Actions column of the query you want to remove.
 - To remove all listed queries, click **Remove All**.

Manage with a console

Connect the packetstore to a console to remotely run support scripts and upgrade firmware on the packetstore from the console.

The packetstore connects to the console through a tunneled connection. Tunneled connections are required in network environments where a direct connection from the console is not possible because of firewalls or other network restrictions.

Before you begin

 **Note:** This procedure only enables you to perform management functions from a connected console or Reveal(x) 360. To search and download packets from the ExtraHop system, follow the instructions in [Connect sensors and console to the packetstore](#).

1. In the Trace Cluster Settings section, click **Manager**.
2. Click **Manage with Command Appliance**.
3. Configure the following settings:
 - Command appliance hostname : Type the hostname or IP address of the console.
 - Command appliance setup password : Type the `setup` user password for the console.
 - Trace appliance nickname : Type a friendly name for the ExtraHop packetstore. If no nickname is entered, the node is identified by the hostname.
4. Select the Manage with Command appliance checkbox and then click **Manage**.