ExtraHop 9.2
ExtraHop Explore Admin UI Guide

© 2024 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: 2024-07-22

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 Explore Admin UI 6
Supported browsers 6

Status and Diagnostics 7
Health 7
Audit Log 9
Fingerprint 9
Advanced Options 9
Generate a new fingerprint 9
Configure externally signed SSL certificate 9
Support Scripts 10
Run the default support script 10
Run a custom support script 10
Explore Cluster Status 10
Delete records 11
Restore the cluster state 12

Network Settings 13
Connect to ExtraHop Cloud Services 13
Configure your firewall rules 14
Connect to ExtraHop Cloud Services through a proxy 14
Bypass certificate validation 15
Connectivity 15
Configure an interface 16
Interface throughput 17
Set a static route 18
Enable IPv6 for an interface 18
Global proxy server 19
ExtraHop Cloud proxy 19
Bond interfaces 19
Create a bond interface 20
Modify bond interface settings 20
Destroy a bond interface 20
Notifications 21
Configure email settings for notifications 21
Add a new notification email address on an Explore or Trace appliance 22
Configure settings to send notifications to an SNMP manager 22
Download the ExtraHop SNMP MIB 23
Send system notifications to a remote syslog server 23
SSL Certificate 23
Upload an SSL certificate 23
Generate a self-signed certificate 24
Create a certificate signing request from your ExtraHop system 24
Trusted Certificates 25
Add a trusted certificate to your ExtraHop system 25

Access Settings 26
Passwords 26

Change the default password for the setup user 26
Support Access 26
Generate SSH key 26
Regenerate or revoke the SSH key 27
Users 27
Add a local user account 27
Users and user groups 28
Local users 28
Remote Authentication 28
Remote users 28
User groups 29
User privileges 29
Sessions 34
Remote Authentication 34
Configure remote authentication through LDAP 34
Configure user privileges for remote authentication 36
Configure remote authentication through RADIUS 37
Configure remote authentication through TACACS+ 38
Configure the TACACS+ server 39
API Access 40
Manage API key access 41
Configure cross-origin resource sharing (CORS) 41
Generate an API key 41
Privilege levels 41

Appliance Settings 45

Running Config 45
Save system settings to the running config file 45
Edit the running config 46
Download the running config as a text file 46
Disable ICMPv6 Destination Unreachable messages 46
Disable specific ICMPv6 Echo Reply messages 46
Services 47
Configure the SNMP service 47
Configure the SNMPv1 and SNMPv2 service 47
Configure the SNMPv3 service 48
Firmware 48
Upgrade the firmware on your ExtraHop system 48
Pre-upgrade checklist 49
Upgrade the firmware on a console and sensor 49
Upgrade the firmware on recordstores 50
Upgrade the firmware on packetstores 50
Upgrade connected sensors in Reveal(x) 360 51
System Time 51
Configure the system time 52
Shutdown or restart 53
Restart an Explore appliance component 53
License 54
Register your ExtraHop system 54
Register the appliance 54
Troubleshoot license server connectivity 55
Apply an updated license 55
Update a license 55
Disks 56

Explore Cluster Settings 57

Create a recordstore cluster 57
Cluster Members 60
Remove a node from the cluster 60
Manager and Connected Appliances 61
Cluster Data Management 61
Connect to a Command appliance 61
Restore the cluster state 62

Introduction to the ExtraHop Explore Admin UI

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

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

After you have deployed your ExtraHop recordstore, see the Explore 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 page displays metrics and logging data about the current state of the Explore appliance and enables system administrators to view the overall system health.

Health
Provides metrics to view the operating efficiency of the Explore appliance.

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

Fingerprint
Provides the unique hardware fingerprint for the Explore appliance.

Support Scripts
Enables you to upload and run support scripts.

Explore Cluster Status
Provides status information about the cluster, including indices.

Health

The Health page provides a collection of metrics that enable you check the operation of the Explore 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
Specifies the percentage of CPU usage associated with the Explore appliance user

CPU System
Specifies the percentage of CPU usage associated with the Explore appliance.

CPU Idle
Identifies the CPU idle percentage associated with the Explore appliance.

CPU IO
Specifies the percentage of CPU usage associated with the Explore appliance IO functions.

Service Status
Reports the status of Explore appliance system services

exadmin
Specifies the amount of time the Explore appliance web portal service has been running.

exconfig
Specifies the amount of time the Explore appliance config service has been running

exreceiver
Specifies the amount of time the Explore appliance receiver service has been running.

exsearch
Specifies that amount of time that the Explore appliance search service has been running.

Interfaces
Reports the status of Explore appliance network interfaces.

RX packets

Specifies the number of packets received by the Explore appliance on the specified interface.

RX Errors

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

RX Drops

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

TX Packets

Specifies the number of packets transmitted by the Explore appliance on the specified interface.

TX Errors

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

TX Drops

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

RX Bytes

Specifies the number of bytes received by the Explore appliance on the specified interface.

TX Bytes

Specifies the number of bytes transmitted by the Explore appliance on the specified interface.

Partitions

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

Name

Specifies the Explore appliance settings that are stored on disk.

Options

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

Size

Specifies the size in gigabytes for the identified component.

Utilization

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

Record Sources

Displays metrics about the records that are sent from the Discover appliance to the Explore cluster.

Source EDA

Displays the name of the Discover appliance that is sending records to the Explore cluster.

Last Update

Displays the timestamp when record collection began. The value is reset automatically every 24 hours or whenever the Explore appliance is restarted.

RX Bytes

Displays the number of compressed record bytes received from the Discover appliance.

Record Bytes

Displays the number of bytes received from the Discover appliance.

Record Bytes Saved

Displays the number of bytes successfully saved to the Explore appliance.

Records Saved

Displays the number of records successfully saved to the Explore appliance.

Record Errors

Displays the number of individual record transfers that resulted in an error. This value indicates the number of records that did not transfer successfully from the exreceiver process.

TXN Errors

Displays the number of bulk record transactions that resulted in an error. Errors in this field might indicate missing records.

TXN Drops

Displays the number of bulk records transactions that did not complete successfully. All records in the transaction are missing.

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.

Advanced Options

On Explore appliances, you can configure an externally signed certificate. Signed certificates can enable you to meet the compliance needs of your company. The fingerprint is automatically re-generated.

By default, the fingerprint is derived from the public key of the internal SSL certificate. This separate SSL certificate only encrypts communications between ExtraHop appliances and is not required for communication between ExtraHop appliances and external HTTP clients.

Generate a new fingerprint

Note: You do not need to generate a fingerprint before you configure an externally signed certificate.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. Click **Fingerprint**.
3. Click **Advanced Options**.
4. Click **Generate new fingerprint**.
5. Click **OK**.

Configure externally signed SSL certificate

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. Click **Fingerprint**.
3. Click **Advanced Options**.

4. Click **Configure externally signed SSL certificate**.
5. Copy the certificate request from the text box and submit it to your Certificate Authority (CA).
6. After you receive the signed SSL certificate from your CA, return to the Configure Externally-signed SSL Certificate page in the Administration settings and paste the content of the certificate file (.crt) into the second text box.
7. Click **Install**.
   After the certificate is installed, a new fingerprint is generated from the newly added public key.
8. Repeat these steps for all other Explore appliances in the cluster.

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.

Explore Cluster Status

The Explore Cluster Status page provides details about the health of the Explore appliance.

The metrics on this page can help you troubleshoot problems and determine why the Explore cluster is not performing as expected. In addition, you can delete a set of records by date from this page.

Index Summary

Displays metrics related to the number of indices, shards, and primary records stored on the appliance.

Cluster Node Summary

Displays the number of dedicated manager nodes, dedicated data nodes, and data eligible manager nodes in the Explore cluster.

Index Details

Date (UTC)

Displays the date the index was created.

ID

Displays the ID of the index. An ID other than 0 means that an index with the same date, but from a different source exists on the cluster.

Source

Displays the hostname or IP address of the Discover appliance where the record data originated.

Records

Displays the total number of records sent to the Explore appliance.

Size

Displays the size of the index.

Status

Displays the replication status of data on the cluster.

Shards

Displays the number of shards in the index.

Unallocated Shards

Displays the number of shards that have not been allocated to a node. Unallocated shards are typically replica shards that must be kept on a different node than the node with the corresponding primary shard, but there are not enough nodes in the cluster. For example, a cluster with just one member will not have a place to store the replica shards, so with the default replication level of 1, the index will always have unassigned shards and have a `yellow` status.

Relocating Shards

Displays the number of shards that are moving from one node to another. Relocating shards typically occurs when an Explore node in the cluster fails.

Delete records

In certain circumstances, such as moving an Explore cluster from one network to another, you might want to delete all of the records from a cluster.

You can delete records by index, which is a collection of records that were created on the same day. Indexes are named according to the following pattern:

```
<node-id>-<date>-<index-id>
```

For example, an index dated `2016-5-16` contains records that were created on May 16, 2016 (dates are specified in UTC). You can delete all data for a given day or span of days; for example, you might want to delete record content that you know contains sensitive information.

1. In the Status and Diagnostics section, click **Explore Cluster Status**.
2. In the Index Details section, select the checkbox for each index that you want to delete.

   The Source column displays the name of the sensor that collected the data.

3. Click **Delete Selected**.
4. Click **OK**.

Restore the cluster state

In rares instances, the Explore cluster might not recover from a `Red` status, as seen in the Status section on the Explore Cluster Status page. When this state occurs, it is possible to restore the cluster to a `Green` state.

When you restore the cluster state, the Explore cluster is updated with the latest stored information about the Explore nodes in the cluster and all other connected Discover and Command appliances.

Important: If you have recently restarted your Explore cluster, it might take an hour before the cluster status `Green` appears, and restoring the cluster might not be necessary. If you are unsure whether you should restore the cluster state, contact ExtraHop Support.

1. In the Explore Cluster Settings section, click **Restore Cluster State**.
2. On the Restore Cluster State page, click **Restore Cluster State**.
3. Click **Restore Cluster** to confirm.

Network Settings

The Network Settings section includes 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 Explore appliance has four 10/100/1000baseT network ports and two 10GbE SFP+ network ports. By default, the Gb1 port is configured as the management port and requires an IP address. The Gb2, Gb3 and Gb4 ports are disabled and not configurable.

You can configure either of the 10GbE networks ports as the management port, but you can only have one management port enabled at a time.

Before you begin configuring the network settings on an Explore appliance, verify that a network patch cable connects the Gb1 port on the Explore appliance to the management network. For more information about installing an Explore appliance, refer to the Deploy the EXA 5200 recordstore guide or contact ExtraHop Support for assistance.

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

Before you begin

- Reveal(x) 360 systems are automatically connected to ExtraHop Cloud Services, however, you might need to allow access through network firewalls.

- You must apply the relevant license on the ExtraHop system before you can connect to ExtraHop Cloud Services. See the License FAQ for more information.
- You must have setup or system and access administration privileges to access Administration settings.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **ExtraHop Cloud Services**.
3. Click **Terms and Conditions** to read the content.
4. Read the terms and conditions, and then select the checkbox.
5. Click **Connect to ExtraHop Cloud Services**.

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

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

Configure your firewall rules

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

Open access to Cloud Services

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

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

Open access to Cloud Recordstore

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

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

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

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

Connect to ExtraHop Cloud Services through a proxy

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

Before you begin
Verify whether your proxy vendor is configured to perform machine-in-the-middle (MITM) when tunneling SSH over HTTP CONNECT to localhost:22. ExtraHop Cloud Services deploys an encrypted inner SSH

tunnel, so traffic will not be visible to MITM inspection. We recommend that you create a security exception and disable MITM inspection for this traffic.

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

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

Bypass certificate validation

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

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

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

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

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

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

Connectivity

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

Interface Status

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

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

Network Settings

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

Proxy Settings

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

Bond Interface Settings

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

Interfaces

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

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

Configure an interface

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

Option	Description
Disabled	The interface is disabled.
Monitoring (receive only)	Monitors network traffic.
Management	Manages the ExtraHop sensor.
Management + 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 + RPCAP/ERSPAN/VXLAN/ GENEVE Target	Manages the ExtraHop sensor and captures traffic forwarded from a packet forwarder, ERSPAN*, VXLAN**, or GENEVE***. While 10 GbE management + capture interfaces on the EDA 10200, EDA 9200, and ETA 8250 can conduct management functions at 10 Gbps speeds, processing traffic such as ERSPAN, VXLAN, and GENEVE is limited to 1 Gbps. **Tip:** In environments with asymmetric routing adjacent to the high-performance interfaces, ping replies might not get back to the sender.
High-Performance ERSPAN/VXLAN/GENEVE Target	Captures traffic forwarded from ERSPAN*, VXLAN**, or GENEVE***. This interface mode enables the port to handle more than 1 Gbps. Set this interface mode if the ExtraHop sensor has a 10 GbE port. This interface mode only requires that you configure an IPv4 address.

*The ExtraHop system supports the following ERSPAN implementations:

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

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

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

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

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

   - **Auto-negotiate**
   - **10 Gbps**
   - **25 Gbps**
   - **40 Gbps**
   - **100 Gbps**

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

5. 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. Configure the TCP health check port. This setting is only configurable on high-performance interfaces and is required when ingesting GENEVE traffic from an AWS Gateway Load Balancer (GWLB). The port number value must match the value configured in AWS. For more information, see Forward GENEVE-encapsulated traffic from an AWS Gateway Load Balancer.
7. (Optional) Enable IPv6.

   For more information about configuring IPv6, see Enable IPv6 for an interface.
8. (Optional) Manually add routes.
9. 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 interfaces on your ExtraHop system together into a single logical interface that has one IP address for the combined bandwidth of the member interfaces. Bonding interfaces enable a larger throughput with a single IP address. This configuration is also known as link aggregation, port channeling, link bundling, Ethernet/network/NIC bonding, or NIC teaming. Bond interfaces cannot be set to monitoring mode.

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

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

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

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

Create a bond interface

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

1. Click **Create Bond Interface**.
2. Configure the following options:

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

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

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

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

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

Modify bond interface settings

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

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

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

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

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

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

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

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

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

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

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

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

Destroy a bond interface

When a bond interface is destroyed, the separate interface members of the bond interface return to independent interface functionality. One member interface is selected to retain the interface settings for

the bond interface and all other member interfaces are disabled. If no member interface is selected to retain the settings, the settings are lost and all member interfaces are disabled.

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

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

Field	Description	Examples
Common Name	The fully qualified domain name (FQDN) of the ExtraHop system. The FQDN must match one of the Subject Alternative Names.	*.example.com discover.example.com
E-mail Address	The email address of the primary contact for your organization.	webmaster@example.com
Organizational Unit	The division of your organization handling the certificate.	IT Department
Organization	The legal name of your organization. This entry should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.	Example, Inc.

Field	Description	Examples
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

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

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

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

Trusted Certificates

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

Add a trusted certificate to your ExtraHop system

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

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

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

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

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

Access Settings

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

Passwords

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

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

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

Change the default password for the setup user

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

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

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

Support Access

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

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

Generate SSH key

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

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

Regenerate or revoke the SSH key

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

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

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

Users

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

Add a local user account

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

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

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

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

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

   • Password: The password for this account.

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

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

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

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

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. For Reveal(x) Enterprise, users with system access and administration privileges can access all areas of the ExtraHop system, including packets, session keys, and detections. For Reveal(x) 360 system access and administration privileges, access to packets, session keys, and detections must be assigned separately.

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Activity Maps							
Create, view, and load shared activity maps	Y	Y	Y	Y	Y	Y	N
Save activity maps	Y	Y	Y	Y	Y	N	N
Share activity maps	Y	Y	Y	Y	N	N	N
Alerts							
View alerts	Y	Y	Y	Y	Y	Y	Y
Create and modify alerts	Y	Y	Y	N	N	N	N
Analysis Priorities							
View Analysis Priorities page	Y	Y	Y	Y	Y	Y	N
Add and modify analysis levels for groups	Y	Y	Y	N	N	N	N
Add devices to a watchlist	Y	Y	Y	N	N	N	N
Transfer priorities management	Y	Y	Y	N	N	N	N
Bundles							

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Create a bundle	Y	Y	Y	N	N	N	N
Upload and apply a bundle	Y	Y	Y	N	N	N	N
View list of bundles	Y	Y	Y	Y	Y	Y	N
Dashboards							
View and organize dashboards	Y	Y	Y	Y	Y	Y	Y
Create and modify dashboards	Y	Y	Y	Y	Y	N	N
Share dashboards	Y	Y	Y	Y	N	N	N
Detections	**Note:** Machine learning detections require a connection to ExtraHop Cloud Services. Administrators can configure the Detections Access Control global policy to specify which 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
Acknowledge Detections	Y	Y	Y	Y	Y	N	N
Modify detection status and notes	Y	Y	Y	Y	N	N	N
Create and modify investigations	Y	Y	Y	Y	N	N	N
Create and modify tuning rules	Y	Y	Y	N	N	N	N
Device Groups	Administrators can configure the Device Group Edit Control global policy to specify whether users with limited write privileges can create and edit device groups.						
Create and modify device groups	Y	Y	Y	Y (If the global privilege policy is enabled)	N	N	N

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Metrics							
View metrics	Y	Y	Y	Y	Y	Y	N
Notification Rules							
Create and modify detection notification rules	Y	Y	Y	N	N	N	N
Create and modify threat briefing notification rules	Y	Y	Y	N	N	N	N
Records (Explore appliance)							
View record queries	Y	Y	Y	Y	Y	Y	N
View record formats	Y	Y	Y	Y	Y	Y	N
Create, modify, and save record queries	Y	Y	Y	N	N	N	N
Create, modify, and save record formats	Y	Y	Y	N	N	N	N
Scheduled Reports (Command appliance)							
Create, view, and manage scheduled reports	Y	Y	Y	Y	N	N	N
Threat Intelligence							

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Manage threat collections	Y	Y	N	N	N	N	N
View threat intelligence information	Y	Y	Y	Y	Y	Y	N
Triggers							
Create and modify triggers	Y	Y	Y	N	N	N	N
Administrative Privileges							
Access the ExtraHop Administration settings	Y	Y	N	N	N	N	N
Connect to other appliances	Y	Y	N	N	N	N	N
Manage other appliances (Command appliance)	Y	Y	N	N	N	N	N
Manage users and API access	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.

Detections 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.
  - No 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**.

Packet and Session Key Access

- Packet slices only
- Packets only

- Packets and session keys
- No access

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**
   - **Packet slices only**
   - **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**
   - **Packet slices only**
   - **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**

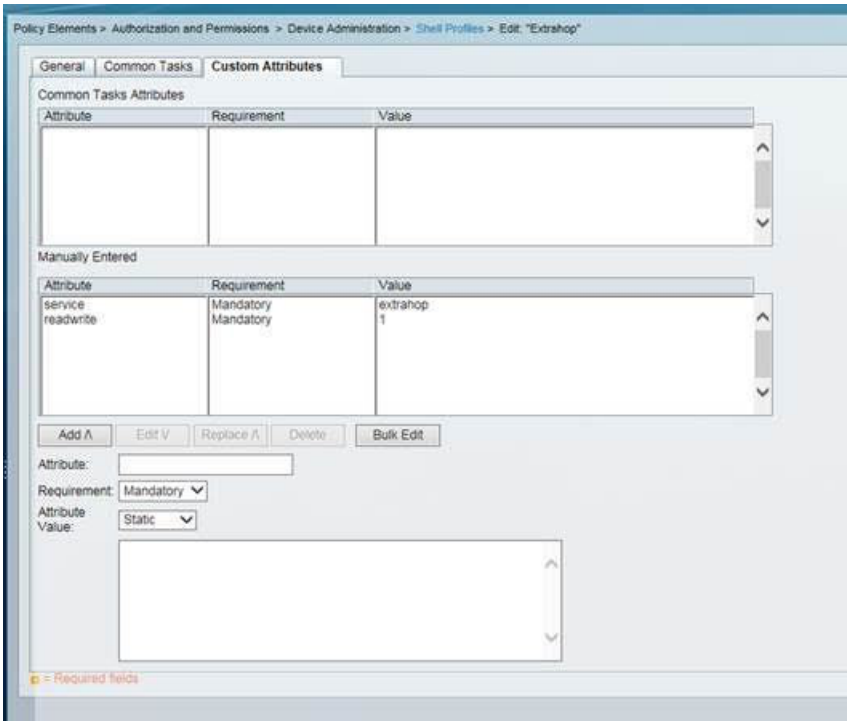
     This option grants remote users read-only access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, and detections.
9. (Optional) Configure packet and session key access. Select one of the following options to allow remote users to download packet captures and SSL session keys.
   - **No access**
   - **Packet slices only**
   - **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 system and access administration privileges can configure whether users can generate API keys for the ExtraHop system. You can allow only local users to generate keys, or you can also disable API key generation entirely.

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

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

Configure cross-origin resource sharing (CORS)

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

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

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

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

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

Generate an API key

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

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

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

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

Privilege levels

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

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

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

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

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

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

Privilege level	Actions allowed
	• Change your own password, but you cannot perform any other administration tasks through the REST API. • View dashboards and activity maps shared with you. • Perform metric and record queries.
"metrics": "restricted"	• 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"	• View and download packets through the `GET/packetcaptures/{id}` operation. This is an add-on privilege that can be granted to a user with one of the following privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"packets": "full_with_keys"	• View and download packets through the `GET/packetcaptures/{id}` operation. This is an add-on privilege that can be granted to a user with one of the following privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"packets": "slices_only"	• View and download the first 64 bytes of packets through the `GET/packetcaptures/{id}` operation. This is an add-on privilege that can be granted to a user with one of the following privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"detections": "full"	• View detections. This is an add-on privilege that can be granted to a user with one of the following privilege levels: • "write": "full"

Privilege level	Actions allowed
	• "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"detections": "none"	• No access to detections. This is an add-on privilege that can be granted to a user with one of the following privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"

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

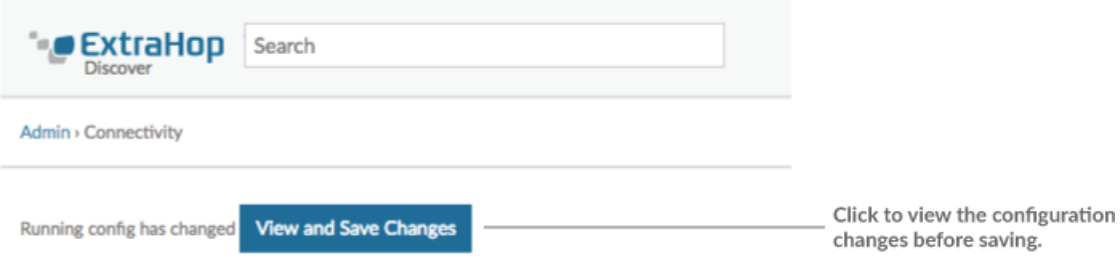
The running configuration file specifies the default system configuration. When you modify system settings, you must save the running configuration file to preserve those modifications after a system restart.

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.

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.

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. You can configure settings for SNMPv1/SNMPv2, and SNMPv3

Configure the SNMPv1 and SNMPv2 service

1. On the Services page, next to SNMP Service, click **Configure**.
2. Configure the following settings to enable the SNMPv3 service:

   Enabled

   Select the checkbox to enable the SNMP service.

SNMPv1 and SNMPv2 Enabled

Select the checkbox to enable the SNMPv1 and SNMPv2 service.

SNMP Community

Type a friendly name for the SNMP community.

SNMP System Contact

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

SNMP System Location

Type a location for the SNMP system.

3. Click **Save Settings**.

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

Configure the SNMPv3 service

1. On the Services page, next to SNMP Service, click **Configure**.
2. Configure the following settings to enable the SNMPv3 service:

SNMPv3 Enabled

Select the checkbox to enable the SNMPv3 service.

SNMPv3 User Name

Type the name of the user that can access the SNMPv3 service.

Authentication and Privacy Mode

Select **Authentication and Privacy** or **Authentication and No Privacy** from the drop-down list. If you select **Authentication and Privacy**, you must also complete the **Privacy Password** field.

Authentication Password

Type a password for the user to authenticate to the SNMPv3 service.

Authentication Algorithm

Select **SHA-256** or **SHA-1** as the authentication protocol from the drop-down list.

Privacy Password

Type the password to decrypt SNMPv3 traps. This field is required if you select **Authentication and Privacy**.

3. Click **Save Settings**.

Next steps
Download the ExtraHop 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 9.2 before upgrading your self-managed sensors.
- If you are upgrading from firmware version 8.7 or earlier, contact ExtraHop Support for additional upgrade guidance.
- If you have multiple types of ExtraHop appliances, you must upgrade them in the following order:
  1. Console
  2. Sensors (EDA and Ultra)
  3. Recordstores
  4. Packetstores
- 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 packetsores, 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.

   Note: For sensors, the list includes only firmware versions that are compatible with the version running on the connected console.

4. Click **Download and Install**.

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

Upgrade the firmware on recordstores

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

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

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

Upgrade the firmware on packetstores

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

After the firmware update is installed successfully, the ExtraHop appliance displays the version number of the new firmware on the Administration settings.

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

Before you begin

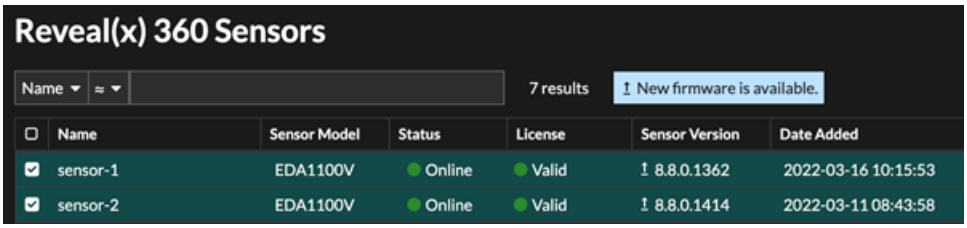
- Your user account must have privileges on Reveal(x) 360 for System and Access Administration or System Administration.

Here are some considerations about upgrading sensors:

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

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

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



3. Select the checkbox next to each sensor that you want to upgrade.
4. In the Sensor Details pane, select the firmware version from the **Available Firmware** drop-down list.

   The drop-down list only displays versions that are compatible with the selected sensors.

   Only the selected sensors that have a firmware upgrade available appear in the Sensor Details pane.
5. Click **Install Firmware**.

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

System Time

The System Time page displays the current time settings configured for your ExtraHop system. View the current system time settings, the default display time for users, and details for configured NTP servers.

System time is the time and date tracked by services running on the ExtraHop system to ensure accurate time calculations. By default, the system time on the sensor or console is configured locally. For better accuracy, we recommend that you configure the system time through an NTP time server.

When capturing data, the system time must match the time on connected sensors to ensure that time stamps are correct and complete in scheduled reports, exported dashboards and chart metrics. If time sync issues occur, check that the configured system time, external time servers, or NTP servers are accurate. Reset the system time or sync NTP servers if needed

The table below contains details about the current system time configuration. Click **Configure Time** to configure system time settings.

Detail	Description
Time Zone	Displays the currently selected time zone.
System Time	Displays the current system time.

Detail	Description
Time Servers	Displays a comma-separated list of configured time servers.

Default display time for users

The Default Display Time for Users section shows the time displayed to all users in the ExtraHop system unless a user manually changes their displayed time zone.

To modify the default display time, select one of the following options and then click **Save Changes**:

- Browser time
- System time
- UTC

NTP Status

The NTP Status table displays the current configuration and status of all NTP servers that keep the system clock in sync. The table below contains details about each configured NTP server. Click **Sync Now** to sync the current system time to a remote server.

remote	The host name or IP address of the remote NTP server you have configured to synchronize with.
st	The stratum level, 0 through 16.
t	The type of connection. This value can be `u` for unicast or manycast, `b` for broadcast or multicast, `l` for local reference clock, `s` for symmetric peer, `A` for a manycast server, `B` for a broadcast server, or `M` for a multicast server.
when	The last time when the server was queried for the time. The default value is seconds, or `m` is displayed for minutes, `h` for hours, and `d` for days.
poll	How often the server is queried for the time, with a minimum of 16 seconds to a maximum of 36 hours.
reach	Value that shows the success and failure rate of communicating with the remote server. Success means the bit is set, failure means the bit is not set. `377` is the highest value.
delay	The round trip time (RTT) of the ExtraHop appliance communicating with the remote server, in milliseconds.
offset	Indicates how far off the ExtraHop appliance clock is from the time reported by the server. The value can be positive or negative, displayed in milliseconds.
jitter	Indicates the difference, in milliseconds, between two samples.

Configure the system time

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

Before you begin

Important: Always configure more than one NTP server to increase the accuracy and reliability of time kept on the system.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.

2. In the **Appliance Settings** section, click **System Time**.
3. Click **Configure Time**.
4. Select your time zone from the drop-down list then click **Save and Continue**.
5. On the Time Setup page, select one of the following options:
   - Set time manually

     Note: You cannot manually set the time for sensors that are managed by a console or Reveal(x) 360.
   - Set time with NTP server
6. Select **Set time with NTP server** and then click **Select**.

   The ExtraHop time servers, `0.extrahop.pool.ntp.org`, `1.extrahop.pool.ntp.org`, `2.extrahop.pool.ntp.org`, and `3.extrahop.pool.ntp.org` appear in the first four Time Server fields by default.
7. Type the IP address or fully qualified domain name (FQDN) for the time servers in the Time Server fields. You can have up to nine time servers.

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

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

Shutdown or restart

The Explore Admin UI provides an interface to halt, shutdown, and restart the Explore appliance components.

System

Restart or shut down the Explore appliance.

Admin

Restart the Explore appliance administrator component.

Receiver

Restart the Explore receiver component.

Search

Restart the Explore search service.

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

Restart an Explore appliance component

1. On the Admin page in the Appliance Settings section, click **Shutdown or Restart**.
2. Select **Restart** for the component you want to restart:
   - System (can also be shutdown completely)
   - Admin
   - Receiver
   - Search

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:

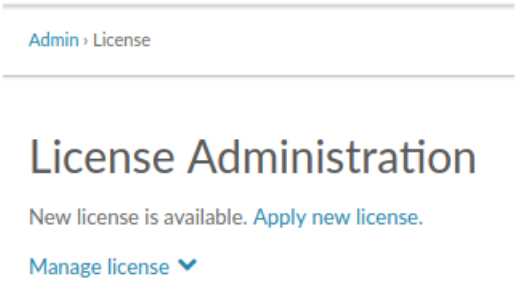
```
Non-authoritative answer:
d.extrahop.com  nameserver = ns0.use.d.extrahop.com.
d.extrahop.com  nameserver = ns0.usw.d.extrahop.com.
```

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/FGHIjklm12nopqrstuvwXYZAB12345678abcde901abCD;
   12ABCDEFG1HIJklmnOP+1aA=;
   =abcd;
   -----END EXTRAHOP LICENSE-----
   ```
6. Click **Update**.

Disks

The Disks page provides information about the configuration and status of the disks in your Explore appliance. The information displayed on this page varies based on whether you have a physical or virtual appliance.

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. For more information, see the Notifications section.

The following information displays on the page:

Drive Map

(Physical only) Provides a visual representation of the front of the Explore appliance.

RAID Disk Details

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

Firmware

Displays information about disks reserved for the Explore appliance firmware.

Utility (Var)

Displays information about disks reserved for system files.

Search

Displays information about disks reserved for data storage.

Direct Connected Disks

Displays information about virtual disks on virtual machine deployments, or USB media in physical appliances.

Explore Cluster Settings

The Explore Cluster Settings section provides the following configurable settings:

Join Cluster

Join an ExtraHop recordstore to an existing cluster. This setting appears only for single nodes that have not yet been joined to a cluster.

Cluster Members

Displays all of the nodes that are members of the cluster.

Cluster Data Management

Displays settings to configure the data replication level, enable or disable shard reallocation, and enable or disable record ingest. These settings are applied to all nodes in the cluster.

Manager

Displays the hostname of the console that is configured to manage the ExtraHop recordstore as well as a list of all sensors and consoles connected to the recordstore.

Manage with Command Appliance

Configure settings to enable a console to remotely run support scripts on the ExtraHop recordstore.

Restore Cluster State

Restore the cluster to a healthy state. This setting only appears if the cluster displays a status of `red` on the Cluster Status page.

Create a recordstore cluster

For the best performance, data redundancy, and stability, you must configure at least three recordstores in a cluster.

Important: If you are creating a recordstore cluster with six or more nodes, you must configure the cluster with manager nodes. For manager node instructions, see Deploying manager nodes.

In the following example, the recordstores have the following IP addresses:

- Node 1: 10.20.227.177
- Node 2: 10.20.227.178
- Node 3: 10.20.227.179

You will join nodes 2 and 3 to node 1 to create the recordstore cluster. All three nodes are data nodes. You cannot join a data node to a manager node or join a manager node to a data node to create a cluster.

Important: Each node that you join must have the same configuration (physical or virtual) and the same ExtraHop firmware version.

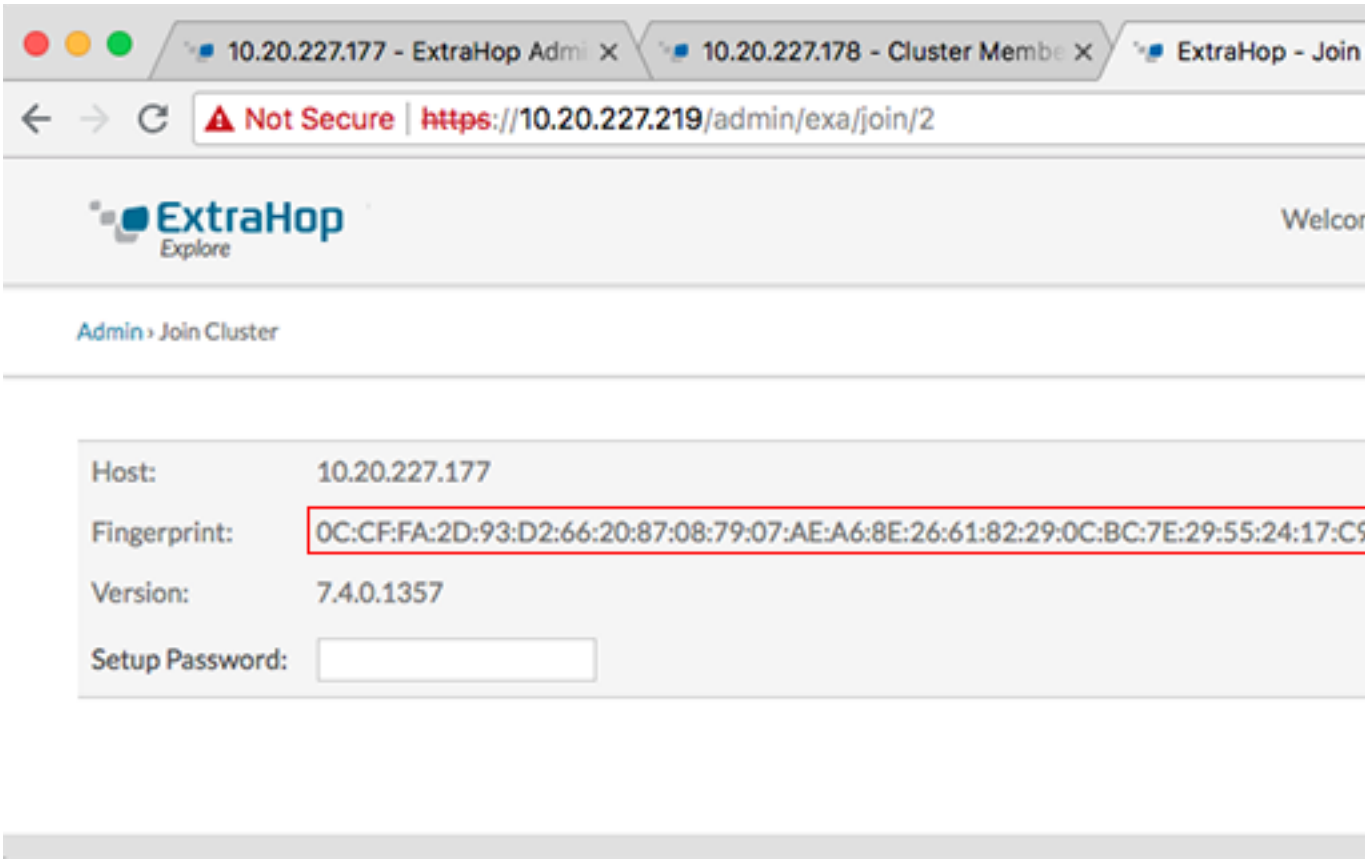
Before you begin

You must have already installed or provisioned the recordstores in your environment before proceeding.

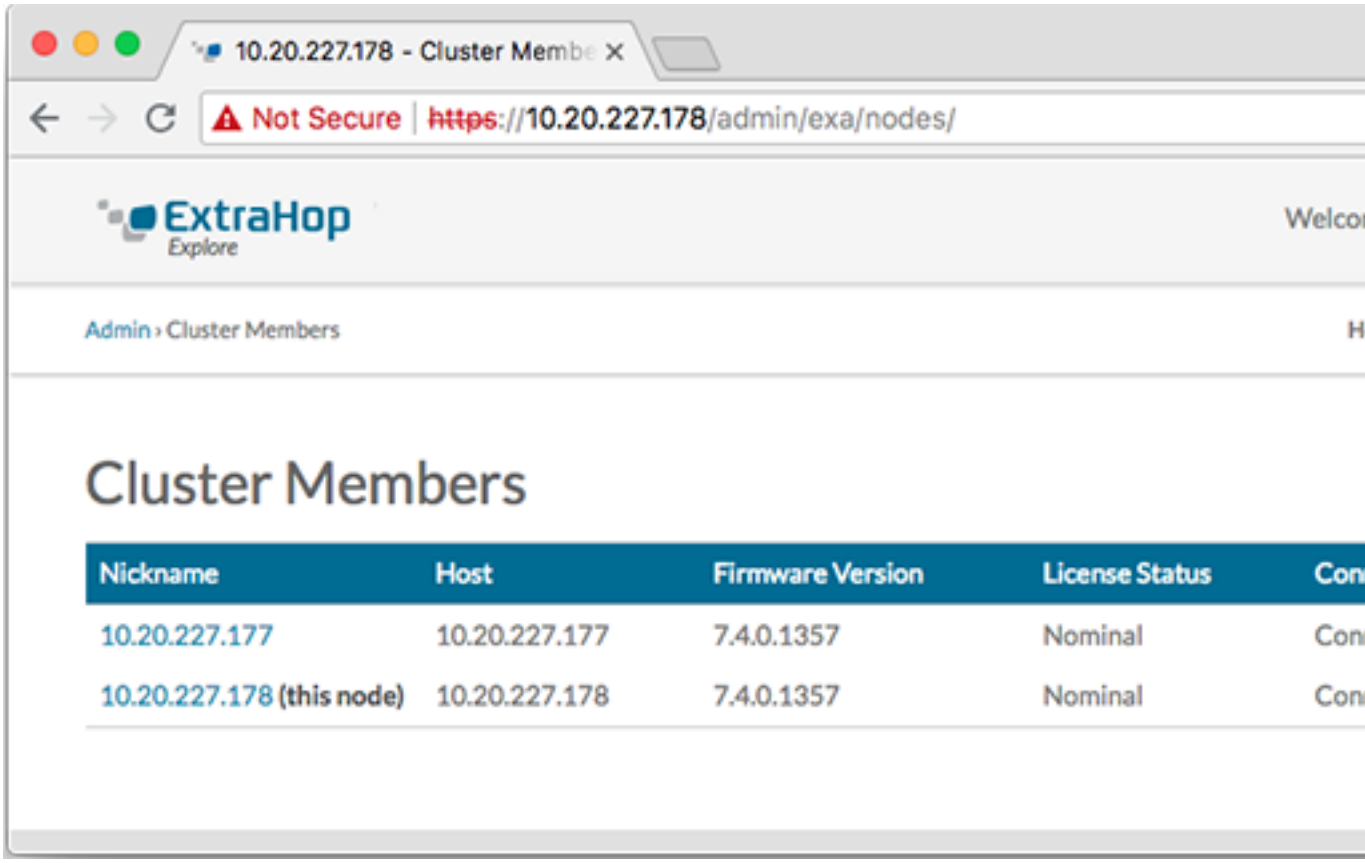
1. Log in to the Administration settings on all three recordstores with the setup user account in three separate browser windows or tabs.
2. Select the browser window of node 1.
3. In the Status and Diagnostics section, click **Fingerprint** and note the fingerprint value. You will later confirm that the fingerprint for node 1 matches when you join the remaining two nodes.
4. Select the browser window of node 2.
5. In the Explore Cluster Settings section, click **Join Cluster**.
6. In the Host field, type the hostname or IP address of data node 1 and then click **Continue**.

Note: For cloud-based deployments, be sure to type the IP address listed in the Interfaces table on the Connectivity page.

7. Confirm that the fingerprint on this page matches the fingerprint you noted in step 3.



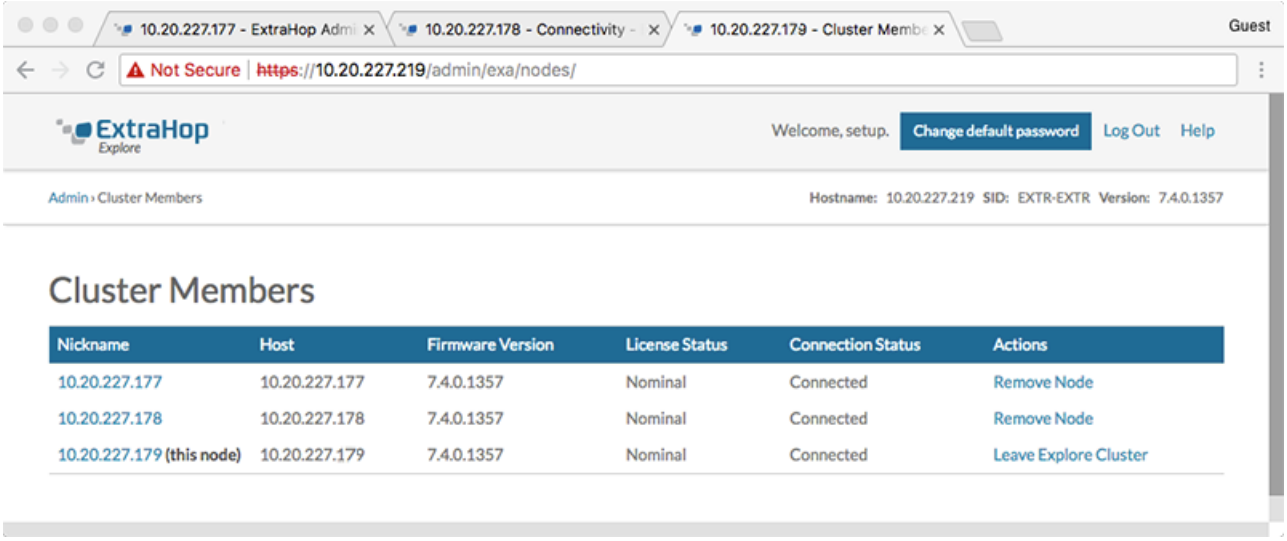
8. In the Setup Password field, type the password for the node 1 `setup` user account and then click **Join**. When the join is complete, the Explore Cluster Settings section has two new entries: **Cluster Members** and **Cluster Data Management**.
9. Click Cluster Members. You should see node 1 and node 2 in the list.



10. In the Status and Diagnostics section, click **Explore Cluster Status**. Wait for the Status field to change to `Green` before adding the next node.
11. Repeat steps 5 - 10 to join each additional node to the new cluster.

    Note: To avoid creating multiple clusters, always join a new node to an existing cluster and not to another single appliance.

12. When you have added all of your recordstores to the cluster, click **Cluster Members** in the Explore Cluster Settings section. You should see all of the joined nodes in the list, similar to the following figure.



13. In the Explore Cluster Settings section, click **Cluster Data Management** and make sure that **Replication Level** is set to **1** and **Shard Reallocation** is **ON**.

Next steps

Connect the console and sensors to ExtraHop recordstores

Cluster Members

If you have multiple nodes connected to an Explore cluster, you can view information about each node.

The table on this page provides the following information about each node in the cluster.

Nickname

Displays the IP address or nickname of the Explore appliance.
To assign a nickname, or change the existing nickname of a cluster member, click the IP address or nickname in the Nickname column, type a name in the Name field, and then click **Rename Node**.

Host

Displays the IP address of the Explore appliance.

Firmware Version

Displays the firmware version of the Explore appliance. Every node in the cluster must have the same firmware version to prevent unexpected behavior when replicating data across all nodes.

License Status

Displays the current status of the ExtraHop license. The License Status field displays one of the following states:

Nominal

The Explore appliance has a valid license.

Invalid

The Explore appliance has an invalid license. New records cannot be written to this node and existing records cannot be queried.

Pre-Expired

The Explore appliance has a license that is expiring soon.

Pre-Disconnected

The Explore appliance cannot connect to the ExtraHop license server.

Disconnected

The Explore appliance has not connected to the ExtraHop license server for more than 7 days. New records cannot be written to this node and existing records cannot be queried.

Connection Status

Displays whether the appliance is connected to the other members in the cluster. The possible connection states are `Connected` and `Unreachable`.

Actions

Remove an Explore node from the cluster.

Remove a node from the cluster

1. In the Explore Cluster Settings section, click **Cluster Members**.
2. In the Actions column, choose one of the following options:
   - Click **Leave Explore Cluster** if you want to remove the node that you are currently logged in to, and then click **OK** to confirm.
   - Click **Remove Node** next to the node you want to remove and then click **Remove Node** to confirm.

Manager and Connected Appliances

The Manager and Connected Appliances section includes the following information and controls.

Manager

Displays the hostname of the console that is configured to manage the ExtraHop recordstore. To connect to a Command appliance through a tunneled connection, click **Connect to 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 Command appliance as the manager.

Note: The Explore appliance can be managed by only one Command appliance.

Clients

Displays a table of all Discover appliances and Command appliances connected to the Explore appliance. The table includes the hostname of the connected client and the client product key.
Click **Remove Client** in the Actions column to remove a connected client.

Cluster Data Management

The Cluster Data Management page enables you to adjust settings for how records are collected and stored on your Explore cluster. You must connect an ExtraHop sensor to the recordstore cluster before you can configure replication level and shard reallocation settings.

You can manage how record data is stored on your recordstore cluster.

- Change the replication level to determine how many copies of each record are stored. A higher number of copies improves fault tolerance if a node fails and also improves the speed of query results. However, a higher number of copies takes up more disk space and might slow the indexing of the data.

Option	Description
0	Data is not replicated to other nodes in the cluster. This level allows you to collect more data on the cluster; however, if there is a node failure, you will permanently lose data.
1	There is one copy of the original data stored on the cluster. If one node fails, you will not permanently lose data.
2	There are two copies of the original data stored on the cluster. This level requires the most disk space but provides the highest level of data protection. Two nodes in the cluster can fail without permanently losing data.

- Enable or disable shard reallocation. Shard reallocation is enabled by default. Prior to taking the node offline for maintenance (for example, upgrading firmware, replacing disks, power cycling the appliance, or removing network connectivity between recordstore nodes), you should disable shard reallocation. After node maintenance is complete, enable shard reallocation.
- Enable or disable record ingest. Record ingest is enabled by default and controls whether records can be written to your recordstore cluster. You must disable record ingest prior to upgrading firmware.

Connect to a Command appliance

Connect to a Command appliance to remotely run support scripts and upgrade firmware on the Explore appliance.

This procedure connects the Explore appliance to the Command appliance through a tunneled connection. Tunneled connections are required in network environments where a direct connection from the Command

appliance is not possible because of firewalls or other network restrictions. When possible, you should always connect appliances directly from the Command appliance.

1. In the Explore Cluster Settings section, click **Connect to a Command Appliance**.
2. Configure the following settings:
   - Command appliance hostname: The hostname or IP address of the Command appliance.
   - Command appliance setup password: The `setup` user password for the Command appliance.
   - Explore node nickname (Optional): A friendly name for the Explore node. If no nickname is entered, the node is identified by the hostname.
3. Select the Manage with Command appliance checkbox and then click **Connect**.

Restore the cluster state

In rares instances, the Explore cluster might not recover from a `Red` status, as seen in the Status section on the Explore Cluster Status page. When this state occurs, it is possible to restore the cluster to a `Green` state.

When you restore the cluster state, the Explore cluster is updated with the latest stored information about the Explore nodes in the cluster and all other connected Discover and Command appliances.

Important: If you have recently restarted your Explore cluster, it might take an hour before the cluster status `Green` appears, and restoring the cluster might not be necessary. If you are unsure whether you should restore the cluster state, contact ExtraHop Support.

1. In the Explore Cluster Settings section, click **Restore Cluster State**.
2. On the Restore Cluster State page, click **Restore Cluster State**.
3. Click **Restore Cluster** to confirm.