



ExtraHop 6.2

ExtraHop Explore Admin UI Guide

© 2018 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: 2018-10-27

ExtraHop Networks
Seattle, WA 98101
877-333-9872 (US)
+44 (0)203 7016850 (EMEA)
+65-31585513 (APAC)
www.extrahop.com

Contents

Introduction to the ExtraHop Explore Admin UI	6
Supported Browsers	7
Navigation	8
Log in and log out of the Admin UI	8
Status and Diagnostics	9
Health	9
Audit log	11
Fingerprint	11
Explore Cluster Status	12
Delete records	13
Support packs	13
View the diagnostic support packages on the system	13
Download a selected diagnostic support package	13
Delete a selected diagnostic support package	14
Upload support pack	14
Create a system support pack	14
Network settings	15
Atlas Services	15
Connect to Atlas services	15
Disconnect from Atlas services	15
Connectivity	16
Interface status	16
Change the network settings	16
Change interface 1	17
Enable IPv6 for an interface	18
Set a static route	18
Change the remaining interfaces	19
Notifications	19
Configure the Email Server and Sender settings	19
Test email settings	20
Email addresses	20
Add a new notification email address	20
Delete a disk notification email address	20
SNMP	20
Configure SNMP settings	20
Download the ExtraHop SNMP MIB	21
Configure syslog notification settings	21
SSL certificate	21
Generate a self-signed certificate	21
Upload an SSL certificate	22
Upload the SSL certificate	22
Add a trusted certificate to your ExtraHop appliance	22

Access Settings	24
Change password	24
Change the password settings	24
Change the default password for the setup user	24
Support account	25
Enable the Support account	25
Regenerate the Support account key	25
Disable the Support account	25
Users	25
Add a user	26
Modify an account	26
Delete a user account	26
Sessions	27
Delete active sessions	27
Remote authentication	27
LDAP	27
Configure LDAP authentication	28
RADIUS	29
Configure RADIUS authentication	29
TACACS+	30
Configure TACACS+ authentication	30
API access	30
Manage API access	30
Enable CORS for the ExtraHop REST API	31
Generate an API key	31
Delete an API key	31
Explore cluster settings	32
Join an Explore cluster	32
Cluster Members	32
Remove a node from the cluster	33
Leave an Explore cluster	33
Manager and Connected Appliances	33
Data Management	34
Replication	34
Shard reallocation	34
Connect to a Command appliance	34
Restore the cluster state	35
Appliance Settings	36
Firmware	36
Upgrade to a new firmware version	36
Delete firmware versions	37
System time	37
Configure the system time	38
Shutdown or restart	38
Restart an Explore appliance component	39
License	39
View the licensing system information	39
Register an existing license	39
Update a module license or add new licenses	39
Running config	40
Saving running config changes	40
Save system configuration settings	41

Revert system configuration changes	41
Edit running config	41
Download running config as a text file	41
Disks	42

Introduction to the ExtraHop Explore Admin UI

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

After you have deployed your Explore appliance, 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 appliances.

- Firefox
- Google Chrome
- Internet Explorer 11
- Safari

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

Navigation

This section describes the general layout of the Admin UI on the ExtraHop Explore appliance.

The toolbar contains the following controls or links:

Change default password

Opens the Change Password page so that you can specify a new Admin UI password. For more information, see the [Change the default password for the setup user](#) section.

Log out

Ends the Admin UI session on the ExtraHop appliance. For more information, see the [#unique_5](#) section.

Help

Opens the [ExtraHop Explore Admin UI Guide](#).

The administration page contains the following sections:

Status and Diagnostics

Verify how the Explore appliance is functioning on the network.

Network Settings

Configure the network settings for the Explore appliance.

Access Settings

Configure access settings to the Explore appliance.

Appliance Settings

Configure the system-level settings for the Explore appliance.

Explore Cluster Settings

Join an Explore cluster and manage cluster settings.

Log in and log out of the Admin UI

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

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



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

3. To log out of the Admin UI, click **Log out** on the toolbar.

Status and Diagnostics

The Status and Diagnostics 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 Packs

Enables you to upload and run support packages.

Cluster Status

Provides status information about the Explore cluster, cluster nodes, and indices.

Health

The Health page provides a collection of metrics that enable you check the operation of the Explore appliance. If issues occur with the Explore appliance, the metrics on the Health page help you to troubleshoot the problem and determine why the appliance is not performing as expected.

The following information is collected on the Health page.

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 Explore 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 the system, broken down by component. The log lists all known events by timestamp with the most recent events at the top of the list. You can configure where to send these logs in the Syslog Settings section.

The appliance collects the following log data and reports the results on the Audit Log page.

Time

Specifies the time at which the event occurred.

User

Identifies the user who initiated the logged event.

Operation

Specifies the system operation that generated the logged event.

Details

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

Component

Identifies the appliance component that is associated with the logged event.

To configure the syslog settings:

1. Click **Configure syslog settings**.
2. In the Destination field, type the name of the of remote syslog server.
3. Click the **Protocol** drop-down list and select **TCP** or **UDP**.
4. In the **Port** field, enter the port number.
5. Click **Test Settings** to verify that the appliance can communicate with the remote syslog server.
6. Once the syslog settings are configured, click **Save**.

Fingerprint

The Fingerprint page displays the device fingerprint for the Explore appliance. When joining a new Explore node or pairing a new publisher or client with the Explore cluster through this node, 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.

Explore Cluster Status

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

Cluster

Status

The following status names can appear:

Ready

The node is available to join an Explore cluster.

Green

All data is replicated across the cluster.

Yellow

The primary shard is allocated but replica shards are not.

Red

One or more shards from the index are missing.



Note: If the status never returns to a yellow or green state, you might have to restore the cluster. For more information, see [Restore the cluster state](#)

Cluster Nodes

Nickname

Displays the nickname of the Explore node when configured on the **Cluster Settings > Cluster Members** page.

Host

Displays the IP address or hostname of the Explore node.

Indices

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.

Unassigned Shards

Displays the number of shards that have not been assigned to a node. Unassigned shards are typically replica shards that need to 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 records from the cluster.

You can delete records by index. An index 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 titled `extrahop-4-2016-5-16-0` indicates that the related records 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 section, click **Cluster Status**.
2. Below the Indices section, select the checkbox for each index that you want to delete. The Source column displays the name of the Discover appliance that collected the data.
3. Click **Delete Selected**.
4. Click **OK**.

Support packs

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

View Support Pack results

View, download, or delete selected support packages.

Upload Support Pack

Upload diagnostic support packages on the ExtraHop system.

Run Default Support Pack

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

View the diagnostic support packages on the system

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

Download a selected diagnostic support package



Note: Support pack files are encrypted and can be decrypted only by ExtraHop Support.

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

Delete a selected diagnostic support package

1. In the Diagnostics section, click **Support Packs**.
2. Click **View Support Pack Results**.
3. Locate the diagnostic support package that you want to delete.
4. Click the **Delete** icon next to the support package create date.
5. At the prompt, click **OK**.

Upload support pack

1. In the Diagnostics section, click **Support Packs**.
2. Click **Upload Support Pack**.
3. Click **Choose File**.
4. Navigate to the diagnostic support package that you want to upload.
5. Select the file and click **Open**.
6. Click **Upload** to add the file to the ExtraHop appliance.

Create a system support pack

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

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

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

Network settings

The Network Settings section 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 Explore appliance [deployment guide](#) or contact ExtraHop Support for assistance.

For specifications, installation guides, and more information about your appliance, refer to docs.extrahop.com.

Atlas Services

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

Connect to Atlas services

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

1. In the Network Settings section, click **Atlas Services**.
2. On the Connect to Atlas Services page, click **Terms and Conditions** to read about the service agreement.
The Atlas subscription services agreement opens in the browser or downloads the file to your computer.
3. Return to the Connect to Atlas Services page and select the checkbox next to **Terms and Conditions**.
4. Click **Test Connectivity** to make sure the connection is successful. If you have problems connecting to the Atlas service, see the [Troubleshoot an Atlas Connection](#) for troubleshooting suggestions.
5. Click **Connect**.

Disconnect from Atlas services

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

1. In the Network Settings section, click **Atlas Services**.
2. Click **OK** to disconnect, and then click **Done**.

Connectivity

To connect the appliance to the host network, the following network configuration is required:

Network Settings

Hostname

Specifies the name of the appliance on the network.

Primary DNS

Specifies the IP address of the primary domain name server for the specified domain

Secondary DNS

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

Interfaces

Interface

Lists the available interfaces on the node.

Mode

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

DHCP

Specifies whether DHCP is enabled or disabled.

IP address

Specifies the static IP address of the appliance on the network

Netmask

Specifies the netmask used to divide the IP address into subnets.

Gateway

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

Routes

Specifies network route information if DHCP is disabled.

MAC Address

Specifies the MAC address of the appliance

IPv6

Specifies whether IPv6 is enabled or disabled.

Interface status

In the Interface Status section, a diagram of the back of the physical Explore appliance displays the following information about the current interface connections:

Blue Ethernet Port

Identifies the management port.

Gray Ethernet Port

Identifies a disabled port.



Note: The Interface Status section only appears for physical appliances.

Change the network settings

To change the network settings:

1. In the Network Settings section, click **Connectivity**.

2. In the Network Settings section, click **Change**.

The Edit Hostname page appears with the following editable fields:

Hostname

Specifies the descriptive device name for the appliance on the network. Devices on the network can be identified by their IP address, MAC address, or by the descriptive name defined in this setting.

Primary DNS

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

Secondary DNS

Functions as the backup server to the primary DNS.

3. Change the settings as needed and click **Save**.


Change interface 1

1. Go to the Network Settings section and click **Connectivity**.
2. In the Interfaces section, click **Interface 1**.

The Network Settings for Interface 1 page appears with the following editable fields:

Interface Mode

The Interface Mode is set to `Management Port` by default. All management, data and intra-node communications are transmitted through the management port.

 **Important:** If you only have one interface configured and you set the Interface Mode on interface 1 to `Disabled` and click **Save**, you will lose your access to the node until the node is manually restarted.

Enable DHCPv4

DHCP is enabled by default. When you turn on the system, interface 1 attempts to acquire an IP address using DHCP. After the DHCP server assigns an IP address to a physical appliance, the IP address appears on the LCD at the front of the appliance.

If your network does not support DHCP, you can disable DHCP and configure a static IP address.

To disable DHCP, clear the **Enable DHCPv4** checkbox and click **Save**. When the browser changes to the new network address, log on to the Admin UI again.

If you are changing from a static IP address to a DHCP-acquired IP address, the changes occur immediately after clicking **Save**, which results in a loss of connection to the Admin UI web page. After the system acquires an IP address, log on to the Admin UI again.

IPv4 Address

The Explore appliance provides configuration settings to acquire an IP address automatically or to configure a static IP address manually. The Explore appliance displays the assigned IP address on the LCD at the front of the appliance. If your network does not support DHCP, you can configure a static IP address using the Explore Admin UI.

To configure the `IP Address` network setting manually, disable DHCP, enter a static IP address, and click **Save**.

Netmask

Devices on a local network have unique IP addresses, but this unique address can be thought of as having two parts: The shared network part that is common to all devices on the network, and a unique host part. Both the shared and unique parts of the IP address are used by the TCP/IP stack for routing.

The shared network parts of the address and host parts are determined by the netmask, which looks like this: 255.255.0.0. In this example, the masked part of the network is represented by 255.255, and the unmasked host part is represented by 0.0, where the number of unique device addresses that can be supported on the network is approximately 65,000.

Gateway

The network's gateway address is the IP address of the device that is used by other devices on the network to access another network or a public network like the Internet. The address for the gateway is often a router with a public IP address.

Enable IPv6

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


Routes

If you do not have DHCP enabled, you can manually set a static route to determine where the traffic goes. For more information about configuring static routes, see [Set a static route](#).

3. Change the settings as needed and then 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**.

Set a static route

Before you begin

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

1. On the Edit Interface page, ensure that the **IPv4 Address** and **Netmask** fields are complete and saved, and click **Edit Routes**.
2. In the Add Route section, type a network address range in CIDR notation in the **Network** field and IPv4 address in the **Via IP** field and then click **Add**.
3. Repeat the previous step for each route you want to add.
4. Click **Save**.

Change the remaining interfaces

1. In the Network Settings section, click **Connectivity**.
2. For each interface that you want to change, click the name for that interface.
In the Network Settings page for the interface, select one of the following interface mode options:
 - Disabled**
The interface is disabled.
 - Management Port**
All management, data, and cluster communications are transmitted through the **Management Port**.
3. Change the settings as needed and click **Save**.

Notifications

The ExtraHop appliance can send alert notifications through email and SNMP traps. If SNMP is specified, then every alert is sent as an SNMP trap to the specified SNMP server. In addition, you can send alerts to a remote server through a syslog export.

The Notifications section in the Network Settings section of the Admin UI includes the following configurable settings.

Email Server and Sender

Configure the email server and sender settings.

Email Addresses

Add individual email addresses to receive disk notifications.


SNMP


Set up SNMP network monitoring.

Syslog

Send appliance data to another system for archiving and correlation.

Configure the Email Server and Sender settings

1. In the Network Settings section, click **Notifications**.
2. Click **Email Server and Sender**.
3. Type the IP address or hostname for the outgoing SMTP mail server in the SMTP Server field.
 -  **Note:** The SMTP server should be the fully qualified domain name (FQDN) or IP address of an outgoing mail server that is accessible from the ExtraHop management network. If the DNS server is set, then the SMTP server can be a FQDN, otherwise it needs to be an IP address.
4. Type the port number for SMTP communication in the SMTP Port field. The default port number is 25.
5. Select one of the following encryption methods from the Encryption drop-down list:
 - **None.** SMTP communication is not encrypted.
 - **SSL/TLS.** SMTP communication is encrypted through the Secure Socket Layer/Transport Layer Security protocol.
 - **STARTTLS.** SMTP communication is encrypted through STARTTLS.
6. Type the email address for the notification sender in the Sender Address field.

-  **Note:** The displayed sender address might be changed by the SMTP server. When sending through a Google SMTP server, for example, the sender email is changed to the username supplied for authentication, instead of the originally entered sender address.

7. Select the Enable SMTP authentication checkbox and then type the SMTP server setup credentials in the Username and Password fields.
8. Click **Save**.

Test email settings

To confirm that the ExtraHop appliance can communicate with the SMTP server:

1. In the Network Settings section, click **Notifications**.
2. Click **Email Server and Sender**.
3. Click **Test Settings**.
4. Enter an email address to receive the test email and then click **Send**.

Email addresses

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

- A virtual disk is in a degraded state.
- A physical disk is in a degraded state.
- A physical disk has an increasing error count.
- A registered Explore node is missing from the cluster. The node might have failed, or it is powered off.

Add a new notification email address

To add a new disk notification email address:

1. In the Network Settings section, click **Notifications**.
2. Under Notifications, click **Email Addresses**.
3. In the **Email address** text box, type the recipient email address.
4. Click **Save**.

Delete a disk notification email address

To delete a disk notification email address:

1. In the Network Settings section, click **Notifications**.
2. Under Notifications, click **Email Addresses**.
3. Click the red delete icon (X) to the right of the email address.
4. On the Delete page, click **OK**.

The running config changes when you add or remove an email address. To preserve your changes, click **View and Save Changes**. For more information, see the Running Config section.

SNMP

The state of the network is 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.

Configure SNMP settings

To configure the SNMP settings:

1. In the Network Settings section, click **Notifications**.
2. Under Notifications, click **SNMP**.

3. On the SNMP Settings page, in the **SMTP Monitor** field, type the hostname for the SNMP trap receiver. Multiple names can be entered, separated by commas.
4. In the **SNMP Community** field, enter the SNMP community name.
5. In the **SNMP Port** field, type the SNMP port number for your network that is used by the SNMP agent to respond back to the source port on the SNMP manager.
The default response port is 162.
6. Click **Test Settings**. You cannot continue until the test is successful.
7. Click **Save**.

Download the ExtraHop SNMP MIB

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

To download the ExtraHop SNMP MIB:

1. Go to the Network Settings section and click **Notifications**.
2. Under Notifications, click **SNMP**.
3. Under SNMP MIB, click the **Download ExtraHop SNMP MIB**.
The file is typically saved to the default download location for your browser.

Configure syslog notification settings

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



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

1. In the Network Settings section, click **Notifications**.
2. Click **Syslog**.
3. On the Syslog Notification Settings page, type the following information:
 - **Destination:** The IP address of the remote syslog server.
 - **Protocol:** From the drop-down, select which protocol to use to send information to your remote syslog server.
 - **Port:** The port number for your remote syslog server. By default, this is set to 514.
4. (Optional) Click **Test Settings** to verify that your syslog settings are functioning properly.
5. Click **Save**.

SSL certificate


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

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

Generate a self-signed certificate


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

4. On the Generate Certificate page, click **OK** to generate the SSL self-signed certificate.

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

Upload an SSL certificate

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


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

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

Upload the SSL certificate

To upload an SSL certificate:

1. On the Admin page under Network Settings, click **SSL Certificate**.
2. Click **Manage certificates**.
3. Next to Upload certificate, click **Choose File** and navigate to the certificate that you want to upload.

 **Note:** The certificate must be a PEM file that contains both the certificate and private key.


4. Click **Open**, and then click **Upload**.

Add a trusted certificate to your ExtraHop appliance


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

Before you begin

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

 **Important:** To trust the built-in system certificates and any uploaded certificates, you must also enable SSL certificate validation on the LDAP Settings page or Email Settings page.

1. Log into the Admin UI.
2. In the Network Settings section, click **Trusted Certificates**.
3. The ExtraHop appliance ships with a set of built-in certificates. Select Trust System Certificates if you want to trust these certificates, and then click **Save**.
4. To add your own certificate, click **Add Certificate** and then paste the contents of the PEM-encoded certificate chain into the Certificate field
5. Type a name into the Name field and click **Add**.

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

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

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

Next steps

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

Access Settings

In the Access Settings section, you can change passwords, enable the support account, and specify users in the ExtraHop appliances for remote authentication. The Access Settings section has the following configurable settings:

Password

Change the password for user accounts.

Support Account

Enable troubleshooting assistance from ExtraHop Support.

Users

Add and delete users, and modify user privileges.

Sessions

View and terminate user sessions on the Admin UI.

Remote Authentication

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

API Access

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


User Groups

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

Change password

Users with administrative privileges to the Admin UI on the appliance can change the password for any user that has an account stored locally in the appliance. For more information about privileges for specific Admin UI users and groups, see the Users section.


Change the password settings

 **Note:** You can only change passwords for local users, not users authenticated with LDAP.

1. In the Access Settings section, click **Change Password**.
2. Select the user from the drop-down list.
3. Type the new password in the New password field.
4. Retype the new password in the Confirm password field.
5. Click **Save**.

Change the default password for the setup user

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

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

1. In the Admin UI, click the blue **Change default password** button.
The Change Password page displays without the drop-down menu for accounts. The password will change for the setup user only.

2. Type the default password in the Old password field.
3. Type the new password in the New password field.
4. Retype the new password in the Confirm password field.
5. Click **Save**.

Support account

Support accounts provide access for the ExtraHop Support team to help customers troubleshoot issues with the ExtraHop appliance and to provide remote analysis reports through Atlas Services.

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

Enable the Support account

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



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

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

Regenerate the Support account key

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



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

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

Disable the Support account

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



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

3. Click **Disable Support Account**.

Users

The Users page provides controls to add and delete users, and to change a user's access privileges in the ExtraHop appliance. Users with administrator-level privileges can add other users.

User accounts can be locally or remotely authenticated and authorized. For more information, see the Remote Authentication section.


The following default accounts are configured on the ExtraHop appliance:

setup


The `setup` account provides full system read and write privileges on the Web UI, Admin UI, and Shell, which is the ExtraHop command-line interface (CLI). For physical appliances, the default password for this account is the service tag number on the right-front bracket of the ExtraHop appliance. For virtual appliances, the password is `default`.

shell

The `shell` account permits access to non-administrative shell commands in the ExtraHop command-line interface (CLI). When accessing the privileged system configuration shell commands, the user types in `enable` and authenticates with the `setup` user password. For physical appliances, the default password for this account is the service tag number on the right-front bracket of the ExtraHop appliance. For virtual appliances, the password is `default`.

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

- When a user is authenticated and authorized locally, the user appears immediately in the managed users list. User permissions are managed in the ExtraHop appliance.
- When user is authenticated remotely but its authorization is managed locally, the user appears in the managed users list after the first login. The user's permissions are managed in the ExtraHop appliance.
- When a user is both authenticated and authorized remotely, the user does not appear in the managed users list. The user's permissions are managed in the remote server.

 **Note:** The local user account overrides all remote user account settings.

Add a user


1. In the Access Settings section, click **Users**.
2. Click **Add User**.
3. In the Personal Information section, type the following information:
 - Login ID: The username for the account. This is the name users will log in with and should not contain any spaces.
 - Full Name: A display name for the user.
 - Password: The new user password. The password must be a minimum of 5 characters
 - Confirm Password: Re-type the password from the previous field.
4. Click **Save**.

Modify an account


To change the account settings for a selected user:

1. In the Access Settings section, click **Users**.
2. Click the name of the user that you want to modify.
3. On the Update User page, modify the permissions or change the full name of the user.

Delete a user account

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

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

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

3. Click **OK**.

Sessions

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

Delete active sessions

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

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

Remote authentication

ExtraHop appliances supports remote authentication for user authentication. Remote authentication enables organizations that have authentication systems such as LDAP, RADIUS, or TACACS+ to allow all or a subset of their users to log on to the appliance with their existing credentials.

Centralized authentication provides the following benefits:

- User password synchronization.
- Automatic creation of ExtraHop accounts for users without administrator intervention.
- Management of ExtraHop privileges based on LDAP groups.

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

- LDAP (such as OpenLDAP or Active Directory)
 - Administrators can grant access to all known users or restrict access by applying LDAP filters.
- RADIUS
- TACACS+

LDAP

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

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

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

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

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

Configure LDAP authentication

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



Note: Clicking the back button in your browser during this procedure could result in lost changes.

3. On the LDAP Settings page, type the following information:

Hostname

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

Port

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

Base DN

Specifies the base of the LDAP search used to find users. The base DN must contain all user accounts that will have access to the ExtraHop appliance. The users can be direct members of the base DN or nested within an OU within the base DN if the **Whole Subtree** option is selected for the Search Scope specified below. Consult your LDAP administrator to learn what your organization selects.

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

Server Type

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

Search Filter

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

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

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

Search Scope


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

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

Bind DN

Specifies the Distinguished Name (DN) used by the ExtraHop appliance to authenticate with the LDAP server to perform the user search. The bind DN must have list access to the base DN and any OU, groups, or user account required for LDAP authentication. If this value is not set, then an anonymous bind is performed. Note that anonymous binds

are not enabled on all LDAP servers. To verify whether anonymous binds are enabled, contact your LDAP administrator. Using the active directory canonical name `example.com/people`, Bind DN examples include: `cn=admin, ou=users, dc=example, dc=com` and `uid=nobody, ou=people, dc=example, dc=com`

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

Bind Password

Specifies the password used when authenticating with the LDAP server as the bind DN specified above. If you are using an anonymous bind, leave this setting blank. In some cases, an unauthenticated bind is possible, where you supply a Bind DN value but no bind password. Consult your LDAP administrator for the proper settings.

Encryption

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

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

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

- **LDAPS:** This option specifies LDAP wrapped inside SSL, typically on port 636.
- **StartTLS:** This option specifies the use of TLS LDAP, typically on port 389. (SSL is negotiated before any passwords are sent.)

Full Access DN

Specifies which users can access the Explore appliance admin UI. If a DN is specified, only users in the specified DN will be able to log in. If the field is left blank, all users in the base DN will be able to log in.

Refresh Interval

Specifies when LDAP user information is refreshed. Type a time value in the Refresh Interval field or leave the default setting of 1 hour. The refresh interval ensures that any changes made to user or group access on the LDAP server are updated on the ExtraHop appliance.

4. Click **Test Settings**.

If the test succeeds, the message `LDAP settings test succeeded` appears. If the test fails, the message `LDAP settings test failed` appears. Resolve any errors before continuing.

5. Click **Save & Continue**.
6. Click **Done**.

RADIUS

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

Configure RADIUS authentication

1. In the Access Settings section, click **Remote Authentication**.
2. In the Methods section, select **RADIUS** from the Remote authentication method drop-down, then click **Continue**.
3. On the Add RADIUS Server page, type the following information:
 - **Host:** The hostname or IP address of the RADIUS server. Make sure that the DNS of the ExtraHop appliance is properly configured if you use a hostname.
 - **Secret:** The shared secret between the ExtraHop appliance and the RADIUS server. Contact your RADIUS administrator to obtain the shared secret.
 - **Timeout:** The amount of time the ExtraHop appliance will wait for a response from the RADIUS server before it attempts to connect again.

4. Click **Add Server**.
5. Click **Save and Finish**.
6. Click **Done**.

 **Note:** Remote users have full write access permissions to the Admin UI.


TACACS+

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

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

Configure TACACS+ authentication

1. Go to the Access Settings section and click **Remote Authentication**.
2. In the Methods section, select **TACACS+** and click **Continue**.
3. On the Add TACACS+ Server page, enter the host, secret, and timeout information and click **Add Server**.
4. Add multiple servers as needed.
5. Click **Continue**.
6. Click **Save & Finish**.
7. Click **Done**.


 **Note:** By default, remote users have full write access.

API access

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

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

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

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

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

See the [ExtraHop REST API Guide](#)  for more information.

Manage API access

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

1. In the Access Settings section, click **API Access**.
2. In the Manage Access section, select one of the following options:
 - **Allow all users to generate an API key**

Local and remote users can generate API keys.

- **Only local users can generate an API key**

Only users created on the appliance can generate API keys.

- **No users can generate an API key**

API keys cannot be generated. Selecting this option will delete any

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

Next steps

Save the changes to the [running config](#) file.

Enable CORS for the ExtraHop REST API

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

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

Add an allowed origin

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

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

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



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

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

Delete an allowed origin

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

1. In the Access Settings section, click **API Access**.
2. In the CORS Settings section, modify one of the following access configurations.
 - To delete a specific URL, click the delete (X) icon next to the origin you want to delete.
 - To disable access from any URL, clear the **Allow API requests from any Origin** checkbox.
3. Click **Save Settings**.

Generate an API key

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

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

Delete an API key

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

Explore cluster settings

The Explore Cluster Settings section provides the following configurable settings:

Join Cluster

Join an Explore appliance to an existing Explore cluster. This setting appears only for single nodes that have not yet been joined to an Explore cluster.

Cluster Members

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

Managers and Clients

Displays the hostname of the Command appliance that is configured to manage the Explore appliance as well as a list of all Discover appliances and Command appliances connected to the ExtraHop Explore appliance.

Data Management

Displays settings to set the data replication level and enable or disable shard reallocation.

Connect to a Command Appliance

Configure settings to enable a Command appliance to remotely run support packs on the Explore appliance

Restore Cluster State

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

Join an Explore cluster

To join a single Explore node to an existing Explore cluster:

1. In the Explore Cluster Settings section, click **Join Cluster**.
2. In the Host text box, type the host name or IP address of a node in the Explore cluster and then click **Continue**.
3. Verify the fingerprint that appears matches the fingerprint of the Explore node that you are joining.
4. In the Setup Password field, type the password for the `setup` user.
5. Click **Join**.

Cluster Members

The Explore Cluster Members page displays the following properties for each node in the Explore 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.

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.

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 for the node you want to remove, click **Remove Node**.
3. Click **Remove Node** to confirm.

Leave an Explore cluster

You can remove the local Explore node from an Explore cluster to remove all saved data on the node.

1. In the Explore Cluster Settings section, click **Cluster Members**.
2. In the Actions column, click **Leave Explore Cluster**.



Warning: Leaving an Explore cluster deletes all saved data on the Explore node.

3. Click **OK**.

Manager and Connected Appliances

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

Manager

Displays the hostname of the Command appliance that is configured to manage the Explore appliance. 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.


Data Management

You can configure the replication level of data on the Explore cluster. Additionally, you can enable and disable shard reallocation. You must connect a Discover appliance to the Explore cluster before you can configure replication level and shard reallocation settings.

Replication

You can change the replication level to specify the number of copies of the collected data stored on the cluster. 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.

1. In the Cluster Settings section, click **Data Management**.
2. Select one of the following replication levels from the Replication Level drop-down list:

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.  Important: Select this option when configuring a single-node cluster.
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. This option is not valid with single-node clusters.

3. Click **Update Replication Level**.

Shard reallocation

Data in an Explore cluster is split up into manageable chunks called shards. Shards might need to be created or moved from one node to another, as in the case of a node failure.

Shard reallocation is enabled by default. Prior to updating the firmware or taking the node offline for maintenance (for example, replacing disks, power cycling the appliance, or removing network connectivity between Explore nodes), you should disable shard reallocation by doing the following:

1. In the Cluster Settings section, click **Data Management**.
2. Under Shard Reallocation, click **Disable Shard Reallocation**.
3. After node maintenance is complete, enable shard reallocation by clicking **Enable Shard Reallocation**.

Connect to a Command appliance

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

The Explore appliance connects 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.


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 rare instances, the Explore cluster might not recover from a `red` status, as seen in the Status section on the 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 appliances (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.

Appliance Settings

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

Running Config

Download and modify the running configuration file.

Services

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

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.

Reset Packetstore

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

Firmware

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

The Admin UI includes the following firmware configuration settings:

Upgrade

Upload and install new ExtraHop appliance firmware versions.

Delete

Select and delete installed firmware versions from the ExtraHop appliance.

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

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



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

Upgrade to a new firmware version

Important: When you upgrade the firmware on nodes in an Explore cluster, always upgrade one node at a time and wait for the Explore cluster status to return to `Green` before updating the remaining nodes.

1. In the Appliance Settings section, click **Firmware**.
2. On the Firmware page, click **Upgrade**.
3. On the Upgrade Firmware page, select from the following options:
 - Click **Choose File**, navigate to the .tar file that you want to upload, and click **Open**.
 - Click **retrieve from URL instead** and enter the URL.

If the device has less than 300MB of space remaining, a warning message appears with a link to clean up the disk. We recommend that you perform a disk cleanup before uploading new firmware to ensure continued device functionality.

4. Click **Upgrade**.
The system initiates the firmware upgrade. You can monitor the progress of the upgrade with the Updating progress bar.
After the firmware update is installed successfully, the ExtraHop appliance displays the firmware version on the Admin UI page.
5. Repeat steps 1 through 4 for each additional node in the cluster.
6. If you upgraded multiple nodes in an Explore cluster, enable shard reallocation from the **Explore Cluster Settings > Data Management** page.

Delete firmware versions

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

1. In the **Appliance Settings** section, click **Firmware**.
2. Click **Delete**.
3. On the Remove Version page, select the checkbox next to the firmware images that you want to delete or select the **Check all** checkbox.
Selecting the **All** option does not allow you to select and delete the active firmware version.
4. Click **Delete Selected**.
5. Click **OK**.

System time

When capturing data, it is helpful to have the time on the ExtraHop appliance match the local time of the router. The ExtraHop appliance can set time locally or synchronize time with a time server. By default, system time is set locally, but we recommend that you change this setting and set time through a time server.

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

In the System Time section, the following information appears:

- Time Zone. Displays the currently selected time zone.
- System Time. Displays the current system time.
- Time Servers. Displays a comma-separated list of configured time servers.

The following information for each configured NTP server appears in the NTP Status table:

remote

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

st

The stratum level, 0 through 16.

t

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

when

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

poll

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

reach

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

delay

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

offset

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

jitter

Indicates the difference, in milliseconds, between two samples.

Configure the system time

1. In the **Appliance Settings** section, click **System Time**.
2. Click **Configure Time**.
3. Select your time zone from the drop-down list then click **Save and Continue**.
4. On the Time Setup page, select one of the following options:
 - Set time manually
 - Set time with NTP server
5. Select the **Set time with NTP server** radio button, then click **Select**.
The `pool.ntp.org` public time server appears in the Time Server #1 field by default.
6. 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.

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

Manage license

Provides an interface to add and update the ExtraHop appliance

System Information

Displays the identification and expiration information about the ExtraHop appliance.

Features

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

View the licensing system information

1. In the Appliance Settings section, click **License**.
2. On the License Administration page, under System Information, view the Extra Hop appliance information.

Register an existing license

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

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

If the test does not pass, open DNS server port 53 to make a connection or contact your network administrator.

4. Click **Register** and wait for the licensing server to finish processing.



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

5. Click **Done**.

Update a module license or add new licenses

1. In the Appliance Settings section, click **License**.

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

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

```

-----BEGIN EXTRAHOP LICENSE-----
serial=ABC123D;
dossier=1234567890abcdef1234567890abcdef;
mod_cifs=1;
mod_nfs=1;
mod_amf=0;
live_capture=1;
capture_upload=1;
10G=1;
triggers=0;
poc=0;
early_access_3.1=0;
activity_map=1;
ssl_acceleration=0;
ssl_decryption=0;
+++;
ABCabcDE/FGHIjklm12nopqrstuvwxyzAB12345678abcde901abCD;
12ABCDEFGH1HIJklmnOP+1aA=;
=abcd;
-----END EXTRAHOP LICENSE-----

```

5. Click **Update**.

Running config

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

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

Save config or Revert config

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

Edit config

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

Download config as a file

Download the system configuration to your workstation.



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

Saving running config changes

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

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

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

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

Save Configuration

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

Running Config*

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

Save*

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

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

Save system configuration settings

To save any modified system configuration settings:

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

Revert system configuration changes

To revert your changes without saving them to disk:

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

Edit running config

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

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

Download running config as a text file

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

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

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

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.