ExtraHop 6.0
ExtraHop Trace Admin UI Guide

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

Published: 2017-09-01

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

Contents

About this guide

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

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

After you have deployed your Trace appliance, see the Trace Post-deployment Checklist.

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

Navigation

This section describes the general layout of the Admin UI on a Trace 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 usersection.

Log out

Ends the Admin UI session on the Trace appliance. For more information, see the Log in and log out section.

Help

Opens the built-in ExtraHop Trace Admin UI Guide.

The administration page contains the following sections:

Status

Verify how the Trace appliance is functioning on the network.

Network Settings

Configure the network settings for the Trace appliance.

Trace Cluster Settings

View the Command appliance configured as the manager of the Trace appliance as well as a list of all paired Discover and Command appliances.

Access Settings

Configure access settings to the Trace appliance.

System Settings

Configure the system-level settings for the Trace appliance.

Diagnostics

Troubleshoot Trace appliance issues.

Log in and log out

The Admin UI on the Trace appliance is a secure web page that requires a user name and a password to access the interface.

1. To log into the Admin UI on the Trace appliance, type your user name in the **Username** field and your password in the **Password** field, and then click **Log In**.

   Note: The default user name is `setup` and the password is the service tag number on the pullout tab on the front of the appliance.

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

Browser compatibility

The following browsers are compatible with all ExtraHop appliances.

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

- Safari 9

Status

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

Health

Provides metrics about the operating efficiency of the Trace appliance.

Disks

Provides information about the disks in the Trace appliance.

Audit Log

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

Fingerprint

Provides the unique hardware fingerprint for the Trace appliance.

Health

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

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

CPU System

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

CPU Idle

Displays the CPU idle percentage associated with the Trace appliance.

CPU IO

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

Service Status

Reports the status of Trace appliance system services.

exadmin

Displays the time the Trace appliance web portal service started.

exconfig

Displays the time the Trace appliance config service started.

excap

Displays the time the Trace appliance capture service started.

Interfaces

Reports the status of Trace appliance network interfaces.

RX packets

Displays the number of packets received by the Trace appliance on the specified interface.

RX Errors

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

RX Drops

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

TX Packets

Displays the number of packets transmitted by the Trace appliance on the specified interface.

TX Errors

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

TX Drops

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

RX Bytes

Displays the number of bytes received by the Trace appliance on the specified interface.

TX Bytes

Displays the number of bytes transmitted by the Trace appliance on the specified interface.

Partitions

Reports the status and usage of Trace 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

Displays the Trace appliance settings that are stored on disk.

Options

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

Size

Displays the size in gigabytes for the identified component.

Utilization

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

Disks

The Disks page provides information about the configuration and status of the disks in your Trace 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

Provides a visual representation of the front of the Trace appliance.

RAID Disk Details

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

Datastore

Displays information about disks reserved for data storage and the option to encrypt the datastore disk. For more information, see the Encrypt the packetstore disk section.

Direct Connect Disk

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

Firmware

Displays information about disks reserved for the firmware.

Utility

Displays information about disks reserved for system files.

Encrypt the packetstore disk

You can encrypt the disk that packet captures are stored on for increased security. The disk is secured with 256-bit AES encryption.

Warning: You cannot decrypt a packet capture disk after it is encrypted. You can reformat an encrypted disk; however, all data stored on the disk will be lost.

1. In the Status section, click **Disks**.
2. In the Datastore section, click **Disk Encryption Settings**.
3. Click **Encrypt Disk**.
4. Specify a disk encryption key.

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

5. Click **Encrypt**.

Change the packet capture disk encryption key

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

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

5. Specify a new disk encryption key.

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

6. Click **Change Key**.

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 Trace appliance. When pairing the Trace appliance with a Discover 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.

Network settings

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

Connectivity

Configure network connections.

SSL Certificate

Generate and upload a self-signed certificate.

Notifications

Set up alert notifications through email and SNMP traps.

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

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

Connectivity

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

Network Settings

Host Name

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 Trace appliance displays the following information about the current interface connections:

Blue Ethernet Port

Identifies the management port.

Green Ethernet Port

Identifies the monitoring port.

Gray Ethernet Port

Identifies a disabled port.

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**.

Modify an interface

1. In the Network Settings section, click **Connectivity**.
2. In the Interfaces section, click the name of the interface you want to modify.

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

   Interface Mode

   Each interface can be configured as follows:

Interface	Interface mode
Interface 1	• Disabled • Management Port
Interface 2	• Disabled • Management Port
Interface 3	• Disabled

Interface	Interface mode
	• Monitoring Port • Management Port
Interface 4	• Disabled • Monitoring Port • Management Port
Interface 5	• Disabled • Monitoring Port
Interface 6	• Disabled • Monitoring Port

Important: If you only have one management interface configured and you set the interface mode to **Disabled** and click **Save**, you will lose your access to the node until the appliance is manually restarted.

Enable DHCPv4

DHCP is enabled by default. When you turn on the system, Interface 3 attempts to acquire an IP address through DHCP. After the DHCP server assigns an IP address to a physical appliance, the IP address appears on the LCD screen on 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 into 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. After the system acquires an IP address, log into the Admin UI again.

IPv4 Address

If you do not have DHCP enabled, you must manually configure a static IP address.

Netmask

If you do not have DHCP enabled, you must enter the netmask for your network.

Gateway

If you do not have DHCP enabled, you must enter the gateway 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

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

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

1. In the Network Settings section, click **Notifications**.
2. Click **Email Server and Sender**.
3. On the Email Settings page, type the following information:

   SMTP Server
   The IP address for the outgoing SMTP mail server.

   Note: The SMTP server should be the FQDN or IP address of an outgoing mail server that is accessible from the management network. If the DNS server is set, then the SMTP server can be a FQDN, otherwise it needs to be an IP address

   Sender Address
   The email address for the notification sender.
4. 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.

Email addresses

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.

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**.

Trace cluster settings

The Trace Cluster Settings section includes the following sections:

Managers and Clients

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

Query Status

View a list of all packet queries generated from paired Command and Discover appliances.

Trace manager and clients

The Trace Manager and Clients page contains the following information and controls:

Trace Cluster Manager

Displays the hostname of the Command appliance that is configured to manage the Trace appliance. The Trace cluster manager is configured on the Command appliance. For more information, see the Manage connected appliances from a Command cluster section in the ExtraHop Admin UI Guide.

Click **Remove Manager** to remove the Command appliance as the cluster manager.

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

Clients

Displays a table of all Discover appliances and Command appliances paired to the Trace appliance. The table includes the hostname of the connected client and the client product key.

View open packet queries

If the number of simultaneous packet queries exceeds the maximum allotted system memory, errors might occur and you must delete in progress or completed queries before you can create new queries. Queries are cached until you navigate away from the Packet Query page in the ExtraHop Web UI.

The following information is available on the Packet Query Status page.

Start Time

Displays the time that the packet query started.

Time Elapsed

Displays the running time of the packet query.

Status

Displays the status of the packet query.

Packets Found

Displays the number of packets returned from the query.

Memory Used

Displays the amount of system memory allocated to the query.

Query Memory Usage

Displays the percentage of total system memory that is currently allocated to in progress or cached packet queries.

Disk Cache Usage

Displays the percentage of packets that are cached.

Remove packet queries

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

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

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 includes the following configurable settings:

Change 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.

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 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 user name 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.
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. It enables organizations that have authentication systems such as LDAP, RADIUS, or TACACS+ to allow all or a subset of their users to log on to the appliance using their existing credentials.

Centralized authentication provides the following benefits:

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

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

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

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

LDAP

The ExtraHop 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 uses.

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

Server Type

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

Search Filter

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

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

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

Search Scope

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

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

Bind DN

Specifies the Distinguished Name (DN) used by the ExtraHop appliance to authenticate with the LDAP server to perform the user search. The bind DN must have list access to the base DN and any OU, groups, or user account required for LDAP authentication. If this value is not set, then an anonymous bind is performed. Note that anonymous binds are not enabled on all LDAP servers. To verify whether anonymous binds are enabled, contact your LDAP administrator. Using the active directory canonical name `example.com/people`, Bind DN examples include: `cn=admin, ou=users, dc=example,dc=com` `uid=nobody,ou=people,dc=example,dc=com`

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

Bind Password

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

Encryption

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

- **None**: This options specifies the use of cleartext TCP sockets, typically port 389. Warning: All passwords are sent across the network in cleartext in this mode.
- **LDAPS**: This option specifies LDAP wrapped inside SSL, typically on port 636.

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

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.

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.

System settings

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

Firmware
Update the ExtraHop system firmware.

System
Configure the system time.

Shutdown or Restart
Halt and restart status times.

License
Update the license to enable add-on modules.

Running Config
Download and modify the running configuration file.

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:

Update
Upload and install new ExtraHop appliance firmware versions.

Delete
Select and delete installed firmware versions from the ExtraHop appliance.

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

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 updating the firmware on a Command appliance, first update the Command appliance, next update all Discover nodes, and finally update each Explore and Trace appliance individually. To function correctly, the Command appliance and Discover nodes must have the same minor version of ExtraHop firmware.

Update to a new firmware version

1. In the System Settings section, click **Firmware**.
2. On the Firmware page, click **Update**.
3. On the Update 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 **Update**.

   The system initiates the firmware update. You can monitor the progress of the update 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.

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 **System 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 change this setting and set time through a time server.

Configure the system time

1. In the **System Settings** section, click **System Time**.
2. Click **Configure Time**.
3. Click to select from the **Select time zone drop-down** list.
4. Click **Save and Continue**.
5. Select the **Use NTP server to set time** radio button, then click **Select**.

   The `pool.ntp.org` public time server is entered by default.
6. Change the default IP address or add a second IP address in the two available time server fields, and then click **Save**.
7. Click **Done**.

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

Shutdown or restart the system

You can shut down or restart the Trace appliance in the Admin UI.

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

License

The 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 System Settings section, click **License**.
2. On the License Administration page, under System Information, view the Explore appliance information.

Register an existing license

Discover appliances must be registered before they are added to a Command cluster.

1. In the System 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 nodes that are managed by a Command cluster.
5. Click **Done**.

Update a module license or add new licenses

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

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

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

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

5. Click **Update**.

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.

Diagnostics

The Diagnostics section includes the following pages:

Exception Files

Enable or disable the Trace appliance exception files.

Support Packs

Upload and run support packages.

Enable writing to exception files

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

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

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

Disable writing to exception files

1. In the **Diagnostics** section, click **Exception Files**.
2. On the Enable/Disable Exception Files page, click **Disable Exception Files**.

Support packs

When you receive assistance from ExtraHop Support, you might need to load an ExtraHop-provided support pack to apply a special setting, make a small adjustment to the system, or get help with remote support or enhanced settings. 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**.