ExtraHop Explore

Admin UI Guide

Version 5.0

Publication Date: 1/15/2016

Table of Contents

Post-Deployment Actions

After you deploy the ExtraHop Explore appliance, take the following actions. Refer to the section of the Explore appliance specified in each action below, except where noted.

1. **Password**: Maintain system security after the evaluation period.
   Change the default password. For more information, see the **Change Password** section.
2. **NTP**: Time is critical in the Explore appliance, particularly when doing event correlation with time-based metrics and logs.
   Verify that the NTP settings are correct for your infrastructure, test settings, and sync NTP. For more information, see the **System Time** section.
3. **Time Zone**: The correct time zone is critical to run scheduled reports at the correct time.
   Ensure the Explore appliance has the correct time zone. For more information, see the **System Time** section.
4. **Remote Authentication**: Credential sprawl is a headache. The Explore appliance integrates with RADIUS, TACACS, and LDAP for remote integration.
   Set up remote authentication. For more information, see the **Remote Authentication** section.
5. **Firmware Update**: Explore appliance firmware is updated often with enhancements and resolved defects.
   Verify that you have the current firmware. For more information, see the **Firmware** section.
6. **Audit Logging**: The Explore appliance can send events to a remote syslog collector.
   Configure the Explore appliance to send audit logs. For more information, see the **Audit Log** section.
7. **SMTP Settings**: The Explore appliance can email alerts and system-health notifications.
   Set up and test notifications. For more information, see the **Email Server and Sender** section.
8. **System Notifications**: The Explore appliance can send email when it detects problems.
   Create an email group to receive notifications. For more information, see the **Notifications** section.
9. **iDRAC**: Each physical Explore appliance appliance has an iDRAC port, similar to iLO or KVM over Ethernet.

Connect and configure the iDRAC port. For more information, see the **Configuring the iDRAC Remote Access Console** section.

10. **SSL Certificate**: Each Explore appliance appliance ships with a self-signed certificate. If you have a PKI deployment, generate your own certificate and upload it to each Explore appliance appliance.

    Generate and deploy an SSL certificate for each Explore appliance appliance. For more information, see the **SSL Certificate** section.

11. **DNS 'A' Record**: It is easier to access an Explore appliance by hostname than by IP address.

    Create an 'A' record in your DNS root ("exa.yourdomain.local") for each Explore appliance in your deployment. Refer to your DNS administration manual.

About This Guide

The Explore Admin UI Guide provides detailed information about the administrator features and functionality for the Explore appliance, and how to join the Explore appliance to ExtraHop Discover and Command appliances.

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

For additional documentation, visit https://docs.extrahop.com.

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 Explore appliance Admin UI.

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 Password** section.
- **Log out**: Ends the Explore appliance Admin UI session. For more information, see the **Log in and Log out** section.
- **Help**: Opens the *Explore appliance Administration UI Guide*.

The administration page contains the following sections:

- **Status**: Verify how the Explore appliance is functioning on the network.
- **Network Settings**: Configure the network settings for the Explore appliance.
- **Cluster Settings**: Join an Explore appliance cluster and manage cluster settings.
- **Access Settings**: Configure access settings to the Explore appliance.
- **System Settings**: Configure the system-level settings for the Explore appliance.
- **Diagnostics**: Troubleshoot Explore appliance issues.

Log in and Log out

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

To log in to the Explore appliance Admin UI, 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 `default`.

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** 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.
- **Cluster Status**: Provides status information about the cluster, cluster nodes, and indices.
- **Disk**: Provides information about the disks in the Explore appliance.
- **Fingerprint**: Provides the unique hardware fingerprint for the Explore appliance.
- **Audit Log**: Enables you to view event logging data and to change syslog settings.

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.

Cluster Status

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

Cluster

- **Status**: The following status names can appear:
    - **green**: All data is replicated across the cluster.
    - **yellow**: The primary shard is allocated but replica shards are not. The cluster status is always **yellow** when there is only one Explore appliance.
    - **red**: One or more shards from the index are missing.
- **Nodes**: Displays the number of Explore appliancenodes in the cluster.

Cluster Nodes

- **Nickname**:Displays the nickname of the Explore appliance node when configured on the **Cluster Settings** > **Cluster Members** page.
- **Host**: Displays the IP address of the Explore appliance node.

Indices

- **Name**: Displays the name of the index.
- **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.
- **Replicas**: Displays the number of copies of data stored across the cluster. The number that appears is the configured number of replicas, not the actual number of replicas. By default, the **Replicas** value is 1. You can change the replication level in **Cluster Settings** > **Data Management**.
- **Shards**: Displays the number of shards in the index.
- **Active Shards**: Displays the number of active 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 setting 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 appliance in the cluster fails.

Delete all Records

In certain circumstances, such as moving the ExtraHop system from one network to another, you might want to delete all records (indices) from the cluster. To delete all records, complete the following steps:

1. In the **Status** section, click **Cluster Status**.
2. Below the **Indices** section, click **Delete All Records**.
3. Click **OK**.

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 Connect Disk**: (Virtual only) Displays information about virtual disks.

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

---

ExtraHop EXA Admin UI Guide

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.

Audit Log

The Explore appliance 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**.

The Explore appliance collects the following log data and reports the results on the Logs page.

- **Time**: Specifies the time at which the event occurred.
- **User**: Identifies the Explore appliance user who initiated the logged event.
- **Operation**: Specifies the Explore appliance 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 Explore appliance component that is associated with the logged event.

To change 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 Explore appliance system can communicate with the remote syslog server.
6. Once the syslog settings are configured, click **Save**.

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 setting. 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 Explore appliance system's network settings, 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.

Connectivity

To connect the Explore 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.

ExtraHop EXA Admin UI Guide

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 Explore 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 Explore appliance.

Change the network settings

To change the network settings:

1. Go to the **Network Settings** section and 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 Explore 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 alphanumeric 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**.

To 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.
   - **DHCP**: DHCP is enabled by default. When you turn on the system, interface 1

ExtraHop EXA Admin UI Guide

attempts to acquire an IP address using DHCP. After the DHCP server assigns an IP address to a physical appliance, the IP address apears 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, uncheck the **DHCP** 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.

- **IP 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.

- **MAC Address**: The Media Access Control (MAC) address is a unique identifier assigned to network devices for communication on the network. MAC addresses are assigned by the device manufacturer. The Explore appliance MAC address is printed on the label that is affixed to the bottom of the appliance. The unique MAC address for the appliance is set automatically and it cannot be changed in the Admin UI.

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

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

To manually set a 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**. The Admin UI redirects to the **Network Settings for Interface <interface number>** page.

To change the remaining interfaces:

1. Go to the **Network Settings** section and 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**.

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.

SSL Certificate

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

To configure the **SSL Certificate** settings:

1. Launch the Admin UI in your browser and enter your access credentials.
2. On the Admin page under **Network Settings**, click **SSL Certificate**.
3. Click **Manage certificates**.
4. Click **Build SSL self-signed certificate based on hostname**.
5. On the Generate Certificate page, click **OK** to regenerate the SSL self-signed certificate based on the hostname.
   The default hostname is *extrahop*.

The Explore system generates the self-signed certificate and private key that can be uploaded to the server. Under **Certificate Information**, you can view the self-signed certificate information generated for the specified host.

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**.

Notifications

Alerts are useful only if someone is notified about the alert when it is triggered. The Explore system uses two types of alert notifications: email and SNMP traps. If SNMP is specified, then every alert will be sent as an SNMP trap to the defined SNMP server. If an email notification group is specified, then emails will be sent to the groups assigned to the alert.

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 Explore appliance data to another system for archiving and correlation.

Email Server and Sender

Configuring Email Settings

To configure the **Email Server and Sender** settings:

1. Go to the Network Settings section and click **Notifications**.
2. Under **Notifications**, click **Email Server and Sender**.
3. On the **Email Settings** page, in the **SMTP Server** field, enter 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 Explore appliance 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. In the **Sender Address** field, enter the email address for the notification sender.
5. Click **Save**.

Testing Email Settings

To test that the Explore appliance can communicate with the SMTP server:

1. Go to the **Network Settings** section and click **Notifications**.
2. Click **Email Server and Sender**.
3. Click **Test Settings**.
4. Enter an email address to receive the test email.
5. When the SMTP server configuration is confirmed, log in to the Explore appliance and configure an alert.

Email Addresses

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

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

To add a new disk notification email address:

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

To delete a disk notification email address:

1. Go to the **Network Settings** section and click **Notifications**.
2. Under **Notifications**, click **Email Addresses**.
3. Click the red delete icon 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

Simple Network Management Protocol (SNMP) is used to monitor the state of the network. 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. Go to the Network Settings section and click **Notifications**.
2. Under **Notifications**, click **SNMP**.
3. On the **SNMP Settings** page, in the **SMTP Monitor** field, enter 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, enter 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 **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**.
4. The file is saved to the default download location for your browser.

Syslog

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

To configure the syslog notification settings for alerts:

1. Go to the **Network Settings** section and click **Notifications**.
2. Under **Notifications**, click **Syslog**.
3. In the **Destination** field, enter the IP address of the remote syslog server.
4. Click the **Protocol** drop-down list and select **TCP** or **UDP**.
5. In the **Port** field, enter the port number. The port is set to 514 by default.

Cluster Settings

The Cluster Settings section includes the following configurable settings:

- **Join Cluster**: Join the Explore appliance to an existing Explore cluster.
- **Cluster Members**: Displays all of the nodes that are members of the Explore cluster.
- **Clients**: Displays 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.

Join Cluster

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

1. Go to the **Cluster Settings** section and 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 that the number matches the fingerprint of the Explore cluster node that you are joining.
4. In the **Setup Password** field, enter the Setup user's password.
5. Click **Join**.
6. When the cluster join succeeds, click **OK**.

Cluster Members

The **Cluster Members** page lists all of the nodes in the Explore cluster.

- **Nickname**: Add or change the name of a cluster member.
- **Host**: Displays the IP address of the Explore node.
- **Actions**: Remove an Explore node from the cluster.

To add or change the nickname of a node:

1. In the **Nickname** column, click the IP address or name of the node.
2. In the **Name** field, type a name for the node.
3. Click **Rename Node**.

To remove a node from the cluster:

1. In the **Actions** column, click **Leave Cluster**.
2. Confirm the action by clicking **OK**.

Clients

The **Clients** page displays a list of all ExtraHop Discover appliances and ExtraHop Command appliances connected to the Explore appliance.

- **Host**: Displays the host name of the connected client.
- **Product Key**: Displays the product key for the client.
- **Action**: Allows you to remove any 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 need more than one Explore appliance to set 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. Go to the **Cluster Settings** section and click **Data Management**.
2. Select one of the following replication levels from the **Replication Level** drop-down list:
   0: Data is not replicated to other nodes in the cluster. This level allows you to collect more data on the cluster; however, if there is a node failure, you will permanently lose data.
   1: There is one copy of the original data stored on the cluster. If one node fails, you will not permanently lose data.

2: There are two copies of the original data stored on the cluster. This level requires the most disk space but provides the highest level of data protection. Two nodes in the cluster can fail without permanently losing data.

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 upgrading the firmware on an Explore appliance, you should disable shard reallocation by doing the following:

1. Go to the **Cluster Settings** section and click **Data Management**.
2. Under **Shard Reallocation**, click **Disable Shard Allocation**.
3. After the node firmware is successfully upgraded, enable shard reallocation by clicking **Enable Shard Reallocation**.

Access Settings

In the Access Settings section, you can change passwords, enable the support account, and define users in the Explore system for remote authentication.

- **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 Explore system.
- **Remote Authentication**: Enable users to log on to the Explore system using their existing credentials.

Change Password

Explore appliance Admin UI administrators have privileges to change the password for any user that has an account stored locally in the Explore appliance Admin database. For more information about privileges for specific Admin UI users and groups, refer to **Users**.

Change the Password Settings

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

1. Go to the **Access Settings** section and click **Change Password**.
2. On the **Change Password** page, select the user for which you want to set the password. In the **New password** field, type the new password.
3. In the **Confirm password** field, type the new password.
4. Click **Save**.

Change the Default Password for the setup User

ExtraHop recommends changing the default password for the setup account as soon as the evaluation period is complete. 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.

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

Support Access

The support account provides access for the ExtraHop Support team to help customers troubleshoot issues with the Explore appliance. This setting should be enabled only if your organization's Explore appliance system administrator requests hands-on assistance from the ExtraHop Support team.

To enable the support account:

1. Go to the **Access Settings** section and click **Support Account**.
2. To enable the support account, click **Enable Support Account**.
3. The next page contains an encrypted key used by ExtraHop Support to access the Explore appliance. Copy the contents of the PGP message and send it to support@extrahop.com.
4. Click **Done** to return to the **Support Access** page.

To disable the support account, click the **Disable Support Account** button.

To regenerate a support account key:

1. Go to the **Access Settings** section and click **Support Account**.
2. On the **Support Access** page, click **Regenerate Key**, and then click **Regenerate** to confirm the action.
3. The next page contains an encrypted key used by ExtraHop Support to access the ExtraHop appliance. Select the contents of the PGP message on this page and send it to support@extrahop.com.
4. Click **Done** to return to the **Support Access** page.

Users

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

User accounts can be locally or remotely authenticated and authorized. For more information, refer to **Remote Authentication**.

- When a user is authenticated and authorized locally, the user appears immediately in the managed users list. The user's permissions are managed in the Explore system.
- 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 Explore system.
- 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

To add a user to the Explore system:

1. Go to the Access Settings section and click **Users**.
2. The current users and their permissions are listed. Click the **Add User** button.
3. Fill in the **New User** form. All fields are required. Enter the personal information, select the correct permission for the user, and then select the **Enabled** checkbox. Each enabled user must have a permission selected.
4. Click **Save**.

The Users page displays the newly created user in the list.

Modify an Account

To change the account settings for a selected user:

1. Go to the Access Settings section and select **Users**.
2. The current users and their permissions are listed. Click the **Change** link next to the account to be modified.
3. On the **User:[User]** page, modify the permissions or change the full name and then click **Save**.

The Users page displays with the changes shown.

> **Note**: To remove an account from the system, click **Delete** next to the name of the account on the Users page. Remote user records are removed from the ExtraHop system only when they are manually deleted.

On the Command appliance, you can set additional permissions to access the Admin UI. To change the account settings for a selected user on an Command appliance:

1. Go to the Access Settings section and select **Users**.
2. The current users and their permissions are listed. Click the **Change** link next to the account to be modified.
3. On the **User:[User]** page, modify the permissions or change the full name and then click **Save**. When **Cluster Node UI Privileges** is selected, the user has access to specific clusters and nodes as permitted by the LDAP settings.

Default Accounts

The following accounts are preconfigured in the system. Only the setup account is accessible at https://[IP address]/admin, where [IP address] is the IP address displayed on the LCD at the front of the Explore appliance.

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

The **setup** account has full access privileges. The default password for this account is the service tag number on the right-front bracket of the appliance.

Sessions

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

View Active Sessions

To view active sessions, go to the **Access Settings** section and click **Sessions**.

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.

To delete an active session for a specific user:

1. In the **Sessions** table, click the red **x** at the end of the row for the specific user.
2. On the Delete Session page, click **OK**.

To delete all active user sessions:

1. Click the **Delete All** button.
2. On the Delete all sessions page, click **OK**.

Remote Authentication

The Explore system 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 Explore system using their existing credentials.

Centralized authentication provides the following benefits:

- User password synchronization
- Automatic creation of Explore accounts for users without administrator intervention
- Management of Explore 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 Explore systems to all known users or restrict access by using LDAP filters.

LDAP

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

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

To authenticate with LDAP on the ExtraHop system:

1. Go to the **Access Settings** section and click the **Remote Authentication**.
2. In the **Methods** section, select the **LDAP** option and click **Continue**.
3. On the LDAP Settings page, complete the following fields:
   - **Hostname** (required): Specifies the hostname or IP address of the LDAP server. Make sure that the Explore system's DNS is properly configured when using host-names.
   - **Port** (required): 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** (required): 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 Explore system. The users can be direct members of the base DN or nested within an OU within the base DN if the **Whole Subtree** option is selected for the **Search Scope** defined below. Consult your LDAP administrator to learn what your organization uses. Examples include:
     - Active directory canonical name: `example.com/people`
       LDAP base DN: `ou=people,dc=example,dc=com`
     - Active directory canonical name: `example.com/people/employees/portland`
       LDAP base DN: `ou=portland,ou=employees,ou=people,dc=example,dc=com`
   - **Login Attribute** (required): Specifies the login attribute that holds the user's username attribute in the LDAP database. Examples include:
     - *uid*: A username attribute typically used in Unix LDAP environments.
     - *sAMAccountName*: An account name attribute typically used in Active Directory (AD) environments.
   - **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. Options include:
    - **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`, it would find a user `uid=jdoe,dc=example,dc=com`, but would not find `uid-d=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`, it would find both the user `uid=jdoe,dc=example,dc=com` and `uid-d=jsmith,ou=seattle,dc=example,dc=com`.
- **Bind DN**: If set, this specifies the Distinguished Name (DN) used by the Explore system 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. 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
```

To verify whether anonymous binds are enabled, contact your LDAP administrator.
- **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. Again, consult your LDAP administrator for the proper settings.
- **SSL**: 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.)

If you are not sure which options are available, consult your LDAP administrator.

> Clicking your browser's **Back** button during this process could result in lost changes.

4. Click **Test Settings**. If the settings test succeeded, a message in green text appears near the top of the page. If the settings test failed, a message in red text lists the errors.

5. Click **Save & Continue**.

6. Click **Done**.

7. Determine whether you want to do local or remote authentication.

   a. **Local authorization**: By default, remote users have full write access. If you wish to grant all remote users read-only privileges by default, select **Remote users have Read Only access**.

      You can add read-write permissions on a per-user basis later through the Users page in the Admin UI.

   b. **Remote authorization**: You may also choose to obtain a permissions level from a remote server. When you select the **Obtain permissions...** option, you must complete at least one of the following fields to define the remote permissions:

      These must be groups (not organizational units) that are pre-defined on the LDAP Server. A user account with access must be a direct member of a defined group. User accounts that are a member of a group that is a member of a group defined above will not have access. If the groups are not present, they will not be authenticated on the ExtraHop system.

      The ExtraHop system supports the following types of group membership:

      - **Active Directory**: memberOf
      - **Posix**: posixGroups, groupofNames, and groupofuniqueNames

      Examples:

      Given the base DN:

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

      and the bind DN:

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

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

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

      and is nested within:

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

      would have read-only access on the ExtraHop system.

      Examples of accounts with access:

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

      cn=admin,ou=seattle,ou=washington,dc=usa,dc=example,dc=com

      Examples of accounts without access:

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

8. Click **Save & Finish**.
9. Click **Done**.

RADIUS

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

To configure RADIUS authentication for the Explore system:

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

The **Remote Authentication** page appears with the new settings.

TACACS+

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

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

To configure TACACS+ authentication for the Explore system:

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. Determine whether you want to do local or remote authentication.

a. **Local Authorization**: By default, remote users have full write access. If you wish to grant all remote users read-only privileges by default, select **Remote users have Read Only access**.

b. **Remote Authorization**: On the TACACS+ server, set up the ExtraHop service by adding the attribute `service=extrahop` and setting one of the following permissions.

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

Example:

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

7. Click **Save & Finish**.
8. Click **Done**.

System Settings

You can configure the following components of the Explore system in the System Settings section:

- **Firmware**: Update the Extrahop system firmware.
- **System Time**: 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 the Explore appliance.

The Explore Admin UI includes the following firmware configuration settings:

- **Update**: Upload and install new Explore appliance firmware versions.
- **Delete**: Select and delete previously installed firmware versions from the Explore appliance.

You can download the latest firmware at the 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 then 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: Each Explore node in the cluster must be updated individually.

To update the Explore system firmware:

1. On the Admin page under **Cluster Settings**, click **Data Management**. This option only exists if you have more than one Explore node. If you only have a single Explore node, skip to step 3.

ExtraHop EXA Admin UI Guide

2. Under **Shard Reallocation**, click **Disable Shard Reallocation**. Disabling shard real-location prevents the cluster from moving data files from one node to another while the update is in process.

3. On the Admin page under **System Settings**, click **Firmware**.

4. On the **Firmware** page, click the **Update**.

5. To specify the firmware file:

    - Click **Choose File**, navigate to the .tar file that you want to upload, and click **Open**.
    OR
    - 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. ExtraHop strongly recommends performing a disk cleanup before uploading new firmware to ensure continued device functionality.

6. Click **Update**.
    The system initiates the firmware update. You can monitor the progress of the update with the **Updating** progress bar.

7. After the firmware update is installed successfully, the Explore system displays the version number of the new firmware image. If the **Automatically Restart** checkbox is selected, the system automatically restarts after the firmware is upgraded.

8. After restarting, on the Admin UI main page, view the firmware version that appears at the top of the page.

9. Verify that the firmware version number displayed matches the version that you down-loaded from ExtraHop.

10. On the Admin page under **Cluster Settings**, click **Data Management**.

11. Under **Shard Reallocation**, click **Enable Shard Reallocation**.

12. Repeat steps 1 through 11 for each additional Explore node in the cluster.

Deleting Firmware Versions

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

To delete firmware images from the Explore system:

1. On the Admin page under **System Settings**, click **Firmware**.

2. On the **Firmware** page, click **Delete**.

3. On the Installed Firmware Images page, click the checkbox next to the firmware image that you want to delete.

    > **Note**: You can select multiple versions.

4. If you want to delete all installed firmware images, click the **Check all** checkbox.

> **Note**: Selecting the **Check all** option does not allow you to select and delete the active firmware version.

5. Click **Delete Selected**.
6. Click **OK** to confirm that you want to delete the selected firmware versions

The selected firmware images are removed from the Explore system.

System Time

When capturing data, it is helpful to have the time on the Explore system match the local time of the router. The Explore system can rely on setting time locally, or it can keep the system time accurate by using time servers. You can use the default time server setting, `pool.ntp.org`, or you can configure the system time manually.

To configure the system time:

1. Go to the **System Settings** section and click **System Time**.
2. Click the **Configure Time** button.
3. Click the **Time Zone** drop-down list and select a time zone. Click **Save & Continue**.
4. Select the **Use NTP server to set time** radio button and click **Select**.
5. To set the NTP servers, enter the IP addresses for the time servers and click **Save**.

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

> **Note**: If needed, select the **Set clock manually** radio button to adjust the date and time. Set the date and time values, and then click **Save**. The System Clock time setting is not UTC, but it reflects the time zone currently set in the Time Zone section.

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

Shutdown or Restart

The Admin UI provides an interface to halt, shutdown, and restart the Explore system. The Explore appliance Admin UI includes restart controls for the following system components:

- **System**: Restart or shut down the Explore system.
- **Admin**: Restart the Explore admin component.
- **Receiver**: Restart the Explorereceiver component.
- **Search**: Restart the Explore search service.

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

System

To restart or shut down the Explore system:

1. On the Admin page under **System Settings**, click **Shutdown or Restart**.
2. Next to **System**, click **Restart**.
3. At the prompt, click **Restart**.

Admin

To shut down and restart the ExtraHop admin:

1. On the Admin page under **System Settings**, click **Shutdown or Restart**.
2. Next to **Admin**, click **Restart**.
3. At the prompt, click **OK**.

Receiver

To shut down and restart the Explore receiver:

1. On the Admin page under **System Settings**, click **Shutdown or Restart**.
2. Next to **Capture Status**, click **Restart**.
3. At the prompt, click **OK**.

Search

To shut down and restart the Explore search:

1. On the Admin page under **System Settings**, click **Shutdown or Restart**.
2. Next to **Search**, click **Restart**.
3. At the prompt, click **OK**.

License

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

- **System Information**: Displays the identification and expiration information about the Explore appliance.
- **Features**: Displays the list of licensed Explore system features (such as Activity Mapping) and whether the licensed features are enabled or disabled.
- **Manage License**: Provides an interface to add and update licenses for Explore system features and modules.

To view the licensing system information:

1. On the Admin page under **System Settings**, click **License**.
2. On the **License Administration** page, under **System Information**, view theExplore system information.

To register an existing license:

1. On the Admin page under **System Settings**, click **License**.
2. On the License Administration page, under **Manage License**, click **Register**.
3. (Optional) On the Register Appliance page, click the **Test Connectivity** button.
   The ExtraHop license server uses DNS records to determine whether a connection is possible.
   If the test does not pass, open DNS server port 53 to make a connection or contact your system administrator.
4. Click the **Register** button.
5. Wait for the license server to finish processing, and then click **Done**.

To update a module license or add new licenses to the Explore system:

1. On the Admin page under **System Settings**, click **License**.
2. On the License Administration page, under **Manage License**, click **Update**.
3. 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 system as well as key-value pairs to enable the module licenses and other ExtraHop system 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-----
```

4. Click **Update**.

Running Config

The **Running Config** settings let you make changes to the default Explore appliance system configuration settings and then save those settings to disk. The **Running Config** page provides an interface to view and modify the code that defines the default system configuration and save changes to the current running configuration so the modified settings are enabled after a system restart.

The Explore appliance Admin UI includes the following controls to manage the default running system configuration settings:

- **Save config**: Save changes to the current default system configuration.
- **Revert config**: Revert any unsaved changes to the system configuration.
- **Edit config**: View and edit the underlying code that defines the Explore appliance default system configuration.
- **Download config as a file**: Download the system configuration to your workstation. Making configuration changes to the code on the **Edit config** page is not recommended. You can make most modifications using other pages in the Admin UI.

Save config

When you modify any of the Explore appliance default system configuration settings, you need to confirm the updates by saving the new settings.

To save any modified system configuration settings:

1. Go to the **System Settings** section and click **Running Config**.
2. On the **Running Config** page, click **Save**.
3. In the confirmation dialog box, click Done.

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 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, these changes will be lost.

For example, if you make a change to a protocol classification setting on the Protocol Classification page, the change (in memory) takes effect immediately, but it does not permanently change the running configuration until you save the changes. As a reminder that the running configuration has changed, the Admin UI provides the following three notifications:

- **View and Save Changes**: 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 the **View & Save Changes** button, 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 config***: The Admin UI adds a red asterisk (*) next to the **Save config** 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.

To revert your changes without saving them to disk:

1. On the **Running Config** page, click **Revert config**.
2. Click **Revert** again.
3. Click **OK** to confirm the action.

Edit

The Explore Admin UI provides an interface to view and modify the code that defines 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 **Edit Running Config** page.

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

Download config as a file

You can download the **Running Config** settings to your workstation in text file format. Click **Download config as a file** and open the text file to make changes locally before copying them into the **Edit Running Config** window.

Diagnostics

The **Diagnostics** section includes the following pages:

- **Receiver Health**: Displays metrics about the records that are sent from the exreceiver process to the Explore cluster.
- **Support Packs**: Upload and run Explore appliance support packages.

Receiver Health

The following metrics appear on the **Receiver Status** page:

- **Activity since**: Displays the timestamp when record collection began. The value is reset automatically every 24 hours or whenever the Explore appliance is restarted.
- **Compressed Network Bytes Received**: Displays the number of compressed record bytes received from the Discover appliance.
- **Record Bytes Received**: 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.
- **Transaction Errors**: Displays the number of bulk record transactions that resulted in an error. Errors in this field might indicate missing records.
- **Transaction Drops**: Displays the number of bulk records transactions that did not complete successfully. All records in the transaction are missing.

ExtraHop EXA Admin UI Guide

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 Explore appliance 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 Explore appliance system.
- **Apply System Support Pack**: Execute a selected diagnostic support package.

View Support Pack Results

You can view, download, or delete the diagnostic support packages that have been uploaded to the Explore appliance.

To view the diagnostic support packages on the system:

1. Go to the **Diagnostics** section and click **Support Packs**.
2. Under **Support Packs**, click the **View Support Pack Results**.

To download a selected diagnostic support package:

1. Go to the Diagnostics section and click **Support Packs**.
2. Under **Support Packs**, click the **View Support Pack Results**.
3. Locate the diagnostic support package that you want to download.
4. Click the **Download** icon next to the support package create date.
5. At the prompt, click the **Save File** option, and then click **OK**.

To delete a selected diagnostic support package:

1. Go to the Diagnostics section and click **Support Packs**.
2. Under **Support Packs**, click the **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

To upload a selected diagnostic support package:

1. Go to the **Diagnostics** section and click **Support Packs**.
2. Under **Support Packs**, 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 Explore appliance.

System Support Pack

Some support packs only perform a function on the Explore appliance, while others 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 Support Pack Results page. If it does not, you can go to the Support Pack Results page from the **Support Packs** page.

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

1. Go to the Diagnostics section and click **Support Packs**.
2. Under **Support Packs**, click **Apply System Support Pack**.
3. Click **OK**.