

Deploy the ExtraHop Explore Appliance

Published: 2019-02-08

This guide explains how to install and configure the rack-mounted ExtraHop Explore appliance.

System requirements

Your environment must meet the following requirements to deploy an Explore appliance:

Appliance

2U of rack space and 2x750W of power

Network Access

- The following TCP ports must be open:

TCP ports 80 and 443

Enables you to administer the Explore appliance through the Web UI. Requests sent to port 80 are automatically redirected to HTTPS port 443.

TCP port 9443

Enables Explore nodes to communicate with other Explore nodes in the same cluster.

Install the Explore appliance

To install the Explore appliance, complete the following steps.

- Rack mount the Explore appliance.


Install the Explore appliance in your data center with the included rack-mounting kit. The mounting kit supports most four-post racks with either round or square holes.

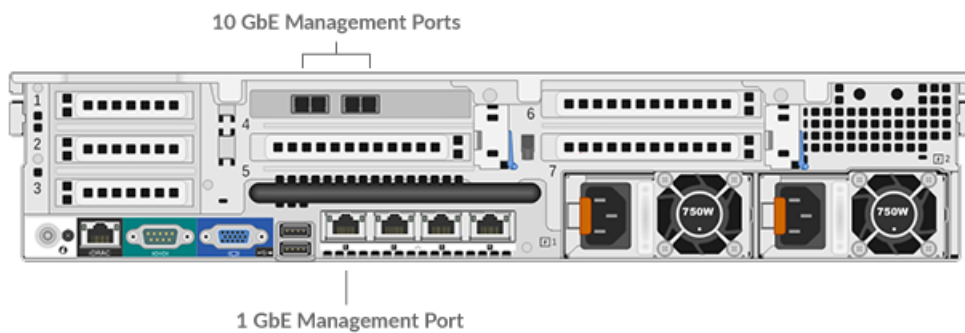
- Connect port 1.

The Explore appliance contains a set of four 10/100/1000 BASE-T network ports. Only the first port on the left is active. Connect the 1GbE port on the Explore appliance to the management network with a network patch cable.

- Optional: Connect a 10 GbE port

Connect one of the 10 GbE ports on the appliance with a 10 GbE cable to your network to manage the Explore appliance. Note which port you are connecting to so you can configure this port later through the Admin UI.

 **Note:** You can configure only one port as an Explore appliance management port.



Configure an IP address

DHCP is enabled by default on the ExtraHop appliance. When you power on the appliance, interface 1 attempts to acquire an IP address through DHCP. If successful, the IP address appears on the home screen of the LCD. If an IP address has not been configured, the LCD displays `No IP`.

If your network does not support DHCP, you can configure a static IP address through the LCD menu on the front panel or through the command-line interface (CLI).

Configure a static IP address through the CLI

You can access the CLI by connecting a USB keyboard and SVGA monitor to the appliance or through an RS-232 serial cable and a terminal-emulator program. The terminal emulator must be set to 115200 bps with 8 data bits, no parity, 1 stop bit (8N1), and hardware flow control should be disabled.

1. Establish a connection to the ExtraHop appliance.
2. At the login prompt, type `shell` and then press ENTER.
3. At the password prompt, type the service tag number found on the pullout tab on the front of the appliance, and then press ENTER.
4. Enable privileged commands by running the following command:

```
enable
```

5. At the password prompt, type the service tag number, and then press ENTER.
6. Enter configuration mode by running the following command:

```
configure
```

7. Enter the interface configuration mode by running the following command:

```
interface
```

8. Run the `ip` command and specify the IP address and DNS settings in the following format: `ip ipaddr <ip_address> <netmask> <gateway> <dns_server>`

For example:

```
extrahop[EXA](config-if)# ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
```

9. Leave the interface configuration section:

```
exit
```

10. Save the running config file:

```
running_config save
```

11. Type `y` and then press ENTER.

Configure a static IP address through the front panel

Complete the following steps to configure the IP address from the front panel. If an IP address has not been configured, the front panel displays `No IP`. If the system is plugged in and powered off, the LCD screen displays `ExtraHop`.

1. Press the **Select** (checkmark) button. Navigate with the left and right arrow buttons, and select **Net**.
2. Select **Host**. The screen displays the host name. Scroll up the screen and select the up arrow.
3. Select **DHCP** to see how the IP address is configured. Navigate with the left and right arrow buttons to select an option, and press the **Select** button.

4. From the Net screen, select **IP** and change the digits with the left and right arrow buttons. On the selected digit, click the **Select** button. The digit blinks when selected. While the digit is blinking, change the digits with the left and right arrow buttons.
5. After you have entered the number, click **Select** to navigate up the screen and select the up arrow. On the Save screen, select **Yes**.
6. Wait to be redirected to the Net screen. Repeat steps 2-6 to set IP addresses for the netmask, gateway, and up to two DNS servers.
7. Optional: Scroll back to the Home menu and select **iDRAC**. Configure IP addresses for the iDRAC DHCP, IP, netmask, gateway, and DNS.
8. From the Net screen, select Errors to view system events such as CPU errors, undetected hard drives, or missing power supplies. When an error occurs, the LCD turns amber and displays the error.
9. If there are multiple errors, scroll between the error messages with the left and right arrow buttons. Press the **Select** button to exit the error screen. The **Clear** option removes the list of messages from the error screen.

Configure the Explore appliance

After you configure an IP address for the Explore appliance, you can log into the Explore Admin UI through the following URL: `https://<explore_ip_address>` and complete the following recommended procedures.



Note: The default login username is `setup` and the password is the service tag number on the pullout tab on the front of the appliance. You can modify user names and passwords in the Explore Admin UI.

- [Register the ExtraHop appliance](#)
- [Configure the 10GbE management port](#)
- [Create an Explore cluster](#)
- [Configure the system time](#)
- [Configure email notifications](#)
- [Pair the Explore appliance to Discover and Command appliances](#)
- [Send record data to the Explore appliance](#)

Register the ExtraHop appliance

Complete the following steps to apply a product key supplied by ExtraHop Support.

If you do not have a product key, contact support@extrahop.com.



Tip: To verify that your environment can resolve DNS entries for the ExtraHop licensing server, open a terminal application on your Windows, Linux, or Mac OS client and run the following command:

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

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

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

1. In your browser, type the URL of the ExtraHop Admin UI, `https://<extrahop_ip_address>/admin`.
2. Review the license agreement, select **I Agree**, and then click **Submit**.
3. On the login screen, type `setup` for the username.
4. For the password, select from the following options:

- For 1U and 2U appliances, type the service tag number found on the pullout tab on the front of the appliance.
 - For the EDA 1100, type the serial number displayed in the `Appliance info` section of the LCD menu. The serial number is also printed on the bottom of the appliance.
 - For a virtual appliance, type `default`.
5. Click **Log In**.
 6. In the System Settings section, click **License**.
 7. Click **Manage License**.
 8. Click **Register**.
 9. Enter the product key and then click **Register**.
 10. Click **Done**.

(Optional) Configure the 10GbE management port


1. In the Network Settings section, click **Connectivity**.
2. In the Interfaces section, click **Interface 5** or **Interface 6**. Make sure you select the same interface as the physical port you connected the 10GbE cable to. Interface 5 is the 10GbE port to the left on the rear of the appliance.
3. From the **Interface Mode** drop-down list, select **Management Port**.
4. Configure the rest of the network settings.
5. Click **Save**.
6. In the Interfaces section, click **Interface 1**.
7. From the Interface Mode drop-down list, select **Disabled**.
8. Click **Save**.
9. Click the **View and Save Changes** button at the top of the page to save the running config file.
10. Click **Save**. Your connection to the Web UI through interface 1 is terminated.
11. Log in to the Web UI again to connect through the newly configured 10GbE interface.

Create an Explore cluster

Before you begin

Log into the Admin UI of each Explore node, click **Fingerprint** in the Status section, and note the value listed in the Fingerprint field. The fingerprint of each node should be verified during the join process.

If you are deploying three or more Explore nodes, join the nodes to create a cluster.

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

1. Log into the Admin UI of any new Explore node.
2. In the Cluster Settings section, click **Join Cluster**.
3. In the Host text box, type the hostname or IP address of any of the other new nodes and then click **Continue**.
4. Verify that the fingerprint displayed on the page matches the fingerprint of the Explore node that you are joining. If these fingerprints do not match, communication between the nodes might have been intercepted and altered.
5. In the Setup Password field, type the password for the `setup` user.
6. Click **Join**.
7. In the Status section, click **Cluster Status**.
8. Wait for the Status field to change to `green`.
9. Repeat steps 1 - 8 to join each additional node to the new cluster.



Note: Always join a new node to the existing cluster and not another unjoined node, or you will create multiple clusters.

10. Click **Cluster Members** in the Cluster Settings section to confirm that all of the nodes are listed on the page.

Configure the system time

By default, the Explore appliance synchronizes the system time through the pool.ntp.org network time protocol (NTP) server. If your network environment prevents the Explore appliance from communicating with this time server, you must configure an alternate time server source.



Note: Time synchronization is critical to ensuring proper cluster operations and maintaining consistent views of data across both Discover and Explore appliances. We strongly recommend that you either keep the default system time setting or configure settings for a different NTP server.

1. In the System Settings section, click **System Time**.
2. Click **Configure Time**.
3. Click the Time Zone drop-down list and select a time zone. Click **Save and Continue**.
4. Select the Use NTP server to set time radio button and then click **Select**.
5. Type the IP addresses for the time server, and then click **Save**.
6. Click **Done**.
7. Click **Sync Now** to sync system time on the Explore appliance with the remote time server.

Configure email notifications

You must configure an email server and sender before the ExtraHop appliance can send notifications about system alerts by email.

You can receive the following alerts from the system:

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

Pair the Explore appliance to Discover and Command appliances

After you deploy the Explore cluster, you must establish a connection from all ExtraHop Discover and Command appliances to the Explore cluster before you can query records. If you manage all of your Discover appliances from a Command appliance, you only need to perform this procedure from the Command appliance.



Important: If you have an Explore cluster, pair the Discover appliance to each Explore node so that the Discover appliance can distribute the workload across the entire Explore cluster.

1. Log into the Discover or Command appliance Admin UI.
2. In the ExtraHop Explore Settings section, click **Configure Explore Cluster**.
3. Click **Add New**.
4. In the Host #1 Host field, type the hostname or IP address of any Explore appliance in the Explore cluster.
5. For each additional Explore appliance in the cluster, click **Add New** and enter the individual hostname or IP address in the corresponding Host field.
6. Click **Save**.
7. Note the information listed for Fingerprint. Verify that the fingerprint listed on this page matches the fingerprint of the Explore appliance (**Host #1**) listed on the Fingerprint page in the Explore Admin UI.

8. In the Explore Setup Password field, type the password of the Explore appliance.
9. Click **Join**, and then click **Done**.

Send record data to the Explore appliance

After your Explore appliance is paired with all of your Discover and Command appliances, you must configure the type of records you want to store. See the following documentation for more information about Explore configuration settings, how to generate and store records, and how to create record queries.

- [ExtraHop Explore Admin UI Guide](#)
- [ExtraHop Explore Settings](#) section in the [ExtraHop Admin UI Guide](#).
- [Records](#) section in the [ExtraHop Web UI Guide](#).
- [ExtraHop Trigger API Reference](#)