Deploy the ExtraHop Explore Appliance

Published: 2019-01-08

In this guide, you will learn how to configure the rack-mounted EXA 5100 ExtraHop Explore appliance and to join multiple Explore appliances to create an Explore cluster.

For the best performance, data redundancy, and stability, you must configure at least three Explore appliances in an Explore cluster.

System requirements

To install the Explore appliance, your environment must meet the following requirements:

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.

Before you begin
All Explore nodes in an Explore cluster must be physically located in the same datacenter. This configuration helps reduce any network latency that might affect the collection of records.

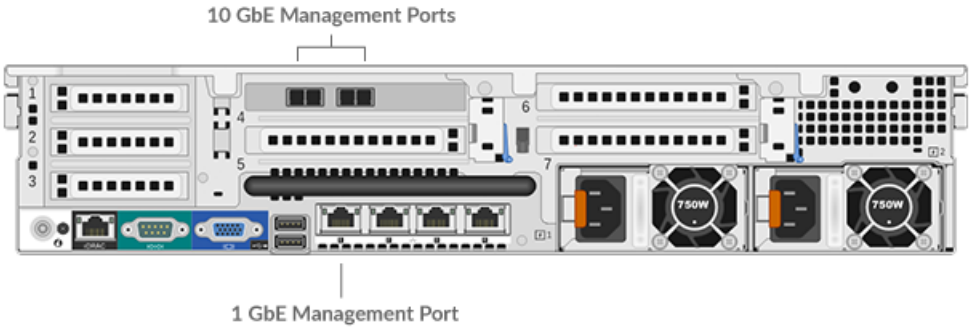
1. Rack mount the Explore appliance.

   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.
2. 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.
3. 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.



4. Connect the power cords.

   Connect the two supplied power cords to the power supplies on the back of the appliance.
5. Plug the power cords into a power outlet. If the appliance does not power on automatically, press the power button on the front of the appliance.

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. Make sure that the default management interface is connected to the network and the link status is active.
2. Press the select button (#) to begin.
3. Press the right arrow (>) button to select **Net** and then press the select button.
4. Press the right arrow button twice to highlight **DHCP** and then press the select button.
5. Press the right arrow button to select **Static** and then press the select button.
6. Press the right arrow button to select **IP** and then press the select button. The currently configured IP address appears.
7. Press the right arrow button until the first digit you want to change is highlighted.
8. Press the select button. The digit blinks when selected. While the digit is blinking, press the left arrow (<) or right arrow (>) button to change the digit value.
9. After you have chosen the correct digit, press the select button.
10. Repeat steps 7-9 for each remaining digit you want to change.
11. Press the left arrow button to navigate to the up arrow ↑ on the display and press the select button.
12. On the Save screen, select **Yes** and then press the select button.
13. Wait a moment to be redirected to the Net screen. Repeat the actions above to set the mask, gateway, and up to two DNS servers.
14. Configure the iDRAC DHCP, IP, mask, gateway, and DNS in the same manner as the IP address.

Configure the Explore appliance

After you configure an IP address for the Explore appliance, log into the Explore Admin UI, `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 Admin UI.

- Register the ExtraHop appliance
- Configure the 10GbE management port
- Configure the system time
- Configure email notifications
- Create an Explore cluster
- Connect 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.

If you do not have a product key, contact your ExtraHop account team.

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 Appliance 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.

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 Appliance 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 **Set time with NTP server** radio button and then click **Select**.
5. Type the IP address or hostname for the time server, and then click **Save**.

   Note: You can configure up to 9 time servers.

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.

Create an Explore cluster

If you are deploying more than one Explore appliance, join the appliances together to create a cluster. For the best performance, data redundancy, and stability, you must configure at least three Explore appliances in an Explore cluster.

In the following example, the Explore appliances have the following IP addresses:

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

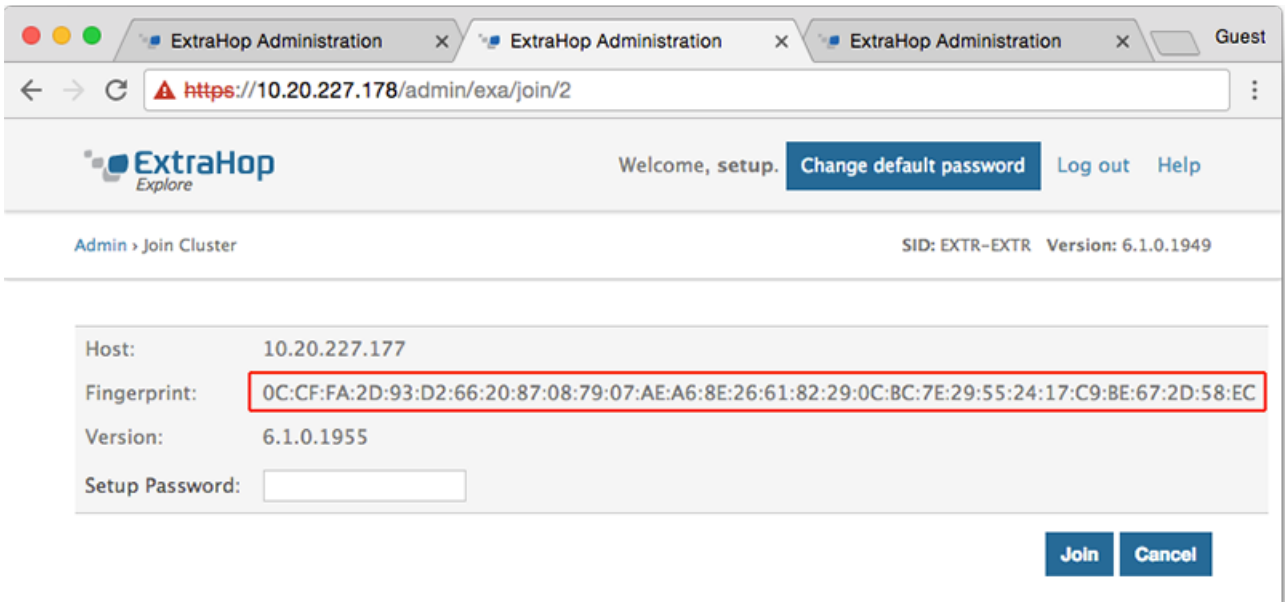
You will join nodes 2 and 3 to node 1 to create the Explore cluster.

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

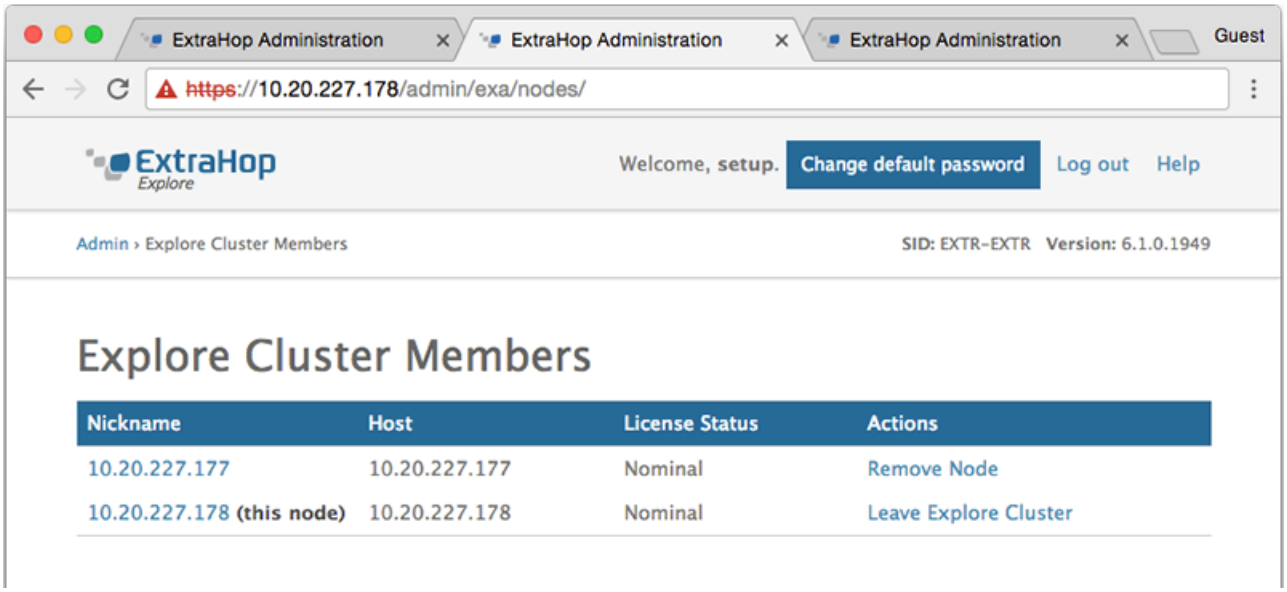
1. Log into the Admin UI of all three Explore appliances with the setup user account in three separate browser windows or tabs.
2. Select the browser window of node 1.
3. In the Status and Diagnostics section, click **Fingerprint** and note the fingerprint value. You will later confirm that the fingerprint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

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

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



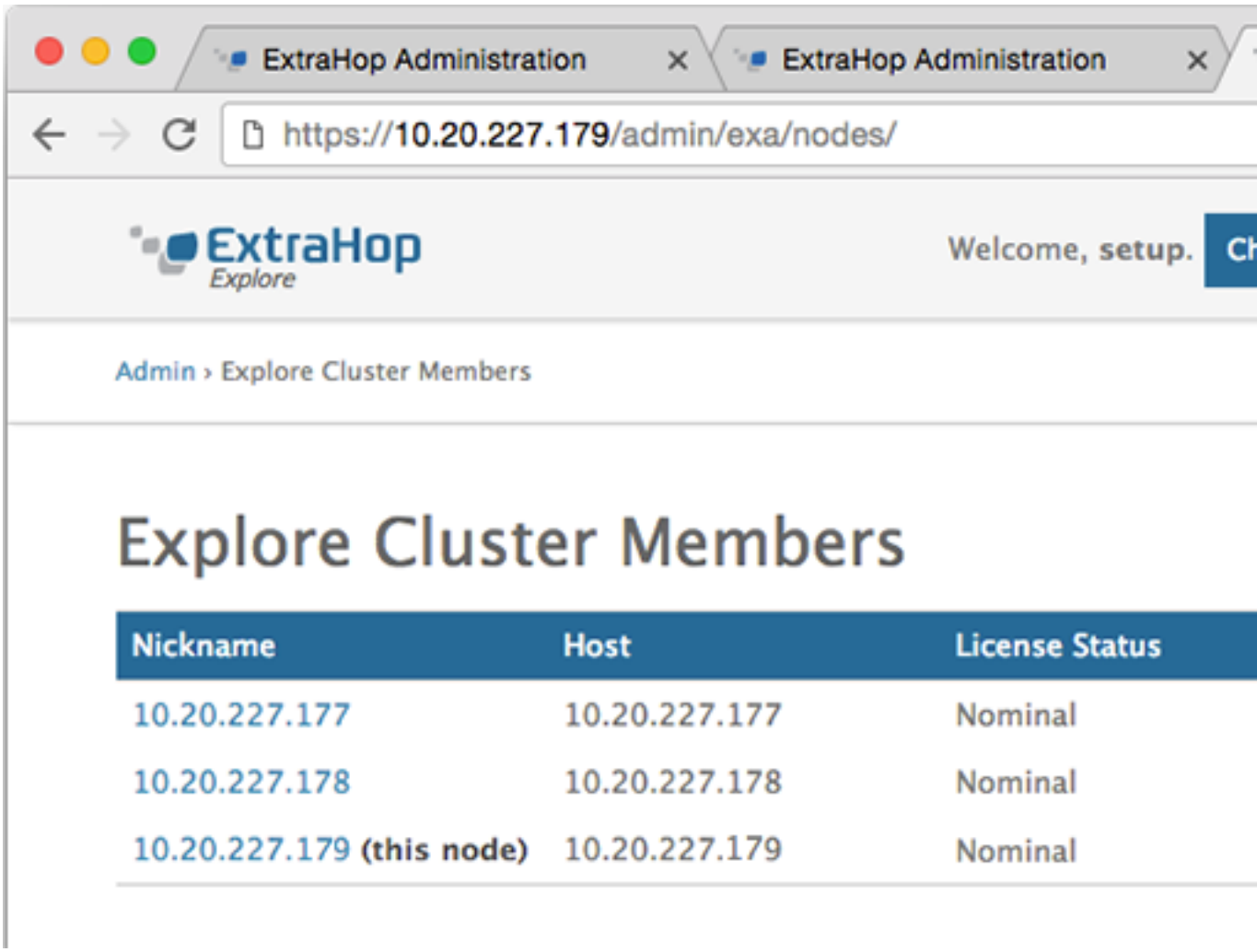
8. In the Setup Password field, type the password for the node 1 `setup` user account and then click **Join**.
   When the join is complete, the Explore Cluster Settings section has two new entries: **Explore Cluster Members** and **Data Management**.
9. Click Explore Cluster Members. You should see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



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

> **Tip:** To avoid creating multiple clusters, always join a new node to the existing cluster and not to another single appliance.

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



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

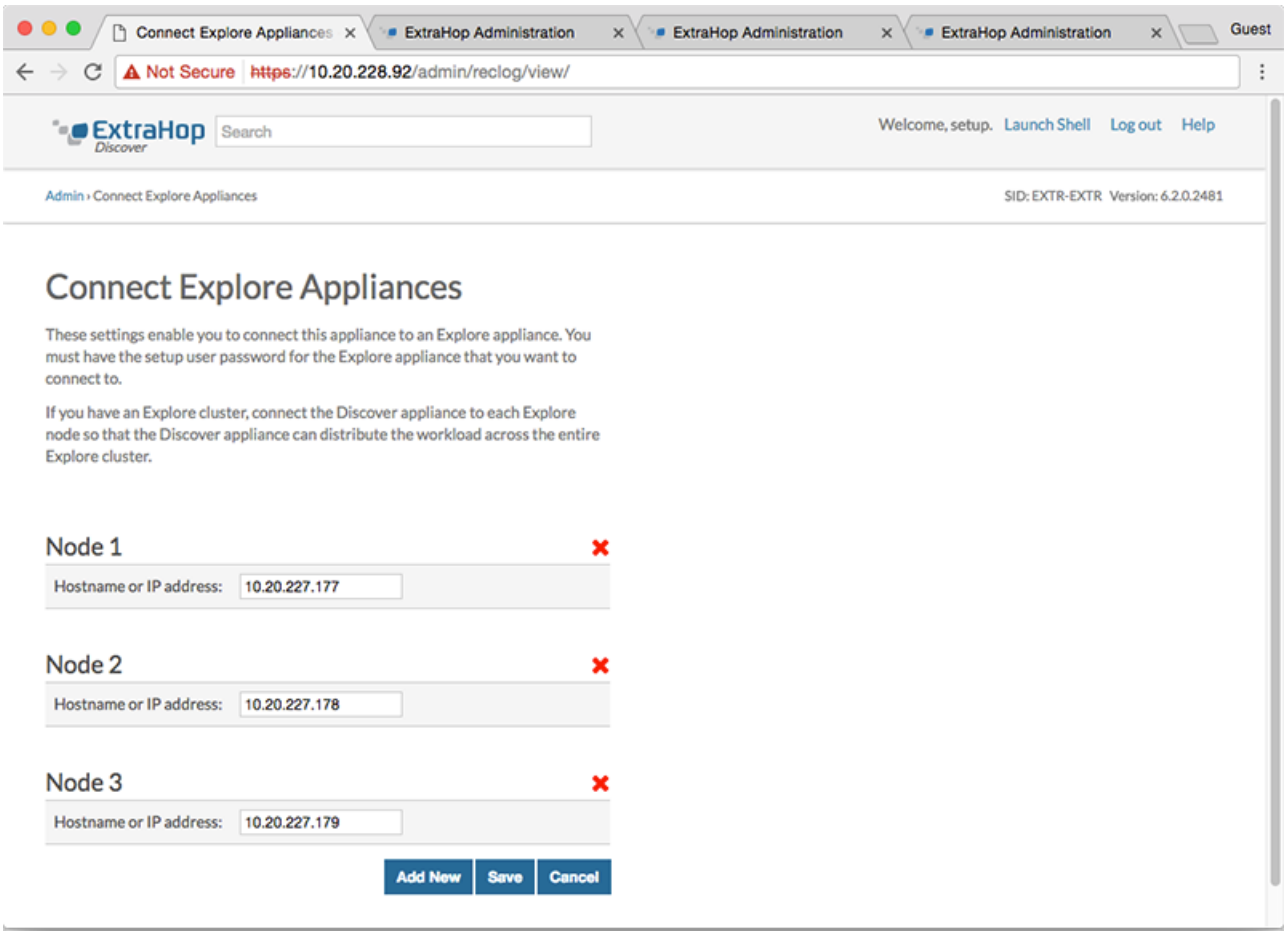
Connect the Explore appliance to Discover and Command appliances

After you deploy the Explore appliance, you must establish a connection from all ExtraHop Discover and Command appliances to the Explore appliance before you can query records.

Important: If you have an Explore cluster of three or more Explore nodes, connect the Discover appliance to each Explore node so that the Discover appliance can distribute the workload across the entire Explore cluster.

Note: If you manage all of your Discover appliances from a Command appliance, you only need to perform this procedure from the Command appliance.

1. Log into the Admin UI of the Discover or Command appliance .
2. In the ExtraHop Explore Settings section, click **Connect Explore Appliances**.
3. Click **Add New**.
4. In the Explore node 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 Explore node field.



6. Click **Save**.
7. Confirm that the fingerprint on this page matches the fingerprint of node 1 of the Explore cluster.
8. In the Explore Setup Password field, type the password for the Explore node 1 `setup` user account and then click **Connect**.
9. When the Explore Cluster settings are saved, click **Done**.

Next steps

Important: If you only deployed a single Explore appliance, after you connect to your Discover or Command appliance, you must log into the Admin UI on the Explore appliance and set the **Explore Cluster Settings** > **Data Management** > **Replication Level** to **0**.

Send record data to the Explore appliance

After your Explore appliance is connected to all of your Discover and Command appliances, you must configure the type of records you want to store.

See Records concepts for more information about Explore configuration settings, how to generate and store records, and how to create record queries.