

Collect flow records

Published: 2017-11-16

You can automatically collect all flow records, which are network-layer communications between two devices over an IP protocol. If you enable this feature, but do not add any IP addresses or port ranges, all detected flow records are captured.

Before you begin

- You must connect your Explore appliances to your Discover appliance before you can collect flow records. See [Connect the Explore appliance to Discover and Command appliances](#).
- You must have [full system privileges](#) to configure automatic flow record collection.

Configuring flow records for automatic collection is fairly straight-forward and can be a good way to test that your appliances are connected.

1. Log into the Admin UI on your Discover appliance.
2. In the ExtraHop Explore Settings section, click **Automatic Flow Records**.
3. Select the **Enabled** checkbox.
4. In the Publish Interval field, type a number between 60 and 21600. This value determines how often records from an active flow are sent to the Explore appliance. The default value is 1800 seconds.
5. In the IP Address field, type a single IP address or IP address range in IPv4, IPv6, or CIDR format. Then, click the green plus (+) icon. (You can remove an entry by clicking the red delete (X) icon.)
6. In the Port Ranges field, type a single port or port range. Then, click the green plus (+) icon.
7. Click **Save**.

Flow records that meet your criteria are now automatically sent to your connected Explore appliance. Wait a few minutes for records to be collected, and then verify that flow records are being collected in the next step.

8. Click **Records** from the top navigation to launch a query. If you do not see any records, wait a few minutes and try again. If no records appear after five minutes, review your configuration or contact [ExtraHop Support](#).