Device Discovery FAQ

Published: 2018-07-17

Here are some answers to frequently asked questions about device discovery.

How does the ExtraHop system discover devices?

The ExtraHop system automatically discovers and classifies devices. First, the ExtraHop system creates an L2 device entry for every locally observed MAC address over the wire. Then, the ExtraHop system creates an L3 device entry for every locally observed IP address included in an Address Resolution Protocol (ARP) response.

Here are some important considerations about L3 device discovery:

- L2 devices that share the same MAC address with an L3 device have a parent-child relationship. This means that an L2 parent device can have one or more L3 child devices.
- To discover L3 devices outside of your network, you can create a custom device or enable remote device discovery.
- If a router has proxy ARP enabled, the ExtraHop system creates an L3 device for each IP address that the router answers ARP requests for.

You can search for L2 and L3 devices in the ExtraHop system by their IP address, MAC address, or name (either a hostname observed from DNS traffic or a custom name that you assign to the device).

For more information, see Device discovery.

What is an L3 device?

An L3 device entry in the ExtraHop system includes an IP address that is observed from local traffic or traffic detected from a router. ExtraHop automatically creates an L3 device entry for every locally observed IP address. For L3 devices that receive Advanced Analysis, L2-L7 protocol metrics are available. The ExtraHop appliance also tracks a single L2 parent device entry for each router MAC address that is associated with the same IP address.

What is an L2 device?

An L2 device entry in the ExtraHop system includes a MAC address only. If the ExtraHop system later observes a local IP address associated with an L2 device's MAC address, the ExtraHop system then creates a child L3 device entry. L2 parent devices that are not gateways or custom devices do not count towards licensed analysis capacity. These L2 devices receive L2 Analysis.

For more information, see Analysis priorities concepts.

Why can't I find a device?

If you cannot find a device in the ExtraHop system, it could be related to one of the following reasons:

- The device is outside of a locally-monitored broadcast domain. You can configure remote discovery in the ExtraHop Admin UI to create devices for a subnet or range of remote IP addresses. For example, if you want to monitor traffic associated with a remote branch office, the ExtraHop system can be configured to discover devices for each IP address at that office. You can also manually create a custom device in the Discover appliance to monitor traffic for a specific IP address.
- The device has not been active since the ExtraHop system was deployed. An active device is one that sends data over the wire to other devices. Devices that only receive traffic are not discovered.
- All traffic for the device is being filtered by IP address or port filters on the ExtraHop system.

What is a custom device?

Custom devices are manually created in the Discover appliance, and can be configured to collect metrics across IP addresses and ports as a single device. You might create a custom device to track individual devices outside of your local broadcast domain or you might create a single custom device to collect metrics for several known IP addresses for a remote site or cloud service. You can add a custom device to the watchlist to guarantee that the custom device receives Advanced Analysis.

For more information, see Remote device discovery and custom devices.

How do I check my device limit and device counts?
In 7.2, the device limit is the same as the Advanced Analysis capacity, which is the number of devices that can receive Advanced Analysis. Additional capacity for Standard Analysis and Discovery Mode is now available.

For more information, see Analysis levels.

What is the watchlist?

The watchlist is a way to prioritize individual devices for Advanced Analysis. For more information, see Add a device to the watchlist and the Analysis Priorities FAQ.

Can I export a list of devices to a CSV file?

Yes. Click **Metrics** at the top of the page and then click **Devices** in the left pane. In the upper right corner of the page, click the command menu ⋮ and then click **CSV**. A CSV file downloads, which contains each device's name, MAC address, IP address, discovery time, and description (if available).

Can I change the role of my device in the ExtraHop system?

Yes, you can update the device role in device properties. The ExtraHop system assigns a device type, or role, to a newly discovered device based on the type of observed wire data traffic associated with the device.

For more information, see Change or add a device role.

Can I change the name of my device in the ExtraHop system?

Yes, you can change the device name in device properties.

For more information, see Change a device name.