

Device Discovery FAQ

Published: 2018-07-07

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

- [How does the ExtraHop system discover devices?](#)
- [What is an L3 device?](#)
- [What is an L2 device?](#)
- [Why can't I find a device?](#)
- [What is a custom device?](#)
- [What is a device limit?](#)
- [What is limited analysis?](#)
- [What is L2 analysis?](#)
- [How do I check my device limit and device counts?](#)
- [What does eligible for licensing mean?](#)
- [What is the whitelist?](#)
- [How do I know which devices are in the whitelist?](#)
- [How do I add devices to the whitelist in batches?](#)
- [Can I change the role of my device in the ExtraHop system?](#)
- [Can I change the name of my device in the ExtraHop system?](#)

How does the ExtraHop system discover 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:

- The IP address for the L3 device is associated with a single MAC address, which has an L2 device entry.
- 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.

After a device is discovered, the ExtraHop system begins to collect metrics for the device. As soon as metrics are available for a device, 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 and to learn about L2 device discovery mode, 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. When an L3 device is in not in [limited analysis](#), L2 - L7 protocol activity is tracked against that L3 device. 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. ExtraHop automatically creates an L2 device entry for every locally observed MAC address, and network throughput activity for that MAC address is tracked against that L2 device. 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 have a parent relationship with any L3 devices having the same MAC address. The L2 parent device entry remains in the ExtraHop system and does not count against licensed [device limits](#). L2 parent devices are also exempt from the [whitelist](#).

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.

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.

For more information, see [Remote device discovery and custom devices](#) [↗](#).

What is a device limit?

A device limit is the total number of devices that can be in full analysis. Full analysis means that the Discover appliance collects complete L2-L7 protocol metrics for that device. If more devices are discovered on your network after the device limit is reached, those devices are placed into limited analysis.

The device limit for your appliance is determined by the license you acquired. The device limit ensures that your ExtraHop appliance operates efficiently when there are too many devices on your network.

What is limited analysis?


Devices that are discovered after the device limit is exceeded can be placed into limited analysis. When a device limit is reached, there are too many devices on your network for the Discover appliance to fully analyze. The ExtraHop system only collects network metrics from L2 and L3 protocols for devices placed into limited analysis.

For more information, see [View the device limit and device counts](#) [↗](#).

What is L2 analysis?

L2 analysis only applies to L2 devices that have a parent relationship with any L3 devices having the same MAC address. The L2 parent device is exempt from the counting against the licensed [device limits](#). The ExtraHop system only collects network metrics from L2 and L3 protocols for devices in L2 analysis.

How do I check my device limit and device counts?

Log into the ExtraHop Web UI and click the System Settings  icon. Then, click **Device Limits**. The device limit for your appliance is listed at the top.

Next to the device limit is the number of active devices that are in limited analysis. This number will be zero if the active device count, or number of active devices discovered on your appliance, is below the device limit. If the number of limited analysis devices is not zero, then the device limit is the same as the number of devices in full analysis.

To see the current device count, or the number of active devices discovered by the ExtraHop system, select Eligible for Licensing in the drop down menu to the left of the Search button and then click **Search**. Note the number displayed at the bottom left of the page.

For more information, see [View the device limit and device counts](#).

What does eligible for licensing mean?

Devices that are actively communicating with other devices on your network are eligible for licensing. Devices that are not active, or have not been discovered by the ExtraHop appliance, are not considered eligible for licensing. However, inactive devices that were discovered in the past can be added to the Eligible for Licensing list again if they become active.

For more information, see [View the device limit and device counts](#).

What is the whitelist?

The whitelist is a way to prioritize devices that you want to make sure receive full analysis in case your device limit is exceeded. Devices that are added to the whitelist are reserved for full analysis when they are actively communicating with other devices. If a device is not on the whitelist, it might be placed into limited analysis.

For more information, see [Add or remove devices from the whitelist](#).

How do I know which devices are in the whitelist?

Log into the Web UI on the Discover appliance and click the **System Settings** icon. Then, click **Device Limits**. Click the number displayed next to “Whitelist” to view each device that has been added to the whitelist.

How do I add devices to the whitelist in batches?

Log into the Web UI on the Discover appliance and click the **System Settings** icon. Then, click **Device Limits**. In the table of devices, select the checkbox next to all of the devices that you want to add to the whitelist. Then, click the **Add to Whitelist** icon in the upper right corner above the table.

For more information, see [Add or remove devices from the whitelist](#).

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](#).