

Device Discovery FAQ

Published: 2017-04-19

This document provides answers to frequently asked questions about how device discovery works in the ExtraHop system.

- [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?](#)
- [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?

The ExtraHop system automatically discovers devices that are active on your local network. There are two device discovery modes: layer 3 (L3) discovery and layer 2 (L2) discovery.

L3 discovery is the default discovery mode. An L3 device entry is created in the ExtraHop system for every locally observed IP address over the wire that meets the following criteria:

- An Address Resolution Protocol (ARP) response for the IP address was detected, allowing the ExtraHop appliance to associate the IP address with an MAC address.
- The associated MAC address of the L3 device entry is not the MAC address of an L3-routing device.

L2 discovery creates an L2 device entry for every locally observed MAC address over the wire. All IP addresses associated with a MAC address are aggregated into a single device entry.

For more information, see [Device discovery](#) in the ExtraHop Web UI Guide.

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. The ExtraHop appliance also tracks a single L2 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 entry based on the device MAC address, and all activity is tracked against that device. If the ExtraHop system later observes a local IP address associated with that L2 device MAC address, the ExtraHop system then creates an L3 device entry. The L2 device entry remains in the ExtraHop system.

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 [Custom devices](#) in the ExtraHop Web UI Guide.

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 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 [Device limits and limited analysis](#) in the ExtraHop Web UI Guide.

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 for your Discover appliance](#) in the ExtraHop Web UI Guide.

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 current device count on your Discover appliance](#) in the ExtraHop Web UI Guide.

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 devices to the whitelist](#) in the ExtraHop Web UI Guide.

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 devices to the whitelist](#) in the ExtraHop Web UI Guide.

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 a device role](#) in the ExtraHop Web UI Guide.

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 the name of a device](#) in the ExtraHop Web UI Guide.