Analysis priorities

Published: 2025-01-29

The ExtraHop system analyzes traffic and collects data from all discovered devices on a single sensor. Each discovered device receives an analysis level that determines what data and metrics are collected for a device. Analysis priorities determine which analysis level a device receives.

Important: Analysis priorities can be centrally managed from a console.

Video Take the related training: Analysis Priorities

Analysis levels

The ExtraHop system intelligently analyzes devices and automatically assigns an analysis level, and you can also configure the analysis level for devices and groups of devices.

Note: Records and packets are available for all devices on ExtraHop systems that are configured with a recordstore or packetstore, regardless of analysis level.

Each device receives one of the following analysis levels.

Discovery Mode

The ExtraHop system identifies known device hardware and software, authenticated users, and assigned and associated IP addresses. The ExtraHop system also generates detections and charts that show protocol activity observed on the device. All devices receive a minimum of this analysis level, except for L2 parent devices.

Standard Analysis

The ExtraHop system includes at least one week of L2-L3 metric and peer relationship data that you can instantly explore through detections, charts, and activity maps. The ExtraHop system also identifies known device hardware and software, authenticated users, and assigned and associated IP addresses. Learn how to prioritize groups for Standard Analysis.

Advanced Analysis

The ExtraHop system includes at least one week of L2-L7 metrics from over 50 protocols and peer relationship data that you can instantly explore through detections, charts, and activity maps, as well as custom dashboards, reports, and alerts. The ExtraHop system also identifies known device hardware and software, authenticated users, and assigned and associated IP addresses. Learn how to prioritize groups for Advanced Analysis or add an individual device to a watchlist.

L2 Parent Analysis

L2 Parent Analysis is only applicable if L3 Discovery is enabled on the ExtraHop system. Except for gateways and routers, L2 parent devices automatically receive this analysis level, which collects L2-L3 protocol metrics and activity maps.

Flow Analysis

A flow sensor collects data from flow logs, instead of packets, for analysis by the ExtraHop system. Devices discovered on flow sensors automatically receive this analysis level. Analysis Priorities system settings are not available for flow sensors, and devices in Flow Analysis cannot be added to the watchlist.

See a table that compares these analysis levels.

Prioritizing devices and groups

You can add most devices to a watchlist to ensure Advanced Analysis or you can add device groups to an ordered list that prioritizes devices for Advanced Analysis and Standard Analysis.

Here are some important considerations about prioritizing devices through the watchlist:

- Devices remain on the watchlist even when they are inactive, but metrics are not collected for inactive devices. Even when inactive, watchlist devices remain part of your Advanced Analysis capacity.
- The number of devices in the watchlist cannot exceed your Advanced Analysis capacity.
- Devices can only be added to the watchlist from a device properties page or the device list page. You cannot add devices to the watchlist from the Analysis Priorities page.
- If you want to add several devices to the watchlist, we recommend that you create a device group and then prioritize that group for Advanced Analysis.
- Devices receiving L2 Parent Analysis or Flow Analysis cannot be added to the watchlist.

Here are some important considerations about prioritizing device groups:

- Order device groups from the highest to lowest priority in the list.
- Click-and-drag groups to change their order in the list.

By default, the ExtraHop system intelligently fills Advanced and Standard Analysis levels to maximum capacity. Here are some important considerations about capacity levels and the automatic fill option:

- Devices prioritized in the watchlist or through a prioritized group fill the higher analysis levels first, and then by the earliest-discovered devices.
- Devices are automatically prioritized for Advanced Analysis by the system if the device is associated with certain detections, if the device has accepted or initiated an external connection, or if the device is running common attack tools.
- Device properties such as the role, hardware and software, protocol activity, and detection history can also determine analysis levels.
- The Automatically Fill option is enabled by default. If disabled, all devices that are not in prioritized groups or in the watchlist are removed and the ExtraHop system sets the priority for each device.
- Your ExtraHop subscription and license determine maximum capacity levels.

See the Analysis Priorities FAQ to learn about analysis level capacities and order of precedence.

Compare analysis levels

Analysis Level	Features	How to Receive this Level
Discovery Mode	• Detections • Observed protocols • IP addresses • Authenticated users • Software • Hardware make and model	Devices automatically receive Discovery Mode if not in Standard, Advanced, or L2 Parent Analysis.
Standard Analysis	• L2-L3 metrics • Activity maps • Detections • Observed protocols • IP addresses • Authenticated users • Software • Hardware make and model	Prioritize device groups for Standard Analysis.
Advanced Analysis	• L2-L7 metrics • Custom metrics • Activity maps	Prioritize device groups for Advanced Analysis or add

Analysis Level	Features	How to Receive this Level
	• Detections • Observed protocols • IP addresses • Authenticated users • Software • Hardware make and model	individual devices to the watchlist.
L2 Parent Analysis (Only applicable if L3 Discovery is enabled)	• L2-L3 metrics • Activity maps	L2 parent devices automatically receive L2 Parent Analysis, except for gateways and routers.
Flow Analysis	• L2-L3 metrics • Activity Maps • Observed protocols • IP Address • Cloud instance properties • Limited detection types	Devices automatically receive Flow Analysis if discovered on a flow sensor.