Analysis priorities concepts

Published: 2018-06-08

The ExtraHop system classifies every device on your network. Device traffic is then analyzed based on priorities that you can configure on your appliance.

By default, the ExtraHop system is designed to provide the highest level of analysis possible for your devices based on your available licensed capacity. You can then target specific device groups, activity groups, or individual devices for higher analysis as needed, based on their importance to your network.

This topic explains the different analysis levels and how analysis priorities work.

Analysis levels

Records, packets, and device properties are always available for every device. Note that you must have an Explore appliance to query for records and a Trace appliance to query for packets. Different analysis levels provide additional information about device traffic.

Advanced Analysis

Charts with L2-L7 metrics, activity maps, and information about protocol activity are available for qualifying devices. Your product license determines how many devices qualify for Advanced Analysis. The maximum capacity can range up to 16,000 devices depending on your platform and license.

Important: Contact your ExtraHop representative for more information about the maximum capacity for different platforms and licenses.

There are three ways to prioritize a critical asset for Advanced Analysis:

- Prioritize a device group or activity group.
- Add the device to the watchlist.
- Automatically fill Advanced Analysis to capacity with the earliest discovered devices.

Standard Analysis

Charts with L2-L3 metrics, activity maps, and information about protocol activity are available for qualifying devices. Your platform determines how many devices qualify for Standard Analysis. The maximum capacity can range up to 100,000 devices depending on your platform and license.

Important: Contact your ExtraHop representative for more information about the maximum capacity for different platforms and licenses.

There are two ways to prioritize devices for Standard Analysis:

- Prioritize a device group or activity group.
- Automatically fill Standard Analysis to capacity with the earliest discovered devices.

Discovery Mode

All devices qualify for Discovery Mode, which classifies each device by protocol activity. Devices in Discovery Mode do not count towards your Advanced and Standard Analysis capacity.

L2 Analysis

Charts with L2-L3 metrics and activity maps are available for qualifying devices, which are L2 devices that are not gateways or custom devices. Devices in L2 Analysis do not count towards your Advanced and Standard Analysis capacity.

See a table that compares the different analysis levels.

Capacity

The number of devices that receive higher analysis levels varies by your ExtraHop platform and license. Your platform determines the total analysis capacity, which is the number of devices that can receive Standard Analysis or Advanced Analysis. Your license then specifies how much of this total capacity is available for Advanced Analysis.

For example, the total analysis capacity for an EDA 9200 is 50,000 concurrently active devices. Up to 8,000 of those active devices can be in Advanced Analysis. Contact your ExtraHop representative for more information about the analysis capacity for each ExtraHop platform.

Note: Device limits have been replaced with Advanced Analysis capacity, and additional analysis capacity is now available. For more information, see Analysis Priorities FAQ.

Analysis priority rules

Analysis priorities enable you to create an ordered list of device groups and activity groups that dynamically receive the analysis level you want. While you can still designate a specific device for Advanced Analysis, prioritizing groups lets the ExtraHop system automatically adjust and manage your devices based on the rules that make sense for your network.

If you have not configured your appliance for analysis priorities, devices will fill the highest analysis level available based on your licensed capacity and device discovery date. Devices first fill Advanced Analysis, then Standard Analysis, and finally Discovery Mode.

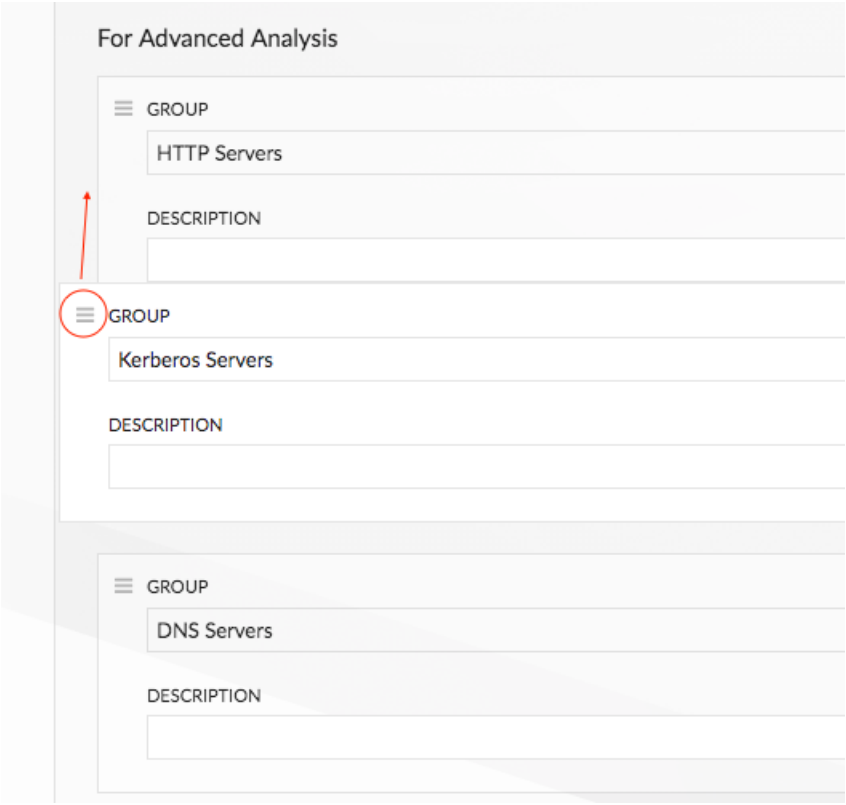
In addition to prioritizing groups, you can add individual devices to a watchlist for Advanced Analysis and you can set an automatically-fill option that elevates devices based on your available capacity.

By default, the analysis priorities for your devices are managed on the Discover appliance that is observing and analyzing your network traffic. If you have multiple Discover appliances and prefer to manage them from a connected Command appliance, you can transfer management to the Command appliance.

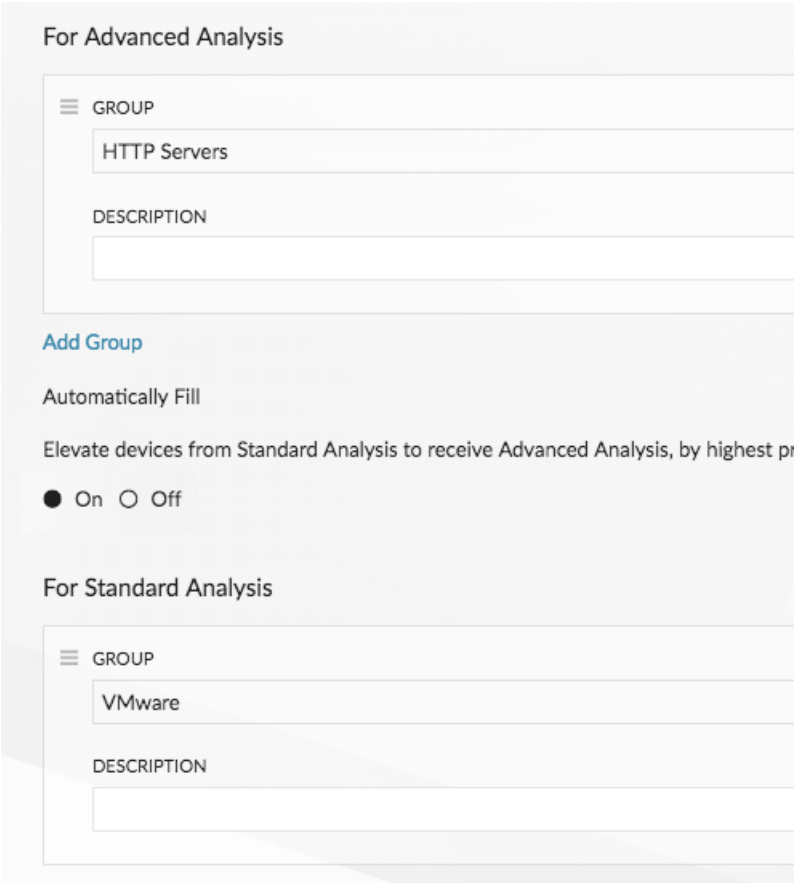
Prioritizing groups

You can prioritize both activity groups and device groups for either Advanced Analysis or Standard Analysis. On the Analysis Priorities page, groups are ranked in an ordered list, so you can let the ExtraHop system know which devices are the most important to you.

- Click-and-drag groups around the list to reorder their priority.



- Groups at the top of the list have the highest priority. For example, devices in the top-most group in the Standard Analysis list can be elevated to Advanced Analysis when there is remaining capacity after devices in groups are prioritized. In the following figure, devices in the VMware group can receive Advanced Analysis if there is capacity after all the active HTTP servers receive Advance Analysis.



- You can prioritize static device groups, dynamic device groups, and activity groups. This means that you can create a device group, based on custom criteria such as a tag or CIDR block, and then prioritize that group for Advanced or Standard Analysis. Or you can prioritize an activity group, such as LDAP Servers, to prioritize any device that actively communicates over a specific protocol.
- After you add all the groups that you want, be sure to click **Save** at the top of the page.

Warning: Large groups can take up a lot of your capacity, so be selective when adding your groups.

Learn how to prioritize a group for Advanced Analysis or Standard Analysis.

Adding devices to the watchlist

If you have a critical asset outside of your device groups and activity groups that you want to prioritize for Advanced Analysis, add that device to the watchlist. Devices on the watchlist are guaranteed Advanced Analysis and are prioritized before any device in a prioritized group.

- The number of devices in the watchlist cannot exceed your Advanced Analysis capacity, which is determined by your product license.
- You can only add devices 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, create a device group and then prioritize that group for Advanced Analysis.

Important: A device stays on the watchlist whether it is inactive or active. The ExtraHop system cannot collect metrics for inactive devices, so add your devices selectively.

Learn how to add a device to the watchlist.

Automatically filling to capacity

By default, both Standard and Advanced Analysis are configured for the option to Automatically Fill. If analysis priorities are configured and there is capacity, the top-most prioritized groups are elevated to the next highest level, and then the earliest-discovered devices are elevated.

Analysis levels fill from the bottom-up, beginning with Discovery Mode and then reaching up to Advanced Analysis. For example, if neither Standard or Advanced Analysis have prioritized groups, but the automatic-fill option for Advanced Analysis is **On** and while the automatic-fill option for Standard Analysis is **Off**, then Advanced Analysis will fill while the rest of the total analysis capacity remains available.

Important: Turning the Automatically Fill option **Off** will remove all devices that are not in prioritized groups or on the watchlist.

Compare analysis levels

Analysis Level	Features	Maximum Capacity	How to Receive this Level
Advanced Analysis	• L2-L7 metrics • Activity maps • Protocol activity • Records • Packets	• Up to 16,000 devices, depending on your platform and license	• Prioritize device groups and activity groups • Add a device to a watchlist
Standard Analysis	• L2-L3 metrics • Activity maps • Protocol activity • Records • Packets	• Up to 100,000 devices, depending on your platform	• Prioritize device groups and activity groups
Discovery Mode	• Protocol activity • Records • Packets	• Unlimited devices • These devices do not count towards analysis capacity	• All devices not in Standard, Advanced, or L2 Analysis receive Discovery Mode
L2 Analysis	• L2-L3 metrics • Activity maps • Records • Packets	• Unlimited devices • These devices do not count towards analysis capacity	• Only L2 devices that are not gateways automatically receive L2 Analysis