Analysis Priorities FAQ

Published: 2020-03-24

Here are some answers to frequently asked questions about analysis priorities.

How is the device capacity determined for analysis levels?

The number of devices that receive higher analysis levels varies by your ExtraHop platform and license.

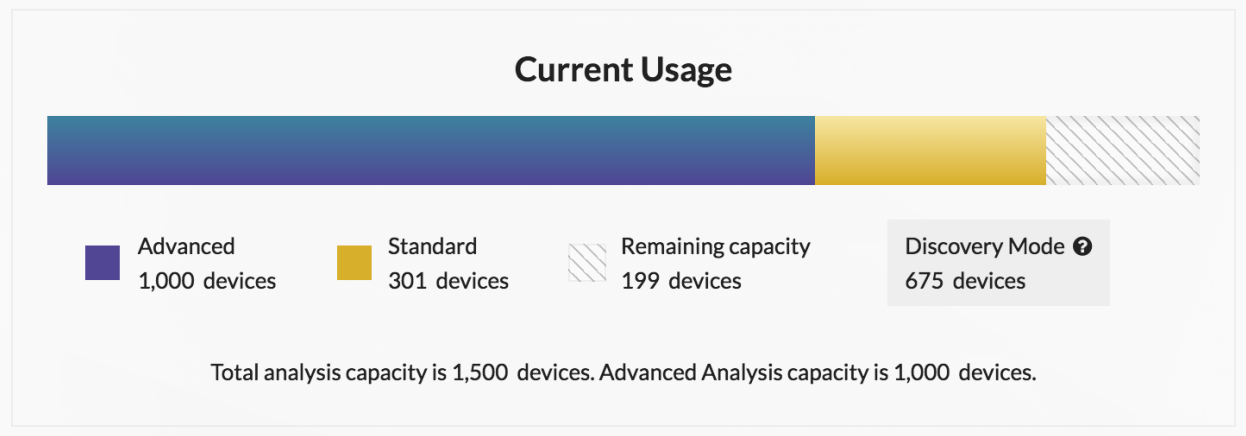
- Your platform determines the total analysis capacity, which is the number of devices that can receive Standard Analysis or Advanced Analysis.
- Your license determines how much of this total capacity is available for Advanced Analysis, which is the highest analysis level.

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.

Where can I find my current usage?

The Analysis Priorities page displays a graph that shows at-a-glance assessment of the number of devices receiving analysis at each level compared to the remaining analysis capacity. Click the System Settings icon and then click **Analysis Priorities**.

The licensed total capacities are displayed below the graph; devices in Discovery Mode do not count against your total capacity.



How do I know which devices are on the watchlist?

Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`, click the System Settings icon and then click **Analysis Priorities**. At the top of the page, click **View the watchlist**.

How do I add multiple devices to the watchlist?

Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`. At the top of the page click **Assets** and then click **Devices** in the left pane. Search for devices on the device list page, and then click the checkbox next to each device that you want to add to the watchlist. Then, click **Add to Watchlist** in the upper right corner of the page.

For more information, see Add a device to the watchlist.

What analysis level do custom devices receive?

Custom devices can receive any analysis level. You can create a device group with all of your custom devices and prioritize that group for Advanced or Standard Analysis. Or you can add an individual custom device to the watchlist.

Which analysis level supports custom metrics?

Custom metrics are only available in Advanced Analysis. If you want to see custom metrics for a specific device, prioritize a group containing the device or add the device to the watchlist.

Which analysis level supports triggers?

A trigger will run for any device that it is assigned to, regardless of analysis level. The analysis level of a device does not affect when the trigger runs. However, if a trigger assigned to a device collects custom metrics, you must prioritize the device for Advanced Analysis before you can view the custom metric data.

Which analysis level supports detections?

Detections are identified for devices in Advanced Analysis.

How do I determine the analysis level for a device?

Find a device and then click on the device name to open the device Overview page. The analysis level is displayed in the device properties section.

From a device list, click the Analysis Level column to sort devices by level.

Extract the device list through the REST API and append an option to filter by analysis level. Full write privileges are required to perform commands through the REST API.

What happens when a prioritized device becomes inactive?

A device can become inactive over time if the device has not sent or received data over the last 30 minutes.

An inactive device that is on the watchlist or is part of a device group does not consume your Advanced or Standard Analysis capacity. When the device becomes active again, it receives Advanced or Standard Analysis based on the configured priority.

If a device is inactive for a specific protocol, and that device is part of a prioritized activity group or a dynamic, activity-defined device group, then the device can remain in Advanced or Standard Analysis for up to 96 hours. For example, an SSL Servers activity group is prioritized for Advanced Analysis. A server that typically receives SSL requests is included in that group. If the server has not sent or received SSL data over the last 30 minutes, but continues to send and receive data over other protocols, then the server remains in Advanced Analysis as part of the SSL Servers activity group. If the server is still inactive over the SSL protocol after 96 hours, then the server is no longer a member of the SSL Servers group, and might stop receiving Advanced Analysis.