Analysis Priorities FAQ

Published: 2018-07-17

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

What is Advanced Analysis?

Advanced Analysis is an analysis level where records, packets, activity maps, and charts with L2-L7 protocol metrics are available for devices. Prioritize groups or add a device to the watchlist to specify which critical assets should receive Advanced Analysis.

For more information, see Analysis priorities concepts.

What is Standard Analysis?

Standard Analysis is an analysis level where records, packets, activity maps, and charts with L2-L3 metrics are available for devices. Prioritize groups to elevate a device or endpoint from Standard Analysis to Advanced Analysis.

For more information, see Analysis priorities concepts.

What is Discovery Mode?

Discovery Mode is an analysis level where records, packets, and information about protocol activity are available for devices. Configure analysis priority rules to elevate a device or endpoint from Discovery Mode to Standard or Advanced Analysis.

For more information, see Analysis priorities concepts.

What is the watchlist?

The watchlist is a way to prioritize individual devices for Advanced Analysis. In 7.2, the whitelist is renamed to the watchlist. For more information, see Add a device to the watchlist.

What happens to device limits and my current device counts when I upgrade to 7.2 or later?

In 7.2, the device limit is the same as the Advanced Analysis capacity, which is the number of devices that can receive Advanced Analysis. However, additional capacity for Standard Analysis and Discovery Mode is now available, which is known as the total analysis capacity. For more information the capacity associated with different analysis levels, see Analysis levels in the Analysis priorities overview.

When you upgrade to 7.2 or later, the following will happen to your existing device counts:

- Devices in Full Analysis will receive Advanced Analysis.
- Devices in Limited Analysis, which means they were discovered after the device limit was reached, receive Standard Analysis and are now available in activity maps. You can also access records, packets, and information about protocol activity for these devices. Prioritize a group for Advanced Analysis or Standard Analysis.
- Additional devices that were discovered after device limit was far exceeded will be in Discovery Mode, which means that records, packets, and information about protocol activity are available for these devices.
- Devices on the whitelist are now available on the watchlist. You can view the watchlist from the Analysis Priorities page.

How do I know which devices are in the watchlist?

Log into the Web UI on the Discover appliance, 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 into the Web UI on the Discover appliance. At the top of the page click **Metrics** and then click **Device** in the left pane. Search for devices on the device list page, and then click the checkboxes next to each device that you want to add to the watchlist. Then, click the **Add to Watchlist** icon ★ 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?

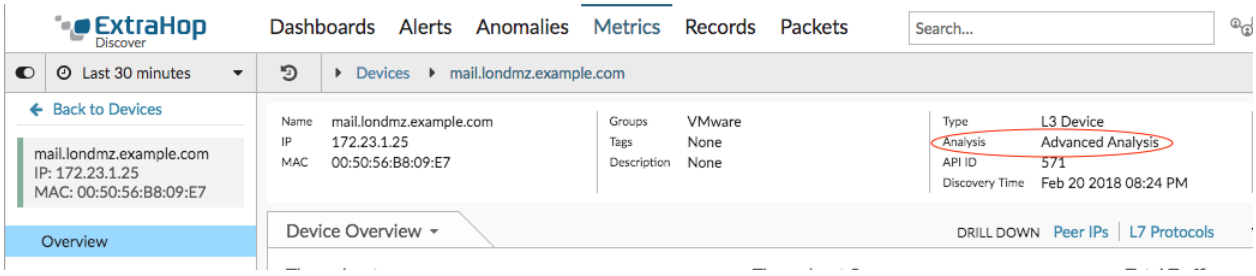
Custom metrics are only available in Advanced Analysis. If you want to see custom metrics for a specific device, prioritize a group containing the device or add the device to the watchlist.

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.

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 listed at the top of the page, as shown in the following figure.

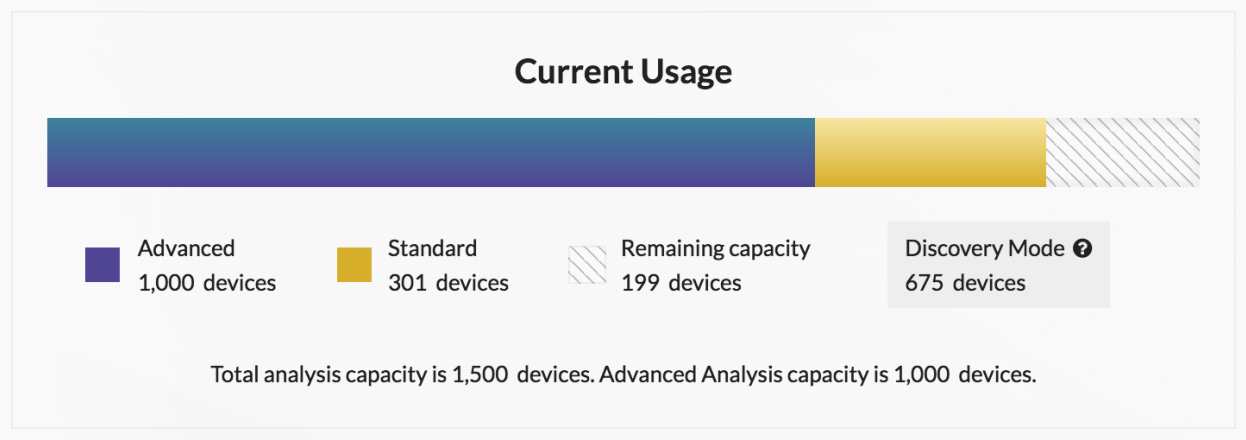


How do I tell if analysis capacity is almost full?

From your Discover appliance, click the System Settings icon and then click **Analysis Priorities**.

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.

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



Do L2 devices receive Advanced Analysis or Standard Analysis?

Gateways, a type of L2 device, can receive Advanced Analysis or Standard Analysis. L2 devices that are not gateways receive L2 Analysis. Records, packets, and charts with L2-L3 metrics are always available for L2 Analysis devices. L2 Analysis devices do not count towards Advanced Analysis or Standard Analysis capacity, which means that these devices are exempt from the watchlist and prioritized groups.

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.