

Prioritize groups for Advanced Analysis


Published: 2018-10-10

The ExtraHop system classifies every device it discovers on your network. Your platform license specifies how much of your total analysis capacity is available for endpoints and critical assets to receive Advanced Analysis. On the Analysis Priorities page, you can target specific device groups or activity groups for Advanced Analysis as needed, based on their importance to your network. Groups are ranked in an ordered list, so you can let the ExtraHop system know which devices are the most important to you.

Here are some important considerations about analysis priorities for [Advanced Analysis](#):

- Devices on the [watchlist](#) are guaranteed Advanced Analysis. If you have devices on the watchlist and prioritized groups, the devices on the watchlist receive Advanced Analysis first.
- Devices within a device group or activity group that are inactive do not affect Advanced Analysis capacity.
- 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.
- You must have full write privileges to edit analysis priorities.

The following steps show you how to prioritize groups with critical assets, such as HTTP servers and DNS servers, for Advanced Analysis:

1. Log into the Web UI of a Discover appliance or Command appliance.
2. Click the System Settings icon  and then click **Analysis Priorities**.
3. If you are managing analysis priorities from a Command appliance, find the Discover appliance with the critical assets you want to prioritize in the Manage Priorities from this Command Appliance section, and then click **Edit Priorities** in the row that contains the Discover appliance.
4. Prioritize groups by completing the following steps:
 - a) In the For Advanced Analysis section, click **adding a group** to add the initial group or **Add Group** to add additional groups.

For Advanced Analysis

Prioritize devices to receive Advanced Analysis by [adding a group](#).

For Advanced Analysis

☰ GROUP ✓ ✕

HTTP Servers ✕

NOTE

[Add Group](#)

- b) In the **Group** drop-down list, type the name of a device group or activity group and then click the group name from the search results. For example, type `HTTP servers` and select the **HTTP Servers** activity group.
 - c) Optional: In the **Note** field, type information about the group such as why this group is a priority for Advanced Analysis.
5. In the Automatically Fill section, make sure **On** is selected.



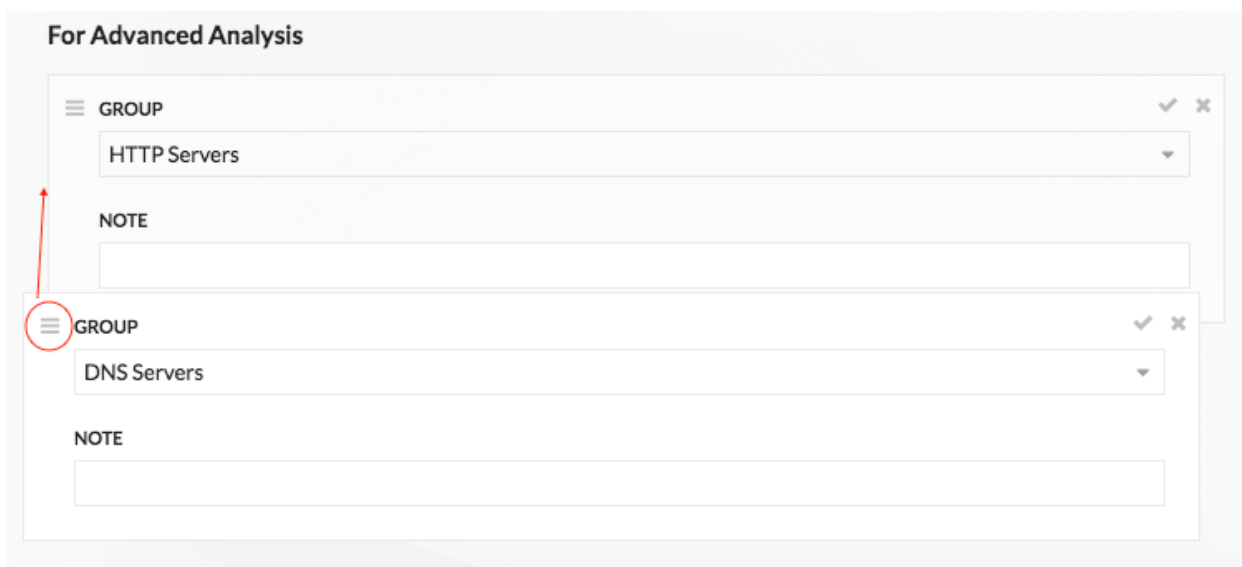
Note: If your appliance is having performance issues, then click **Off**. This selection will remove devices and make sure that only devices in prioritized groups or on the watchlist receive Advanced Analysis.

- 6. At the top of the page, click **Save**.

Next steps

Here are some additional ways to manage and refine groups receiving Advanced Analysis:

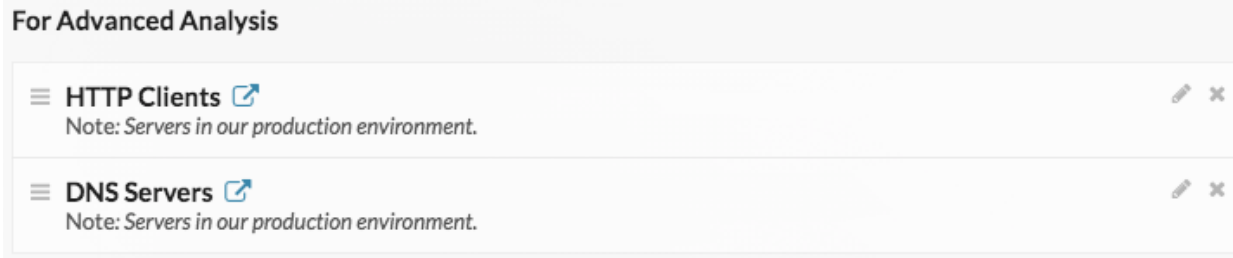
- If you add multiple groups, the groups are prioritized from top to bottom. Click the upper left icon next to Group, and then drag the group to another position in the ordered list.



- Click the check icon to collapse the group. Click the pencil icon to expand the group again, as shown in the following figure.



- Click the go to icon next to a group name to navigate to the device group page. The device group page displays which devices and how many devices are in the group. The icon is only available when the group is



collapsed.

- Click the x icon to remove a group from the list, as shown in the following



figure.