Create a device group based on discovery time

Published: 2018-11-09

The ExtraHop system automatically discovers devices that send and receive traffic over the wire. As new devices appear on your network, you can create a dynamic device group that automatically adds devices based on their device discovery time. You can then prioritize your device group for Advanced Analysis and add your group to dashboard charts, alerts, or triggers.

Tip: You can also add built-in device groups that are based on discovery time. When building charts, configuring alerts, or prioritizing groups, search for the following device group names: New Devices (Last 24 Hours) and New Devices (Last 7 Days).

This procedure shows you how to create a custom dynamic device group with discovery time criteria. To learn more about the different time formats, see Discovery time formats.

1. Log into the Web UI.
2. At the top of the page, click **Metrics**, and then click **Device Groups** in the left pane.
3. In the upper right corner, click **Create Device Group**.
4. In the GROUP NAME field, type a name for the device group.
5. In the GROUP DESCRIPTION field, type any information that can serve as a reference for the discovery time range you specify.
6. Select Dynamic.
7. Below Add devices that match these criteria:, click the first drop-down menu. Scroll down and then click **Discovery time**.
8. In the FROM field, complete one of the following steps:
   - Leave this field empty to specify the first time your appliance received traffic.
   - Enter a fixed date in the Unix Epoch time format or type a value in the relative time format.
9. In the UNTIL field, complete of the following steps:
   - Leave this field empty to specify the present.

     Important: If the FROM field is empty, you cannot leave the UNTIL field empty and must enter a fixed or relative time format.
   - Enter a fixed date in the Unix Epoch time format or type a value in the relative time format.

     Important: The format of the UNTIL field must match the format of the FROM field.
10. Click **Save**.

Next steps

- Create a chart in your dashboard and select your new device group as the source
- Filter activity map connections by group
- Prioritize your device group for Advanced Analysis
- Prioritize your device group for Standard Analysis

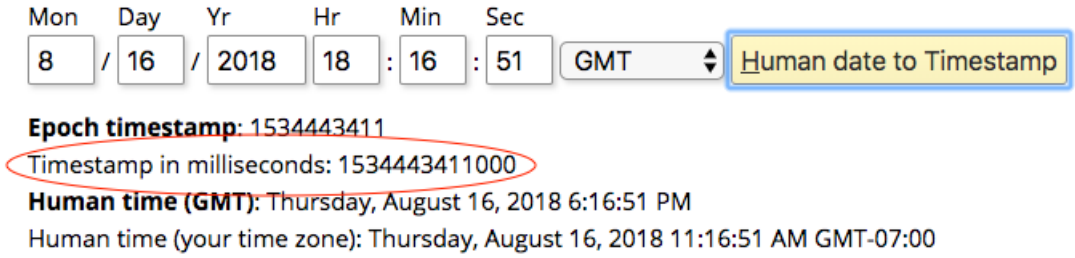
Discovery time formats

When creating a custom device group, the discovery time criteria must be either in Unix Epoch time or a relative time range.

Unix Epoch time

Specific dates must be converted to Unix Epoch time. This conversion helps alleviate discrepancies between time zones and different server times.

You can convert your date into a timestamp with an online tool, such as https://www.epochconverter.com/. After creating the Unix Epoch timestamp, copy and paste the timestamp into the FROM and UNTIL fields for your device group criteria. The timestamp must include milliseconds. For example, to specify August 16, 2018, 6:16:51 PM, enter `1534443411000`, as shown in the following figure.



Example of a valid Unix Epoch time entry

1534238700000

Example of an invalid Unix Epoch time entry

1534238700000ms

Relative time range

To specify a point in time relative to another time point, such as one week ago from now, you must prepend a minus sign to a value and then append one of the following time units: y, M, w, d, h, m, ms. For example, type `-1w` to specify one week ago. You cannot specify a future time range. Relative time ranges must begin with a negative value.

The following table displays supported time units.

Time Unit	Unit Suffix
Year	y
Month	M
Week	w
Day	d
Hour	h
Minute	m
Second	s
Millisecond	ms

Example of a valid relative time entry

-12h

Examples of invalid relative time entry

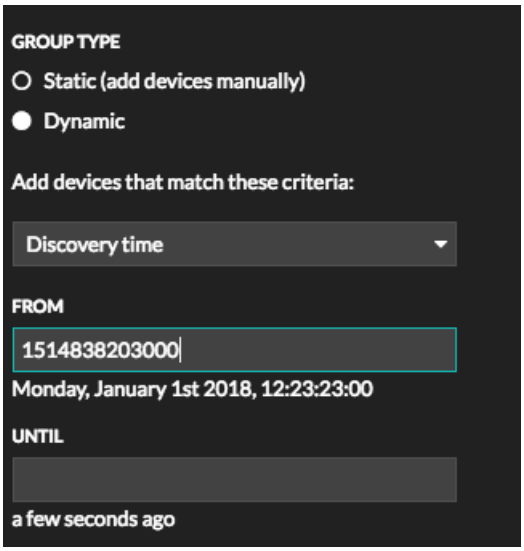
12h

-12H

Discovery time criteria examples

Here are examples of criteria for different discovery time ranges.

From Jan 1, 2018 12:23:23:00 UTC until now



From one month ago until one minute ago