

Create a device group based on discovery time

Published: 2024-04-15

The ExtraHop system automatically discovers devices that send and receive traffic over the wire. In addition to the built-in groups that discover devices added in the last 24 hours and the last 7 days, you can create a custom dynamic device group that automatically adds devices that were discovered during a specific time interval.

To learn about the different time formats, see [Discovery time formats](#).


1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. From the top menu, click **Assets** and then click the **Device Groups** chart.
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. In the Group Type section, click **Dynamic**. The Filter Criteria section appears.
7. Select a match operators from the drop-down list:

| Option | Description |
|------------|---|
| Match All | Filters only devices that match all of the specified filter criteria. |
| Match Any | Filters devices that matches any of the specified filter criteria. |
| Match None | Filters devices that do not match any of the specified filter criteria. |

8. From the categories drop-down list, click **Discovery time**.
9. Select a search operator from the drop-down list:

| Option | Description |
|--------|---|
| = | Filters devices that are an exact match of the discovery time interval. |
| ≠ | Filters devices that do not exactly match the discovery time interval. |

10. In the **From (In Unix time)** field, complete one of the following steps:
 - Leave this field empty to specify the first time your system received traffic.
 - Enter a fixed date in the [Unix Epoch time format](#) or type a value in the [relative time format](#).
11. In the **Until (In Unix time)** 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.

12. 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](#)

Discovery time formats

When creating a custom device group for devices discovered during a specific time interval, 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.

Epoch timestamp: 1534443411

Timestamp in milliseconds: 1534443411000

Human time (GMT): Thursday, August 16, 2018 6:16:51 PM

Human time (your time zone): Thursday, August 16, 2018 11:16:51 AM GMT-07:00

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

The screenshot shows the configuration interface for a device group. Under "Group Type", the "Dynamic (specify filter criteria)" option is selected. The "Filter Criteria" section contains a "MATCH" button, a "Discovery Time" dropdown, an equals sign, and a text input field containing the Unix timestamp "1514838203000". A callout box points to this timestamp with the text "January 1st 2018, 20:23:23.000 UTC". To the right of the input field is a green checkmark icon. Further right is a text input field labeled "Until (In Unix time)..." with a close button (X). A "+ v" button is located below the filter criteria. A "Done" button is at the bottom right.

From one month ago until one minute ago

The screenshot shows the configuration interface for a device group. Under "Group Type", the "Dynamic (specify filter criteria)" option is selected. The "Filter Criteria" section contains a "MATCH" button, a "Discovery Time" dropdown, an equals sign, and two text input fields. The first input field contains "-1M" and has a callout box above it labeled "a month ago" with a green checkmark icon. The second input field contains "-1m" and has a callout box above it labeled "a minute ago" with a green checkmark icon. A "+ v" button is located below the filter criteria. A "Done" button is at the bottom right.