Create a device group

Published: 2024-07-10

You can create device groups that gather metrics for all of the specified devices in a group. With device groups, you can still view metrics for each individual device or group member. Device groups can also be set as a metric source.

Users with limited write privileges ⬈ can create and edit both dynamic and static device groups.

- Create a dynamic device group to automatically add all devices that match specified criteria to the group.
- Create a static device group to manually add each device.

Here are some performance considerations when creating a device group:

- A high number of device groups with a large number of devices will take more time to process.
- Static groups process faster than dynamic groups and are recommended for a set group of devices.
- Dynamic groups with complex criteria might have a higher performance cost.
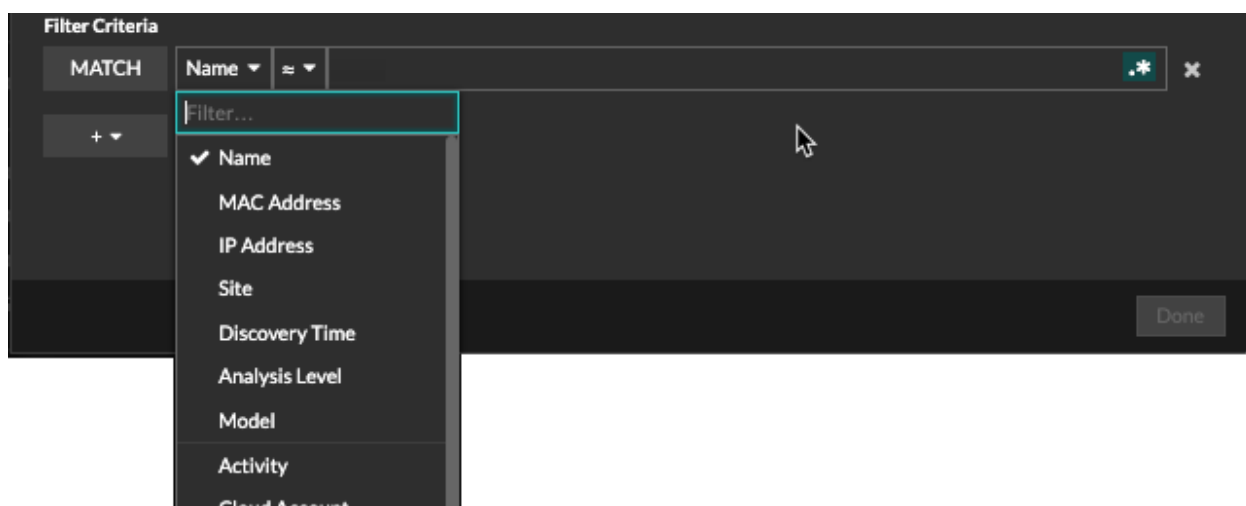
Create a dynamic device group

You can create dynamic device groups with complex filters, which enable you to specify multiple criteria and create nested groups of criteria.

> **Tip:** You can quickly create a dynamic device group from a filtered list of devices on the Devices page. Click **Create Dynamic Group** from the upper right corner.
>
> You can also create a dynamic device group from a built-in device group. From the Assets page, click a role or protocol, update the filter criteria, and then click the Save 🖫 icon from the upper right corner.

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. Click **Create Device Group**.
4. In the **Group Name** field, type a descriptive name to identify the group
5. Optional: From the **Editors** drop-down list, select users with limited write privileges that can edit this device group. This global privilege must be enabled from the Administration settings.

   - The list only displays limited write users with active accounts.
   - Only a user with edit permission for a device group can add other limited write users.

6. Optional: In the **Description** field, add information about this device group.
7. In the Group Type section, click **Dynamic**.
8. In the Filter Criteria section, **Name** and select one of the following categories from the drop-down list:
9. Click **Name** and select one of the following categories from the drop-down list:
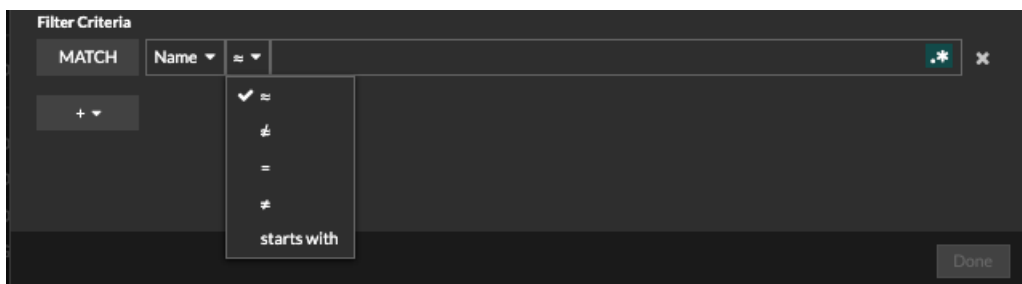
Option	Description
Name	Filters devices by the discovered device name. For example, a discovered device name can include the IP address or hostname.
MAC Address	Filters devices by the device MAC address.
IP Address	Filters devices by IP address in IPv4, IPv6, or CIDR block formats.
Site	Filters devices associated with a connected site. Console only.
Discovery Time	Filters devices automatically discovered by the ExtraHop system within the specified time interval. For more information, see Create a device group based on discovery time ↗.
Analysis Level	Filters devices by analysis level, which determines what data and metrics are collected for a device. You cannot create a dynamic device group for devices filtered by analysis level.
Model	Filters devices by make and model name. The following tips can help you find the device model you want: • Select the exact match operator (=) to view a drop-down list of existing models and model sets. • Select the exact match operator (=) and then select **Custom Models** to filter all devices assigned to a custom model set.
Activity	Filters devices by protocol activity associated with the device. For example, selecting HTTP Server returns devices with HTTP server metrics, and any other device with a device role set to HTTP Server. Also filters devices that accepted or initiated an external connection, which can help you

Option	Description
	determine whether devices are engaged in suspicious activity.
Cloud Account	Filters devices by the cloud service account associated with the device.
Cloud Instance ID	Filters devices by the cloud instance ID associated with the device.
Cloud Instance Type	Filters devices by the cloud instance type associated with the device.
High Value	Filters devices that are considered high value because they provide authentication services, support essential services on your network, or are user-specified as high value.
Currently Active	Filters devices by activity observed on a device in the last 30 minutes.
Network Locality Type	Filters devices by all internal or external network localities.
Network Locality Name	Filters devices by network locality name.
Role	Filters devices by the assigned device role, such as gateway, firewall, load balancer, and DNS Server.
Software	Filters devices by operating system software detected on the device.
Software Type	Filters devices by the type of software observed on the device such as attack simulator, remote access, or database server.
Subnet	Filters devices by the subnet associated with the device.
Tag	Filters devices by user-defined device tags.
Vendor	Filters devices by the device vendor name, as determined by the Organizationally Unique Identifier (OUI) lookup.
Virtual Private Cloud	Filters devices by the VPC associated with the device.
VLAN	Filters devices by the device VLAN tag. VLAN information is extracted from VLAN tags, if the traffic mirroring process preserves them on the mirror port. Only available if the `devices_accross_vlans` setting is set to `False` in the running configuration file.
CDP Name	Filters devices by the CDP name assigned to the device.
Cloud Instance Name	Filters devices by the cloud instance name assigned to the device.

Option	Description
Custom Name	Filters devices by the custom name assigned to the device.
DHCP Name	Filters devices by the DHCP name assigned to the device.
DNS Name	Filters devices by any DNS name assigned to the device.
NetBIOS Name	Filters devices by the NetBIOS name assigned to the device.
Detection Activity	Filters devices with detection activity ⤢ where the device was a participant. Enables additional criteria such as category, risk score, and MITRE technique.

> **Note:** You cannot create a device group that contains this criteria option.

10. Select one of the following operators from the drop-down list; the operators available are based on the selected category:


Option	Description
=	Filters devices that are an exact match of the search field for the selected category.
≠	Filters devices that do not exactly match the search field.
≈	Filters devices that include the value of the search field for the selected category.
≈/	Filters devices that exclude the value of the search field for the selected category.
starts with	Filters devices that start with the value of the search field for the selected category.
exists	Filters devices that have a value for the selected category.
does not exist	Filters devices that do not have a value for the selected category.
match	Filters devices that include the value of the search field for the selected category.
and	Filters devices that match the conditions specified in two or more search fields.

Option	Description
or	Filters devices that match at least one condition specified in two or more search fields.
not	Filters devices that do not match the conditions specified in a search field.

11. In the search field, type the string to be matched, or select a value from the drop-down list. The input type is determined by the selected category.

    For example, if you want to find devices based on Name, type the string to be matched in the search field. If you want to find devices based on Role, select from the drop-down list of roles.

    > **Tip:** Depending on the selected category, you can click the Regex icon in the text field to enable matching by regular expression.
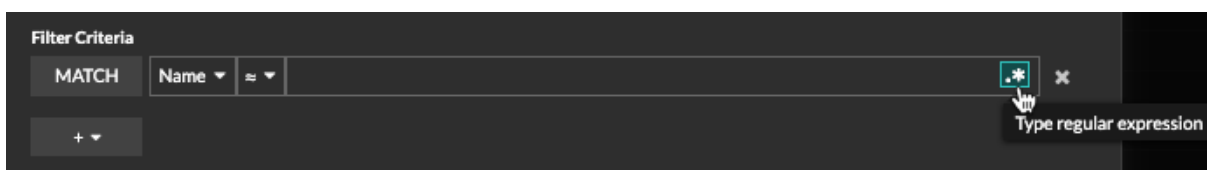
12. Optional: Click the add filter icon [+ ▼] and select **Add Filter** or **Add Filter Group** to specify more criteria at the top or secondary level of the filter.

    For example, if you filter for devices names that start with "acct", you can add a new group of criteria that filters for a certain role or tag within the group of devices that start with "acct".

13. Click **Save**.

You can change the criteria by clicking the group you want to modify from the Device Groups page, and then clicking **Properties**.

Create a static device group

> **Tip:** From the Devices page, you can select the checkbox next to one or more devices and click **Add to Group** to quickly create a static device group or add devices to an existing group.

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. Click **Create Device Group**.
4. In the **Group Name** field, type a name for the new group.
5. Optional: From the **Editors** drop-down list, select users with limited write privileges that can edit this device group. This global privilege must be enabled from the Administration settings.
   - The list only displays limited write users with active accounts.
   - Only a user with edit permission for a device group can add other limited write users.
6. Optional: In the **Description** field, add information about this device group.
7. In the Group Type section, select **Static**.
8. Click **Save**.
   Your device group is now created.
9. Add a specific device to your group.
   a) Click the static device group you want and click **Devices** from the left pane.
   b) Click the Find device… field top of the device table, type the name of the device you want, and then select the device from the list.
   c) Click **Add to Group**.

10. Add devices with specified criteria to your group.

    a)   Click **Devices** in the left pane.

    b)   Find a device ⬀ and then select the checkbox next to the devices you want to add to your group.

    c)   At the top of the device table, click **Add to Group**.

    d)   From the Add to Group dialog box, select **Add to an existing group**.

    e)   Select a device group from the Group drop-down list.

    f)   Click **Add to Group**.

Next steps

Remove devices from a group by selecting the checkbox next to the device name and clicking **Remove from Group** in the upper right corner.