

Create a device group

Published: 2024-04-02

You can create both dynamic and static device groups. Dynamic groups automatically add all devices that match specified criteria to the group, while static groups require you to manually add each device.

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.

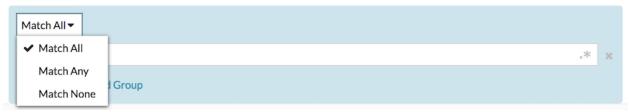


Tip: You can quickly create a dynamic device group from a filtered list of devices on the Devices page. Click **Create Dynamic Group** from the upper right corner.

You can also create a dynamic device group from a built-in device group. From the Devices 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 **Device Groups** in the left pane.
- 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, click **Match All** and then select one of the following match operators from the drop-down list:

FILTER CRITERIA

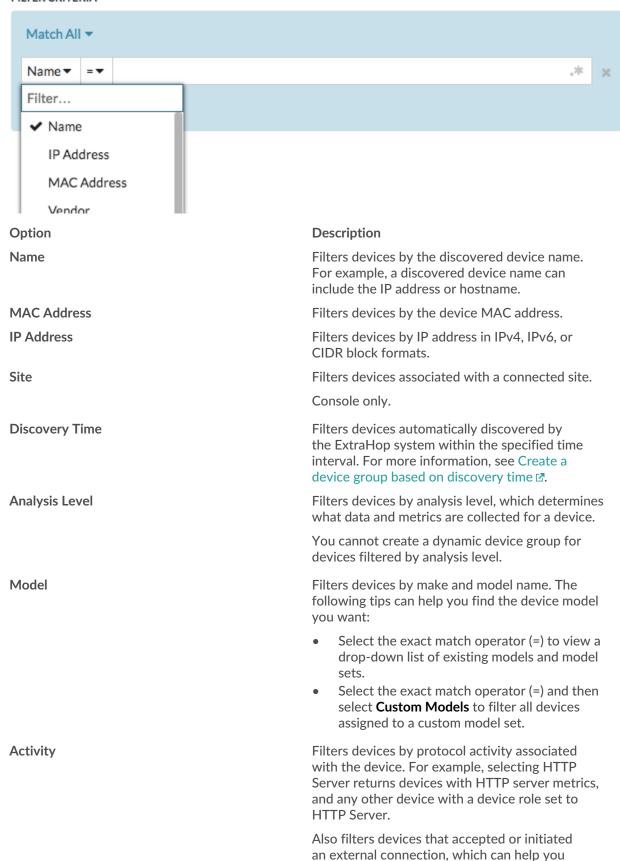


Option	Description
Match All	Filters only devices that match all of the specified criteria.
Match Any	Filters devices that matches any of the specified criteria.
Match None	Filters devices that do not match any of the specified criteria.

9. Click **Name** and select one of the following categories from the drop-down list:



FILTER CRITERIA





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.

Filters devices by all internal or external network **Network Locality Type**

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.

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.

Custom Name Filters devices by the custom name assigned to

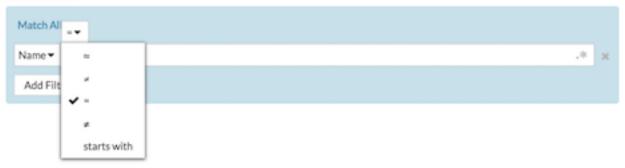
the device.



Option	Description
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.

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

FILTER CRITERIA



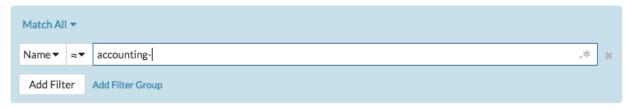
Option	Description
=	Filters devices that are an exact match of the search field for the selected category.
≠	Filters devices that do not exactly match the search field.
≈	Filters devices that include the value of the search field for the selected category.
≈/	Filters devices that exclude the value of 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.

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.

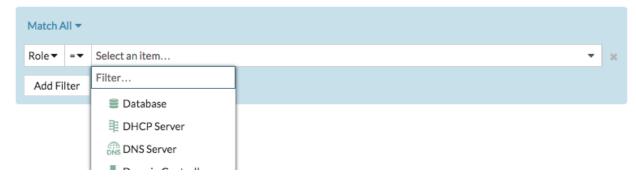
For example, if you want to find devices based on Name, type the string to be matched in the search field. If you want to find devices based on Role, select from the drop-down list of roles.



FILTER CRITERIA



FILTER CRITERIA



Tip: Depending on the selected category, you can click the Regex icon in the text field to enable matching by regular expression.

FILTER CRITERIA



- 12. Optional: Click **Add Filter** to add more filter criteria.
- 13. Optional: Click Add Filter Group to add filter criteria to the results of the original 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".
- 14. 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

- Log in to the ExtraHop system through https://<extrahop-hostname-or-IP-address>.
- 2. Click **Assets** and then click **Device Groups**.
- 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 devices to your group.
 - a) Click **Devices** in the left pane.
 - b) Find a device I 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 **Assign to Group**.
 - d) Select a device group from the Group drop-down list.
 - e) 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.