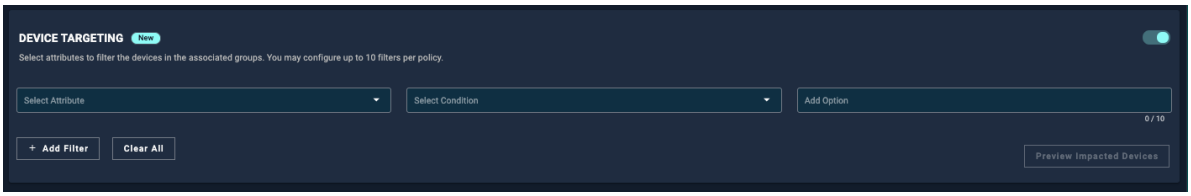
Device Targeting with Filters

Device targeting allows you to execute policies on a filtered collection of devices. All policy types and worklets can be configured to use device filtering.

Creating a Device Filter on a Policy

You can apply filters on new and existing policies or worklets to target devices. It is possible to add up to 10 filters per policy and 10 values per attribute. For details about creating a policy or worklet, see Managing Policies.



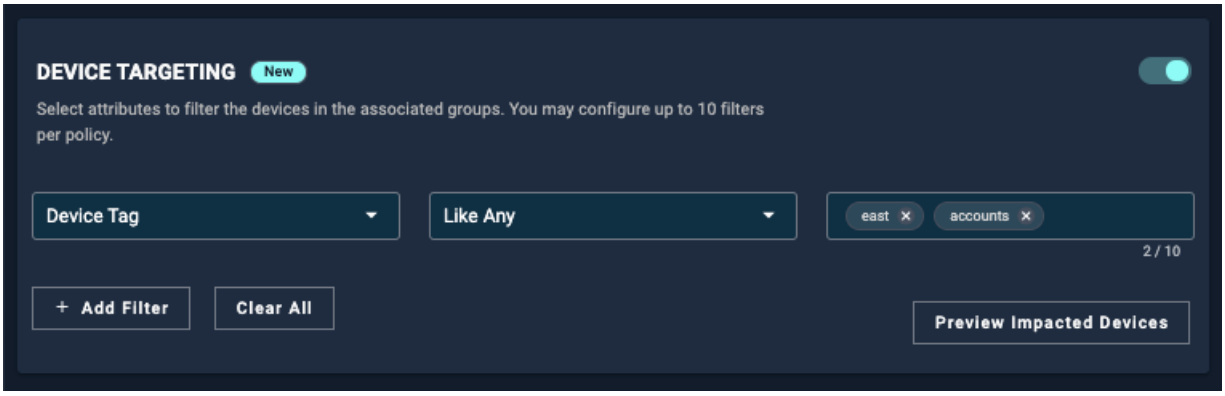
1. From the Create or Edit Policy page, use the toggle to turn on **Device Targeting.**
2. From the **Select Attribute** drop-down menu, select the filter you want to use. You can filter by:
    - Device Tag
    - IP Address
    - Hostname
    - OS
    - OS Version
    - Active Directory Organizational Unit (Windows only)
3. Select from the options available in the **Select Condition** field. The options available depend on the filter selected.
4. Use the **Select Option** menu to enter the options related to the filter. You can select a maximum of 10 options.
5. Click **Preview Impacted Devices** to retrieve a list of all devices that will be included in the policy.
6. If you are creating a new policy or worklet, you must set a schedule and configure user notifications. Click **Create Policy.**
7. If you are editing a policy or worklet, click **Save Policy**.

Filters and their values

You can create up to 10 filters and apply up to 10 options per filter. Each filter row uses an "And" operation. These narrow down the results to fit all filters. The values set within the Options field use an "Or" operation.

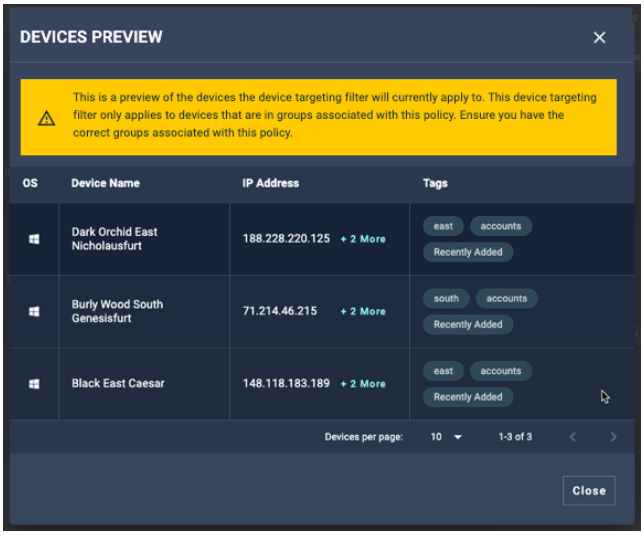
Example 1:

A single filter (row) with multiple values will target any device with option 1 or option 2, or both.



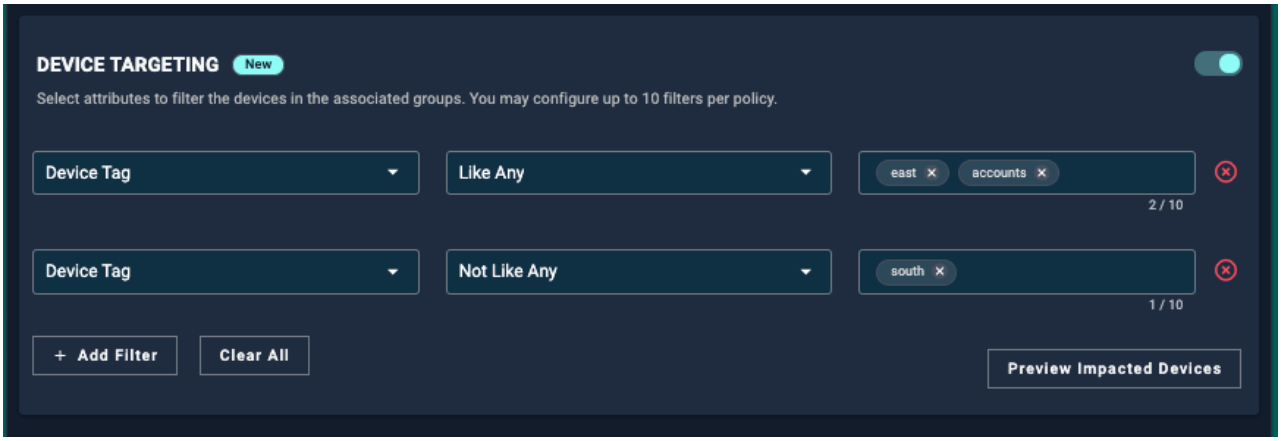
The impacted devices include at least one of the options. Therefore, in this example, the tags "east" and "accounts" include other values and all devices with these tags are impacted.

> **Devices Preview:** This is a preview of the devices the device targeting filter will currently apply to. This device targeting filter only applies to devices that are in groups associated with this policy. Ensure you have the correct groups associated with this policy.

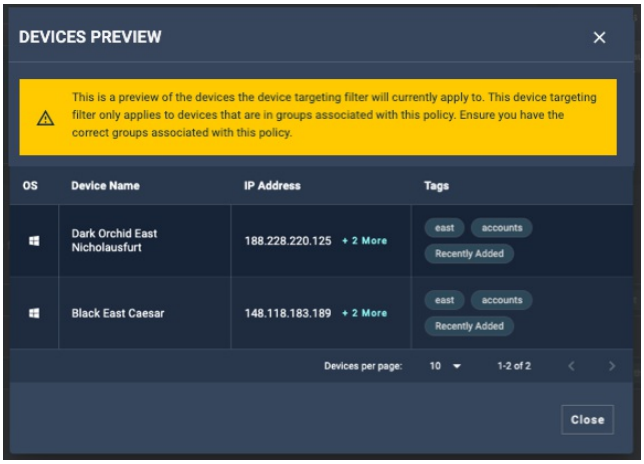


Example 2:

Separate filters (rows) are an "And" condition. In this example, both "east" and "accounts" are valid, however, "south" is not included.



The impacted devices now reflect the conditions required for all filters.

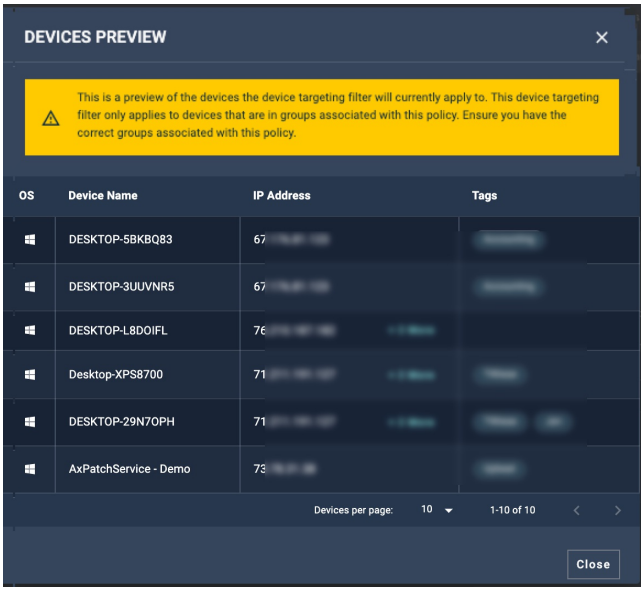


Other filter examples

- Hostname
- IP Addresses
- Active Directory Organizational Unit

Hostname: Use the Hostname to target devices. You can use partial name searches to gather the list of devices that you want to apply a policy to.

The result of this will show all devices that have a Hostname with the value "desktop":



IP Address
Apply "partial" searches to other filter options, for example, you can target IP Addresses within a subnet.

Device Targeting Based on OU Information

You can use the device targeting filter **Active Directory Organizational Unit (AD OU)** to run policies based on Organizational Units. This allows you to filter devices based on your AD structure.

The AD OU information is collected when a device is scanned. Therefore, the policy automatically applies to newly added devices.

The AD OU filter allows you to match a string or strings. Example:

```
/Locations/Sheriff/Computers/CAD Stations/Computers
```

You can target a higher-level OU by using a partial match on the path.

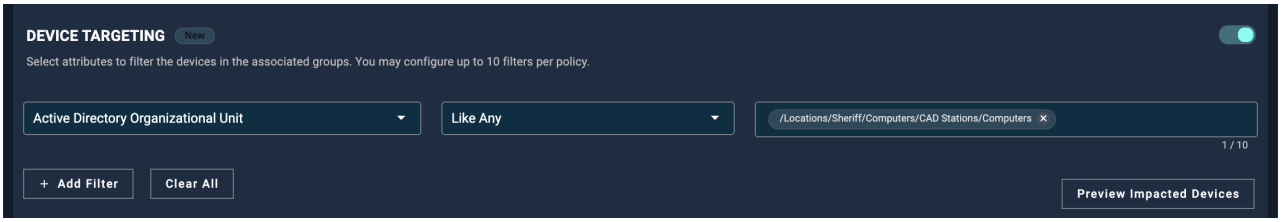
Note:

- The Active Directory OU filter is available only for Windows devices
- The maximum string length is 2048 characters
- You can copy/paste the path structure into the Option field
- This feature requires no direct Active Directory Domain Controller access as we're pulling the AD OU information directly from each device.
- Azure AD OU information requires a hybrid AD and Azure AD setup

Creating an Active Directory Organizational Unit Device Filter

Follow these steps to set up device filtering based on Organizational Units (OU).

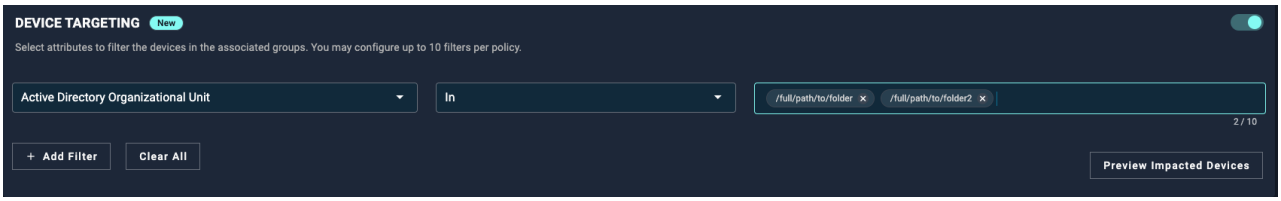
Note: Automox queries Active Directory OU information every time a device is scanned (when adding a device or at least every 24 hours - depending on your scan interval).



1. From the Create or Edit Policy page, use the toggle to turn on **Device Targeting** and activate the feature toggle.
2. From the Select Attribute field, click **Active Directory Organizational Unit**.
3. Use the Select Condition field to select from the following operators: Like Any, Not Like Any, In, Not In.
4. In the **Add Option** field, enter or paste one or more path structures.
5. Click **Preview Impacted Devices** to review the devices affected by the policy.
6. Click **Create Policy** or **Save Policy**. The policy will run according to the schedule.

Targeting specific OUs

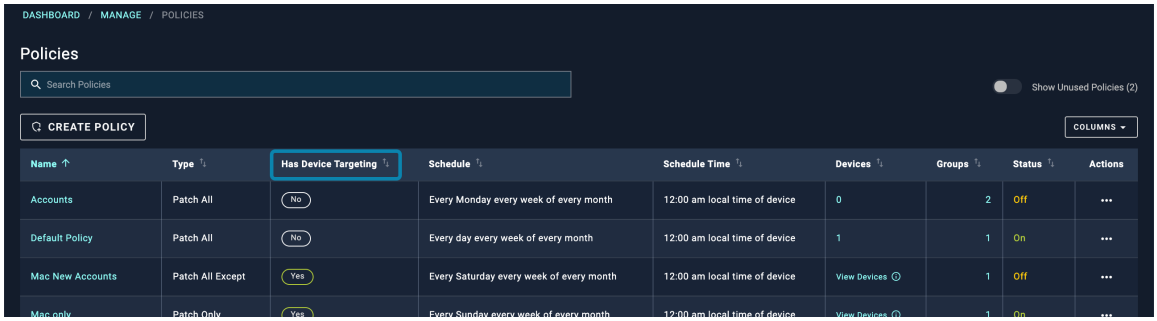
To target a specific OU, use the **In** condition. This filter requires full paths to the OU. Any sub-OUs are not included.



Viewing and Searching for Policies with Device Targeting

You can see if the device filter is configured for the policy from the **Policies** page.

- Use the search field to find the new or updated policy to ensure that device targeting filters are switched on.
- You can also sort the list of policies by the **Has Device Targeting** column.



Deleting a Device Filter

To delete an existing device filter in a policy or worklet, go to Device Targeting on the Edit page.

1. Click the delete  button to remove the device filter.
2. Click **Save Policy**.

Related Topics:

- API Reference Guide: Device Filters Preview - Filter Parameters
- Learn about Flexible Device Targeting