

Policies

<https://campus.barracuda.com/doc/110559943/>

Policies help control the way files are handled by Barracuda Data Inspector.

To view existing policies, use the menu at top-left and navigate to **Settings > Policies**.

A policy determines what action will be taken given a configured set of conditions. Policies can be applied to files belonging to certain groups or users when built-in or [custom classifiers](#) are matched by file data.

Exemptions can also be made, so a policy will not apply for selected groups or users.

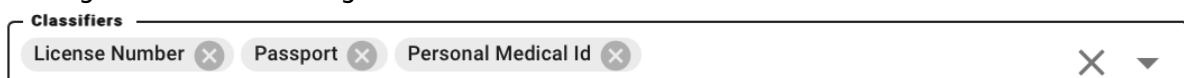
Policies are applied in order starting with the highest ranked policy (**1**). See the priority column on the left side of the policy table. This [order can be changed](#). Once a policy action is enacted, no other policies will be tested against that file. (The one exception to this rule is if the policy Action is *Ignore classifier*. See the [Create a New Policy > Action](#) section below.)

There will always be at least one policy, the **Default** policy. This policy is always enabled and while it can be edited, the name cannot be changed.

Create a New Policy

To create a new policy, click the **Create Policy** button at top-right. In the new policy flyout, configure the following:


- **Policy name** – Name of the new policy.
- **Description** – Optional. A description can be useful when reviewing policies at a future date.
- **Condition** – Add classifier, identity and authorship markers. Each one selected shows as a "chip" in that condition field. Add as many as you like by checking the boxes in the dropdown lists. Remove individual chips by clicking on the **X** next to it or remove all chips in a field by clicking the **X** on the far right side of the field.

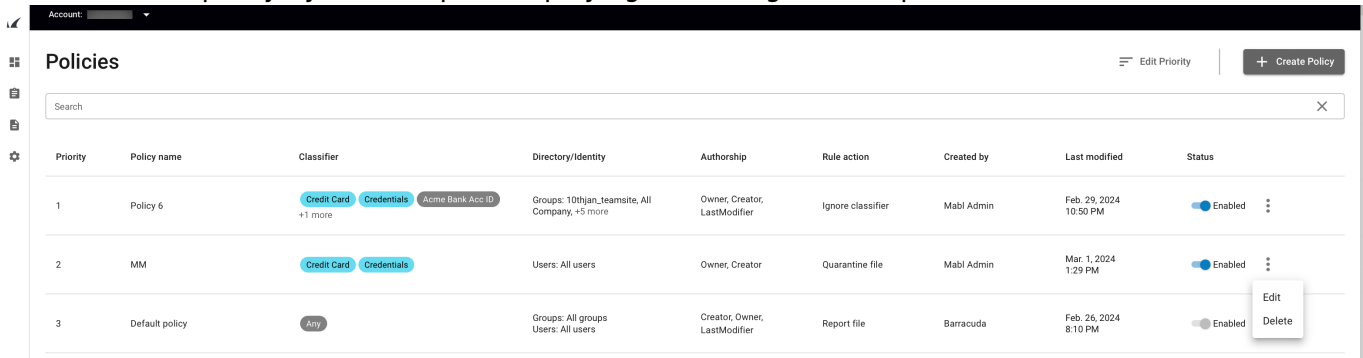





- **If Classifier is** – In the dropdown list, select as many classifiers as you want to be considered. Classifier groups are:
 - **Content classifiers** – The policy will apply to files with content matching these classifiers.
 - Choose from Credit Card, Credentials, Passport, License Number, Personal ID, Personal Medical ID, Tax ID, Suspicious, Malicious, or Financial ID.

- Example: a policy with the Credit Card classifier searches for file content that matches one of the many standard credit card number formats.
- Sharing classifiers – The policy will apply to files with these permissions.
 - Choose from Public Readable, Public Writable, External Readable, or External Writable.
 - External – Available to any user outside of your organization.
 - Public – There are no restrictions regarding who can access the file.
 - Example: Public Readable means a link to the file can be shared with anyone, and that person can read the file contents (but not make edits).
- Custom classifiers – These are the classifiers created by you or people in your organization. You can see and edit them [here](#).
- You can also choose **Any** (at top of list), which includes all classifiers.
- **And Identity is** – Select the groups and/or users the policy can apply to (assuming Authorship and Classifier are also matches.)
 - Example: Classifier = Credit Card, Identity = Group A, Authorship (below) = Owner, Action (below) = Ignore classifier. In this scenario, a file containing *credit card* information *owned* (authorship) by a user in *group A* (identity) is a match for this policy. Therefore, the file classifier will be *Ignored* (action).
- **Except** – Optional. Select the group or user to which the policy will *not* apply.
 - Example: See the scenario for the **And Identity is** example above. Group A = Julie, Dave, and Gina. Except = *Users* Julie. The policy will apply to anyone in Group A except Julie. If Julie owns the file in question, the policy will not be applied.
- **And Authorship of file is** – The **Identity** selected above must have the authorship selected here for the policy to be applied. You can select more than one option.
 - Choose from Owner, Creator, or Last Modifier.
 - Continuing with the example used above (Classifier = Credit Card, Identity = Group A, Group A = Julie, Dave, and Gina, Authorship = Owner, Action = Ignore classifier). A file containing credit card data is created by Dave, *but he is not the file owner* and no other person in Group A owns the file. The policy (Ignoring the configured classifiers) will not be applied because it does not match the Authorship condition. The file can then be acted upon by other policies (possibly Quarantine file, Delete file, etc.)
- **Action** – This is the action to be taken by Data Inspector if a file meets the above conditions. Options are:
 - **Ignore classifier** – No action will be taken by this policy, but the file will continue to be checked against other policies.
 - **Report file** – File will be shown on the [Detections > Unresolved](#) tab.
 - **Quarantine file** – File will be moved to the DI_QUARANTINE folder, which exists at the root level of your company file tree. This folder is created the first time a file is moved to Quarantine.
 - **UnShare file** – Files will have their sharing permissions and links removed and will be restricted to Private. Only the file owners will then have access.
 - **Delete file** – Files will be deleted from the user's drive and moved to the Recycle Bin.

Edit a Policy

To make changes to an existing policy, click the three dots  on the right side of that policy row. Then click **Edit**. The policy flyout will open, displaying the configuration options.



Priority	Policy name	Classifier	Directory/Identity	Authorship	Rule action	Created by	Last modified	Status
1	Policy 6	Credit Card Credentials Acme Bank Acc ID +1 more	Groups: 10thJan_Teamsite, All Company, +5 more	Owner, Creator, LastModifier	Ignore classifier	Mabl Admin	Feb. 29, 2024 10:50 PM	Enabled 
2	MM	Credit Card Credentials	Users: All users	Owner, Creator	Quarantine file	Mabl Admin	Mar. 1, 2024 1:29 PM	Enabled 
3	Default policy	Any	Groups: All groups Users: All users	Creator, Owner, LastModifier	Report file	Barracuda	Feb. 26, 2024 8:10 PM	Enabled 

See the above section for details about each field. Once you have made all changes, click the **Save** button.


The only field that cannot be changed is the **Name** field of the *Default* policy.

Change the Order that Policies are Implemented

Policies are applied in order starting with the highest ranked policy, which is policy **1**. The priority column on the left side of the Policies table shows the order.

To change the order, click **Edit Priority**. Then select a policy and drag it up or down to fit your desired order. Once you have all policies in place, click the **Save** button at top-right.

Other Policy Page Actions

Delete – To delete a policy, click the three dots  on the right side of that policy's row. Then click **Delete**.

Search – Enter all or part of a policy's name in the **Search** field. All policies with names containing the text you entered will be displayed.

Figures

1. classifier-chips.png
2. three-dot.png
3. policy-page2.png
4. three-dot.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.