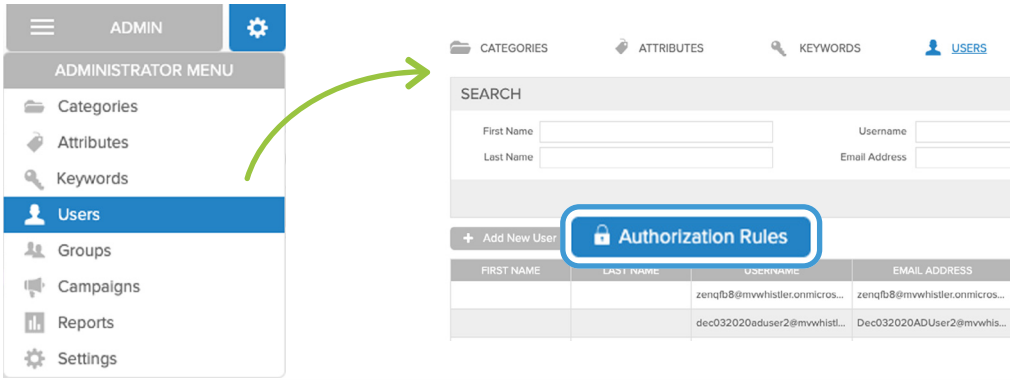
How to Use the MediaValet SSO Authorization Rules Engine

SAML 2.0 AND OPENID IDENTITY PROVIDERS

ACCESSING THE RULES ENGINE

To access the rules engine, navigate to the user management page and click on the **Authorization Rules** button.

If you don't see that button on the user management page, please check that you're logged in using an account that has Administrator permissions.

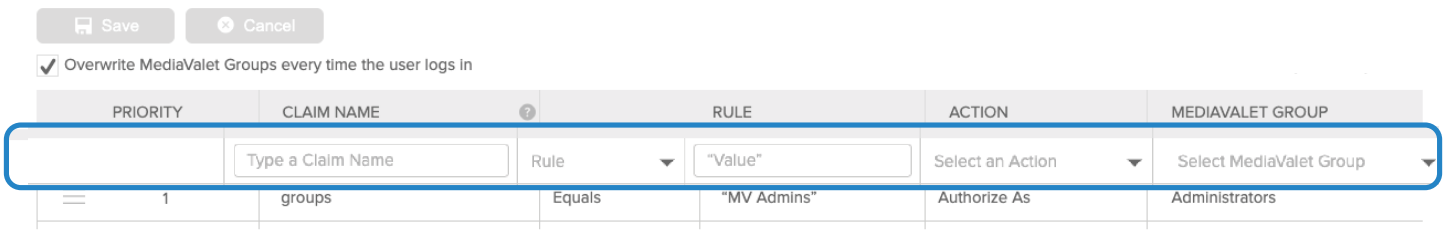


NOTE

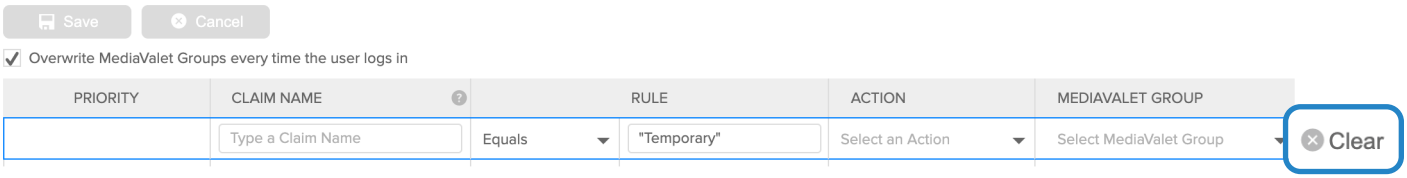
This button will not be displayed unless SSO has been set up for your organization.

CREATING NEW RULES

1. To create a new rule, complete the first row in the table, underneath the header AUTHORIZATION RULES



2. Once the row is complete, click **Add** and the rule will be created as Row 1



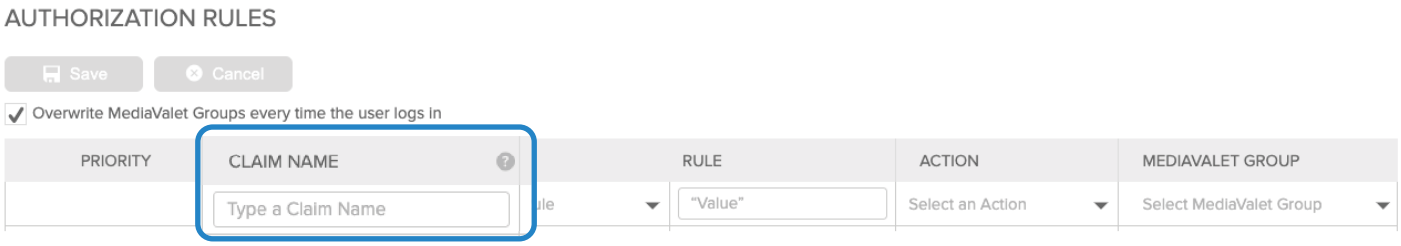
3. The contents of a row can also be removed by clicking **Clear** before the row is added
4. Each authorization rule is comprised of a **condition** and an **outcome**

Authorization Rule: Condition

Claim Name

Claims are pairs of attribute names and values that contain information about a user, as well as meta-information about the identity provider.

e.g. *name/attribute* = email *value* = jon.smith@company.com



The authorization rules engine can only reference claims that were mapped during SSO setup.

Rule

There are two parts to the Rule section: **Rule Operator** and **Rule Value**.

Rule Operator

Within the Rule Operator there are four options to choose from:

Equals: Looks for an exact match, and Includes only exact matches to the Rule Value

Does Not Equal: Looks for an exact match, and includes any results that do not exactly match the Rule Value

Exists: Checks that the claim exists, but doesn't check for any specific values associated with it

Contains: Checks for any and all claims that contain the Rule Value

Rule Value

This is an input field for providing a string for filtering claims, using the operators mentioned above.

Authorization Rule: Outcome

Action

If the claim and rule return a match for a user logging the selection in the Action column will be performed. There are two possible actions: **Authorize As** and **Reject.**

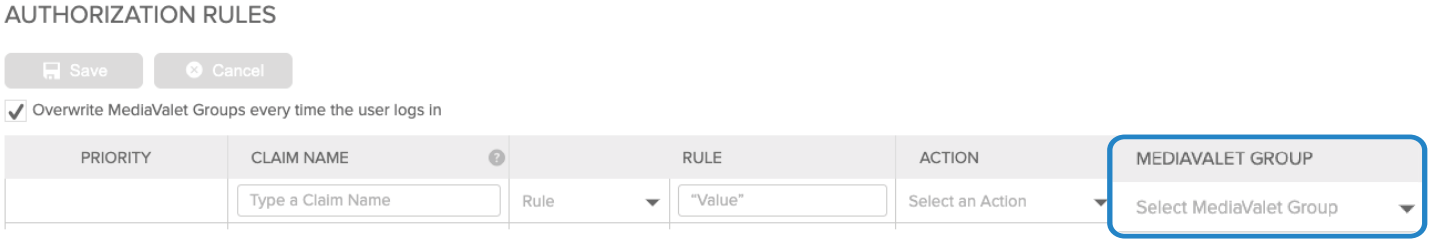
Authorize: Everyone who matches this rule is granted access, and is assigned a MediaValet group

(See below for more information regarding MediaValet groups)

Reject: Everyone who matches this rule is denied access

MediaValet Group

This dropdown contains all default and custom groups in the MediaValet portal. Once a rule is met and the action is *Authorize As*, this determines what level of access the user is granted.

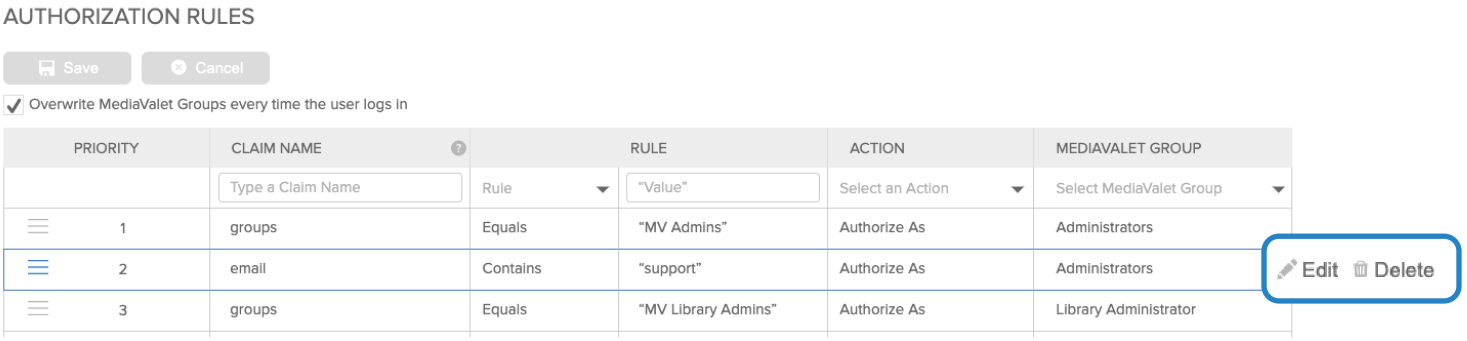


NOTE

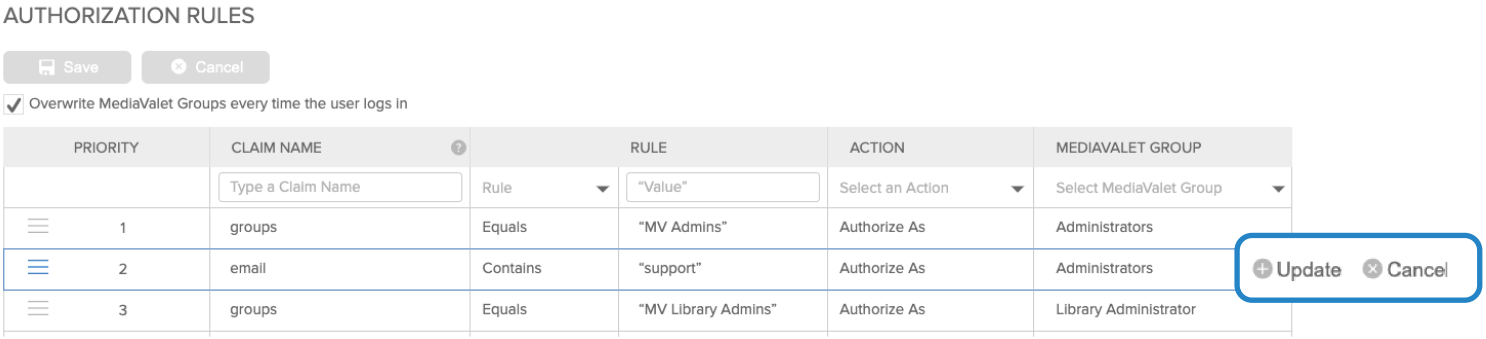
MediaValet groups cannot be deleted if they're used in any rules in the authorization policy. Any authorization rules that reference them must be edited to reference another group or deleted altogether before MediaValet groups can be deleted.

MODIFYING EXISTING RULES

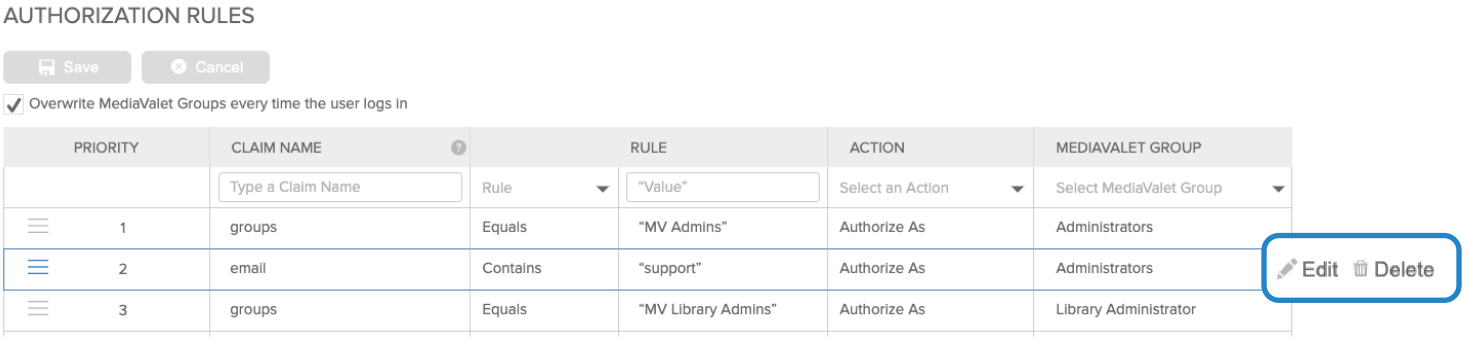
To modify an existing rule, hover over the row and click **Edit** on the right side.



To save changes, click **Update** and to cancel changes, click **Cancel**.

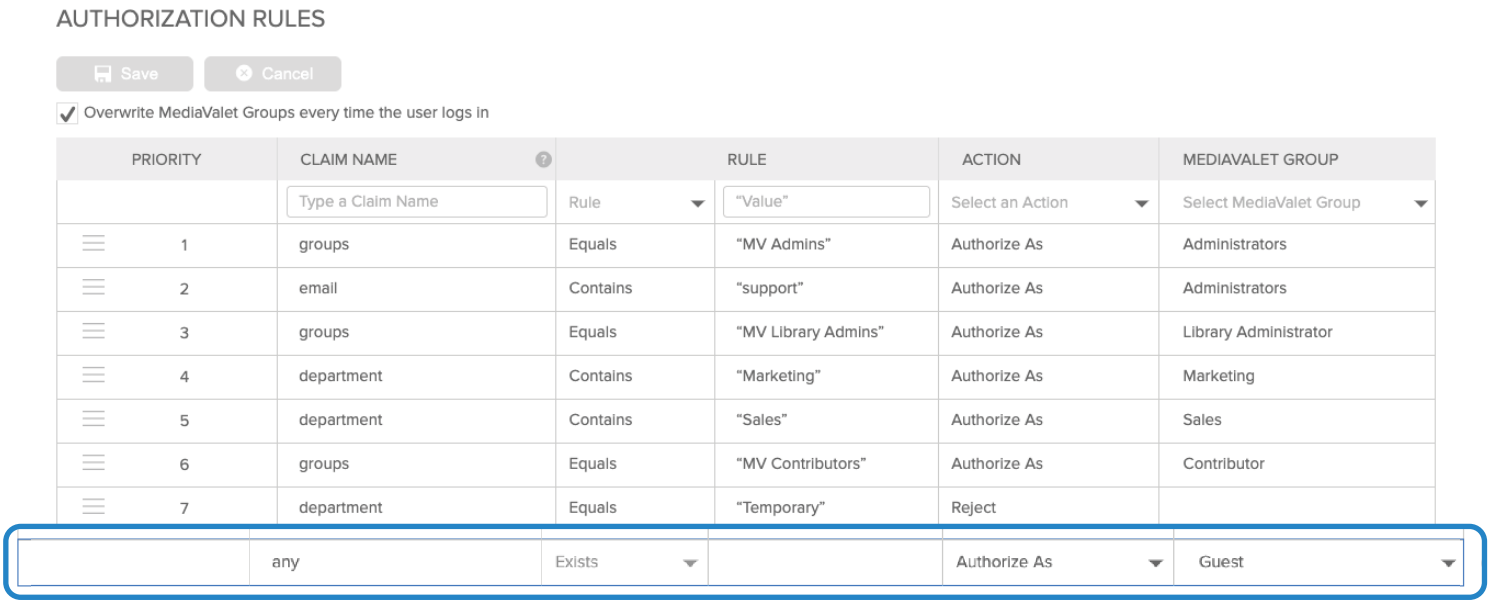


To delete an existing rule, hover over the rule when it's not in edit mode and click **Delete**.



CATCH-ALL "ANY" ROW

The bottom row, sometimes referred to as the "any row," can be added in order to create a catch-all/ fallback rule. This ensures that users who didn't match any of the above rules will still be authorized to access the portal.



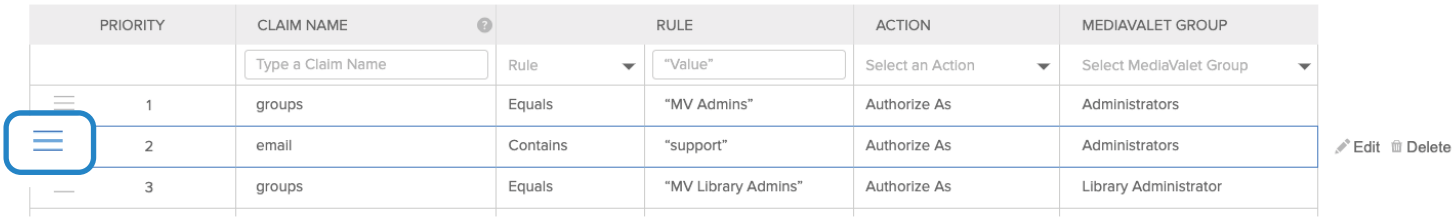
A common rule here is: if any claim exists, *authorize as "Guest."*

SETTING RULE PRIORITY

The authorization rules engine checks rules in order of their priority, starting with rule 1. When a rule has been met, no more rules are checked.

With this in mind, it's important to put the rules with the highest permission level at the top, so that if a user has more than one rule that applies to them, that user is granted access with the highest permission set available to them.

To change the priority of rules, click and hold the hamburger icon (≡) at the left side of the row and drag the row up or down in priority.



NOTE

Priority cannot be changed if there's a row in edit mode. Click **Update** or **Cancel** to exit edit mode, then adjust the priority of the rules.

OVERWRITING MEDIAVALET GROUPS

This checkbox determines if MediaValet Groups get overwritten by group membership in the Identity Provider every time the user logs in.

Leaving this box unchecked means that user permissions can subsequently be changed in the MediaValet user management page, and will not be overwritten by SSO in subsequent logins.

To expand on this:

If the checkbox is *checked:*

- the policy will be re-evaluated and the user will be re-mapped to the policy-defined group every time the user logs in

If the checkbox is *unchecked*

- When the user logs in for the first time, the policy will be evaluated and the user will be mapped to a group
- On subsequent visits, the policy will be re-evaluated only to determine if the user should be rejected or not
    - If the user is NOT logging in for the first time, once they have been authenticated, their level of access is determined by group membership settings in the MediaValet portal

GLOBAL SAVE AND CANCEL

All of the sections above must be saved in order to take effect, by clicking Save in the top left corner. To save, click **Save**.

To cancel any changes on the page, click **Cancel**.