Add a rule (snippet)

> ⚠ Before you create a rule, Armor recommends that you perform a search on the IP address to view Armor's recommendation. To learn how to perform an IP lookup, see Perform an IP Lookup.

Before you create a rule, consider the following statements:

- When you add a rule, your rule may actually override Armor's default whitelist and blacklist policies.
- You cannot use the same IP address in multiple rules, even if the rules are similar in action.
    - For example, if you create a rule to allow 1.1.1.1, then you cannot create a separate whitelist rule for 1.1.1.1/2.
- You cannot edit a rule.
    - If you want to edit a rule to a different list, then you must delete the rule, and then create a new rule.
- Although you can use this screen to research, create, and organize rules, you are responsible for implementing the actual rules in your environment.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Dynamic Threat Blocking**.
3. Click **Rules**.
4. Click the plus (+) icon.
5. Select **Whitelist** or **Blacklist**.
6. Enter an IP address or CIDR.
7. Select an expiration date.
    - You will not receive a notification when a rule has expired; however, you can filter the **Rules** table to view expired rules.
    - If your account contains the **Write Dynamic Threat Blocking Rule Never Expire IP** permission, then as an option, you can mark **Never Expire**.
8. Click **Add Rule**.
    - The newly created rule will appear in the **Rules** section.