# Configure Rule Actions in Rule-Based Policy for Web Policy Management

## Contents

## Introduction

This document describes how to configure rule actions in Rule-Based Policy for web policy management.

## Overview

Rule-Based Policy uses rulesets that match based on identity. Each ruleset contains rules, and each rule matches based on identity, destination, and schedule. The system applies both rulesets and rules in a top-down order of precedence. The identity is matched to the first applicable ruleset, then the first rule that matches the identity, destination, and schedule is applied.

A new feature in Rule-Based Policy allows administrators to assign allow, warn, block, or isolate actions to rule identities for specific destinations and applications.

For instructions on how to configure rulesets and rules, refer to the Manage the Web Policy documentation.

## Actions: Allow, Allow (Secure), Warn, Block, and Isolate

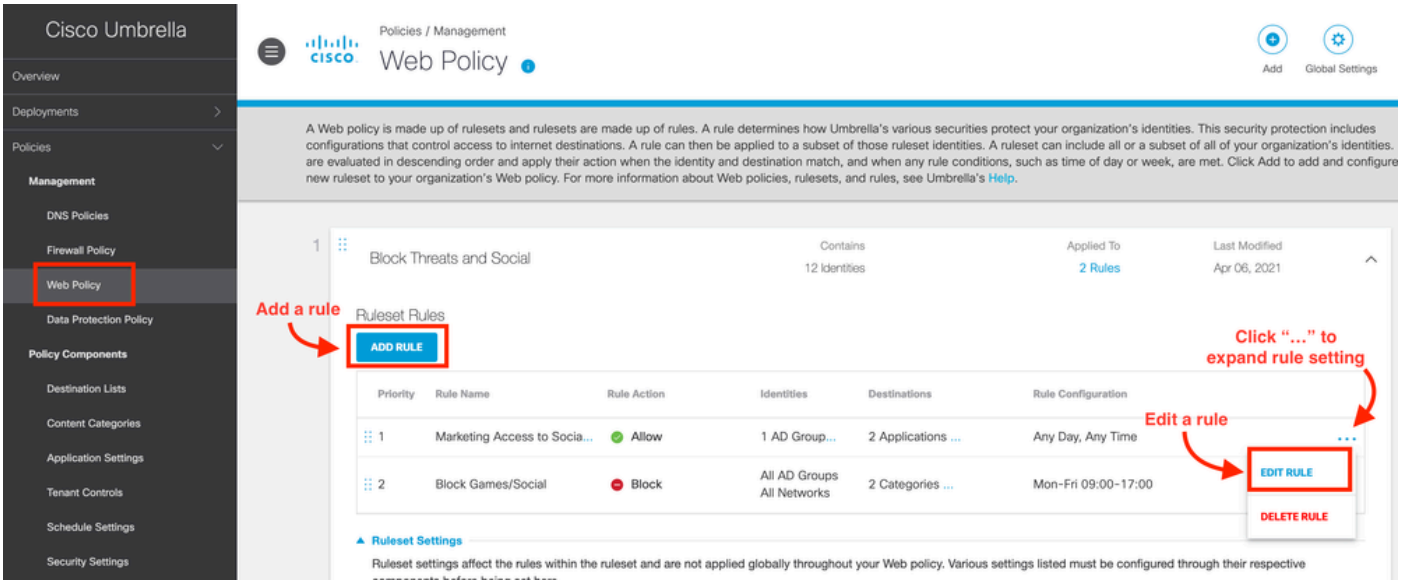
You can assign one of these actions to individual rules in a ruleset:

| | |
|---|---|
| **Allow (Secure)** | Allows access to the destination or application unless a security issue is detected. File Inspection and Security Categories still apply. This is the default action for “allow” unless you select a security override. |
| **Allow** | Allows access to the destination or application without security protection. Security settings cannot be overridden for an entire content category. |
| **Warn** | Presents rule identities with a warning page and an option to continue, instead of blocking access. |
| **Block** | Denies access to the destination. Rule identities cannot override or continue past the block page. |
| **Isolate** | Instead of blocking identities from the destination endpoints, a cloud-based browser hosts the browsing session for that destination. |

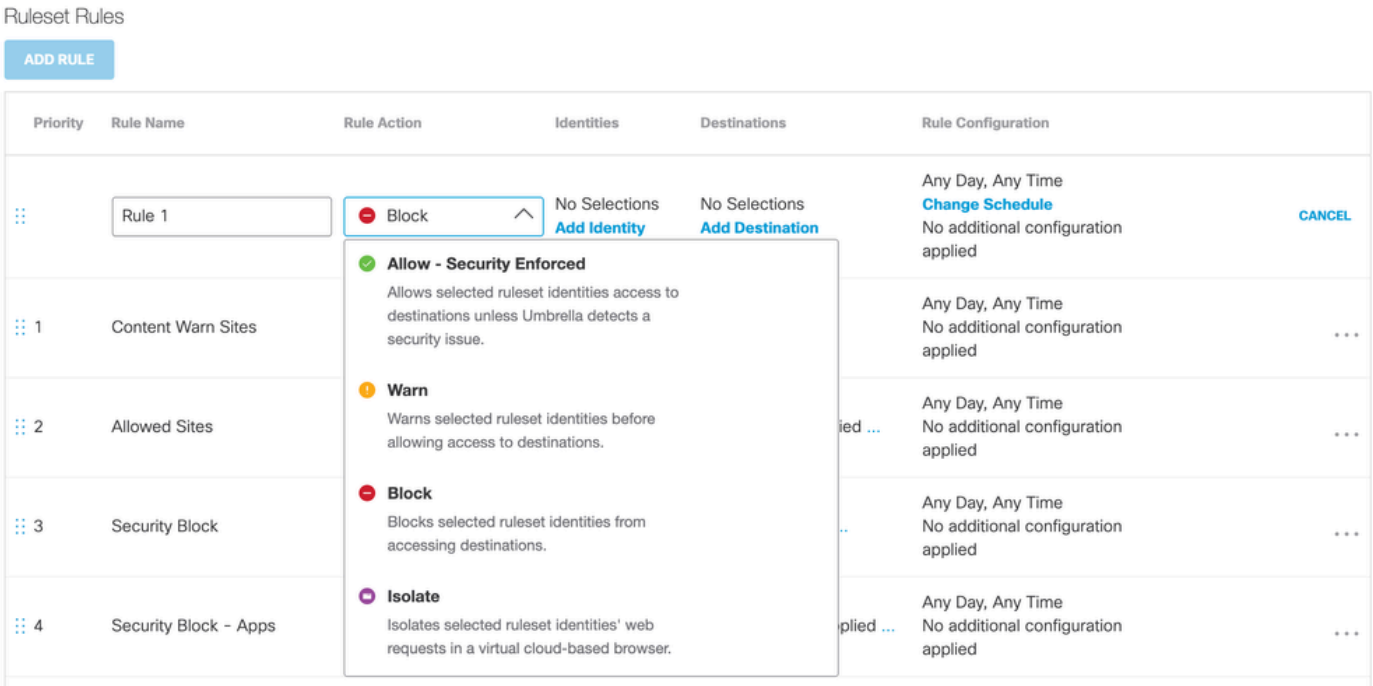
# Set a Rule Action

Select a rule action when you create or edit a rule.

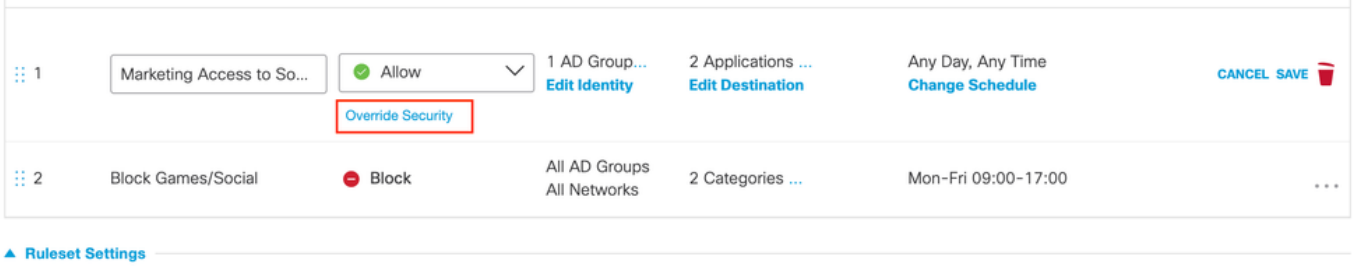
1. Go to**Web Policy > [Select the appropriate Ruleset]**.
2. Click**Add Rule**or**Edit Rule**.




3. In the drop-down menu, select**Allow**,**Warn**,**Block**, or**Isolate**for the destination.




- The default for “allow” applies security and blocks the destination if a threat is detected.
- To allow access without security protection, select the option to "override security."




For more information, [visit the Umbrella Learning Hub for videos about Rule-Based Policies](#).