# Rules & Rulesets (v3)

**NOTE**

> The Rules v3 endpoints are new in the Distributed Cloud AIP API as of March 2023. The Rules v3 and v2 endpoints will work simultaneously while Distributed Cloud AIP migrates all organizations to Rules v3. Once your organization converts to Rules v3, you should begin utilizing the new functionality.

Distributed Cloud AIP takes a behavior-based approach to security alerting, governed by rules that focus on events that you consider important. A rule is a statement that tells software what data to look for and how to react to that data. Distributed Cloud AIP uses the rules enabled in your infrastructure to continuously compare event data to alert criteria. When a rule matches alert criteria, then an alert triggers for the event.

To learn more about the different types of rules available in Distributed Cloud AIP, see Rule Creation Overview.

## Managed and Unmanaged Rules

In addition to your existing, traditional (unmanaged) rules, Rules v3 includes **managed** rules. Distributed Cloud AIP internally coordinates and monitors these managed rules, which you can leverage in your environment to help you save time on rule creation and management.

Distributed Cloud AIP controls specific fields for managed rules, including the title, description, filter, managed suppressions, and managed classifiers. These managed rules will periodically update to ensure that your rules contain the most accurate and up-to-date information. See Rule Release and Changelog for the most recent changes.

**NOTE**

> Rulesets and alerting properties (such as alert frequency) for managed rules are organization-specific, meaning you can change them to better fit your infrastructure. The only fixed fields for managed rules are the title, description, filters, managed classifiers, and managed suppressions.

**Unmanaged, or traditional, rules** are not managed by Distributed Cloud AIP. You can fully customize unmanaged rule titles, descriptions, classifiers, filters, and suppressions to fit your infrastructure's unique needs.

These rules can help you elevate the visibility of security data that matters to you, such as specific user behaviors, container behavior, and/or compliance alignment. Unmanaged rules can also help you to exclude or suppress unactionable or unnecessary data from your environment. For more information about the types of rules you can create, see Rule Creation Overview.

# Create a Ruleset

## Overview

This method enables you to create a new ruleset in your organization.

**NOTE**

> To add a rule to a ruleset, use the Create a Rule or Update a Rule endpoints.

### Sample Query

Create a ruleset in your organization:

```
https://api.threatstack.com/v3/rulesets
```

### Error Handling Tips

- **400**: Incorrect syntax in the message body.
- **409**: The ruleset name duplicates an existing ruleset name.

REQUEST BODY SCHEMA: application/json

Create ruleset object

| | |
|---|---|
| `name`<br>required | string (RuleSetName) [ 1 .. 200 ] characters<br>Name of the ruleset<br><br>**WARNING**: The ruleset name cannot duplicate another ruleset name in the organization. |
| `description`<br>required | string (RuleSetDescription) [ 1 .. 300 ] characters<br>Description of the ruleset |

## Responses

> 200

Success

> 400

Bad parameters

> 401

Unauthorized response

> 429

Rate limit hit

> 500

An internal error has occurred

POST /rulesets

## Request samples

**Payload**

**Content type**
application/json

```
{
  "name": "string",
  "description": "string"
}
```

## Response samples

200 | 400 | 401 | 429 | 500

**Content type**

application/json


```
{
    "id": "e5034ccf-bf8e-4005-b942-737deaf4c491",
    "name": "string",
    "description": "string",
    "createdAt": "2019-08-24T14:15:22Z",
    "updatedAt": "2019-08-24T14:15:22Z"
}
```