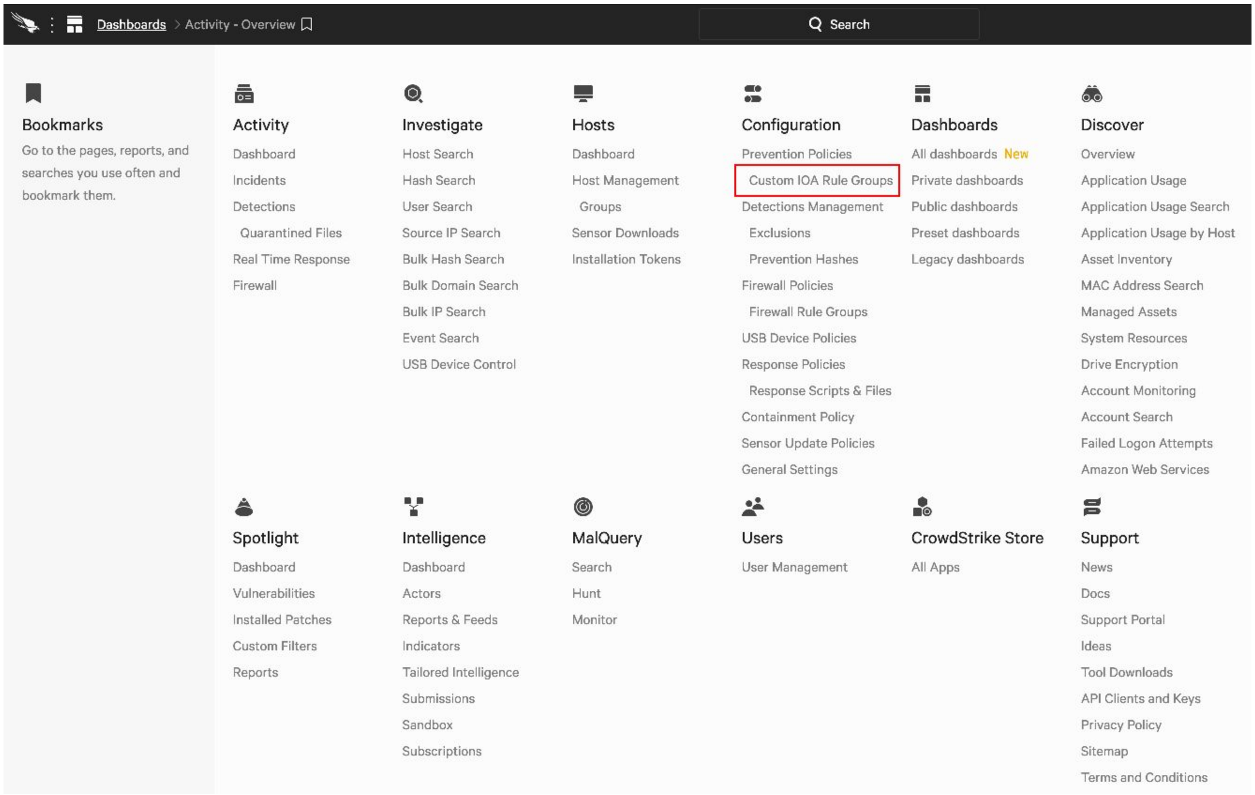
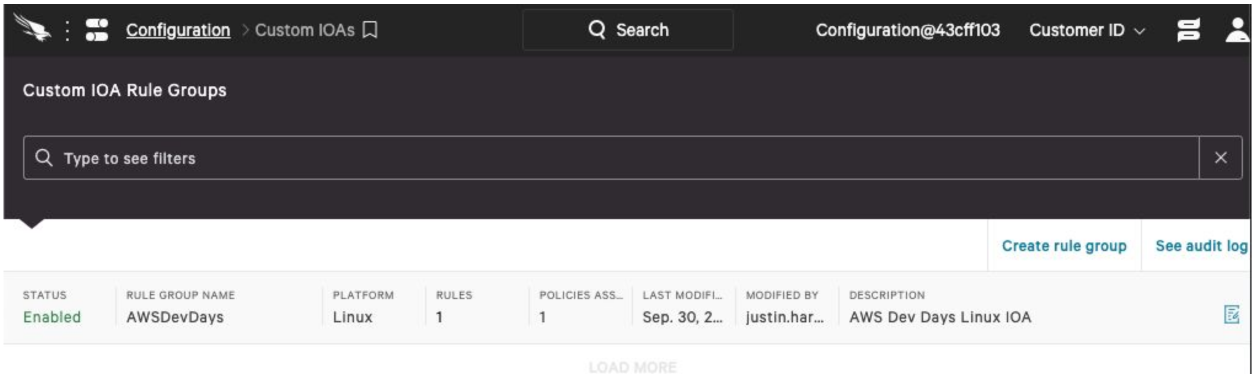
# Creating a Custom Prevention Policy

Log into the CrowdStrike Console

1) Go to *Configuration -> Custom IOA Rule Groups*

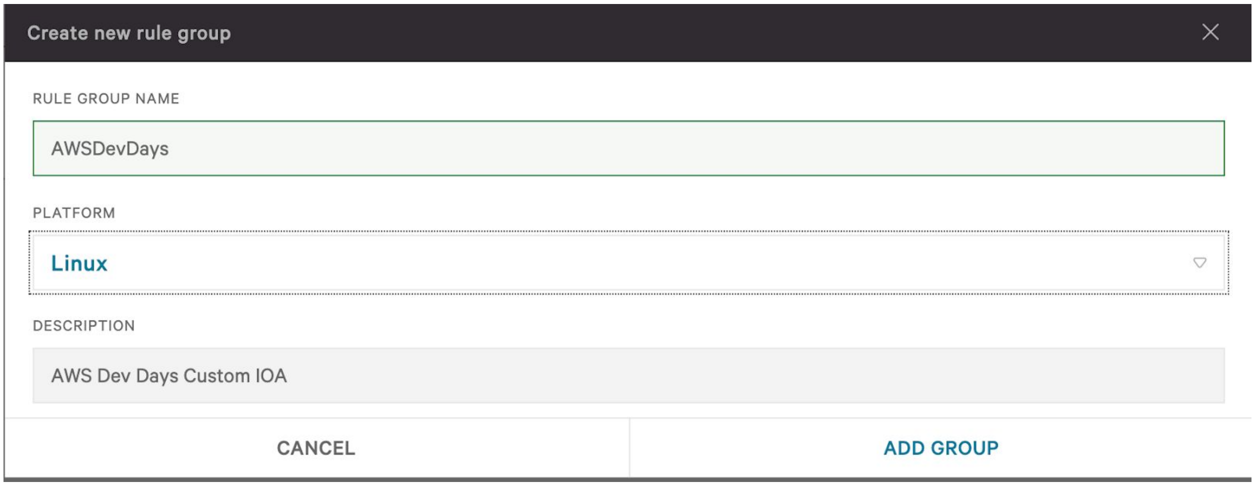


2) Select Create rule group



| STATUS | RULE GROUP NAME | PLATFORM | RULES | POLICIES ASS... | LAST MODIFI... | MODIFIED BY | DESCRIPTION |
|---|---|---|---|---|---|---|---|
| Enabled | AWSDevDays | Linux | 1 | 1 | Sep. 30, 2... | justin.har... | AWS Dev Days Linux IOA |

3) Enter a rule group name



Create new rule group

RULE GROUP NAME

AWSDevDays

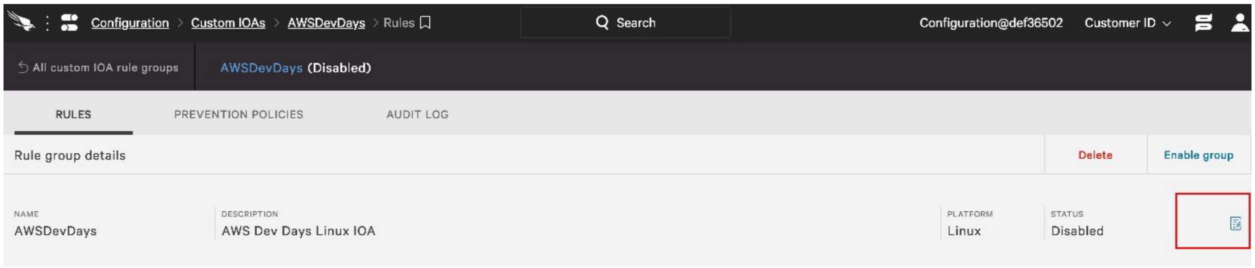
PLATFORM

Linux

DESCRIPTION

AWS Dev Days Custom IOA

4) Edit the rule group



Configuration > Custom IOAs > AWSDevDays > Rules
Search
Configuration@def36502
Customer ID
All custom IOA rule groups

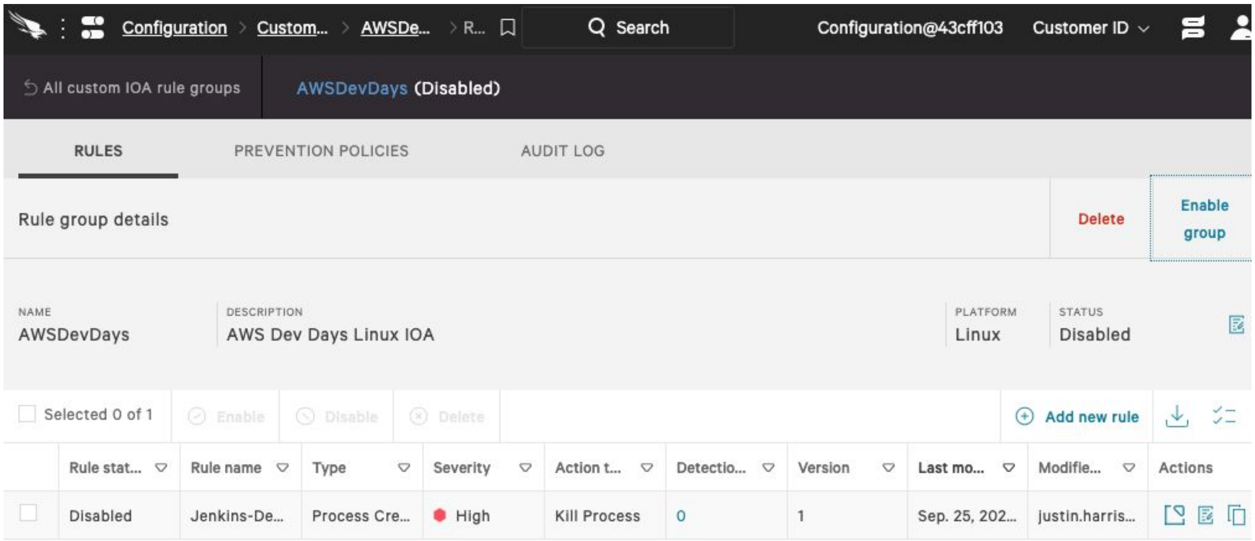
AWSDevDays (Disabled)

NAME: AWSDevDays
DESCRIPTION: AWS Dev Days Linux IOA
PLATFORM: Linux
STATUS: Disabled

5) Create the New Rule with the following values

| ***Parameter*** | ***Value*** |
|---|---|
| RULE TYPE | Process Creation |
| ACTION TO TAKE | Kill Process |
| SEVERITY | High |
| RULE NAME | *<Enter a rule name>* |
| RULE DESCRIPTION | *<Enter a description>* |
| IMAGE FILENAME | .*/bin/nc.traditional.* |
| COMMAND LINE | .*nc -e \/bin\/bash.* |

6) Select “Enable Group”



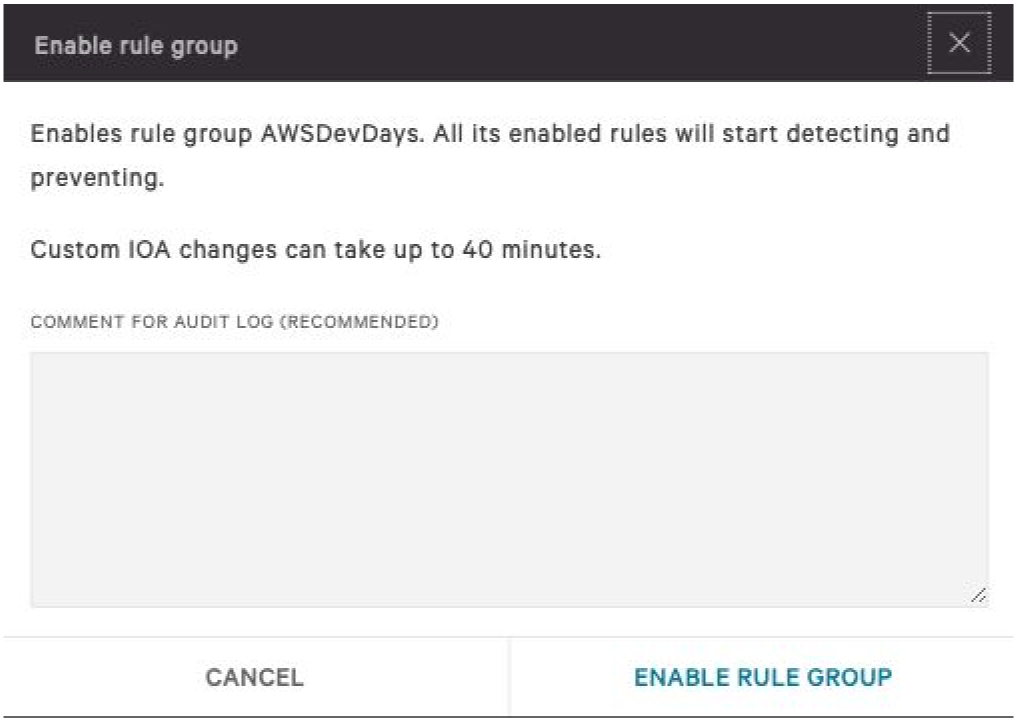
AWSDevDays (Disabled)

Rule group details

| NAME | DESCRIPTION | PLATFORM | STATUS |
|---|---|---|---|
| AWSDevDays | AWS Dev Days Linux IOA | Linux | Disabled |

□ Selected 0 of 1

| | Rule stat... | Rule name | Type | Severity | Action t... | Detectio... | Version | Last mo... | Modifie... | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | Disabled | Jenkins-De... | Process Cre... | ● High | Kill Process | 0 | 1 | Sep. 25, 202... | justin.harris... | |



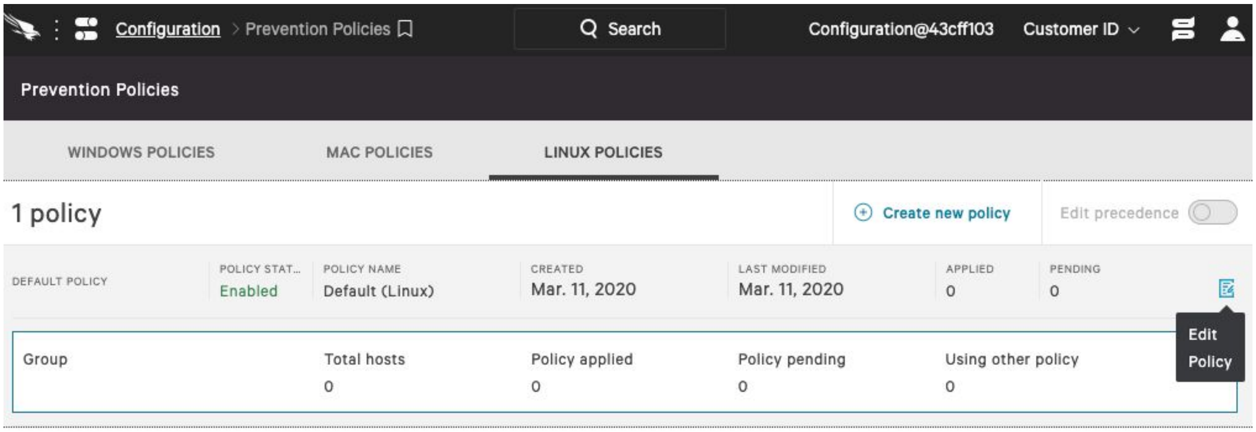
Enable rule group

Enables rule group AWSDevDays. All its enabled rules will start detecting and preventing.

Custom IOA changes can take up to 40 minutes.

COMMENT FOR AUDIT LOG (RECOMMENDED)

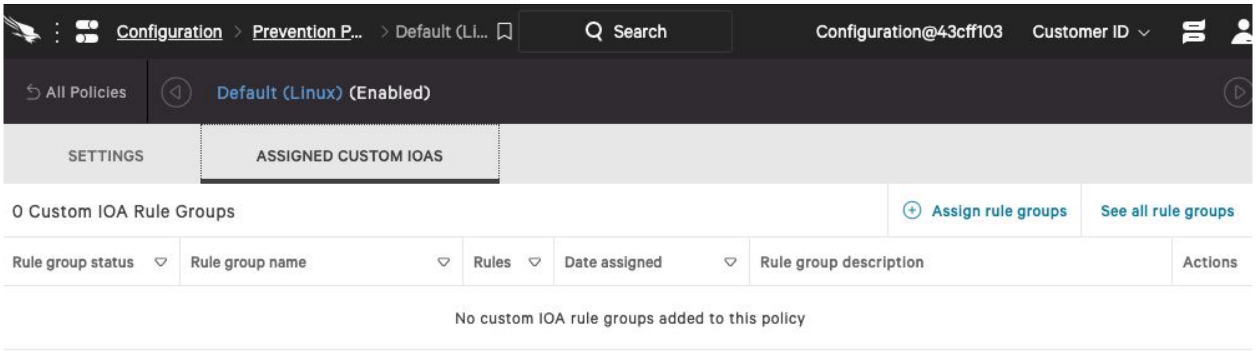
7) Select *Configuration - Prevention Policies*



| DEFAULT POLICY | POLICY STAT... | POLICY NAME | CREATED | LAST MODIFIED | APPLIED | PENDING |
|---|---|---|---|---|---|---|
| | Enabled | Default (Linux) | Mar. 11, 2020 | Mar. 11, 2020 | 0 | 0 |

| Group | Total hosts | Policy applied | Policy pending | Using other policy |
|---|---|---|---|---|
| | 0 | 0 | 0 | 0 |

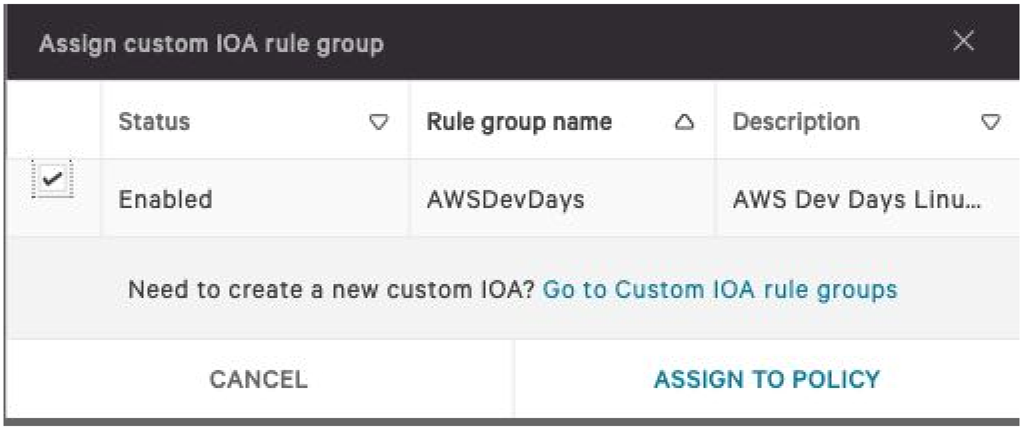
8) Select Linux Policies - ASSIGNED CUSTOM IOAS



| Rule group status | Rule group name | Rules | Date assigned | Rule group description | Actions |
|---|---|---|---|---|---|

No custom IOA rule groups added to this policy

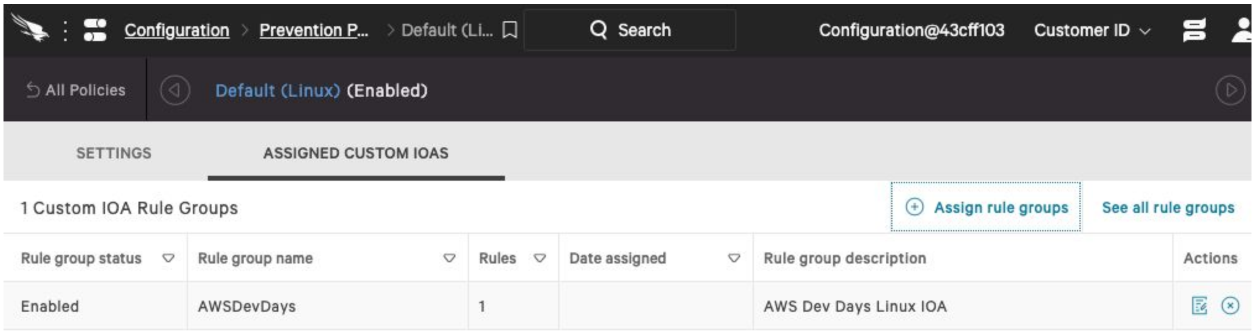
9) Select the Custom IOA that created previously



| | Status | Rule group name | Description |
|---|---|---|---|
| ☑ | Enabled | AWSDevDays | AWS Dev Days Linu... |

Need to create a new custom IOA? Go to Custom IOA rule groups

10) Check that the custom IOA has been assigned to the default Linux policy



1 Custom IOA Rule Groups

| Rule group status | Rule group name | Rules | Date assigned | Rule group description | Actions |
|---|---|---|---|---|---|
| Enabled | AWSDevDays | 1 | | AWS Dev Days Linux IOA | |