Automated Safeguards for Security Groups

- Overview
- Allowed Security Group Rules
- Evaluation and Remediation
  - Evaluation
  - Remediation
- Request Security Rule Exception
- Review Rule Exception Requests
- Track or Cancel an Existing Exception Request
- Disable a Previously Approved Exception Request
- Non-Compliant Security Group Rules Alerting

Overview

ClearDATA has developed Automated Safeguards for Security Groups that allow customers to manage their own security groups and rules in AWS. Customers can still request ClearDATA to manage their Security Groups if they wish.

Allowed Security Group Rules

Customers are able to create new security group rules that use any RFC1918 space (10.0.0.0 /8, 172.16.0.0/12, & 192.168.0.0/16) as the source. If customers wish to use a routable IP address in a Security Group rule they must request an exception. In order for ClearDATA to allow the rule, our Information Security team will review all exception requests against our policies and procedures and make a determination.

Users must be added to the appropriate IAM Group in order to create and modify Security Groups.

> **IPv6**
>
> At this time IPv6 rules are not supported with the Automated Safeguards. If you require an IPv6 address please contact ClearDATA Support.

Evaluation and Remediation

Evaluation

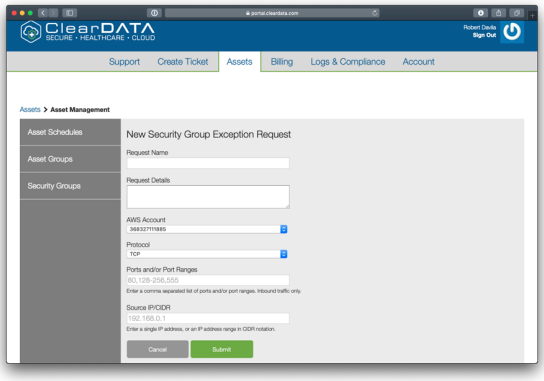
If a new rule is added to a Security Group, or if an existing rule is modified, that change will trigger a reevaluation of the Security Group. Additionally, there are certain events that will trigger an evaluation of existing rules but not a remediation. These events included underlying changes that AWS can make to load balancers, EC2 instances, or network interfaces that generate a *change* event. ClearDATA uses these change events to trigger an evaluation of the rules but it does not trigger a remediation, because there was not a change made to the rules themselves. You may receive an alert for a non-compliance security group as a result of these infrastructure changes.

Remediation

If the new or modified rule is not allowed, and if there is not an existing exception, the rule will be removed from the Security Group. Please contact ClearDATA Support if you need any assistance with creating rules.

Request Security Rule Exception

1. Go to ClearDATA portal
2. Click on “Assets” tab
3. Click on “Security Groups”
4. Click on green “New Exception Request” button
5. Fill the form and click submit



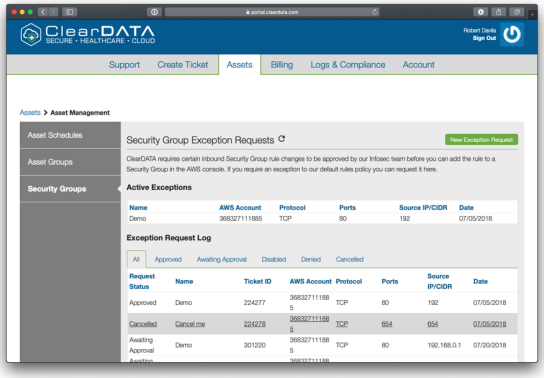
> **Note**
>
> When submitting a request, please ensure each request only contains one source CIDR. If you have multiple CIDR ranges, each will require a separate request.

6. Request will then appear in previous screen with an “Awaiting Approval” Status and a ticket number that can be used to reference the request

Review Rule Exception Requests

Security Group Rule Exception Requests are available in the ClearDATA customer portal.

1. Go to ClearDATA portal
2. Click on “Assets” tab
3. Click on “Security Groups”
4. The view shows:
    a. All approved and activity Security Rule Exceptions
    b. A log of all Security Rule Exception Requests

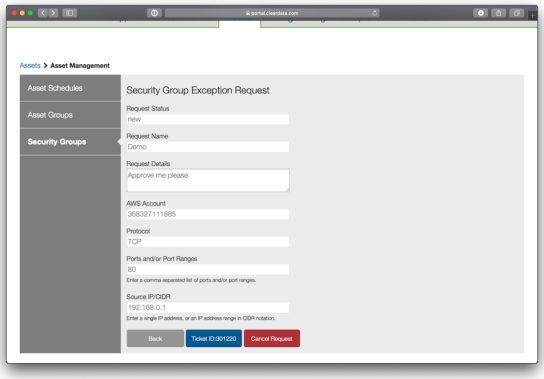


Please note that its is all possible to view all requests by status as well. The status options are:

- Approved
- Awaiting Approval
- Disabled
- Denied
- Cancelled

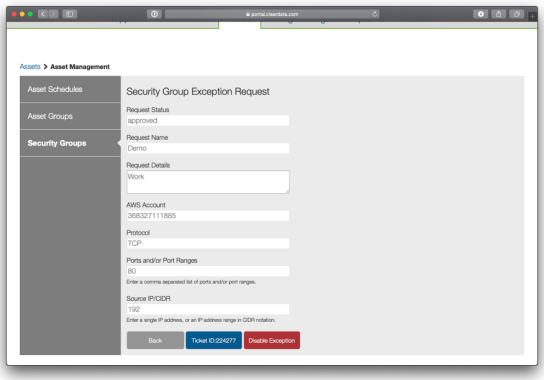
Track or Cancel an Existing Exception Request

1. Go to ClearDATA portal
2. Click on “Assets” tab
3. Click on “Security Groups”
4. Click on the Security Rules Exception
5. To **track** the request refer to the ticket # shown in the blue box or click on the blue box to see latest updates
6. To **cancel** the request, click on the red box “Cancel Request” to cancel the request – Its status will then change from “Awaiting Approval” to “Cancelled”
7. If approved, status will change to “Approved” and it will then be possible to use the rule, if not, status will change to “Denied"



Disable a Previously Approved Exception Request

1. Go to ClearDATA portal
2. Click on “Assets” tab
3. Click on “Security Groups”
4. Click on an “Approved” Security Rules Exception
5. To disable the request click on the red “Disable” requests rule – This will forbid this rule from being used moving forward
   Please note that it is possible to look at the history of the rule by clicking on the blue button



Non-Compliant Security Group Rules Alerting

ClearDATA Automated Safeguards both alert and remediate when a compliance violation is detected. Customers can subscribe to the alerts by following the article Automated Safeguards - Subscribe to Compliance Alerts.