



# Security

Help Documentation

## Security

### Abuse Detection Rule Triggered

The monitoring of Security for an administrators system and/or domain is very important.

Administrators would and need to know if a domain or user has abused any rule that has been put in place. Administrators can utilize the attributes listed below to be notified when a rule has been abused.

Attributes

Time of Day - Enter a time of day to trigger this event.

Rule Type - Select the security rule that you want to trigger this event.

IP Address - Enter an IP address that will trigger this event.

Rule Name - Enter a name for the rule to trigger this event.

### ClamAV Failure

ClamAV is a 3rd party source integrated with SmarterMail to help detect and prevent viruses from entering the system. Administrators can utilize the attributes listed below to notify them when there has been a failure with the ClamAV service.

Attributes

Time of Day - Enter a time of day to trigger this event.

ClamAV IP - Enter the IP address of the ClamAV server that will trigger this event.

ClamAV Port - Enter the port of the ClamAV server that will trigger this event.

Consecutive Failures - Enter the number of failures that needs to be reached to trigger this event.

File Name - Enter the name of the file to trigger this event.

File Size (KB) - Enter the size of the file in KB that will trigger this event.

### Outgoing Message Blocked

Administrators may want to know if outgoing messages are being blocked so they can further investigate why and from whom the message was sent. Administrators can utilize the attributes listed below to be notified when an outgoing message was blocked.

Attributes

Time of Day - Enter a time of day to trigger this event.

From Address - Enter the email address that an email was sent from to trigger this event.

To Address - Enter the email address that an email is sent to trigger this event.

Subject - Enter a task or email subject to trigger this event.

Spam Weight - Enter the spam weight of the message that will trigger this event.

File Name - Enter the name of the file to trigger this event.

## **Virus Found**

Viruses can be very harmful to SmarterMail or the entire system. Administrators can utilize the attributes listed below and be notified if a virus gets through the ClamAV service and is found.

### Attributes

Time of Day - Enter a time of day to trigger this event.

From Address - Enter the email address that an email was sent from to trigger this event.

To Address - Enter the email address that an email is sent to trigger this event.

Subject - Enter a task or email subject to trigger this event.

Virus Name - Enter the name of a virus that will trigger this event.

File Name - Enter the name of the file to trigger this event.