Security Events

Help Documentation

Security Events

System administrators can receive notifications based on the following security events:

- Abuse Detection Rule Triggered - Notifies system administrators when an abuse detection rule has been triggered.
- ClamAV Failure - Notifies system administrators when there has been a failure with the ClamAV service.
- Blacklist Status Changed - Nofities system administrators whent there has been a change in the automatick blacklist check of a particular mail server IP. This can be triggered when a server's blocked status is set to True or False. (Added or removed.)
- Outgoing Message Blocked - Notifies system administrators when an outgoing message is blocked.
- SpamAssassin Failure - Notifies system administrators when there has been a failure with the SpamAssassin service.
- Virus Found - Notifies system administrator if a virus is found on the server.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- ClamAV IP - The IP address of the ClamAV server that will trigger the event.
- ClamAV Port - The port of the ClamAV server that will trigger the event.
- Consecutive Failures - The number of consecutive failures that will trigger the event.
- File Name - The file name that will trigger the event.
- File Size - The size of the file in KB that will trigger the event.
- Name - The full name of the person that will trigger the event.
- IP Address - The IP address that will trigger the event.
- Rule Name - The rule name that will trigger the event.
- Rule Type - The type of security rule that will trigger the event.
- Spam Weight - The spam weight of the message that will trigger the event.
- SpamAssassin IP - The IP address of the SpamAssassin server that will trigger the event.
- SpamAssassin Port - The port of the SpamAssassin server that will trigger the event.
- Subject - The words that will trigger the event if found within the subject of the message.

- To Address - The email address to which the message was sent.
- From Address - The email address from what the message was sent.
- Virus Name - The virus name that will trigger the event.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Execute command-line
- Send email
- Use notification profile