How to Configure Basic, Severity, and Notification Settings for Events

https://campus.barracuda.com/doc/53248798/

It is recommended to modify the default configuration for the events. You can modify the severity, notification, event propagation, and persistence of each event. Events are identified by ID numbers and classified by the severity class as security or operational events.

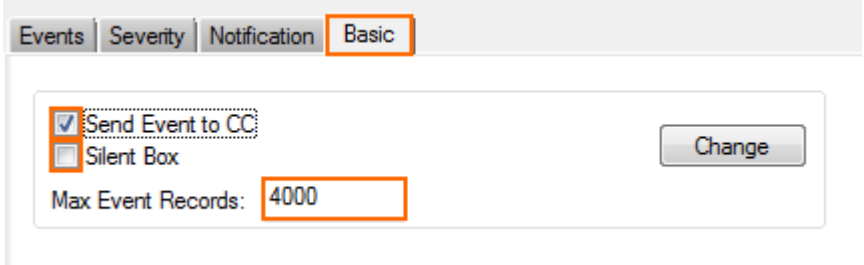
- **Security Events** – ID 1, 2, 3
- **Operative Events** – ID 6, 7, 8

Before You Begin

Look up the event IDs you want to change. For more information, see Operational Events and Security Events.

Step 1. Configure Basic Settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Eventing**.
2. Click **Lock**.
3. Click on the **Basics** tab.
4. To disable forward events to a Control Center, clear the **Send Event to CC** check box.
5. Click **Silent Box** to collect events, but to not send notifications.



6. Enter the maximum number of events in the **Max Event Records**. Records exceeding this limit are dropped.
7. Click **Send Changes** and **Activate**.

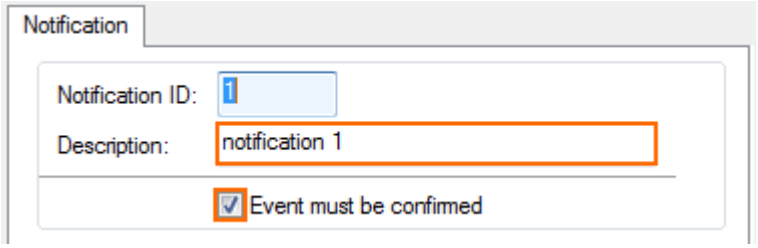
Step 2. Configure Event Notification Settings

Five notifications IDs are available. Configure the notification types that each notification ID sends. To

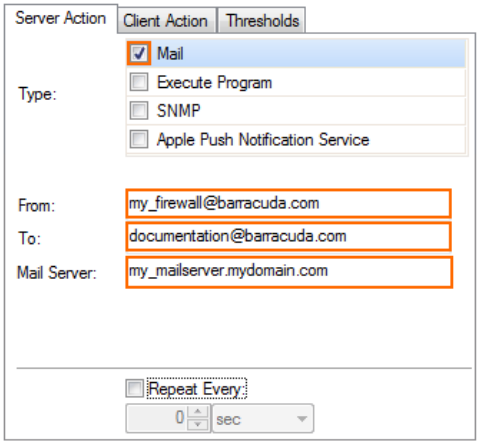
avoid being flooded by notifications, configure thresholds.

> When choosing email notification, be aware that this option requires an email relay or internal email server that does not require authentication.

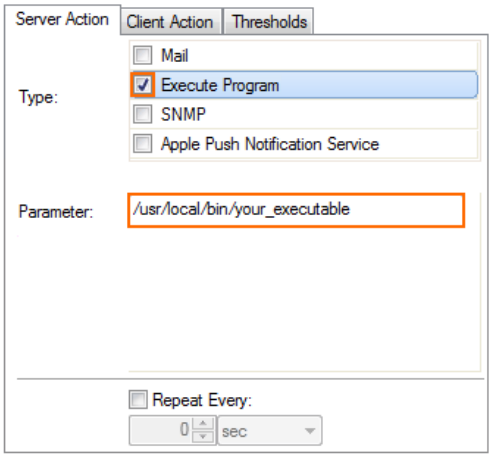
1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Eventing**.
2. Click **Lock**.
3. Click on the **Notifications** tab.
4. Double-click the notification ID you want to edit. The **Detail** window opens.
5. (optional) Modify the **Description**.
6. Click the **Event must be confirmed** check box to require the admin to acknowledge and mark the event as read in the **EVENTS** tab.



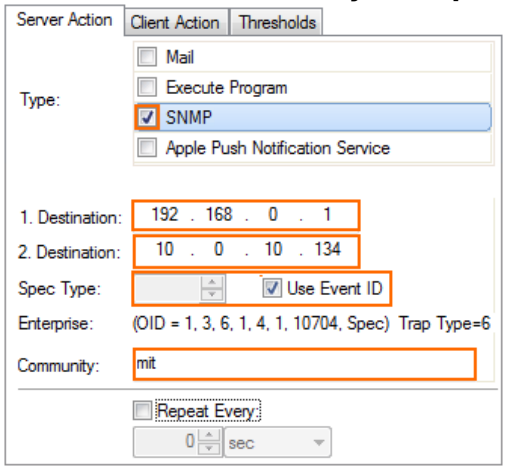
7. In the **Server Action** tab, configure the event notifications carried out by the firewall:
    1. Select and configure the sever action **Types**:
        - **Mail** – Send an email notification using **To**, **From**, and **Mail Server** settings.



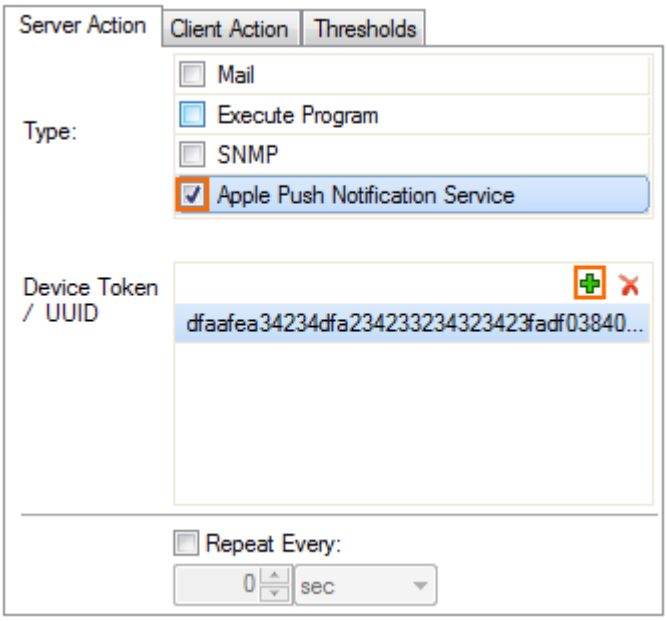
        - **Execute Program** – Executes a script or other executable on the firewall. Enter the executable including the full path as the **Parameter**.



- **SNMP** – To send SNMP traps to a SNMP server, configure up to two SNMP servers and the SNMP **Community** and **Spec Type** settings.

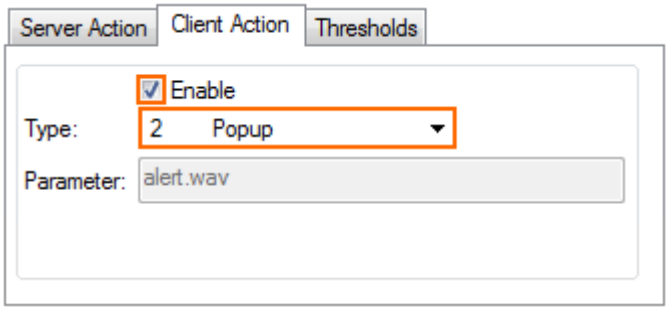


- **Apple Push Notification Service** – To send push notifications to your iOS device running NextGen Remote, enter the **Device token** displayed by the NextGen Remote. You can add multiple iOS devices. For more information, see Barracuda NextGen Remote.

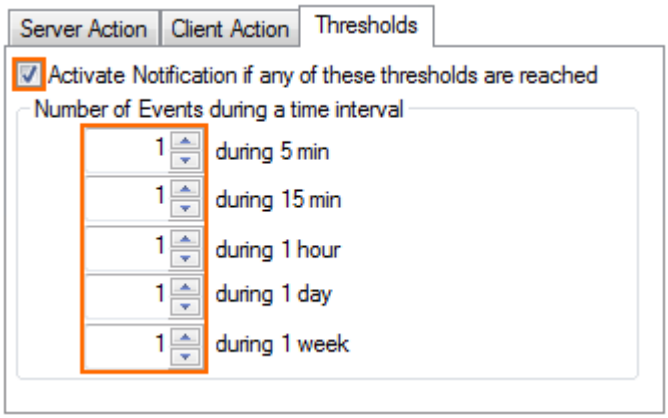


1. To periodically repeat the notifications until the event is read, click the **Repeat Every** check box and configure the timespan between notifications.
2. Click **OK**.
3. For a Control Center, add an Access Rule to permit traffic on port 2195 TCP to the Apple APN servers. For more information about how to add an Access Rule, see How to Create a Pass Access Rule.

8. (optional) Click the **Client Action** tab. The **EVENTS** tab on the NextGen Admin must be set to **LIVE** for these notifications to be executed.
   1. Click the **Enable** check box.
   2. Select the **Type**:
      - **Popup** – A pop-up window opens for each notification on the client running NextGen Admin.
      - **Audio Alert** – A WAV audio file is played.



   3. Click **OK**.
9. Click the **Thresholds** tab.
   1. Click the check box to enable these thresholds before activating the notification.
   2. Enter how often the notifications are sent for each timespan.



3. Click **OK**.

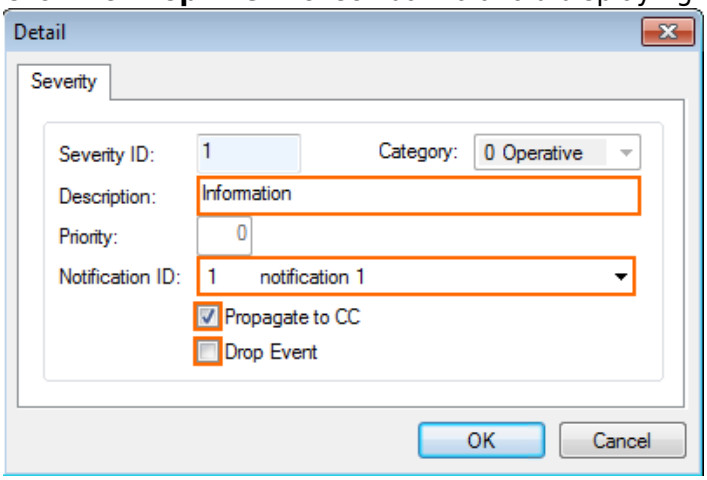
10. Click **Send Changes** and **Activate**.

Repeat this step until all notification IDs are configured to match your needs.

Step 3. Modify Event Severity Settings

Modify the notification type for the severity category and if it is forwarded to the Control Center (only when the firewall is managed).

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Eventing**.
2. Click **Lock**.
3. Click on the **Severity** tab.
4. Double-click on the severity ID you want to edit. The **Detail** window opens.
5. (optional) Modify the **Description**.
6. From the **Notification ID** list, select the notification.
7. To forward the event to the Control Center, click the **Propagate to CC** check box.
8. Click the **Drop Event** check box to avoid displaying these events in the **Events** tab.



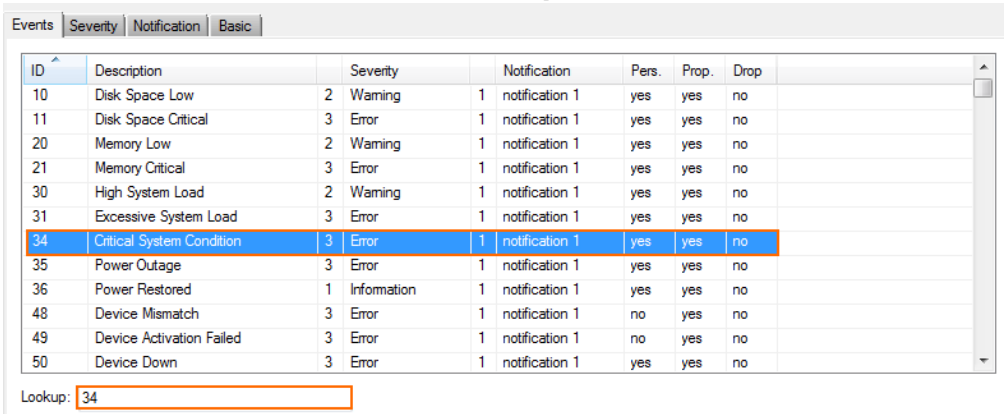
9. Click **OK**.

Repeat this step until all severity IDs are configured to match your needs.

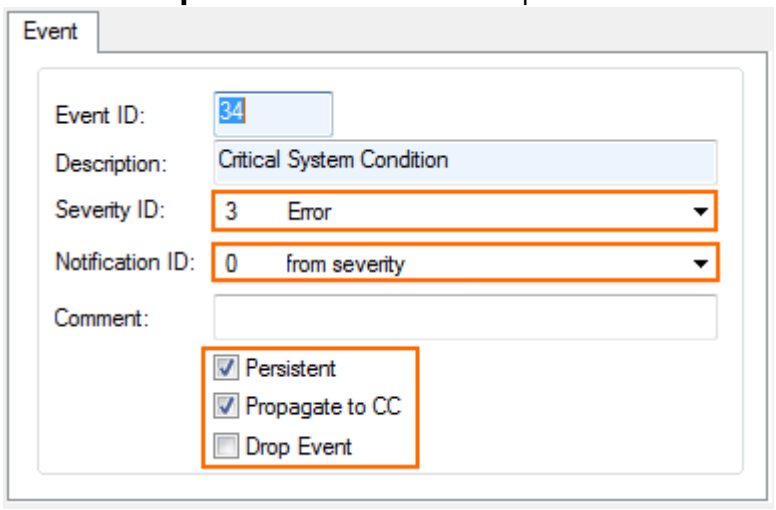
Step 4. Modify the Event Default Severity and Notification IDs

Modify the severity and notification event IDs selected by default for the events.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Eventing**.
2. Enter the **ID** for the events in the **Lookup** field.



3. Double-click the highlighted event. The **Detail** window opens.
4. Select the **Severity ID**.
5. Select the **Notification ID**. Select **from severity** to use the default notification ID for the severity.
6. Click the **Persistent** check box to forward the event only once to the Control Center, even it if occurs multiple times.
7. Click the **Propagate to CC** check box to forward the event to the Control Center. This setting overrules the setting in the basic and severity configurations.
8. Click the **Drop Event** check box to drop the event.



9. Click **OK**.

10. Click **Send Changes** and **Activate**.

Figures

1. events_03.png
2. events_04.png
3. events_05.png
4. events_06.png
5. events_07.png
6. events_08.png
7. events_08a.png
8. events_09.png
9. events_02.png
10. events_01.png
11. events_10.png