

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

<https://campus.barracuda.com/doc/96026549/>

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 severity class as security or operational events.

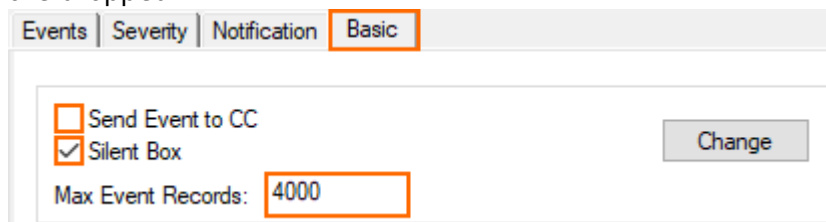
- **Security Events** – ID 6, 7, 8
- **Operative Events** – ID 1, 2, 3, 9

### 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 do not send notifications.
6. Enter the maximum number of events in the **Max Event Records**. Records exceeding this limit are dropped.

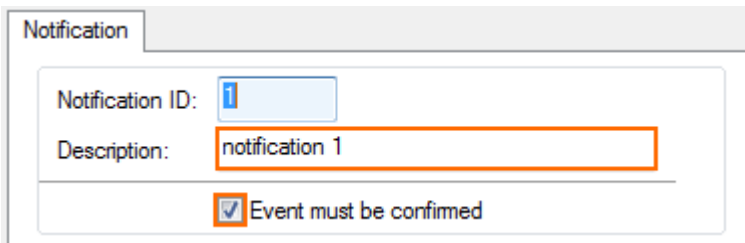


7. Click **Send Changes** and **Activate**.

### Step 2. Configure Event Notification Settings

Five notification IDs are available. Configure the notification types that each notification ID sends. To avoid being flooded by notifications, configure thresholds.

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.

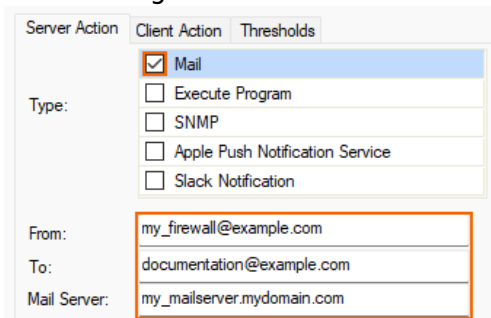


7. In the **Server Action** tab, configure the event notifications carried out by the firewall:
  1. Select and configure the sever action **Types**:

- **Mail** – It is possible to send notifications with email to multiple recipients. When using multiple recipients, separate them with a semicolon or a space character.  
 Note that email notifications support SSL or authentication, using the **System Notifications** at **Configuration Tree > Box > Administrative Settings > Notifications**, but only if the checkbox for this is enabled while the details in the notification itself (server, addresses) are left blank.

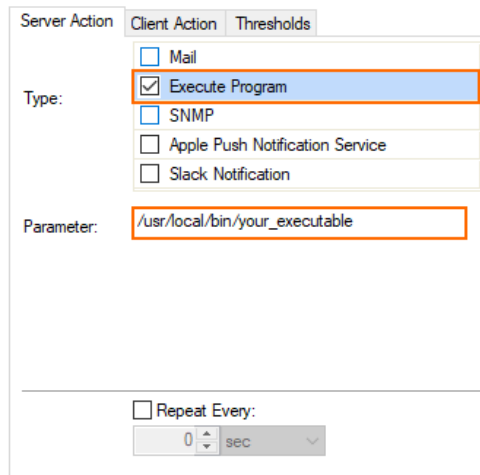
For sending notifications with email, the following configuration options are available:

- **"Legacy" Mode** – If the edit fields for email are configured at **Configuration Tree > Box > Administrative Settings > Notifications** only and the check box STARTTLS is not selected, then notifications are sent unencrypted to the specified email receiver.
- **"Override" Mode** – If you want to have your notifications to be sent to a different recipient as configured at **Configuration Tree > Box > Administrative Settings > Notifications**:
  1. Go to **Configuration Tree > Box > Infrastructure Service > Eventing**, tab **Server Action**.
  2. Activate the check box **Mail**.
  3. Fill out the edit fields **From:**, **To:**, and **Mail Server:** with the required email configuration information.



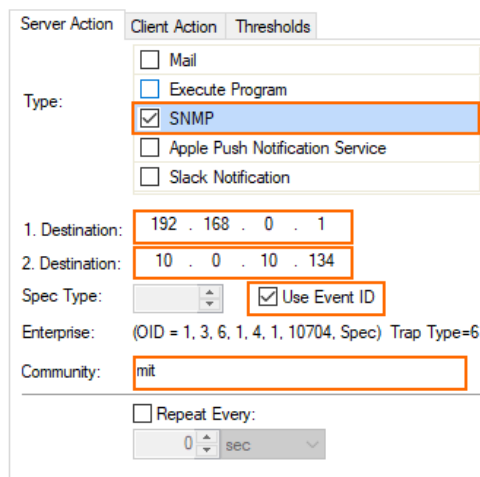
- **Execute Program** – Executes a script or other executable on the firewall. Enter the

executable including the full path as the **Parameter**.



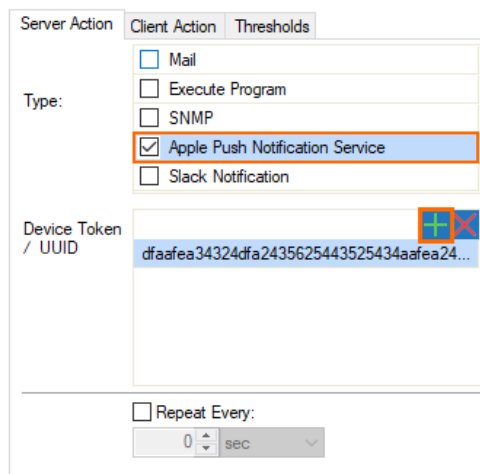
The screenshot shows the 'Server Action' configuration window with the 'Client Action' tab selected. Under the 'Type' section, 'Execute Program' is selected with a checkmark. The 'Parameter' field contains the text '/usr/local/bin/your\_executable'. At the bottom, there is a 'Repeat Every' section with a checkbox and a dropdown menu set to '0 sec'.

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



The screenshot shows the 'Server Action' configuration window with the 'Client Action' tab selected. Under the 'Type' section, 'SNMP' is selected with a checkmark. There are two 'Destination' fields: '1. Destination:' with the value '192 . 168 . 0 . 1' and '2. Destination:' with the value '10 . 0 . 10 . 134'. The 'Spec Type' dropdown is set to 'Use Event ID'. The 'Enterprise' field contains '(OID = 1, 3, 6, 1, 4, 1, 10704, Spec)' and the 'Trap Type' is set to '6'. The 'Community' field contains 'mit'. At the bottom, there is a 'Repeat Every' section with a checkbox and a dropdown menu set to '0 sec'.

- **Apple Push Notification Service** – To send push notifications to your iOS device running Barracuda Firewall Remote Control, enter the **Device token** shown on the Remote Control display. You can add multiple iOS devices.



The screenshot shows the 'Server Action' configuration window with the 'Client Action' tab selected. Under the 'Type' section, 'Apple Push Notification Service' is selected with a checkmark. The 'Device Token / UUID' field contains a long alphanumeric string: 'dfaafea34324dfa2435625443525434aafea24...'. At the bottom, there is a 'Repeat Every' section with a checkbox and a dropdown menu set to '0 sec'.

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**.

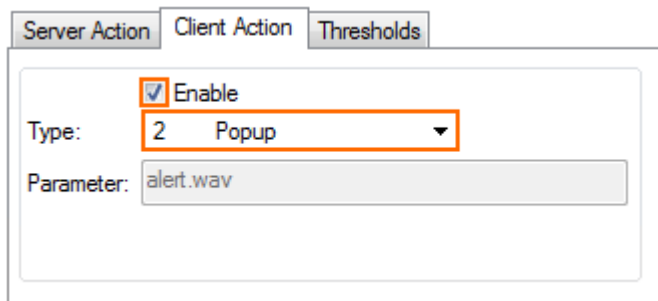
3. For a Control Center, add an access rule to permit traffic on port 2195 TCP to the Apple APN servers. For more information about how to add an Access Rule, see [How to Create a Pass Access Rule](#).

8. (optional) Click the **Client Action** tab. The **EVENTS** tab on Barracuda Firewall 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 Barracuda Firewall Admin.
- **Audio Alert** – A WAV audio file is played.



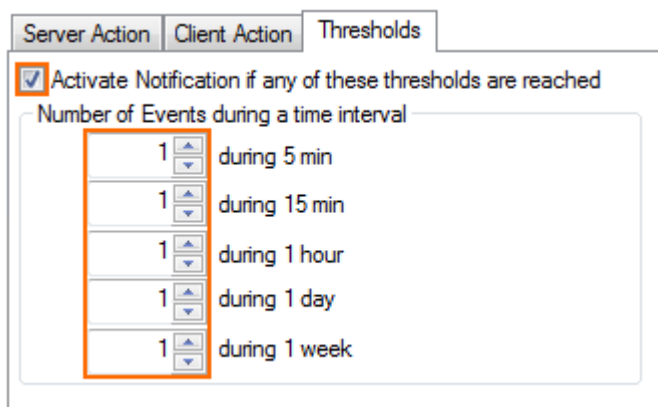
3. Click **OK**.

9. Click the **Thresholds** tab.

1. Click the check box to enable these thresholds before activating the notification. Note that notifications are activated if any of the configured thresholds are reached during the configured time interval.

2. For each of the given time intervals – Adjust the minimum of events that are necessary during the related time interval to trigger a notification.

Example: 2 during 5 min. If 2 events occur within the period of 5 minutes, then a notification will be sent.



Number of Events during a time interval	
1	during 5 min
1	during 15 min
1	during 1 hour
1	during 1 day
1	during 1 week

3. Click **OK**.

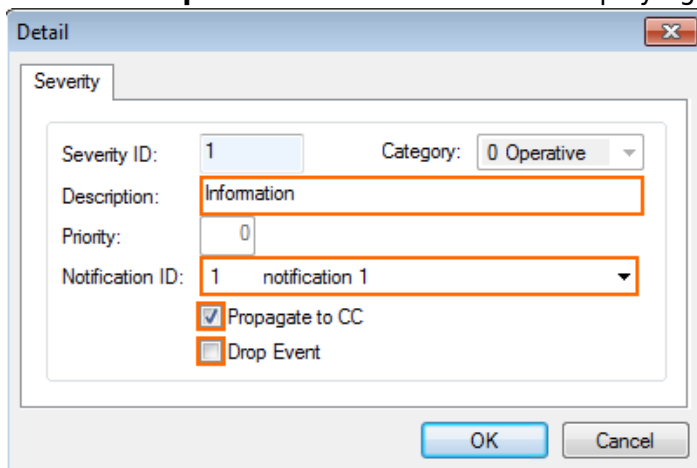
10. Click **Send Changes** and **Activate**.

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.

Events   Severity   Notification   Basic								
ID	Description	Severity	Notification	Pers.	Prop.	Drop		
10	Disk Space Low	2 Warning	1 notification 1	yes	yes	no		
11	Disk Space Critical	3 Error	1 notification 1	yes	yes	no		
20	Memory Low	2 Warning	1 notification 1	yes	yes	no		
21	Memory Critical	3 Error	1 notification 1	yes	yes	no		
30	High System Load	2 Warning	1 notification 1	yes	yes	no		
31	Excessive System Load	3 Error	1 notification 1	yes	yes	no		
34	Critical System Condition	3 Error	1 notification 1	yes	yes	no		
35	Power Outage	3 Error	1 notification 1	yes	yes	no		
36	Power Restored	1 Information	1 notification 1	yes	yes	no		
48	Device Mismatch	3 Error	1 notification 1	no	yes	no		
49	Device Activation Failed	3 Error	1 notification 1	no	yes	no		
50	Device Down	3 Error	1 notification 1	yes	yes	no		

Lookup: 34

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

**Event**

Event ID: 34

Description: Critical System Condition

Severity ID: 3 Error

Notification ID: 0 from severity

Comment:

☒ Persistent  
☒ Propagate to CC  
☐ Drop Event

- Click **OK**.
- Click **Send Changes** and **Activate**.

## Figures

1. eventing\_set\_basic\_configuration\_silent\_logging.png
2. events\_04.png
3. server\_action\_checkbox\_mail.png
4. server\_action\_checkbox\_option\_execute\_program.png
5. server\_action\_checkbox\_option\_SNMP.png
6. server\_action\_checkbox\_option\_apple\_push.png
7. events\_08a.png
8. events\_09.png
9. events\_02.png
10. events\_01.png
11. events\_10.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.