

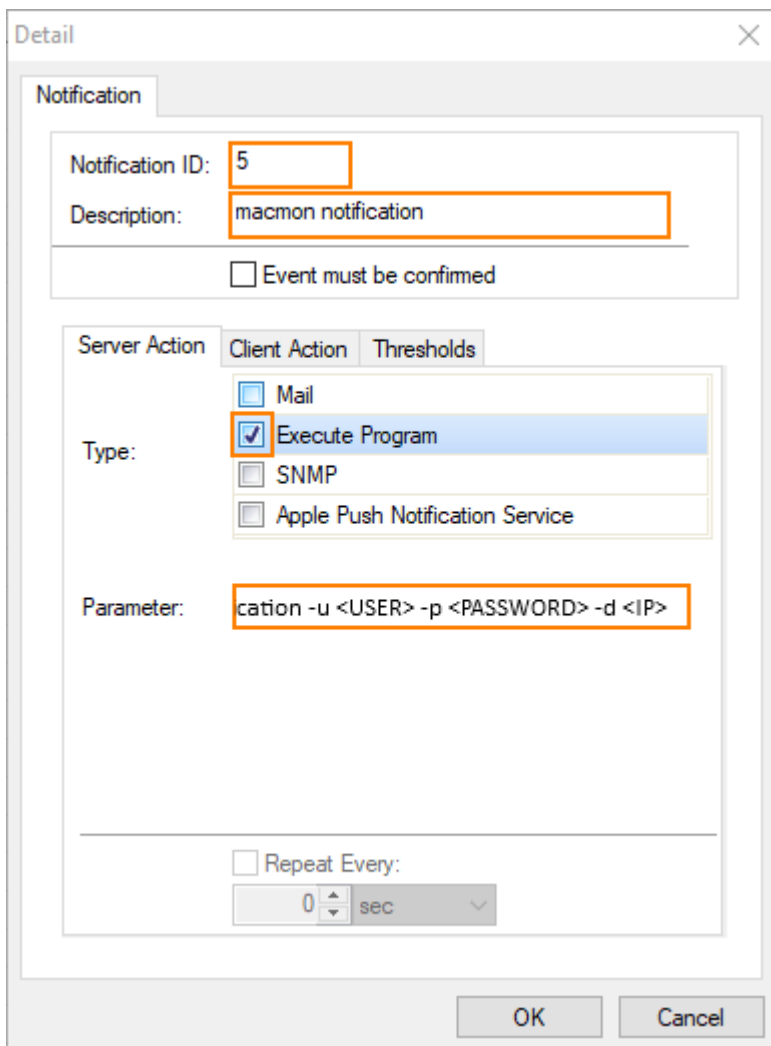
How to Configure macmon Event Notifications to Report an ATP Incident to the macmon System

<https://campus.barracuda.com/doc/79467391/>

macmon Endpoint Security and Network Access Control is capable of collecting threat notifications from other systems in order to protect a network infrastructure from malicious clients. The CloudGen Firewall can be configured to send notifications to the macmon system as soon as ATP detects a threat. If this happens, an event is created. To notify macmon about the event, a script has to be associated with the event. As soon as the event occurs, the configured script is executed and notifies macmon.

Step 1. Create a New Notification for macmon and Assign the macmon Script

1. Go to **CONFIGURATION > Configuration Tree > Infrastructure Services > Eventing**.
2. Click **Lock**.
3. Select **Notification**.
4. Click **New...** in the lower-right corner of the window.
5. The **Detail** window opens.
6. Enter a unique number as the **Notification ID**, e.g., 5.
7. Enter a descriptive name for the macmon notification, e.g., macmon notification.
8. Ensure that the check box **Event must be confirmed** is not selected.
9. Select **Server Action**.
10. For **Type**, select **Execute Program**.
11. For **Parameter**, enter the following string into the edit field. Replace the strings in the angle brackets by real values that are significant for your macmon system:
`/opt/phion/modules/box/boxsrv/event/bin/macmonEventNotification -u <USER> -p <PASSWORD> -d <IP>`



Detail

Notification

Notification ID: 5

Description: macmon notification

☐ Event must be confirmed

Server Action **Client Action** **Thresholds**

Type:

- ☐ Mail
- ☒ Execute Program
- ☐ SNMP
- ☐ Apple Push Notification Service

Parameter: cation -u <USER> -p <PASSWORD> -d <IP>

☐ Repeat Every: 0 sec

OK Cancel

The following list contains the list of valid arguments which are also used for configuring the script as seen above:

Argument	Meaning
-h, --help	Show help message and exit
-u <USER>, --user=<USER>	macmon user name
-p <PASSWORD>, --password <PASSWORD>	macmon password
-d <DESTINATION>, --destination=<DESTINATION>	macmon destination (hostname or IP address)

12. Click **OK**.
13. Click **Send Changes**.
14. Click **Activate**.

Step 2. Check Your Event List

1. Go to **EVENTS**.
2. Check the event list for ATP events. If the notification ID (e.g. ID=5) refers to the configuration set before, the macmon system has been notified about the event.

4402	Subsystem Release Update S
4404	Subsystem Release Update C
4406	Subsystem Release Update A
4408	Firmware Update Failed
4410	Release Inconsistencies Dete
4412	Active Kernel not in RPM-DB
4450	New Software Update
4460	New Product Tip
4500	Mail Data Discarded
4504	Mail Operation Changed
4506	Mail Delivery Refused
4508	Mail Relaying Denied
4512	Mail Rule Notice
4513	Mail Rule Warning
4514	Mail Rule Alert
4600	Attempted Illegal Assignment
5000	User added to ATP quaran
5001	ATP malicious activity detected

Detail

Event

Event ID: 5001

Description: ATP malicious activity detected

Severity ID: 2 Warning

Notification ID: 5 notification 1 - macm

Comment:

☒ Persistent

☒ Propagate to CC

☐ Drop Event

OK

Cancel

5001	ATP malicious activity detected	2	Warning	1	notification 1	yes	yes	no
------	---------------------------------	---	---------	---	----------------	-----	-----	----

Figures

1. `configure_macmon_notification.png`
2. `macmon_malicious_activity_detected.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.