Minimizing SBA Notifications with Check Point GuiDBedit

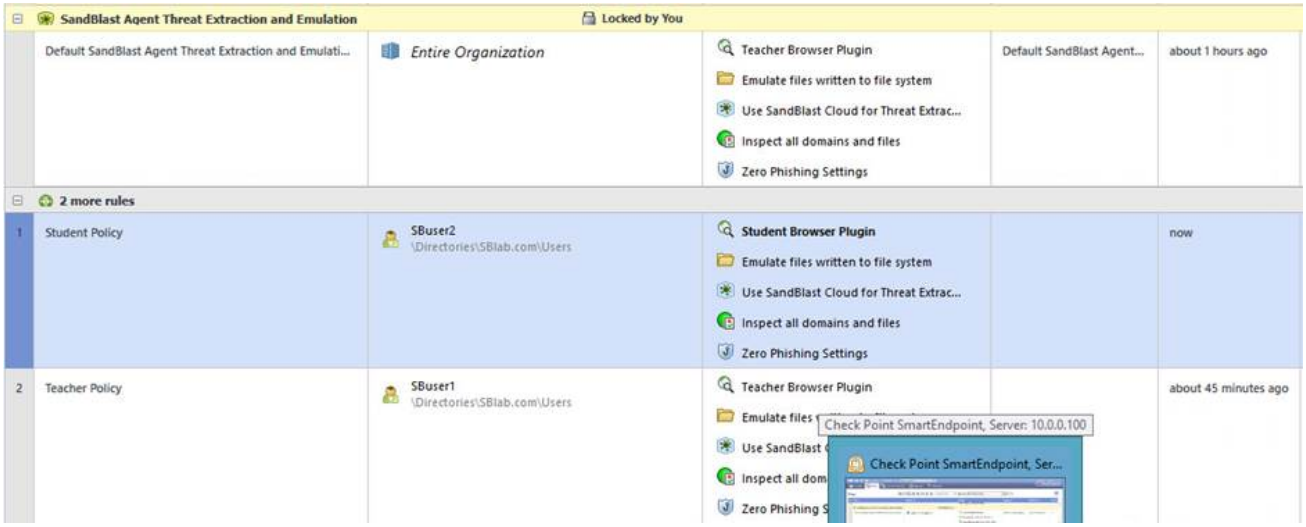
Krzysztof (Chris) Biernacki
Security Engineer – Western Canadian

In some cases, customers needs to minimize notifications to end user as they may get overwhelmed with the notifications. This document will allow you to minimize SBA notifications by modifying the policy using Check Point Database Tool (GuiDBedit).

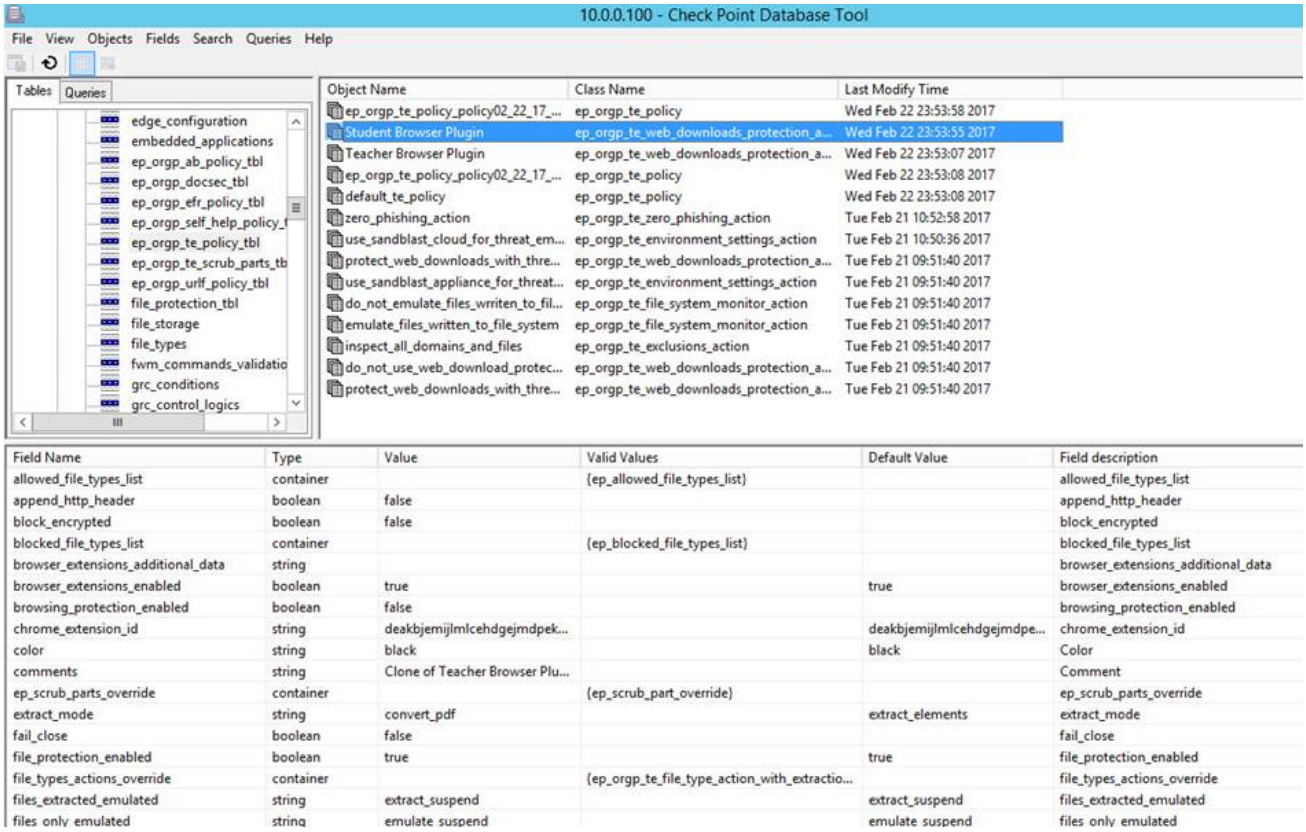
Please refer to sk13009 before proceeding:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk13009

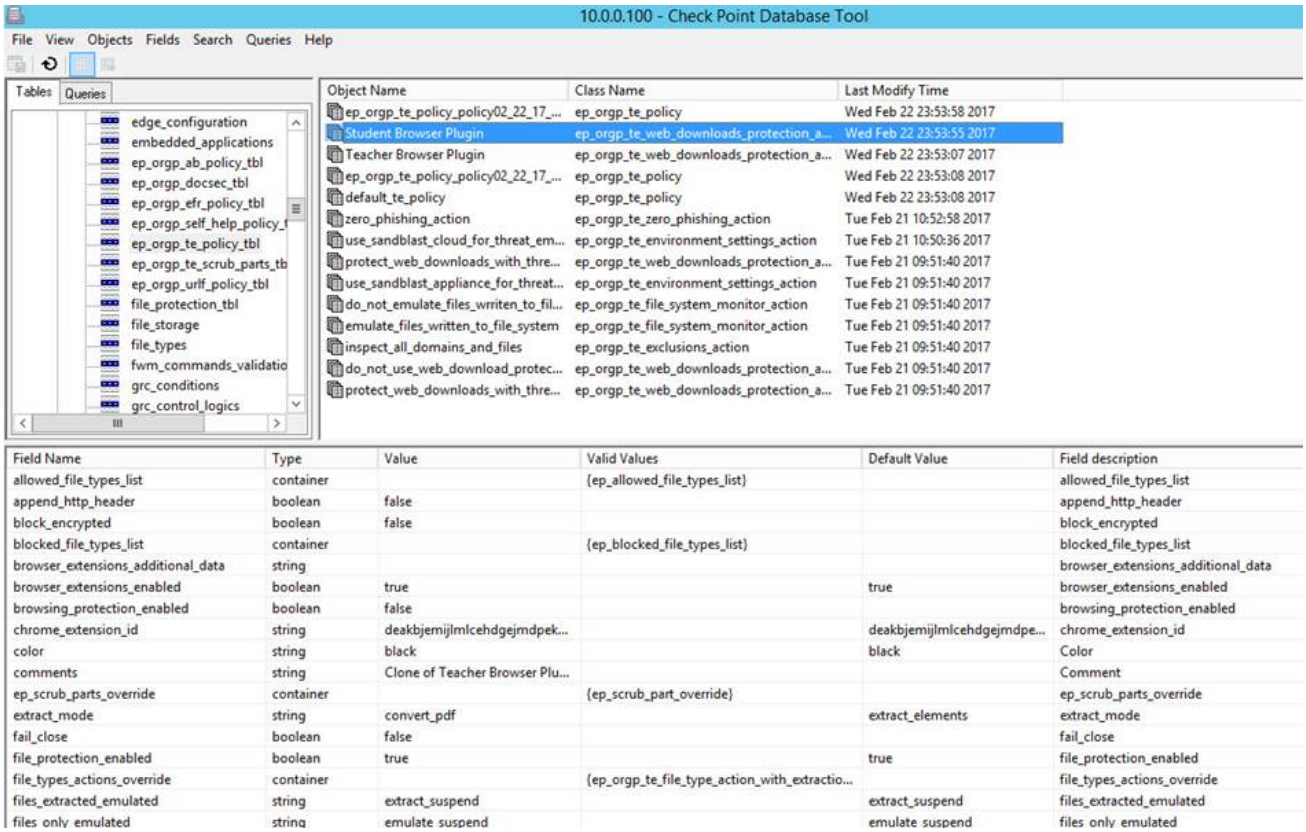
You will want to go to the following: Other -> ep_orgp_te_policy_tbl and you can then go in and edit the policy you set for the users. Show_notifications on my lab is under “Clone of Protect web downloads with Threat Extraction and Emulation”. You need to push and install policy for it to take effect.

A Policy example looks like this: I made one student policy and one teacher policy. Both clean and extract files:



Configure what you can in the GUI, then pop open GUIDBEDIT. You can see in the screenshot that I have both policies in the object list. If I click on the policy, I get the entire granularity to enable and disable notifications.





You need to edit the policy within GUIDBEDIT then you can disable the notifications. You will also need to apply the policy to a Group/User not an OU/Computer.

Procedure

The Database Tool executable - `GuiDBedit.exe` - is located in the same folder where the Smart Console is installed.

To work with database on Security Management Server / Domain Management Server, run:

On Windows OS 32-bit:
C:\Program Files\CheckPoint\SmartConsole\<*RXX*>\PROGRAM\GuiDBedit.exe

On Windows OS 64-bit:
C:\Program Files (x86)\CheckPoint\SmartConsole\<*RXX*>\PROGRAM\GuiDBedit.exe

Warning

Due to the powerful database editing abilities supplied by the tool, only experienced users should work with it. Always backup the Security Management Server / Multi-Domain Security Management Server before performing any changes in the database. Refer to sk54100 - How to back up your system.

