

Minimizing SBA Notifications with Check Point GuiDBedit

Krzysztof (Chris) Biernacki
Security Engineer – Western Canadian

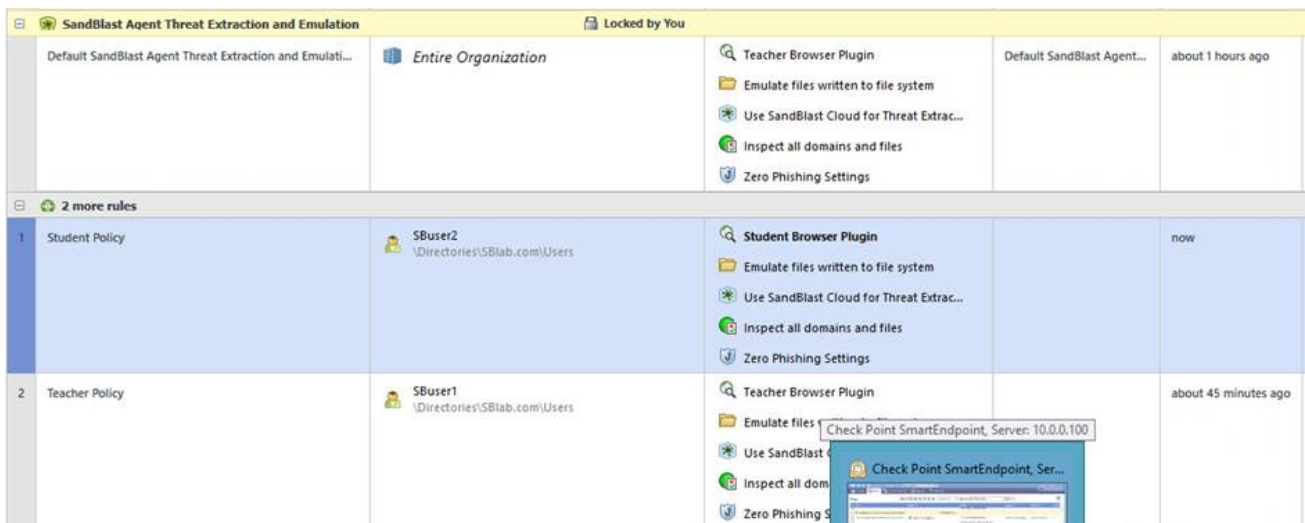
In some cases, customers need to minimize notifications to end user as they may get overwhelmed with the notifications. This document will allow you to minimize SBA notifications by modifying the policy using Check Point Database Tool (GuiDBedit).

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.

10.0.0.100 - Check Point Database Tool

File View Objects Fields Search Queries Help

Object Name	Class Name	Last Modify Time
ep_orgp_te_policy_policy02_22_17...	ep_orgp_te_policy	Wed Feb 22 23:53:58 2017
Student Browser Plugin	ep_orgp_te_web_downloads_protection_a...	Wed Feb 22 23:53:55 2017
Teacher Browser Plugin	ep_orgp_te_web_downloads_protection_a...	Wed Feb 22 23:53:07 2017
ep_orgp_te_policy_policy02_22_17...	ep_orgp_te_policy	Wed Feb 22 23:53:08 2017
default_te_policy	ep_orgp_te_policy	Wed Feb 22 23:53:08 2017
zero_phishing_action	ep_orgp_te_zero_phishing_action	Tue Feb 21 10:52:58 2017
use_sandblast_cloud_for_threat_em...	ep_orgp_te_environment_settings_action	Tue Feb 21 10:50:36 2017
protect_web_downloads_with_thre...	ep_orgp_te_web_downloads_protection_a...	Tue Feb 21 09:51:40 2017
use_sandblast_appliance_for_threat...	ep_orgp_te_environment_settings_action	Tue Feb 21 09:51:40 2017
do_not_emulate_files_writen_to_fil...	ep_orgp_te_file_system_monitor_action	Tue Feb 21 09:51:40 2017
emulate_files_writen_to_file_system	ep_orgp_te_file_system_monitor_action	Tue Feb 21 09:51:40 2017
inspect_all_domains_and_files	ep_orgp_te_exclusions_action	Tue Feb 21 09:51:40 2017
do_not_use_web_download_protect...	ep_orgp_te_web_downloads_protection_a...	Tue Feb 21 09:51:40 2017
protect_web_downloads_with_thre...	ep_orgp_te_web_downloads_protection_a...	Tue Feb 21 09:51:40 2017

Field Name	Type	Value	Valid Values	Default Value	Field description
allowed_file_types_list	container		{ep_allowed_file_types_list}		allowed_file_types_list
append_http_header	boolean	false			append_http_header
block_encrypted	boolean	false			block_encrypted
blocked_file_types_list	container		{ep_blocked_file_types_list}		blocked_file_types_list
browser_extensions_additional_data	string				browser_extensions_additional_data
browser_extensions_enabled	boolean	true		true	browser_extensions_enabled
browsing_protection_enabled	boolean	false			browsing_protection_enabled
chrome_extension_id	string	deakbjemijmlcehdgejmdpek...		deakbjemijmlcehdgejmdpek...	chrome_extension_id
color	string	black		black	Color
comments	string	Clone of Teacher Browser Plu...			Comment
ep_scrub_parts_override	container		{ep_scrub_part_override}		ep_scrub_parts_override
extract_mode	string	convert_pdf		extract_elements	extract_mode
fail_close	boolean	false			fail_close
file_protection_enabled	boolean	true		true	file_protection_enabled
file_types_actions_override	container		{ep_orgp_te_file_type_action_with_extractio...		file_types_actions_override
files_extracted_emulated	string	extract_suspend		extract_suspend	files_extracted_emulated
files only emulated	string	emulate_suspend		emulate_suspend	files only emulated

10.0.0.100 - Check Point Database Tool

File View Objects Fields Search Queries Help

Object Name	Class Name	Last Modify Time
ep_orgp_te_policy_policy02_22_17...	ep_orgp_te_policy	Wed Feb 22 23:53:58 2017
Student Browser Plugin	ep_orgp_te_web_downloads_protection_a...	Wed Feb 22 23:53:55 2017
Teacher Browser Plugin	ep_orgp_te_web_downloads_protection_a...	Wed Feb 22 23:53:07 2017
ep_orgp_te_policy_policy02_22_17...	ep_orgp_te_policy	Wed Feb 22 23:53:08 2017
default_te_policy	ep_orgp_te_policy	Wed Feb 22 23:53:08 2017
zero_phishing_action	ep_orgp_te_zero_phishing_action	Tue Feb 21 10:52:58 2017
use_sandblast_cloud_for_threat_em...	ep_orgp_te_environment_settings_action	Tue Feb 21 10:50:36 2017
protect_web_downloads_with_thre...	ep_orgp_te_web_downloads_protection_a...	Tue Feb 21 09:51:40 2017
use_sandblast_appliance_for_threat...	ep_orgp_te_environment_settings_action	Tue Feb 21 09:51:40 2017
do_not_emulate_files_writen_to_fil...	ep_orgp_te_file_system_monitor_action	Tue Feb 21 09:51:40 2017
emulate_files_writen_to_file_system	ep_orgp_te_file_system_monitor_action	Tue Feb 21 09:51:40 2017
inspect_all_domains_and_files	ep_orgp_te_exclusions_action	Tue Feb 21 09:51:40 2017
do_not_use_web_download_protect...	ep_orgp_te_web_downloads_protection_a...	Tue Feb 21 09:51:40 2017
protect_web_downloads_with_thre...	ep_orgp_te_web_downloads_protection_a...	Tue Feb 21 09:51:40 2017

Field Name	Type	Value	Valid Values	Default Value	Field description
allowed_file_types_list	container		{ep_allowed_file_types_list}		allowed_file_types_list
append_http_header	boolean	false			append_http_header
block_encrypted	boolean	false			block_encrypted
blocked_file_types_list	container		{ep_blocked_file_types_list}		blocked_file_types_list
browser_extensions_additional_data	string				browser_extensions_additional_data
browser_extensions_enabled	boolean	true		true	browser_extensions_enabled
browsing_protection_enabled	boolean	false			browsing_protection_enabled
chrome_extension_id	string	deakbjemijmlcehdgejmdpek...		deakbjemijmlcehdgejmdpek...	chrome_extension_id
color	string	black		black	Color
comments	string	Clone of Teacher Browser Plu...			Comment
ep_scrub_parts_override	container		{ep_scrub_part_override}		ep_scrub_parts_override
extract_mode	string	convert_pdf		extract_elements	extract_mode
fail_close	boolean	false			fail_close
file_protection_enabled	boolean	true		true	file_protection_enabled
file_types_actions_override	container		{ep_orgp_te_file_type_action_with_extractio...		file_types_actions_override
files_extracted_emulated	string	extract_suspend		extract_suspend	files_extracted_emulated
files only emulated	string	emulate_suspend		emulate_suspend	files only emulated

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](#).