

## Sandblast Agent Best Practices – Server Policies – December 2019 – R80.30/E82.XX

### Overview

This guide will cover the recommended SBA & Anti-malware settings for Microsoft server platforms. Use this document as a starting off point to your recommended and tested best practices.

### Architecture Best practices and information





- If your environment has more than 2,000 clients it is recommended to include a policy server(s). Policy servers are used for deployment of blade packages, policies, & logging.
- When deploying Sandblast Agent to clients, it is recommended to do a staggered deployment consisting of 100 clients at time (maximum of 400 clients). SBA deployment packages are large and you may saturate your network or take up the majority of your bandwidth on WAN/VPN links.
- If you have a hub and spoke network, it is recommended to place policy servers at remote locations.
- Do not use the default policy on each blade. It is recommended to clone the default policy and rename it for its purpose. Ex. Endpoints, Server, Finance, Troubleshooting, etc
- Create a single policy for each blade that disables the protection of that blade. Name it “Troubleshooting/Disabled xxxxxx Policy”. When troubleshooting an issue with an endpoint/server you or your staff should....
  - Determine which blade is causing the issue.
  - As a troubleshooting step, place that endpoint/server into the troubleshooting policy.
  - Test
  - Determine the cause and either create an exclusion or reach out to Check Point TAC.
  - DO NOT disable the blade for all endpoints/servers.
  - DO NOT make an exclusion in every blade.
- If you need assistance with compiling a list of common application exclusions including file path, please visit the following link  
<https://social.technet.microsoft.com/wiki/contents/articles/953.microsoft-anti-virus-exclusion-list.aspx>

### Server Assumptions.

- Servers are for application purposes.
- You DO NOT allow regular users to log into the server platform.
- You typically do not use the web browser on the server.
- Server(s) are segmented and protected from the LAN & WAN.

- Only necessary ports are opened for ingress/egress.
- Compile a list of server applications that require high I/O and writing to disk.

Sandblast Agent & Anti-Malware consists of the following Blades.

 <b>Anti-Malware</b>
 <b>SandBlast Agent Anti-Ransomware, Behavioral Guard and Forensics</b>
 <b>SandBlast Agent Anti-Bot</b>
 <b>SandBlast Agent Threat Extraction, Emulation and Anti-Exploit</b>







---

## **Anti-Malware**

### Overview

- Signature based anti-virus protection.
- File are scanned upon access.
- When it comes to Anti-malware updates, you may choose to host updates from the management server locally or receive updates from Check Point over the internet. The default setting is to use the local server, so if you do not setup the database locally or do not change the setting to internet updates, you may see errors after 72 hours that Anti-malware signatures haven't updated on the endpoints.

### Suggested Settings

-  Scan all files upon access
-  Check for malware signature updates every 4 ho...
-  Perform periodic anti-malware scan weekly ever...
-  Periodically scan local hard-drives only
- ▲ Advanced
  -  Optimize malware scan
  -  Quarantine detected malware

Edit Properties - Scan On Access

? X

**Select action:**

Scan all files upon access

**Description:**

All files will be scanned upon process access



Used in 2 rules

**Scan all files upon access**

Processes to exclude from scan :

 Add... |  Edit... |  Remove |  

Process Path

 Detect Unusual Activity Enable Cloud Reputation Services for Files, Web Resources and ProcessesConnection Timeout  ms Enable Web Protection

Mail Protection

 Scan Mail Messages

OK

Cancel

- Exclusion area: What are the key applications on the server that are deemed safe? Excluding safe applications allows them to run as intended without security scanning. Exclusion locations could be where the application is installed as well as any cache folders used by the application. This is assuming that the application doesn't dump or export any files into these folders that could have the chance of being malicious.

**Select action:**

Check for malware signature updates every 2 hours ▾

**Description:**

Signature update will occur every 2 hours , from endpoint policy server and Check Point server

**Check for malware signature updates every 2 hours**

Updater interval: 2 ▾ hours

Signature update will fail after: 60 ▾ seconds without server response

Update signatures from:

Signature Source: Local Endpoint Servers ▾

 If first update fails: External Check Point Signatures Server ▾ If second update fails: Other external source 

OK

Cancel

- Please evaluate what update time interval you would like to use for signature updates.
- Adjust configuration to decide where anti-malware updates come from.

Edit Properties - Periodical Scan Schedule

? X

**Select action:**

Perform periodic anti-malware scan weekly every Sunday at 12 PM

**Description:**

Perform periodic anti-malware scan weekly every Sunday at 12 PM

[Edit Name & Description...](#)**Perform periodic anti-malware scan weekly every Sunday at 12 PM**

Scan period: Week

Day of week: Sunday

Day of month: 1

Scan start hour: 12:00

 Run initial scan after Anti-Malware Blade installation. Allow user to cancel scan. Prohibit cancel scan if more than 30 days passed since last successful scan.

OK

Cancel

- Determine and set when scheduled scans should kick off.
- If you are confident that the server you are deploying to is clean from any threats, you may uncheck the “Run Initial Scan after Anti-malware Blade installation”.
- “Allow user to cancel scan” can be enabled. This may be useful for when an admin is working on the server or if the server is heavily taxed performing a scan during peak hours.

Edit Properties - Scheduled Scan Targets ? X

**Select action:**

Periodically scan local hard-drives only

**Description:**


Schedule scan will scan local drives only

Used in 2 rules

**Periodically scan local hard-drives only**

## Scan Targets

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Critical areas | <input type="checkbox"/> Removable drives     |
| <input type="checkbox"/> Optical drives            | <input type="checkbox"/> Unrecognized devices |
| <input checked="" type="checkbox"/> Local drives   | <input type="checkbox"/> Network drives       |
| <input type="checkbox"/> Mail messages             |   |

## Scan Target Exclusions

- Skip archives and non executables
- Do not scan files larger than:  MB

[Configure files and folders exclusions](#)





OK

Cancel

- If you would like to make exclusions from the scheduled scans, click on the blue link labeled “Configure files and folders exclusions”.

Scan Files and Folders Exclusions ? X

## Files and folders to exclude from scan:

 Add... |  Edit... |  Remove |  

File \ Folder
C:\Program Files (x86)\Microsoft SQL Server\
C:\Program Files\Microsoft SQL Server\
.mdf
.ldf
.ndf

OK

Cancel

Edit Properties - Scan Optimization

? X

**Select action:**

Optimize malware scan

**Description:**


Anti-Malware Scan only checks files that have not been scanned before and files that have been altered since last scan.



Used in 2 rules

**Optimize malware scan**

- Perform scan optimizations
- Scan priority will be lower than other running processes

OK

Cancel

- If you would like to shorten the scheduled scan you may enable “Scan Optimization” which will only scan new or altered files since the last completed scheduled scan.
- To conserve resources on Server platforms, you have the option to give Anti-Malware scheduled scan a lower priority than other running processes.

Edit Properties - Malware Treatment

? X

**Select action:**

Quarantine detected malware

**Description:**


In case malware is detected, the files are isolated from the OS, but are not permanently removed. The user can restore quarantined files, if they are not malicious.



Used in 2 rules

**Quarantine detected malware**

Malware Treatment:

[Exclude infections by name](#)

- Quarantine file if cure failed
- Delete file if cure failed

[Configure threat cloud knowledge sharing](#)

Threat Cloud Sharing

? X

- Allow sending infection info and statistics to Check Point servers for analysis
- Allow sending infected file samples to Check Point servers for analysis


OK

Cancel

OK

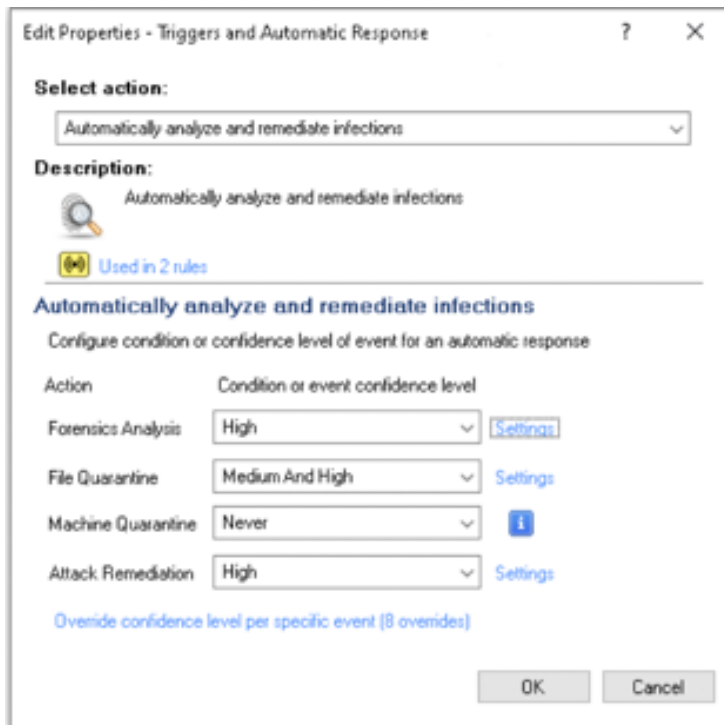
Cancel

- Depending on your corporate policies and compliance, it may make sense to disable the sending of information and files to Check Point. It is recommended to keep these two options enabled.


**SandBlast Agent Anti-Ransomware, Behavioral Guard and Forensics**

### Anti-Ransomware, Behavior Guard and Forensics Blade Overview

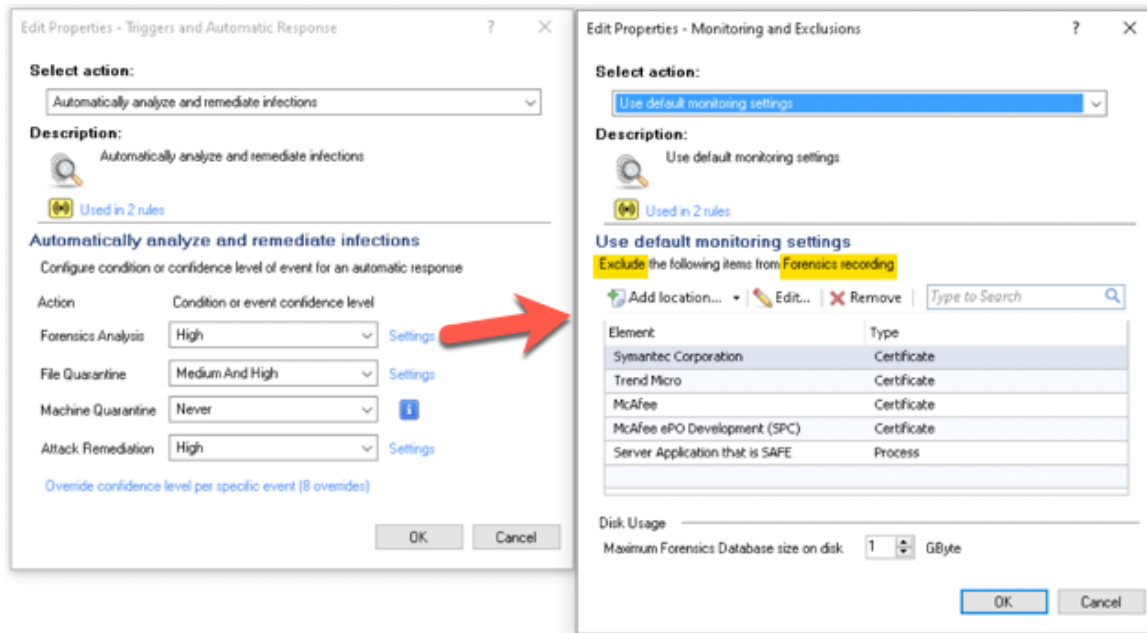
- Anti-Ransomware is an automated process that can take point in time backups of user file data as an executable is trying to read and write to the file system. The process creates honeypot folders and also creates a vaulted folder where the backup files are stored and are only readable by the Check Point system account. This process does not use any 3rd party backup solutions that are built into the operating system.
- Behavior Guard uses real-time dynamic analysis to determine what an executable is trying to do and if it resembles a malware family. BG looks for zero-day behaviors and with the help of other blades stops threats in real-time.
- Forensics helps from an EDR perspective by having a process running to monitor and log what executables do so that in the case of an event, the end user or admin can see a forensics report and save precious time to try and figure out what happened.



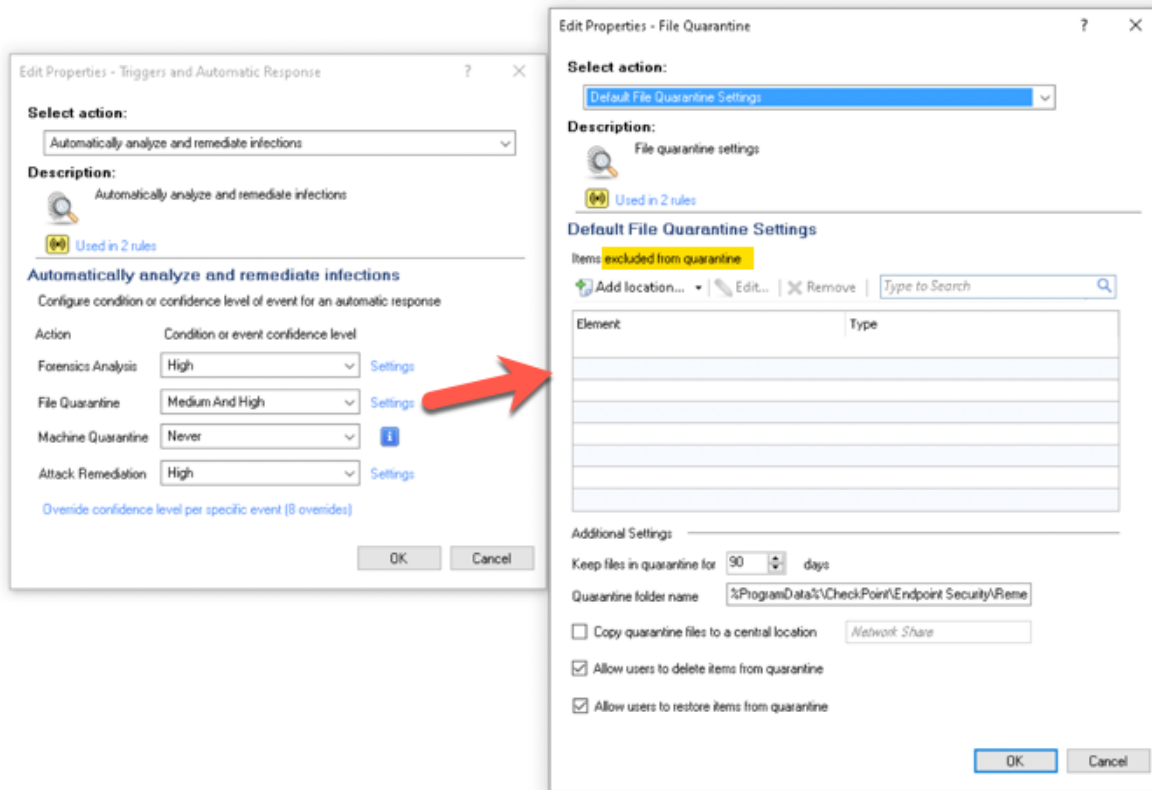
- The Forensics Analysis engine takes up the bulk of resources used by the Sandblast Agent client. This engine runs in the background collecting data in real-time. This process may slow down individual applications. So, as a best practice we are looking specifically for applications that have a lot of I/O and thrashing of disks. Once you have



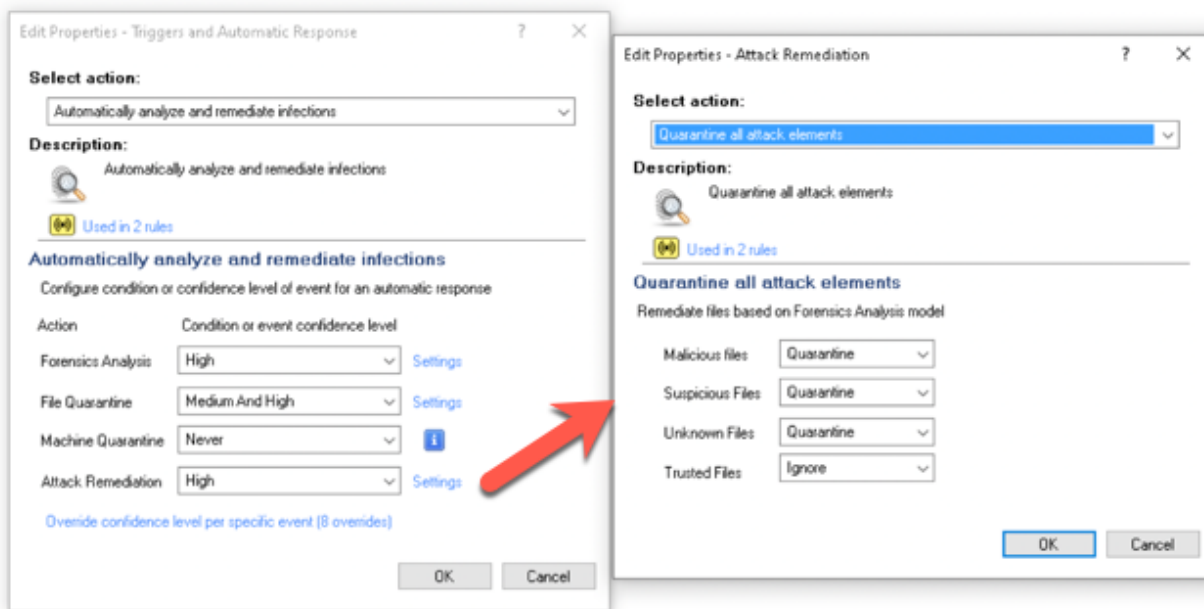
tested and determined the applications that are affected and deemed to be safe, it is recommended to add the application, the folder installation and any cache folders to the exclusion area.

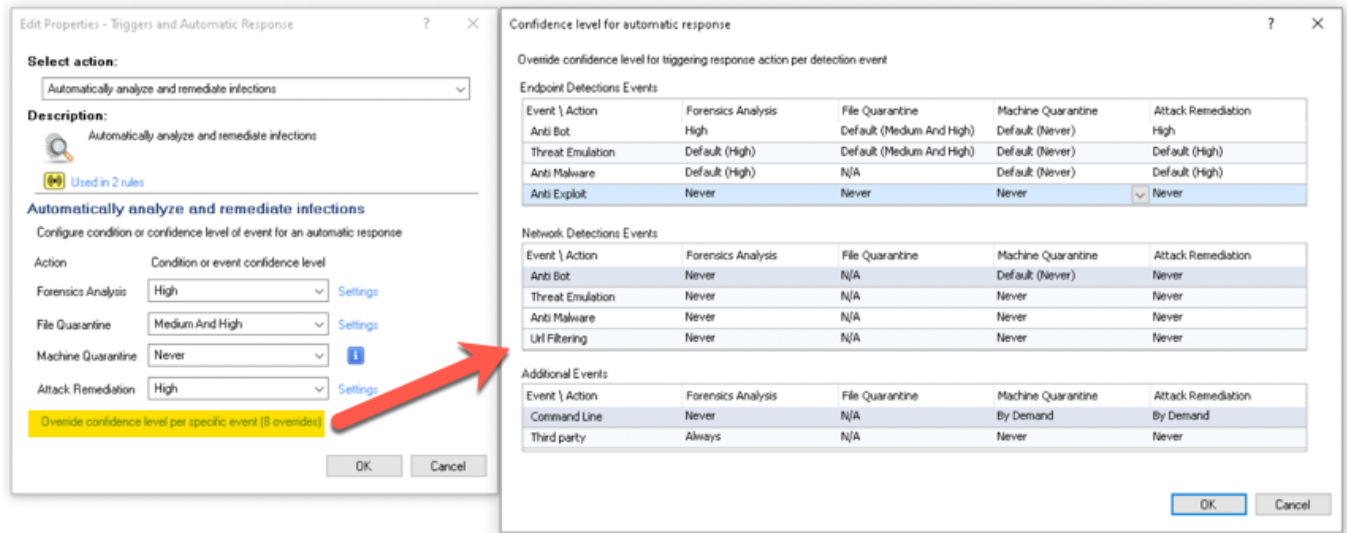


- The above graphic displays where you would input the exclusions for Forensics Analysis. Be 100% certain that whatever you exclude is deemed clean and secure. It is a best practice to provide the full path to folders and executable. The primary reason to exclude an application here is due to performance degradation of the application.

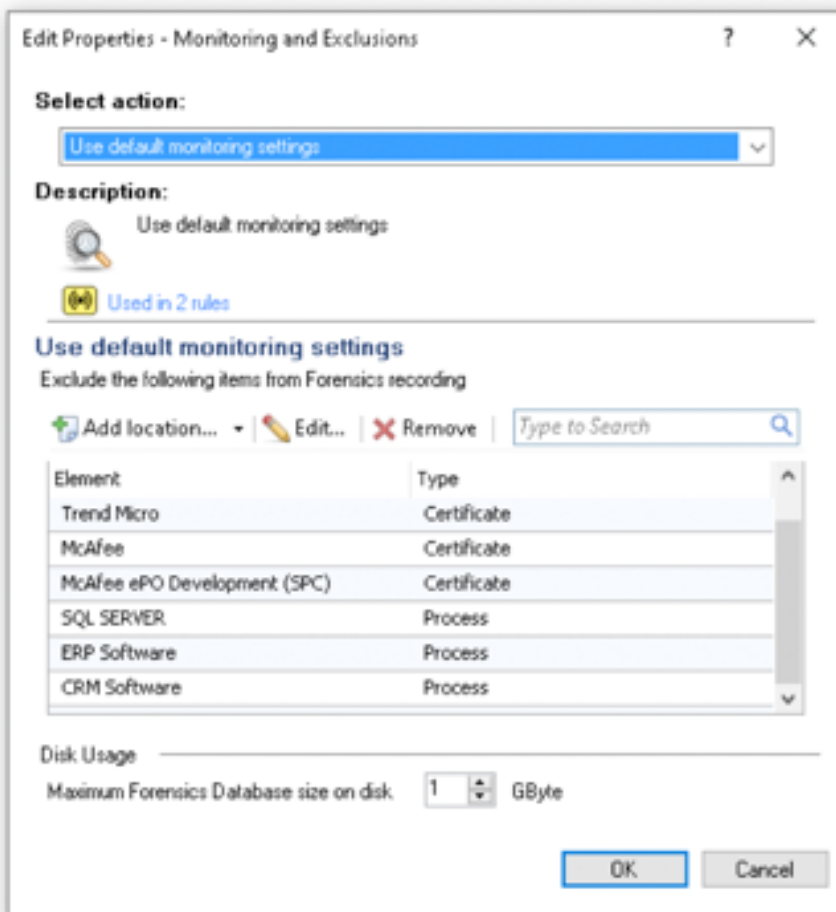


- The next section is for File quarantine exclusions and retention. It is recommended to only make exclusions here for false positives.
- Typically for endpoint clients we encourage admins to disable the ability for users to delete or restore files from the quarantine. It may make sense to keep these enabled for servers because admins should be the only ones accessing servers.





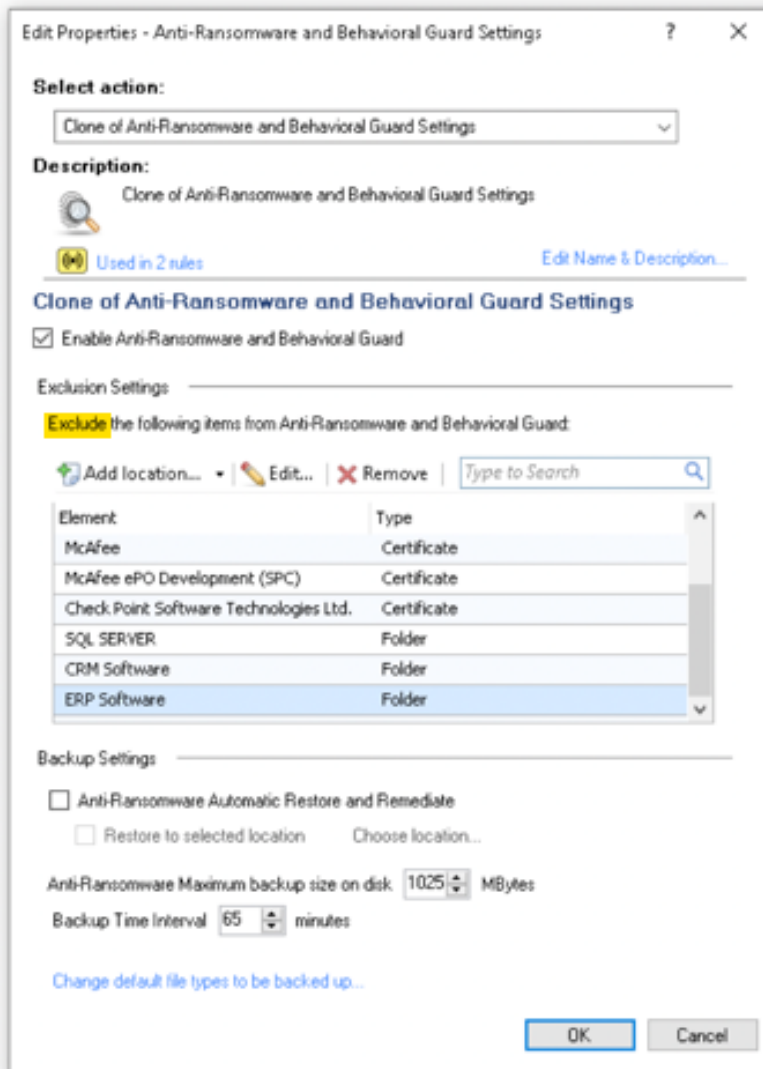
- In the override confidence level section you have the ability to be more granular with specific events and what happens.



- In the next policy section of the blade we have monitoring and exclusion settings. Again, you will want to evaluate what applications are running on the server and if their

performance is degraded due to SBA. Best practice again is to put in the full file path to the application and folder.

We now skip to the last section in the blade to Anti-Ransomware and Behavior Guard Settings

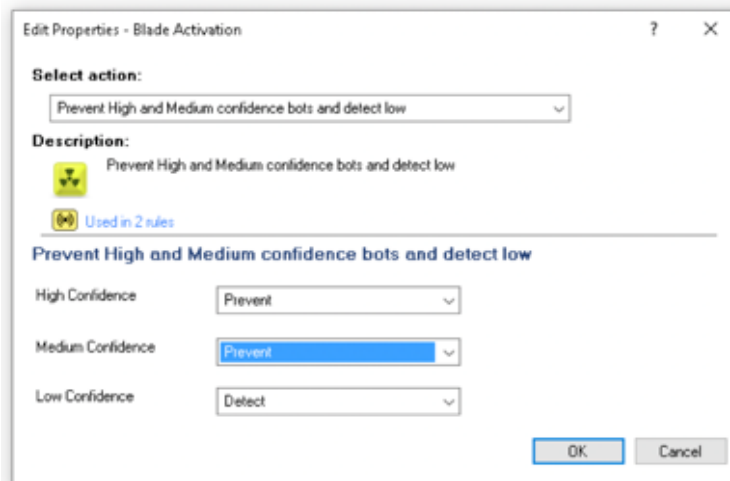


- When it comes to servers, users should never be able to have access, login or store personal files. With that being said, we still need to enable Anit-Ransomware because it is tied to Behavior Guard.
- It is recommended that if you have evaluated and determined an application to be safe, you may add it to the exclusion area.
- Since this is a server platform, it may not make sense to enable automatic AR restore and remediate, especially if server tasks are happening like moving or deleing a lot of files.


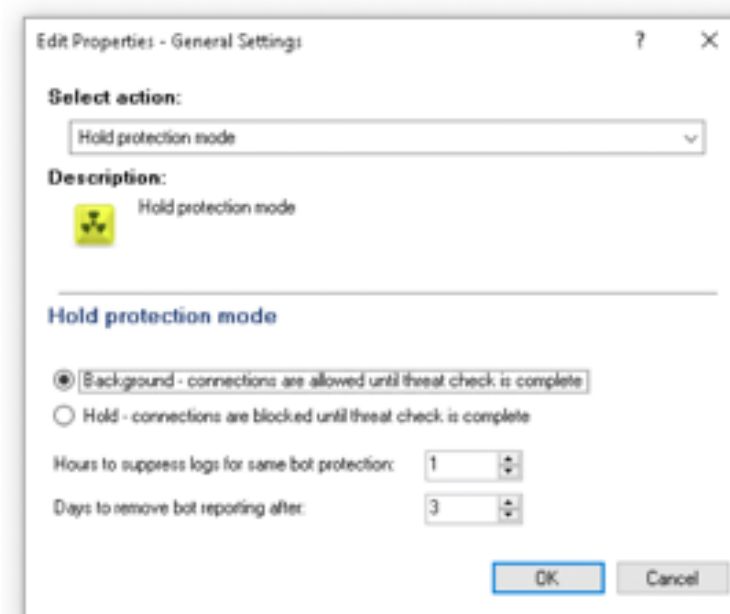
 SandBlast Agent Anti-Bot

## Anti-Bot Blade Overview

- The purpose of this blade is to monitor network traffic to see if it is reaching out to Command and Control centers for instructions on how to pull down malicious code and other instructions.



- In an ideal server setup, the admin should lock down the server to only allow outbound HTTP traffic to the Endpoint management and or policy server(s) and any other approved sites. If not, it is best to set the following settings above.

 SandBlast Agent Threat Extraction, Emulation and Anti-Exploit

## Threat Extraction, Emulation and Anti-Exploit Overview

- This multi-purpose blade is responsible for 0-day protection around file downloads from the web as well as when files are written to disk. It also monitors and does further inspection around the most vulnerable applications with Anti-exploit.
- Threat Extraction is the ability to strip out any live content that could be exploited and very quickly deliver a sanitized copy to the end user right away. This feature only works with the Browser plugin.
- Threat Emulation can run with the browser plugin as a pre-download protection, and it also can run in the background when a supported file is written to the hard disk.
- Anti-Exploit performs additional inspection around the most vulnerable applications like Microsoft Office, Internet Explorer, Edge, Flash, RDP, Java, etc

## Server considerations

- When it comes to a server platform, the administrator should not be using the web browser. There shouldn't be browsing or web downloading directly from a server.
- It is important to have Threat Emulation enabled so that files that do get written to disk are emulated in the background and checked for 0-day threats.
- We are also assuming that there are hourly, daily snapshots and backups of all the data on a server.

Directions on how to disable the installation of the browser plugin.

If you have purchased Sandblast Agent specifically for your server platforms, it may make sense to disable the installation of the browser plugin. If you are also managing client endpoints at the same time, it is not recommended to disable the browser plugin. If you make this change, it will apply to all clients connected to the Endpoint management server. To clarify, it will disable the installation of the browser plugin for all clients including endpoints and servers.

When working with SBA, Chrome extension is enabled by default, while IE can be controlled through GuiDBedit Tool as follows: **until version 80.70 (including)**, the IE is disabled by default, and can be enabled by the following procedure:

1. Close all SmartConsole windows and open the [GuiDBedit Tool](#).
2. Go to *ep\_orgp\_te\_policy\_tbl*
3. In each line with the class name *ep\_orgp\_te\_web\_downloads\_protection\_action*, find the field *browser\_extensions\_additional\_data* and add the value: ***ie\_extension\_disabled=false***
4. Save the changes: go to 'File' menu - click on 'Save All'.
5. Open SmartEndpoint Console.

6. Make a small change in a SandBlast Agent Threat Emulation rule, which will cause it to change policy version number and load changes from GuiDBedit Tool.
7. Install policy in SmartEndpoint.
8. Update policy on Endpoint

**From version 80.71**, the IE extension is enabled by default, and can be disabled by following the below procedure:

1. Close all SmartConsole windows and open the [GuiDBedit Tool](#).
2. Go to `ep_orgp_te_policy_tbl`
3. In each line with the class name `ep_orgp_te_web_downloads_protection_action`, find the field `browser_extensions_additional_data` and add the value: **`ie_extension_disabled=true`**
4. Continue with the steps 4 - 8 from the above instructions.

**Starting from version 80.81**, the Firefox extension is supported in EA quality for Firefox browsers version 57 and up.

The Firefox extension is disabled by default, and can be enabled by the following procedure:

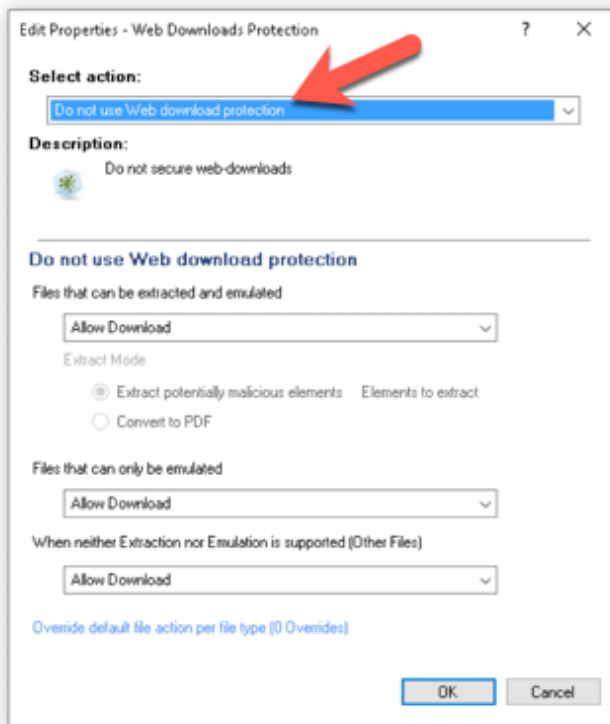
1. Close all SmartConsole windows and open [GuiDBedit Tool](#).
2. Go to `ep_orgp_te_policy_tbl`
3. In each line with the class name `ep_orgp_te_web_downloads_protection_action`, find the field `browser_extensions_additional_data` and add the value:  
**`firefox_extension_disabled=false`**
4. Continue with the steps 4 - 8 from the above instructions.

**Note:** Multiple value can be configured with semicolon (;) symbol as delimiter.

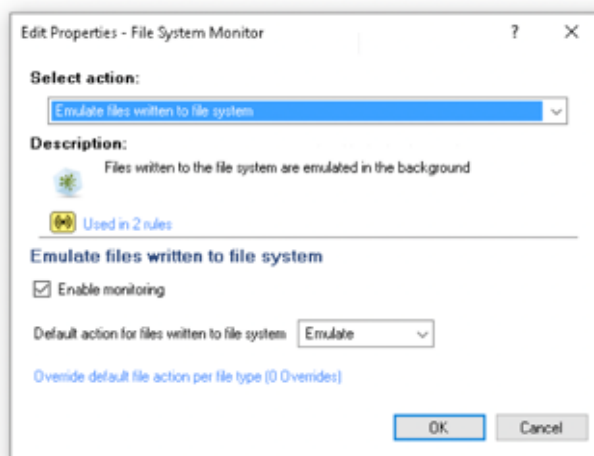
Or as an alternative, you can disable both Chrome and IE by changing the following field.

Modify the field `browser_extension_enabled` from true to false.

## Suggested Configuration options

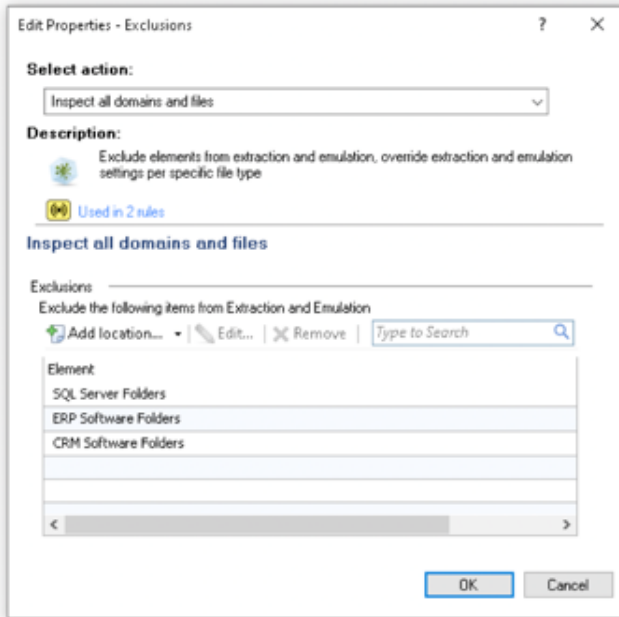


In the web downloads area, select from the dropdown to “Do Not Use Web Download Protection”

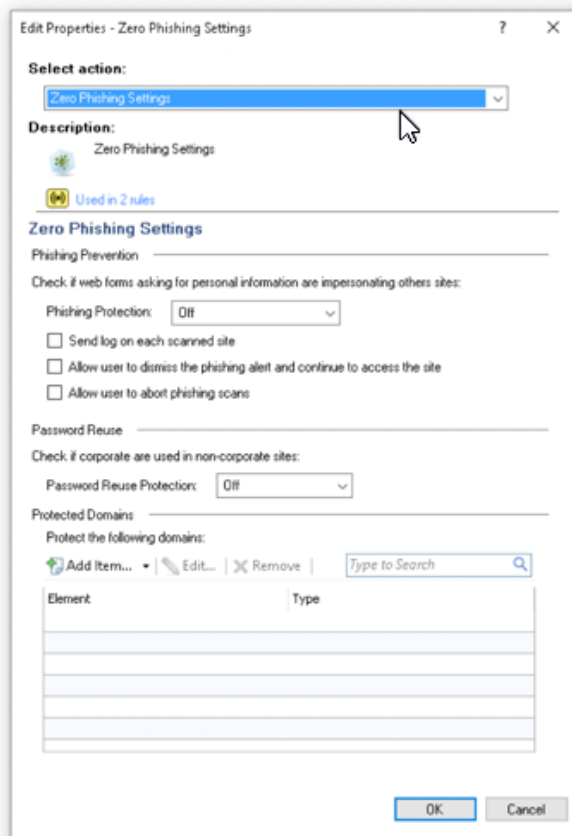


It is recommended that we still Emulate files written to disk. This will be done in the background and will not interfere with the server’s operations.

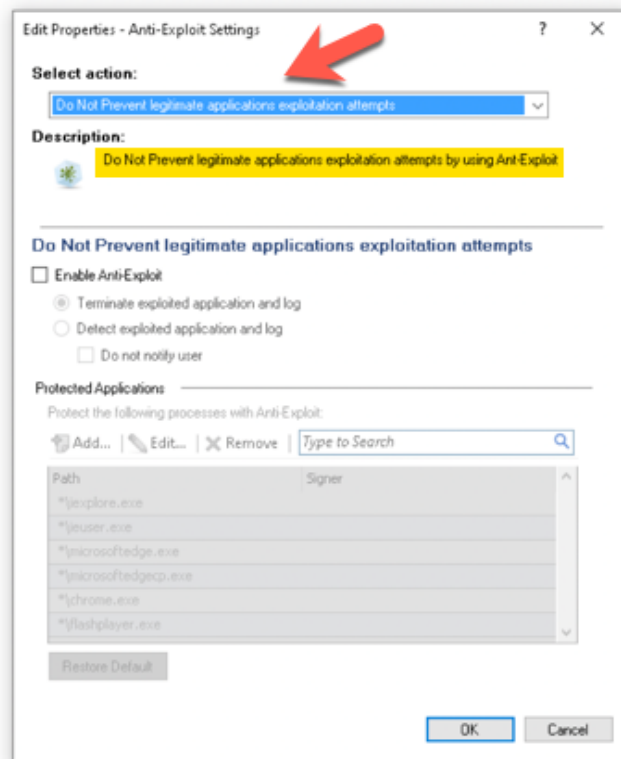




You do have the option under exclusions to add locations and folders of applications you deem to be safe. Only put exclusions of applications you know to be safe. We are only emulating file types that are supported by Threat Emulation. An example would be an application that generates dozens of PDF files to hard disk. These files being generated on the server, should not introduce a security risk and may not need to be emulated.



Zero Phishing and Password Reuse are included in the Browser plugin. It is assumed that admins are not accessing the internet or inputting passwords on a web browser on a server. If you decide to disable the browser plugin deployment, it also makes sense to turn these protections off completely.



### Anti-Exploit Engine

- The Anti-exploit engine further evaluates the most vulnerable applications that are highly exploitable. This includes internet explorer, java, flash, office as well as new protections around the remote desktop protocol.
- It is recommended to enable Anti-exploit especially for RDP protections around vulnerabilities like BlueKeep.  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>
- Please make note that the “Protected Applications” area of the blade is an **“inclusion”** not an exclusion area. Admins should make sure they don’t accidentally add exclusions from other blades into this area. If this is done by mistake, the applications and folder paths that have been added may not function as intended or may experience performance degradation.