vmware

Carbon Black
App Control

Rapid Config Guide

Product Version: 1.8

Document Version: 1.0, February, 2021

Copyrights and Notices

VMware Carbon Black
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400
Fax: 617.393.7499
Web Site: http://www.carbonblack.com
Support E-mail: support@carbonblack.com
User Exchange (Carbon Black Community): https://community.carbonblack.com

Table of Contents

Introduction

This document lists and describes the rapid configs included in Rules Installer v1.8.

Beginning with App Control 8.1.4, agent installers and the rule file that determines their behavior are no longer included as part of an App Control Server installation. You upload rule installer packages separately after you install the server. This allows VMware Carbon Black more flexibility to make new and improved rules available to you independent of server releases.

Important: You must install at least version 8.1.4 CB Protection Server before using the Rules Installer.

Customers who are performing a fresh (non-upgrade) installation of the VMware Carbon Black App Control Server will need to install the Rules Installer before deploying agents. For customers upgrading the App Control Server, we strongly recommend that you install the latest Rules Installer after the server upgrade.

See: "Installing the Rules Installer" on page 7

TIP: You can obtain the latest App Control downloads and documentation on the exchange using this repository: Repository of Carbon Black App Control 8.x Documentation & Downloads

Intended Audience

This documentation provides information for administrators, incident responders, and others who will operate the VMware Carbon Black App Control Console. Staff who manage Carbon Black App Control activities should be familiar with the Microsoft Windows operating system, web applications, desktop infrastructure (especially in-house procedures for software roll-outs, patch management, and anti-virus software maintenance), and the effects of unwanted software.

In addition, if you intend to use features that integrate App Control and Active Directory, you should be familiar with Active Directory concepts and use. Although not necessary for day-to-day users, knowledge of SQL Server management is required for the administrator of the App Control database server at your site.

App Control administrators should also be familiar with the operating systems of clients managed by the App Control server, as well as the software installed on them.

APPLICABILITY NOTE: This content applies to the 1.8.x Rules Installer.

Related Documentation

You will need some or all of the following documentation to accomplish tasks not covered in this user guide. They are available on the Carbon Black User Exchange, specifically, at: Repository of Carbon Black App Control Documentation & Downloads.

Some of these documents are updated with every new released build while others are updated only for minor or major version changes:

- *VMware Carbon Black App Control Operating Environment Requirements*

  This describes the hardware and software platform requirements for App Control Server, the SQL Server database that stores App Control data, and the App Control Agent.

- *VMware Carbon Black App Control Installation Guide*

  This includes instructions for initial installation of the App Control Server and for upgrades of the server from previous releases. Note that installation of *agents* is described in this document.

- *VMware Carbon Black App Control Release Notes*

  This document is specific to the version and build of App Control Server you received. It contains information about new features, corrective content, and known issues with the release.

- *VMware Carbon Black App Control Events Guide*

This document provides a detailed inventory of events recorded by the App Control Server and includes instructions for integrating event data with third-party SIEM systems via Syslog.

- *VMWare Carbon Black App Control Supported Agent Operating Systems*

  The supported operating systems for the current version of the App Control Agent are listed on the Carbon Black User Exchange at https://community.carbonblack.com/t5/Documentation-Downloads/Supported-Carbon-Black-sensors-and-agents/ta-p/33041.

Community Resources

In addition to being a source for user documentation, the Carbon Black User Exchange website at https://community.carbonblack.com provides access to information shared by Carbon Black customers, employees and partners. It includes information and community participation for users of all Carbon Black products.

When you login to this resource, you can:

- ask questions and provide answers to other users' questions
- "vote" to bump up the status of product ideas
- download the latest user documentation
- participate in the Carbon Black developer community by posting ideas and solutions or discussing those posted by others
- view the training resources available for Carbon Black products

NOTE: You must have a login account to access the User Exchange. Contact your Technical Support representative if you need to get an account.

Contacting Support

Please view our Customer Support Guide on the User Exchange for more information about Technical Support:

https://community.carbonblack.com/t5/Support-Zone/Guide-to-Carbon-Black-Customer-Support/ta-p/34324

For your convenience, VMware Carbon Black Technical Support offers several channels for resolving support questions:

- Carbon Black User Exchange:

  https://community.carbonblack.com

- Support Home Page:

  https://www.carbonblack.com/resources/support/ Email: support@carbonblack.com

- Phone: 877.248.9098
- Fax: 617.393.7499

Reporting Problems

When you call or e-mail technical support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and email address
Product version	Product name and version number

Required Information	Description
Hardware configuration	Hardware configuration of the server or computer the product is running on (processor, memory, and RAM)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear on the cover page, or for longer manuals, after the Copyrights and Notices section of the manual.
Problem	Action causing the problem, error message returned, and any other appropriate output
Problem severity	Critical, serious, minor, or enhancement

Installing the Rules Installer

App Control includes a drag-and-drop interface that you use to add new rule files to your server as they become available.

These files are available on the Carbon Black User Exchange. If you have enabled the Carbon Black File Reputation (CDC) connection from your server and the health indicators option within the CDC, a health indicator will inform you when agent installers or rule files newer than the ones you currently have are available.

TIP: You can obtain the latest App Control downloads and documentation on the exchange using this repository: Repository of Carbon Black App Control 8.x Documentation & Downloads

To upload installers for rule files to a server:

1. Log in to the Carbon Black User Exchange and locate the new rules installer.

   Links to these packages are found on the Documentation & Downloads area for App Control on the User Exchange.

   TIP: You can also obtain the latest App Control downloads and documentation on the exchange using this repository: Repository of Carbon Black App Control 8.x Documentation & Downloads

2. Download the **RulesInstaller_1.8.exe** to a filesystem on or accessible to your App Control server.
3. Log in to your App Control Server using an account that has *Manage system configuration* permission.

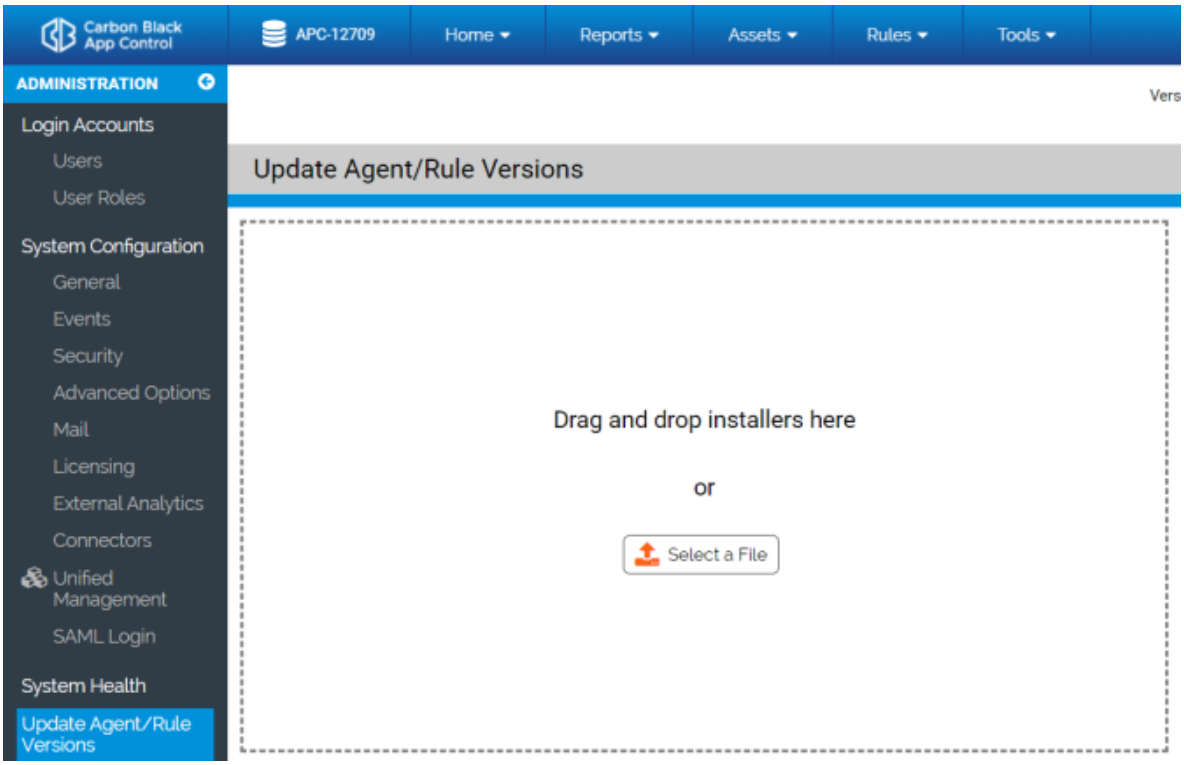
   

   REQUIREMENT: A user must have "*Manage system configuration*" permission to upload and install agent installers and rule files.

4. In the console menu, click on the configuration (gear) icon and choose **Update Agent/Rule Versions**.

5. To install a new rules file on the server, drag the **RulesInstaller_1.8.exe** file from your download folder into the target zone on the **Update Agent/Rule Versions** page, or click Select a file to find the file via a browser.

> **IMPORTANT**: If you are updating the rules file, do not attempt to simultaneously upload any agent files. Each file upload must be complete before the next one is started.



When the upload begins, the server checks to see whether the package is correctly signed. If so, it is installed on the server. Messages report on each stage of the progress (or failure) of the upload and installation.

IMPORTANT: Remain on the Update Agent/Rule Version page while uploads are proceeding. You can navigate to other pages, but since the server is restarted after the upload, activity on another page can be interrupted at an unpredictable point.

6. Once you have finished uploading rules files to a server:

   - If you are setting up a new server, set up the policies you want to control your agents.

     See *Creating and Configuring Policies* in the *App Control User Guide*

   - Choose a policy assignment method.

     See *Assigning Computers to a Policy* in the *App Control User Guide*

   - Install agents on endpoints.

     See Installing *App Control Agents* in the *App Control User Guide*

   - If you are uploading new rules files on an existing server, begin upgrading agents according to the upgrade plan appropriate to your site.

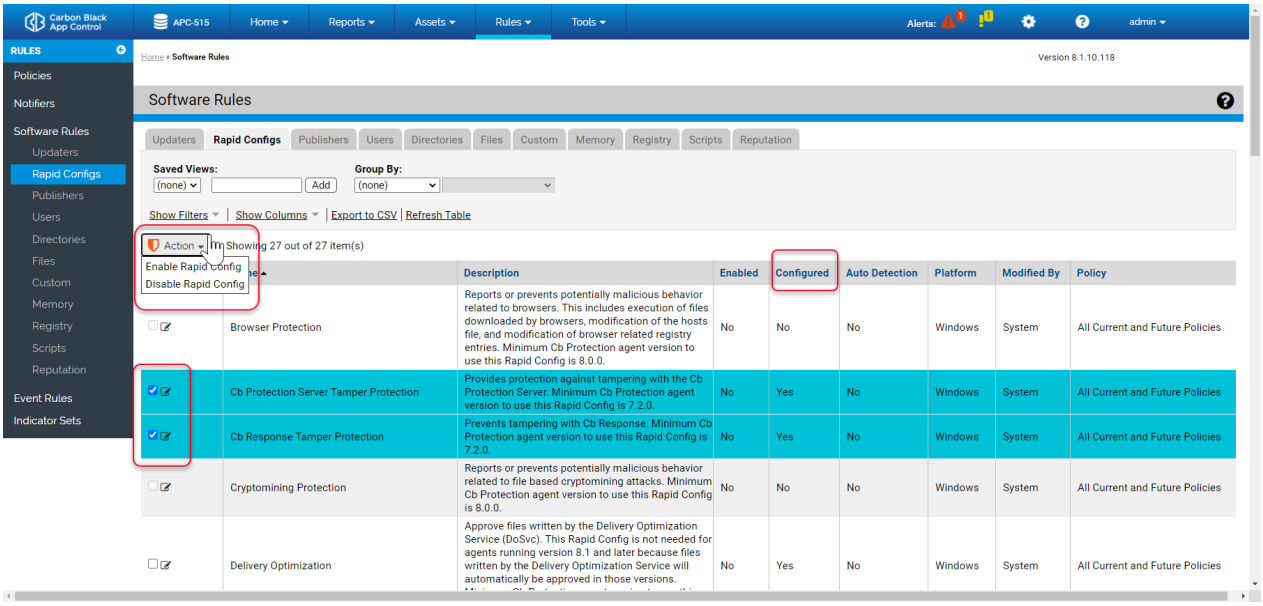
     See *Upgrading App Control Agents* in the *App Control User Guide*.

Configuring and Enabling Rapid Configs

A Rapid Config must be configured before it can be enabled. The actions required for configuration vary depending upon the config:

- In some cases, all configuration settings are built in, and the only changes a user can make are to enable or disable the Rapid Config and change the policies to which it applies.
- If a Rapid Config has editable fields but all of these are either optional fields or already have values, you can enable the config immediately. If a Rapid Config has a setting that could block or report and action, the default is usually “Report”.
- If a Rapid Config has required fields that do not have defaults or values you previously entered, values must be entered into those fields before the config can be enabled.

The Rapid Configs table includes a column showing the configuration status of each config. Any config whose Configuration column shows *Yes* can be enabled directly from the table page. Rapid Configs whose Configuration column shows *No* cannot be selected on that page (their check boxes are grayed out), and must be configured on the Rapid Config Settings page before being enabled.



To enable a configured Rapid Config from Rapid Config table page:

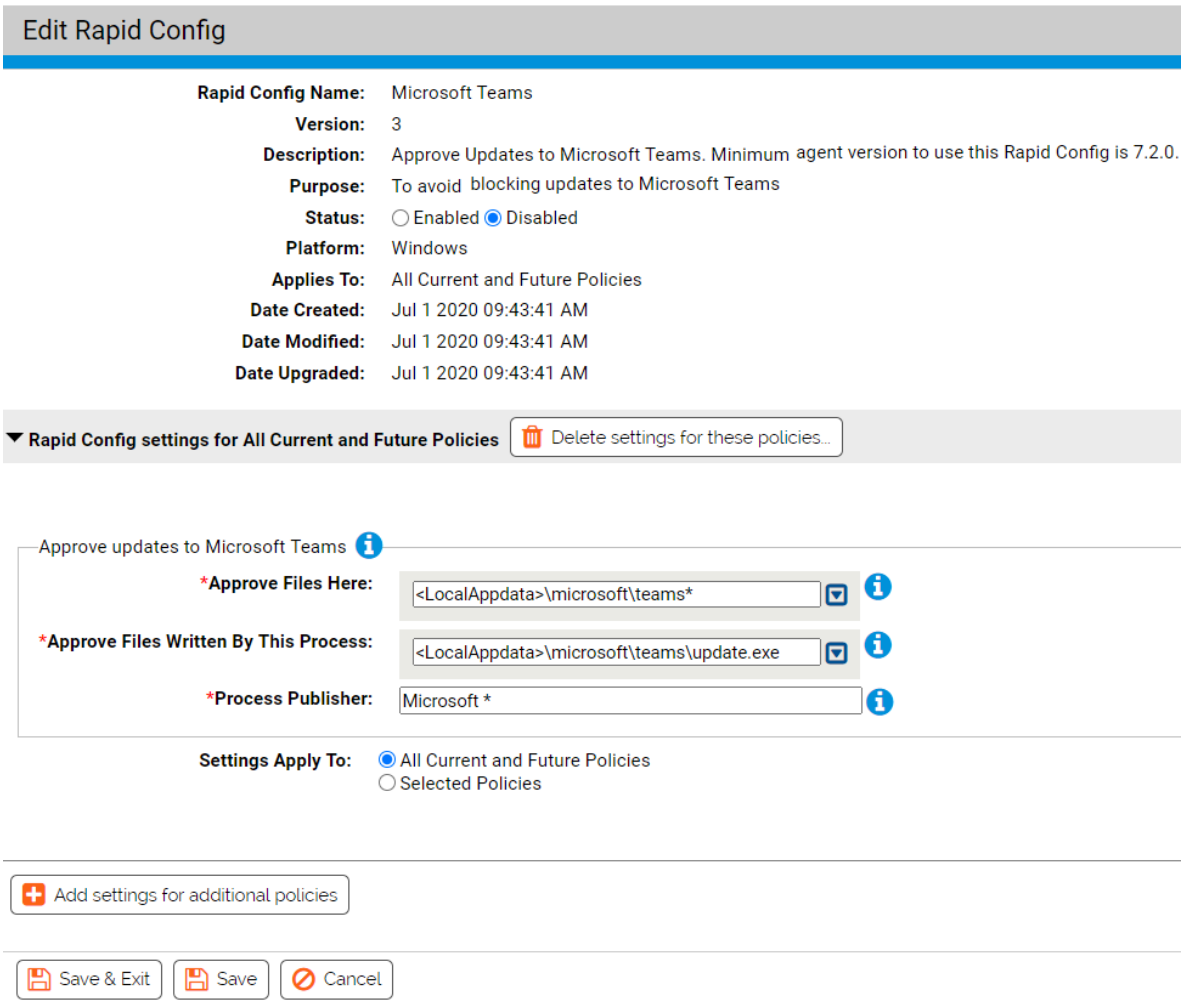
1. On the console menu, choose **Rules > Software Rules**.
2. Click the **Rapid Configs** tab to view configurations.
3. Check the box next to any config(s) you want to enable. Only boxes for configured Rapid Configs can be checked.
4. On the Action menu, choose **Enable Rapid Config**. The config is enabled for all policies, or if you are re-enabling a previously configured Rapid Config, it uses the policy settings choices you made before.

If you want to enable a Rapid Config that is already configured but you want to choose the policies it applies to, use the Rapid Config Settings page.

To enable and select policies for a configured Rapid Config:

1. On the console menu, choose **Rules > Software Rules**.
2. Click the **Rapid Configs** tab to view configurations.
3. Click the **View Details** button next to the configuration you want to view or edit.

   The details of each Rapid Config vary.



4. Ensure that all mandatory fields (with a red asterisk) are filled in. Review remaining fields and ensure they are correctly configured. In most cases, these fields are pre-configured. Click the **Enabled** button when ready.

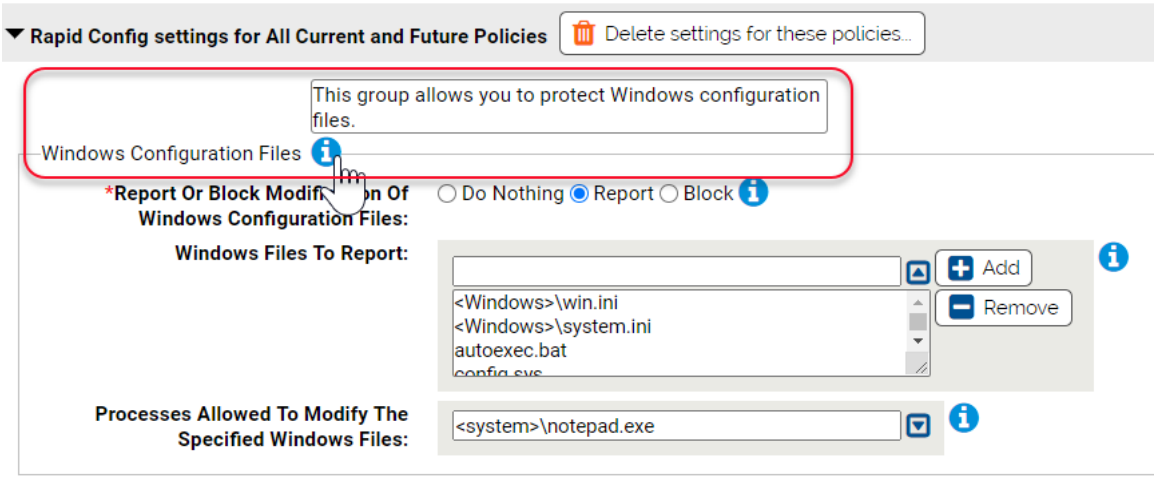
   NOTE:All mandatory fields (with a red asterisk) must be filled out before the config can be enabled. See "User-Configured Rapid Configs" below for more information.

5. In the Applies To field, click the radio button for **All Current and Future Policies** or **Selected policies**.
6. If you chose *Selected policies*, check the box next to each policy for which you want the Rapid Config to be enabled.
7. When you have finished selecting policies, click the **Save** button (to stay on the page) or **Save & Exit** button (to return to the table page) to save the enabled configuration.

User-Configured Rapid Configs

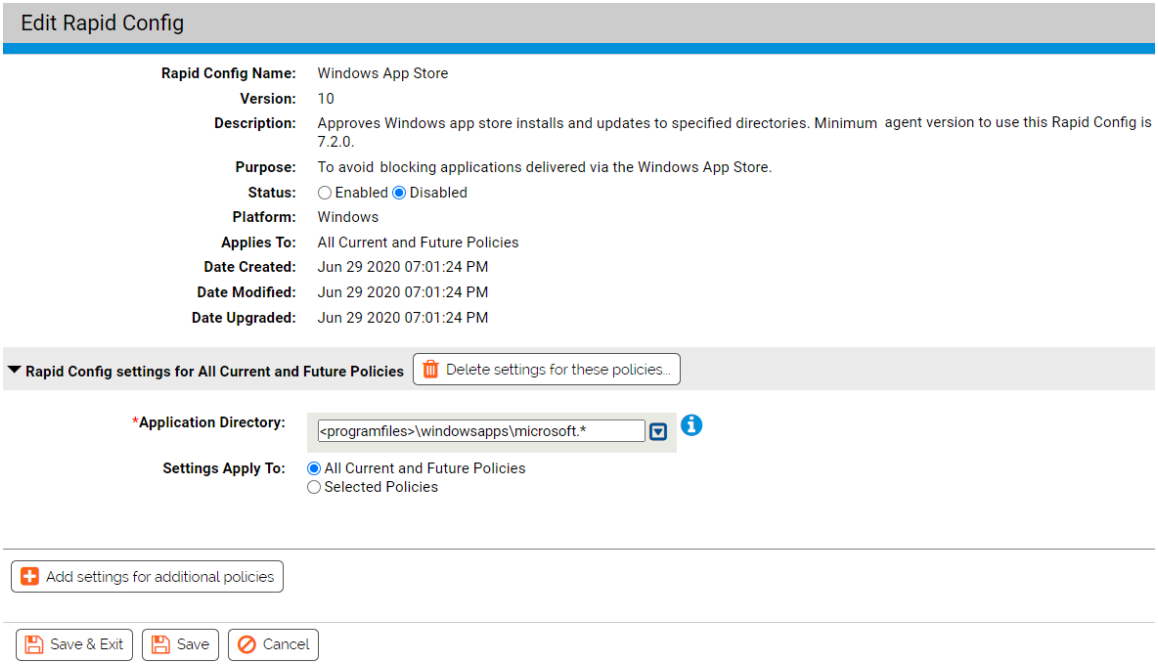
Some Rapid Configs require configuration beyond choosing the policies they apply to. They have additional panels that include a group of configuration settings, and the panels may allow you to choose which policies the *settings* apply to. If you choose to apply the settings to All policies, there is only one additional panel. If you choose specific policies, you can provide different setting values for different policies. You can also provide special settings for some policies and not apply the Rapid Config to other policies at all.

The specific parameters needed vary, but for each customizable configuration, any fields requiring user input have an information icon that displays popup help when you hover the mouse over it. Fields with a red asterisk are mandatory.



To configure and enable a policy-specific Rapid Config:

1. On the console menu, choose **Rules > Software Rules**.
2. Click the **Rapid Configs** tab to view configurations.
3. Click the View Details icon next to the configuration you want to view or edit. Rapid Config details vary.

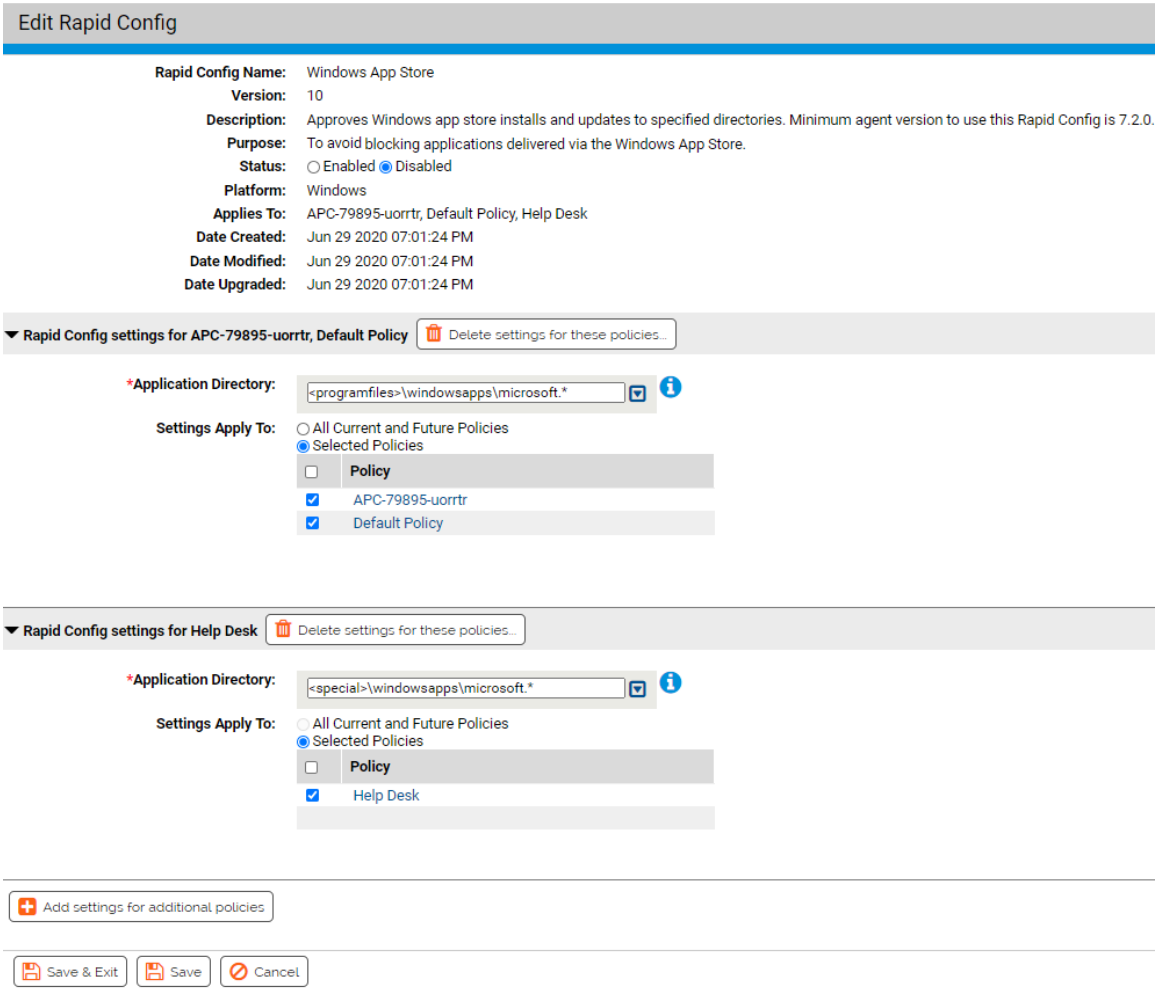


4. Ensure that all mandatory fields (with a red asterisk) are filled in. Review remaining fields and ensure they are correctly configured. In most cases, these fields are pre-configured. Click the **Enabled** button when ready.

> **NOTE**:All mandatory fields (with a red asterisk) must be filled out before the config can be enabled. See "User-Configured Rapid Configs" on page 13 for more information.

5. Click the **Enabled** button.
6. In the Rapid Config settings for All Current and Future Policies panel, hover over the information (i) icons next to each field to see the type of data to enter there. Any field with a red asterisk next to its name is mandatory.
7. Enter the values you want in each mandatory field and any other fields you choose. In some cases, a default value is provided, and you can leave that as the configuration if you choose.

8. In the Settings Apply To field, **All Current and Future Policies** is the default. If you leave that as the setting, you are finished configuring the Rapid Config and can **Save** or **Save & Exit**.
9. If you chose **Selected policies**, the panel name initially changes to New Rapid Config Settings Group. Check the box next to each policy to which you want this group of settings applied. The panel name changes to “Rapid Config settings for <*each policy you checked*>”.
10. If you want to configure a different group of settings for another group of policies, click **Add settings for additional policies** and repeat steps "User-Configured Rapid Configs" on page 13 through "User-Configured Rapid Configs" on page 13. Any policies covered by an existing settings group are not available when you are configuring a new settings group.
11. When you have finished selecting policies, click the **Save** button (to save the Rapid Config and stay on the page) or **Save & Exit** button (to save the rule and return to the table page).



If you later decide to delete a group of settings, you can use click the View Details icon next to this Rapid Config on the Rapid Config table page, and in the Rapid Config Settings page, click **Delete settings for these policies**, and then save the change. The policies affected by that group of settings are no longer affected by this Rapid Config.

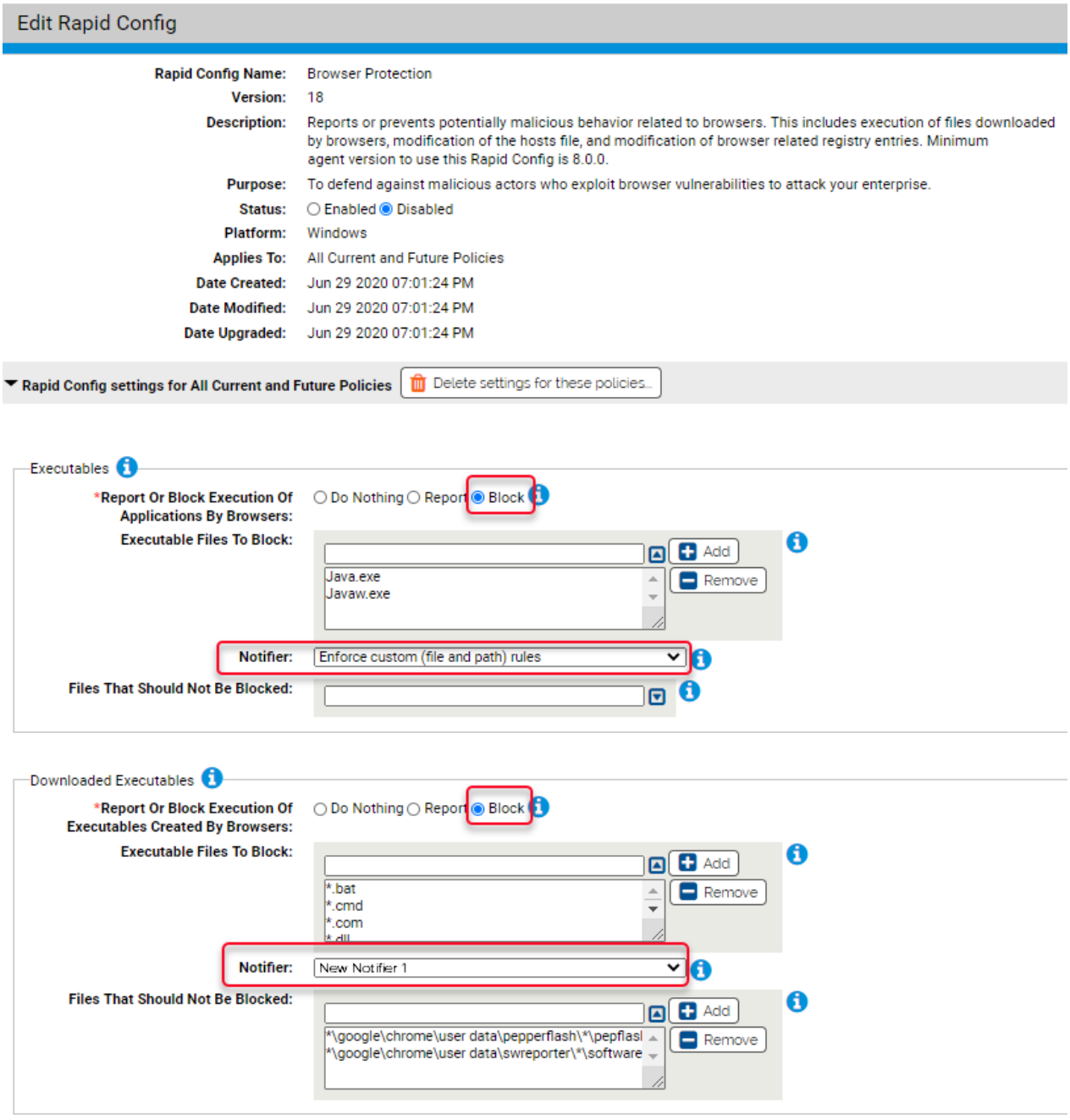
NOTE: If a group of settings has the All Current and Future Policies button activated, clicking **Add settings for additional policies** displays an error dialog. You must deselect at least one policy before creating a new group of settings.

Specifying Notifiers for Rapid Configs

Some rules within Rapid Configs can block actions a user takes. For example, several of the rules that make up the Browser Protection Rapid Config can block:

- Execution of applications *by* browsers
- Execution of applications that were *downloaded from* browsers
- Registry modifications
- Host file modifications

For each one of these actions, you can specify files and paths affected, and you can choose to do nothing, to report the action, or to block the actions matching those settings. If you choose to block them, a Notifier field appears in the panel. That field provides a menu of existing notifiers from which you can choose the appropriate one for each action. When a Rapid Config contains more than one action that can be blocked, you can choose different notifiers for each action you block or use the same one for all. You also can choose Block for some actions and Report or Do Nothing for others.


Edit Rapid Config
Rapid Config Name: Browser Protection
Version: 18
Description: Reports or prevents potentially malicious behavior related to browsers. This includes execution of files downloaded by browsers, modification of the hosts file, and modification of browser related registry entries. Minimum agent version to use this Rapid Config is 8.0.0.
Purpose: To defend against malicious actors who exploit browser vulnerabilities to attack your enterprise.
Status: Enabled Disabled
Platform: Windows
Applies To: All Current and Future Policies
Date Created: Jun 29 2020 07:01:24 PM
Date Modified: Jun 29 2020 07:01:24 PM
Date Upgraded: Jun 29 2020 07:01:24 PM
Rapid Config settings for All Current and Future Policies
Delete settings for these policies...
Executables
*Report Or Block Execution Of Applications By Browsers:
Do Nothing Report Block
Executable Files To Block:
Add
Remove
Java.exe
Javaw.exe
Notifier:
Enforce custom (file and path) rules
Files That Should Not Be Blocked:
Downloaded Executables
*Report Or Block Execution Of Executables Created By Browsers:
Do Nothing Report Block
Executable Files To Block:
Add
Remove
*.bat
*.cmd
*.com
Notifier:
New Notifier 1
Files That Should Not Be Blocked:
Add
Remove
\google\chrome\user data\pepperflash\pepflasl
\google\chrome\user data\swreporter\software

Specifying Paths and Processes

When you specify Path or File in a Rapid Config, you have some of the options that are available in Custom, Registry, and Memory rules. These include:

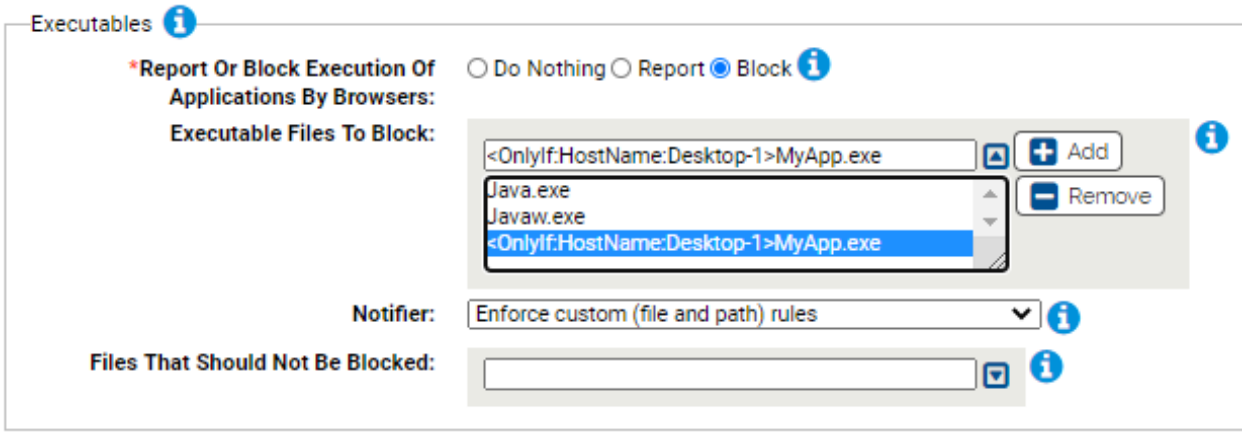
- **Specify a directory or a file/process** – You can enter a path or process specification that exactly identifies a file by path and name so that only that file matches the rule. You also can enter a specification that identifies a directory, and so affects all files or processes in that directory and its subdirectories.
- **Specify a local drive or UNC path (Windows only)** – You can use a local drive name, such as *C:\folder1\subfolder\application.exe*, to identify a local path or process. For a remote path or process, use a UNC path, such as *computer\dir\app.exe*. Mapped drives in a path or process specification are not recognized.
- **Use wildcards –** You can use wildcards ('?' for any one character and '*' for zero or more characters) to expand the scope of a path or process specification, or to help you match a file or folder whose exact location you don't know. Wildcards may be used at the beginning, end or middle of a path.
- **Specify multiple paths or processes** – For some paths and processes, you can add more than one path definition per rule.
- **Use path macros** – You can use special macros to identify certain well known folders, even if you don't know their exact location on agent computers. Macros are platform-specific.

  TIP: For more information regarding Macros, see *Using Macros in Rules* in the *Custom Software Rules* chapter of the User Guide.

- **Use conditional macros** – If you use conditional macros (such as *OnlyIf)*, the condition you set applies only to the specific parameter with the macro. For example, if you set the Browser Protection Rapid Config to report executions of Java.exe, Javaw.exe, and FlashPlayerApp.exe,

plus you added the following parameter*: <OnlyIf:HostName:Desktop-1>MyApp.exe,* the Rapid Config would report execution of MyApp.exe only on *Desktop-1* but it would report execution of Java.exe, Javaw.exe, and FlashPlayerApp.exe on any machine. To apply make all executables conditional, you would have to add the OnlyIf macro to each one.



See Specifying Paths and Processes for more information about options and requirements for path and process specification. Note, however, that some of the options described in that section do not apply to Rapid Configs.

NOTE: If you specify a script file in a Rapid Config that controls execution, the config will not recognize the script and control its execution unless there is a corresponding Script Rule for the file extension and the process that executes the script. See Script Rules for more details.

Automatic Rapid Config Updates

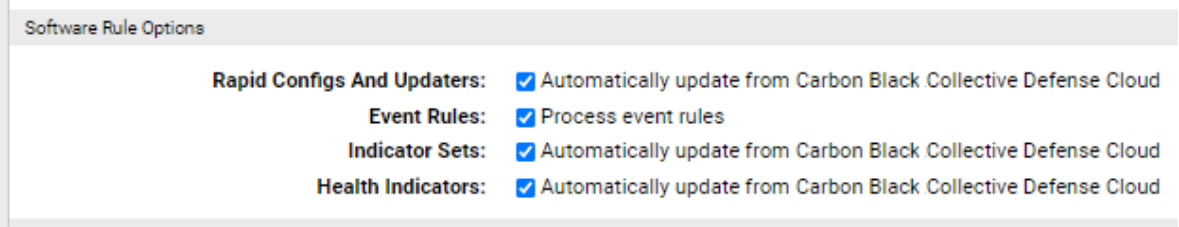
New Rapid Configs may become available, or existing configs may be modified with enhancements or changed because of changes to the applications they apply to. When you install a new version of the Rules Installer, the Rapid Config table is updated to reflect these changes (if any).

By allowing Carbon Black File Reputation to maintain Rapid Configs, you get new and modified versions as soon as they become available, without waiting for a new release of App Control. Enabling Carbon Black File Reputation updates also means that obsolete configurations are deleted from the table. This feature is enabled by default if you have Carbon Black File Reputation enabled.

If you have not activated the integration between the App Control Server and the Carbon Black File Reputation, you can do that on the Licensing tab of the System Configuration page. See Activating Carbon Black File Reputation for details.

To enable or disable cloud updates of Rapid Configs:

1. On the console menu, choose **System Configuration** on the Administration (Gear) menu.
2. On the System Configuration page, click the **Advanced Options** tab. The Advanced Options Configuration page appears, with the Software Rules Options panel at the bottom.
3. At the bottom of the page, click the **Edit** button.
4. In the Software Rule Options panel, the Carbon Black File Reputation updater option is enabled by default:
    - If you *do not want* Carbon Black File Reputation to keep your updaters current, *un-check* the box next to *Automatically update Rapid Configs and Updaters from Carbon Black File Reputation* and then click the **Update** button at the bottom of the page.
    - If you want to *re-enable* automatic updates from Carbon Black File Reputation after they have been disabled, check the box and click the **Update** button.



5. In the Confirm Server Setting Change dialog, click **Yes** to save your changes.

Alerts for Rapid Config Changes from the Cloud

You can enable an alert that will notify you each time a Rapid Config is created, modified, or deleted from the cloud. This is recommended if you have automatic updates enabled.

To enable alerts for Rapid Config updates delivered from the cloud:

1. On the console menu, choose **Tools > Alerts**.
2. Check the box next to the Rapid Config Alert.
3. On the Action menu, choose **Enable Alerts**.

Rapid Configs Included in Rules Installer v1.8

IMPORTANT: Rapid Configs listed below may not be enabled by default. It is the customer's responsibility to verify their configuration.

Table 1: List of Rapid Configs

Name	Brief Description	Platform
Browser Protection	Reports or prevents potentially malicious behavior related to browsers.	Windows
Carbon Black App Control Server Tamper Protection	Provides protection against tampering with the Carbon Black App Control Server.	Windows
Carbon Black EDR Tamper Protection	Prevents tampering with Carbon Black EDR.	Windows
Cryptomining Protection	Reports or prevents potentially malicious behavior related to file based cryptomining attacks.	Windows
Delivery Optimization	Approve files written by the Delivery Optimization Service (DoSvc).	Windows
Domain Controller Logon Scripts	Allows and optionally promotes all files under the Sysvol and NetLogon directories of the specified domain controllers if an agent is a member of the specified domain.	Windows

Name	Brief Description	Platform
Doppelganger Protection	Protect against the exploit known as Doppelganging on windows systems.	Windows
Linux Hardening	Improves the security of computers running Linux by reporting or blocking modification of critical Linux system files.	Linux
Linux System Performance	Improves the performance of computers running Linux by ignoring writes of specified files or by specified processes.	Linux
Microsoft Exchange Server	Improves the performance of Microsoft Exchange servers when running along side Carbon Black App Control.	Windows
Microsoft Office Protection	Improve security by watching for suspicious behavior by Microsoft Office apps.	Windows
Microsoft SCCM	Approves software delivered via Microsoft SCCM.	Windows
Microsoft SQL Server	Improves the performance of Microsoft SQL servers when running alongside Carbon Black App Control.	Windows
Microsoft Teams	Approve Updates to Microsoft Teams.	Windows
Mimikatz Protection	Protect against Mimikatz based attacks on windows systems.	Windows

Name	Brief Description	Platform
Powershell Protection	Improve security by watching for suspicious executions of Powershell.exe.	Windows
Ransomware Protection	Protect against ransomware by reporting or blocking modification to files typically targeted by ransomware.	Windows
Script Processors	Improves the security of computers by ensuring that script processors only run from expected locations.	Windows
Self-Service Approvals	Provides a folder from which normal end-users can approve the execution of unapproved files even when in high enforcement.	Windows
Suspicious Application Protection	Reports or prevents execution of Microsoft applications that are rarely used and can be used maliciously.	Windows
Suspicious Command Line Protection A-M	Reports or prevents behavior by common applications that is suspicious based on command line.	Windows
Suspicious Command Line Protection N-Z	Reports or prevents behavior by common applications that is suspicious based on command line.	Windows

Name	Brief Description	Platform
Suspicious Parent-Child Protection	Reports or prevents behavior by common applications that is suspicious based on parent-child relationships.	Windows
Visual Studio	Approves Visual Studio builds and ignores intermediate build files.	Windows
VMware Workspace ONE	Approves software distributed via VMware Workspace ONE.	Windows
Windows App Store	Approves Windows app store installs and updates to specified directories.	Windows
Windows Hardening	Improves the security of computers running Windows by reporting or blocking modification of critical windows files and registry settings.	Windows
Windows Installer Embedded File Protection	Protect against exploiting Windows installers by embedding malicious content in them.	Windows
WMI Protection	Protect against WIndows Management Instrumentation (WMI) abuse on windows systems.	Windows

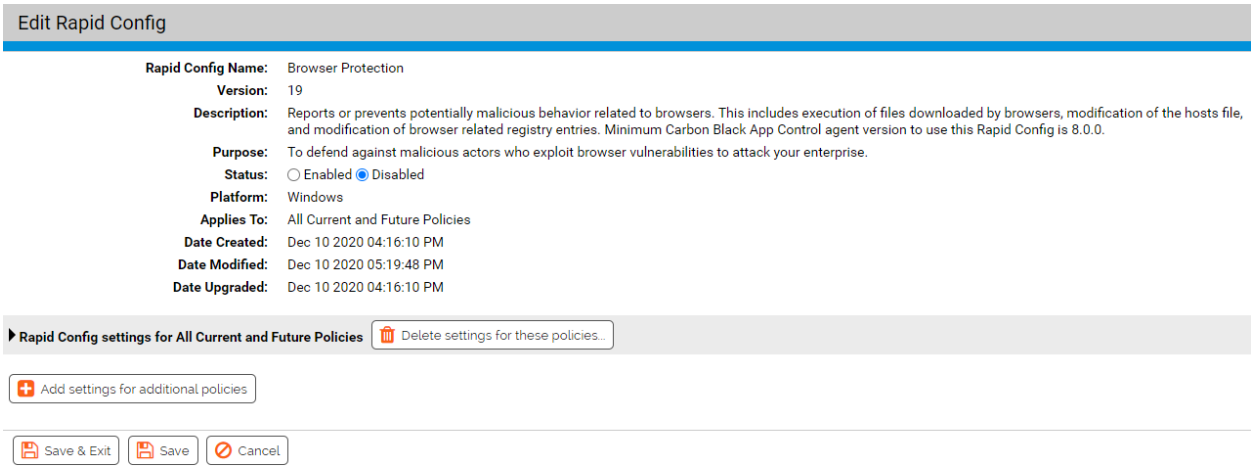
Rapid Config Details

Browser Protection Rapid Config

Purpose: To defend against malicious actors who exploit browser vulnerabilities to attack your enterprise.

Description: Reports or prevents potentially malicious behavior related to browsers. This includes execution of files downloaded by browsers, modification of the hosts file, and modification of browser related registry entries.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

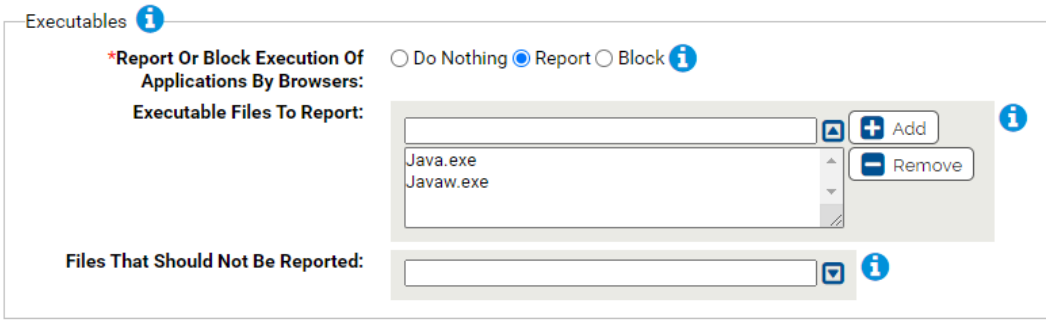
In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

For each of the following sections, specify what action you require.

Executables

Use this group to specify applications that should not be run by browsers.



***Report Or Block Execution Of Applications By Browsers:**
Should execution of the specified applications by browsers be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Executable Files To Report:
Carbon Black App Control will report or block execution of the specified files by a browser. You can add or remove items from this list. By default, the list includes:

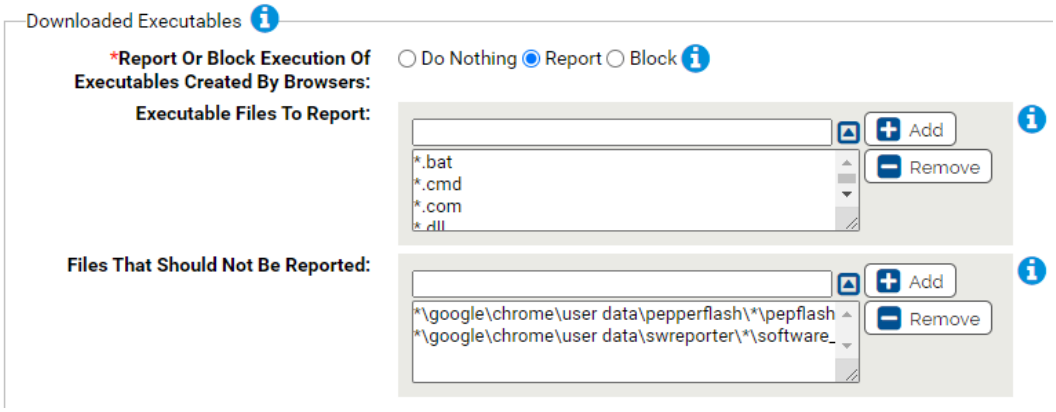
- Java.exeJavaw.exe

Files That Should Not Be Reported:

Execution of files specified here will not be reported or blocked. You can add or remove items from this list. To edit, click the down arrow next to the text box.

Downloaded Executables

Use this group to specify how to handle applications downloaded by browsers.



***Report Or Block Execution Of Executables Created By Browsers:**

Should execution of the specified executables that were created by browsers be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Executable Files To Report:

Carbon Black App Control will report or block execution of the specified files if they were created by a browser. You can add or remove items from this list. Bydefault, the list includes:

- *.bat
- *.cmd
- *.com
- *.dll
- *.exe
- *.msi
- *.scr

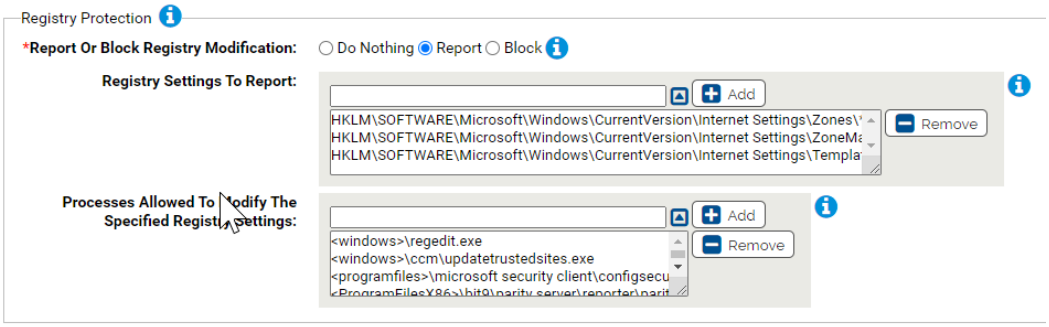
Files That Should Not Be Reported:

Execution of files specified here will not be reported or blocked. You can add or remove items from this list. To edit, click the down arrow next to the text box and select the item to edit. By default, the list includes:

- *\google\chrome\user data\pepperflash*\pepflashplayer.dll
- *\google\chrome\user data\swreporter*\software_reporter_tool.exe

Registry Protection

Use this group to specify registry settings to protect.



***Report Or Block Registry Modification:**

Should modification of the specified registry settings be reported or blocked? You should validate that legitimate registry modifications are not blocked before enabling blocking.

Registry Settings To Report:

Carbon Black App Control will report or block modification of the specified registry settings. You can add or remove items from this list. By default, the list includes:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones*
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap*
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\TemplatePolicies*

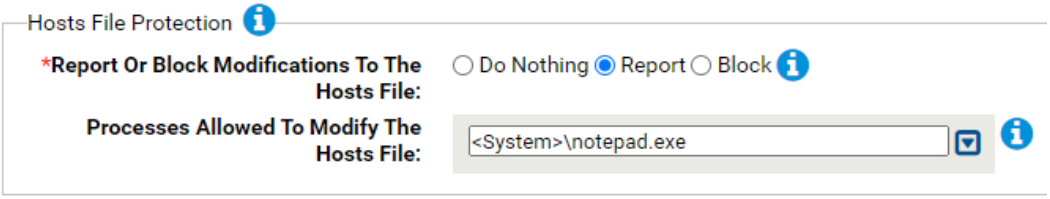
Processes Allowed To Modify The Specified Registry Settings:

Processes specified here will be allowed to modify the specified registry settings. You can add or remove items from this list. By default, the list includes:

- <windows>\regedit.exe
- <windows>\ccm\updatetrustedsites.exe
- <programfiles>\microsoft security client\configsecuritypolicy.exe
- <ProgramFilesX86>\bit9\parity server\reporter\parityreporter.exe

Host File Protection

Use this group to protect the hosts file.



***Report Or Block Modifications To The Hosts File:**

Should modification of the hosts file be reported or blocked? You can specify process that are allowed to modify the hosts file in the next parameter.

Processes Allowed To Modify The Hosts File:

Processes specified here will be allowed to modify the hosts file. You can add or remove items from this list. By default, the list includes:

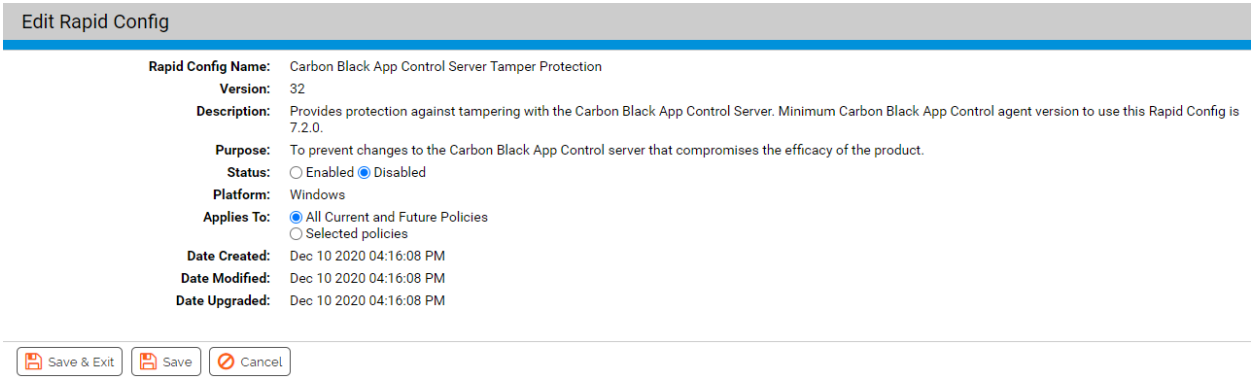
- <System>\notepad.exe

Carbon Black App Control Server Tamper Protection Rapid Config

Purpose:To prevent changes to the Carbon Black App Control server that compromises the efficacy of the product.

Description: Provides protection against tampering with the Carbon Black App Control Server.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



Rapid Config Settings

This rapid config only provides the following options:

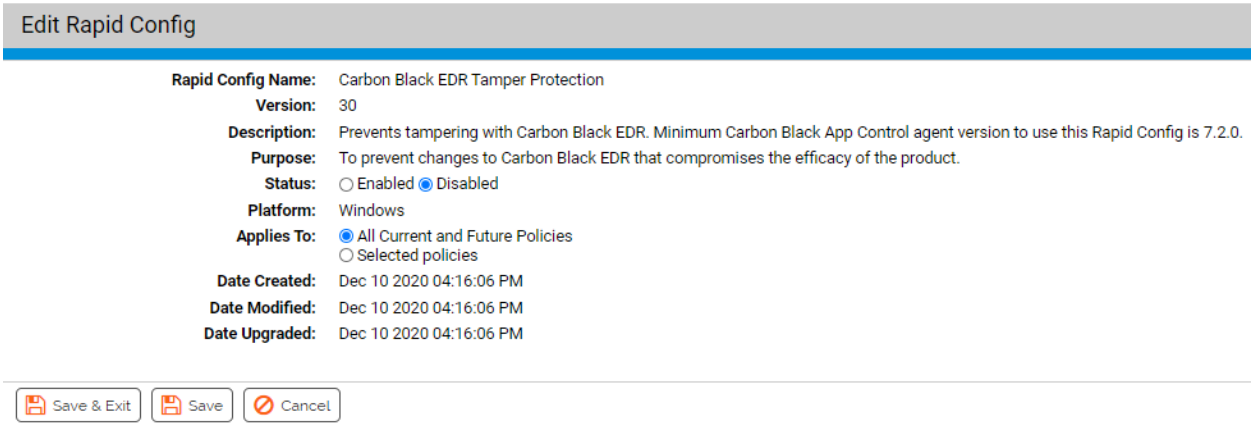
- You can enable or disable it.
- You can specify what policies the rapid config applies to.

Carbon Black EDR Tamper Protection Rapid Config

Purpose:To prevent changes to Carbon Black EDR that compromises the efficacy of the product.

Description: Prevents tampering with Carbon Black EDR.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



Rapid Config Settings

This rapid config only provides the following options:

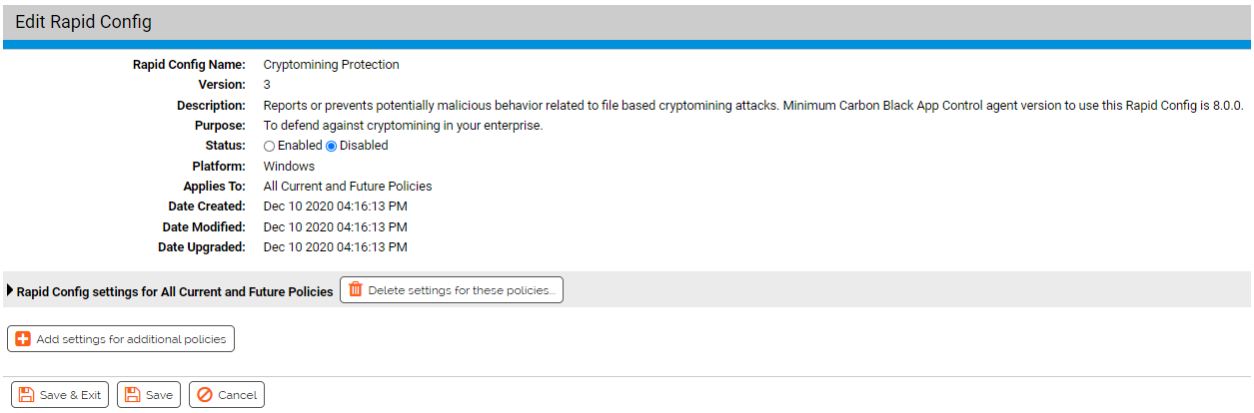
- You can enable or disable it.
- You can specify what policies the rapid config applies to.

Cryptomining Rapid Config

Purpose:To defend against cryptomining in your enterprise.

Description: Reports or prevents potentially malicious behavior related to file based cryptomining attacks.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



What is Cryptomining?

In order for people to obtain cryptocurrency without purchasing it, the currency needs to be mined. Mining uses the processing power of a computer to solve mathematical problems with hashing functions to mine “coins.”

Obviously, having computers running cryptominers becomes a problem when people within and outside of your organization are using your systems without your knowledge. Mining can impact your business processes and electricity bills.

How can App Control Help?

Customers with their endpoints running App Control in High Enforcement will likely be protected from the majority of cryptoming processes. But for added protection or for those endpoints that have not yet moved to High Enforcement (or are not planned for High Enforcement), the Cryptoming Rapid Config can help.

Rapid Config Settings

The Cryptomining Rapid Config focuses on blocking or reporting on executables and command lines matching specific parameters.

Report, Block, or Do Nothing

As with most Rapid Configs, you can choose to **Do Nothing**, **Report**, or **Block** the items or behaviors.

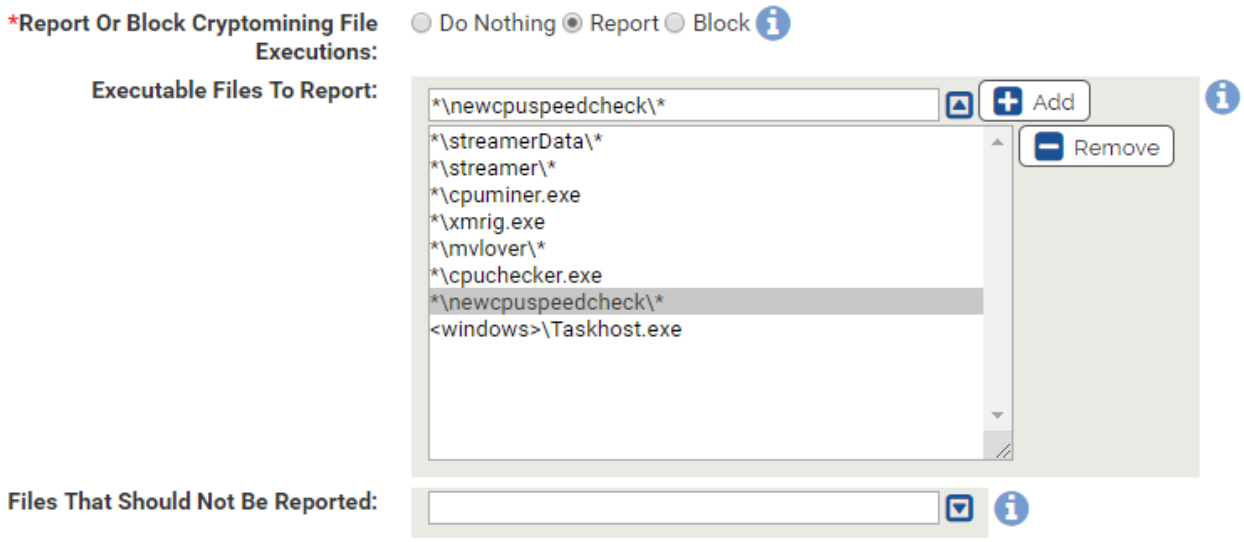
RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

This Rapid Config consists of a single section which defaults to reporting on Cryptomining file executions.

In the process of researching Cryptominers our Threat Research team determined that the majority of these executables had the following filenames or paths:

- *\streamerData*
- *\streamer*
- *\cpuminer.exe
- *\xmrig.exe
- *\mvlover*
- *\cpuchecker.exe
- *\newcpuspeedcheck*
- <windows>\Taskhost.exe

You might be wondering why taskhost.exe is on that list. While taskhost.exe is a Windows process, it's doesn't reside in the Windows directory, the legit taskhost.exe location is in the system32 directory. So if taskhost.exe is running out of the Windows directory, it is likely a malicious file.



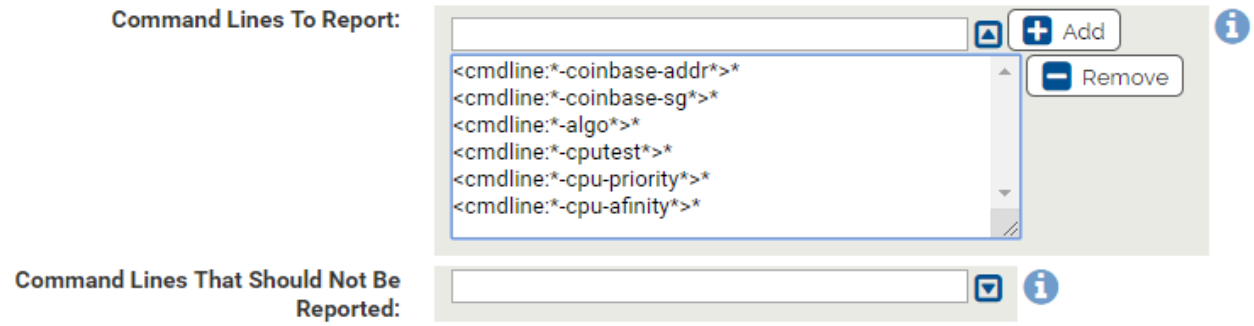
If you are getting blocks or reports on legitimate files because of this list of executables, you can add exceptions. For example, if you have an internally developed application that resides at C:\Program Files\MyBiz\streamer\ and it is getting blocked, you could add the application name to the exception list like *\streamer\myapp.exe.

Command Lines

There are several common parameters that are used by cryptoming tools when they are launched. These commands are:

- -coinbase-addr
- -coinbase-sg
- -algo
- -cputest
- -cpu-priority
- -cpu-affinity

Using the **cmdline** macro, the App Control Windows agent can look for any of these parameters when an executable is launched. If it sees any process launching with any of these parameters, the process will be terminated.



Just like with the executables you can add exceptions to this list. For example, if you have an executable called myapp.exe that uses a -cpu-affinity parameter, you can exclude your application from being blocked or reported on by adding this `<cmdline:*-cpu-affinity*>myapp.exe` in the **Command Lines That Should Not Be Reported** area.

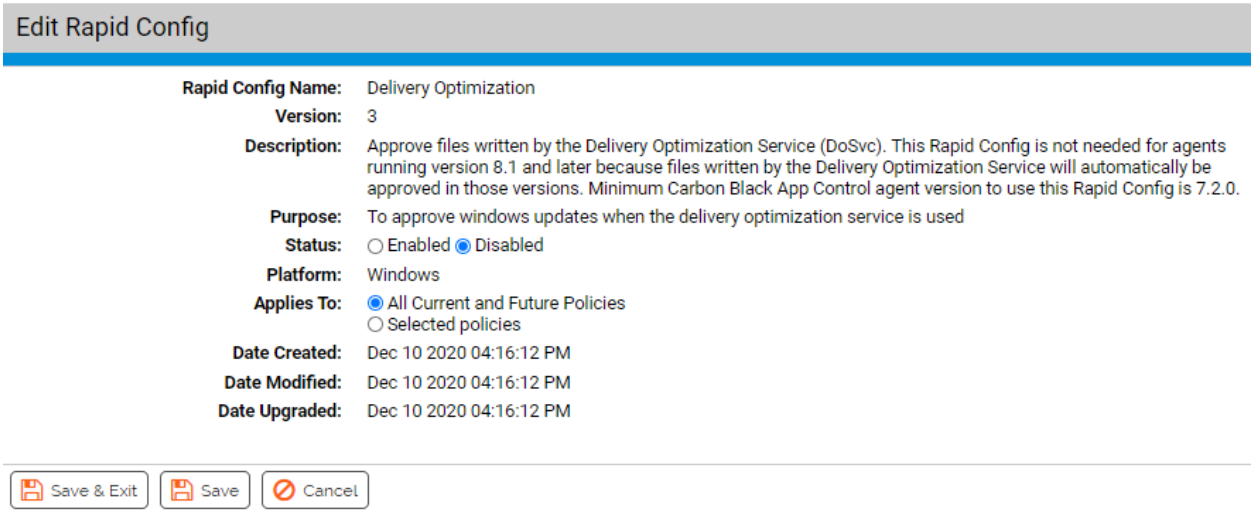
Delivery Optimization Rapid Config

Purpose:To approve windows updates when the delivery optimization service is used.

Description: Approve files written by the Delivery Optimization Service (DoSvc).

NOTE: This Rapid Config is not needed for agents running version 8.1 and later because files written by the Delivery Optimization Service will automatically be approved in those versions.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



Rapid Config Settings

This rapid config only provides the following options:

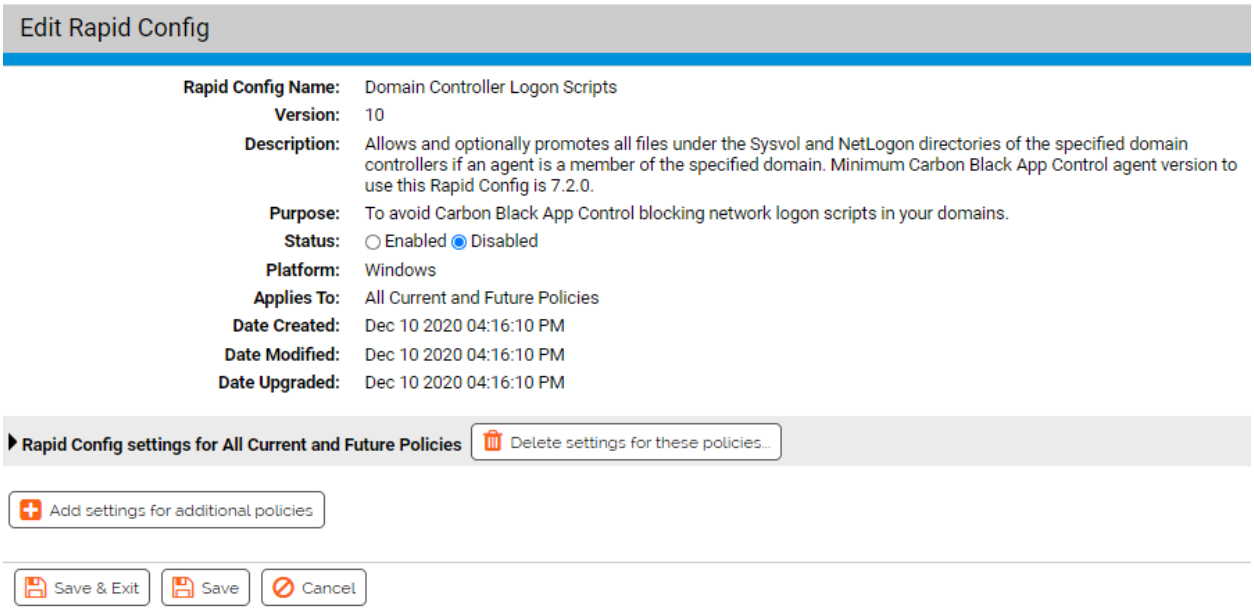
- You can enable or disable it.
- You can specify what policies the rapid config applies to.

Domain Controller Logon Scripts Rapid Config

Purpose:To avoid Carbon Black App Control blocking network logon scripts in your domains.

Description: Allows and optionally promotes all files under the Sysvol and NetLogon directories of the specified domain controllers if an agent is a member of the specified domain.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



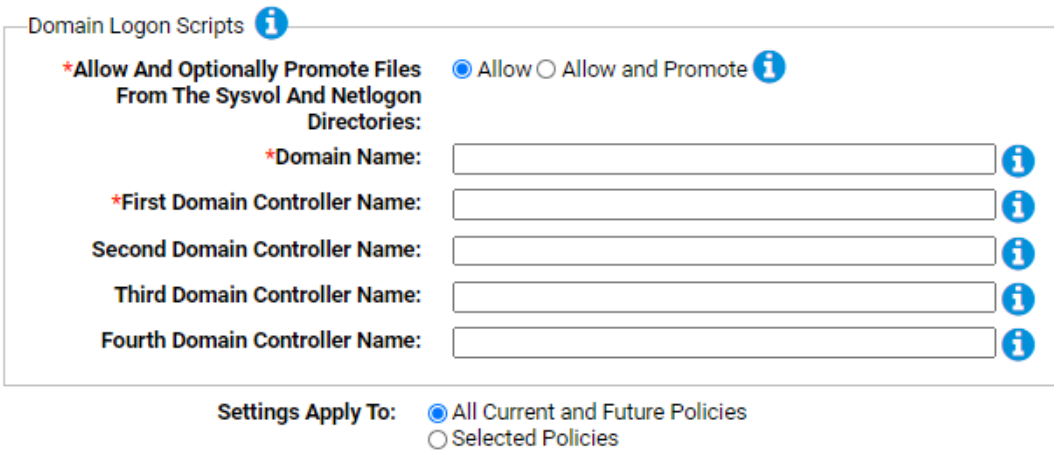
Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

Domain Logon Scripts

This group allows you to specify the location of domain logon scripts that will be allowed to run.



Allow And Optionally Promote Files From The Sysvol And Netlogon Directories:
Should files from the sysvol and netlogon directories on the domain controllers be allowed or allowed and promoted?

Domain Name:
Specify the NETBIOS name of the domain here. Do not include the DNS suffix in the name. For example, use MyDomain rather than MyDomain.local

First Domain Controller Name:
Specify the name of the first domain controller associated with the domain. The names can contain wild cards using an asterisk or question mark, dc1* for example.

Second Domain Controller Name:
Specify the name of the second domain controller associated with the domain, if needed. The names can contain wild cards using an asterisk or question mark, dc1* for example.

Third Domain Controller Name:

Specify the name of the third domain controller associated with the domain, if needed. The names can contain wild cards using an asterisk or question mark, dc1* for example.

Fourth Domain Controller Name:

Specify the name of the fourth domain controller associated with the domain, if needed. The names can contain wild cards using an asterisk or question mark, dc1* for example.

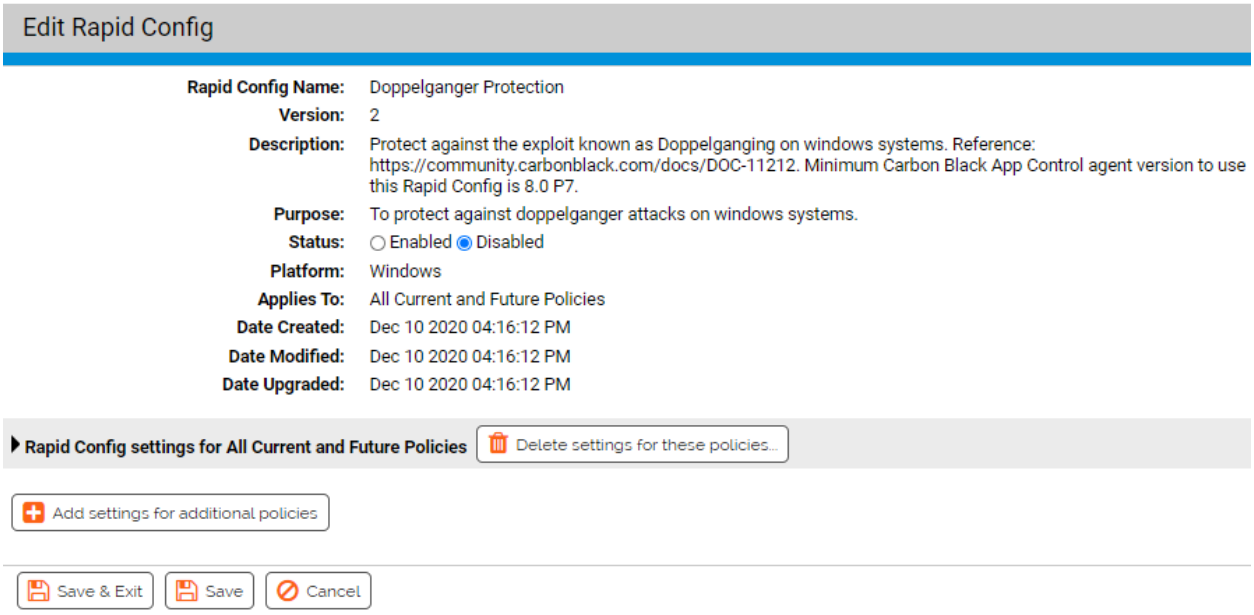
Doppelganger Protection Rapid Config

Purpose: To protect against doppelganger attacks on windows systems.

Description: Protect against the exploit known as Doppelganging on windows systems.

For additional information, see: https://community.carbonblack.com/docs/DOC-11212.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0 Patch 7



What is Doppelganger Protection?

The Process Doppelganging technique uses ntoskrnl to create a transaction subsequently opening a legitimate file into that transaction (for attack purposes the legitimate file would most likely be a signed Microsoft binary).

A malicious payload (in the form of an executable) is then written to that transaction record using the standard API calls (in their POC the malicious payload was encrypted on disk, opened and decrypted by their loader and then written to the transaction record). Their technique then creates a section (via NTCreateSession) for the malicious code (preserving the malicious code), and rolls back the changes to the original legitimate file (the previously created section will not be altered and still contains the malicious code). Their technique then creates a process (and a thread) with a handle to this section, which will appear to be the legitimate process (backed up by legitimate code on disk).

Ultimately this technique is a process that uses the legit Window Loader to run malicious code. As for right now, until we can determine how to best detect this technique, we are suggesting that practitioners focus on the final payload being run. The Cb suite of products will be able to detect the final payload and their associated actions the same as if an attacker used rundll32 or PowerShell to execute the malicious code. Obviously, we want to try and focus on detecting suspicious actions as soon as possible (and we will work to ensure we can detect this technique), but this exploit was developed to evade traditional AV that hooks and scans files (with signatures) at different points prior to the code actually being loaded or executed.

Rapid Config Settings

As with most rapid configs, you can:

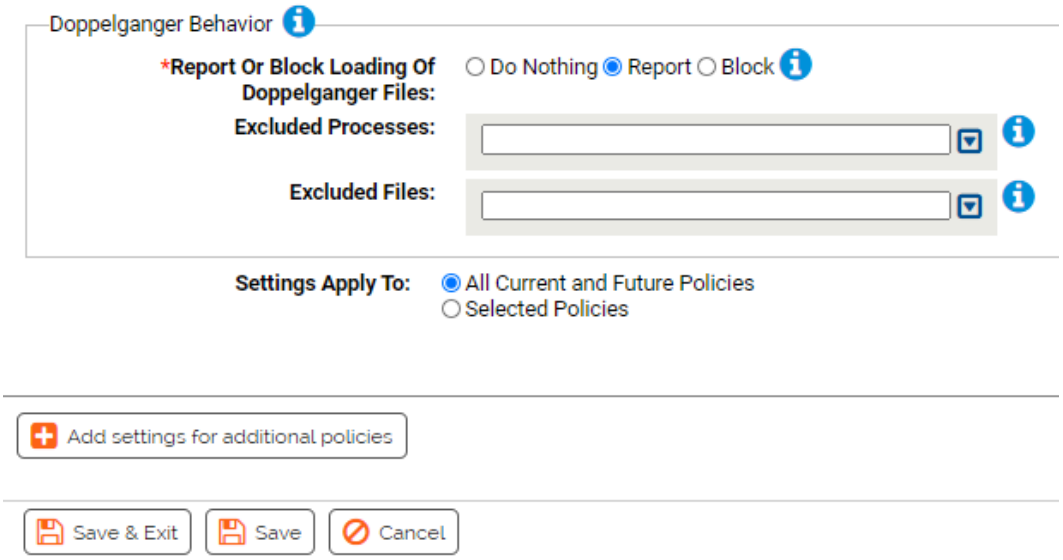
- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors. For each of the following sections, specify what action you require.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

Doppelganger Behavior

You can use these properties to specify how to treat files that appear to be part of a doppelganger exploit.



Report Or Block Loading Of Doppelganger Files:

Should doppelganger behavior be reported or blocked? You should validate that legitimate behavior is not blocked before enabling blocking.

Excluded Processes:

Processes specified here will be allowed to load suspected doppelganger files. You can add or remove items from this list.

Excluded Files:

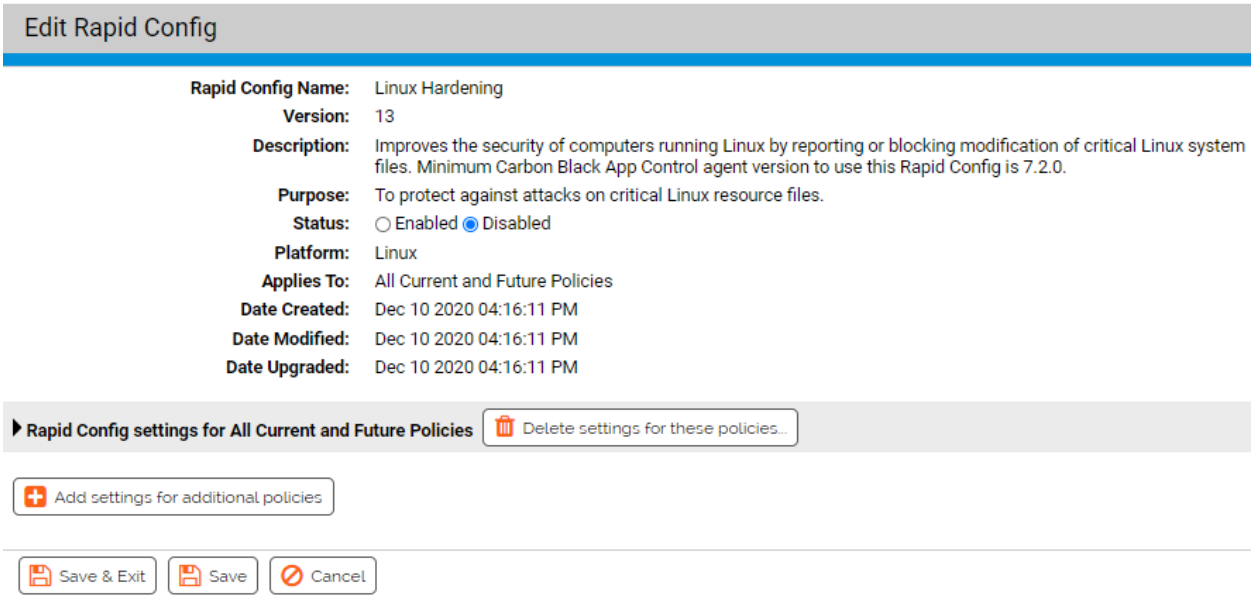
Files specified here will not be reported or blocked. You can add or remove items from this list.

Linux Hardening Rapid Config

Purpose:To protect against attacks on critical Linux resource files.

Description: Improves the security of computers running Linux by reporting or blocking modification of critical Linux system files.

Enabled by Default:	No
Platform:	Linux
Minimum Agent Version Required:	7.2.0



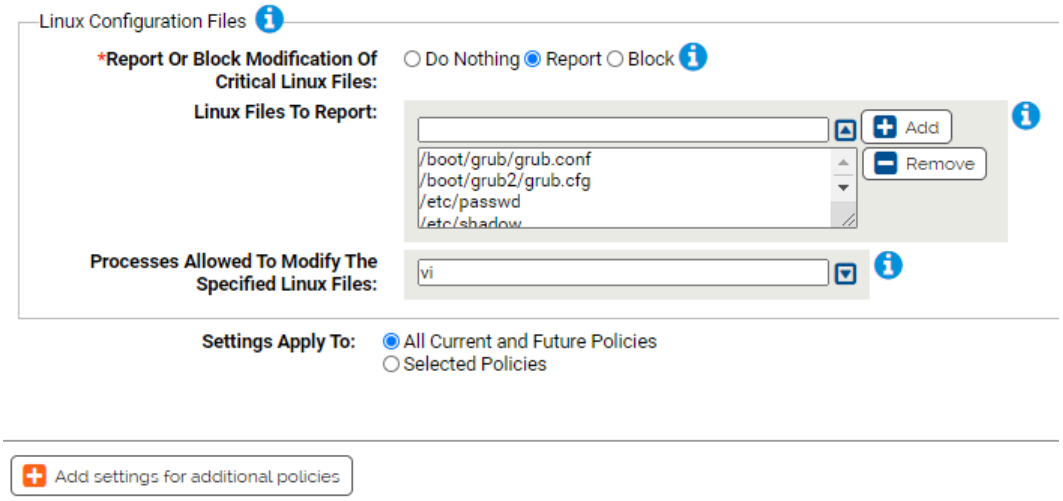
Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors. For each of the following sections, specify what action you require.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.



***Report Or Block Modification Of Critical Linux Files:**

Should modification of the specified files be reported or blocked? You should validate that legitimate modifications are not blocked before enabling blocking.

Linux Files To Report:

Carbon Black App Control will report or block modifications of the specified files. You can add or remove items from this list. The following files are listed by default:

- /boot/grub/grub.conf
- /boot/grub2/grub.cfg
- /etc/hosts
- /etc/sudoers

- /etc/passwd
- /etc/shadow/
- etc/group
- /etc/resolv.conf
- /etc/fstab
- /etc/sysctl.conf

Processes Allowed To Modify The Specified Linux Files:

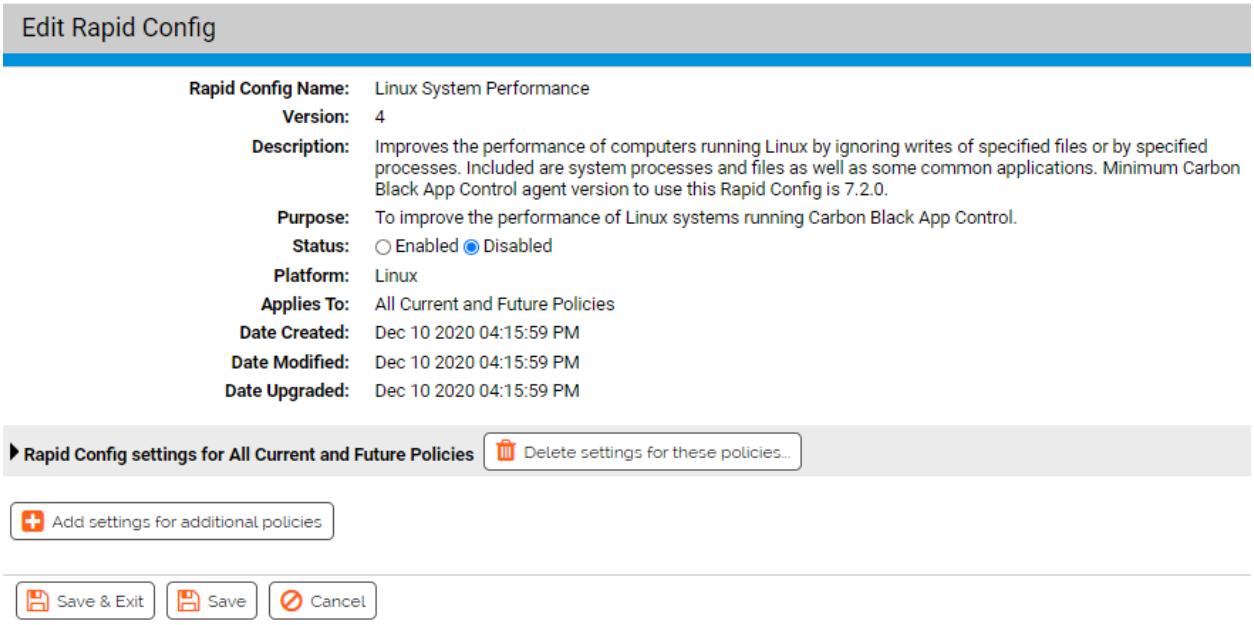
Processes specified here will be allowed to modify the specified Linux files. You can add or remove items from this list.

Linux System Performance Rapid Config

Purpose:To improve the performance of Linux systems running Carbon Black App Control.

Description: Improves the performance of computers running Linux by ignoring writes of specified files or by specified processes. Included are system processes and files as well as some common applications.

Enabled by Default:	No
Platform:	Linux
Minimum Agent Version Required:	7.2.0



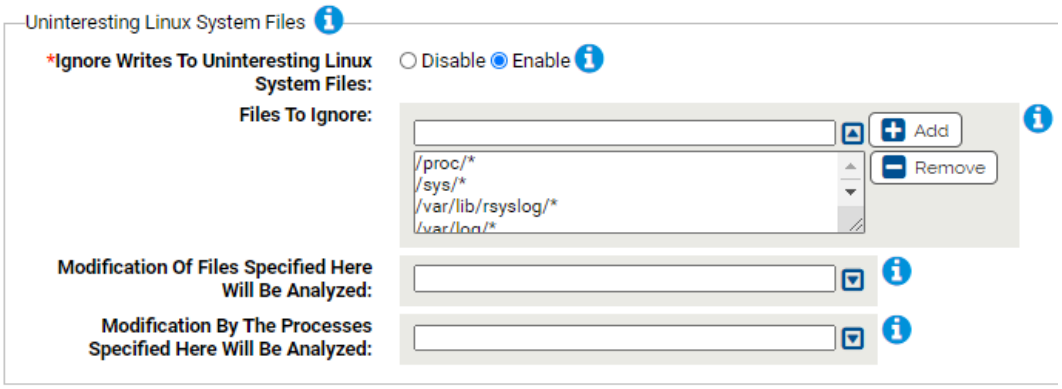
Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

Uninteresting Linux System Files

Use this group to specify uninteresting system files that will be ignored.



***Ignore Writes To Uninteresting Linux System Files:**
Should modification of the specified files be ignored in order to improve performance?

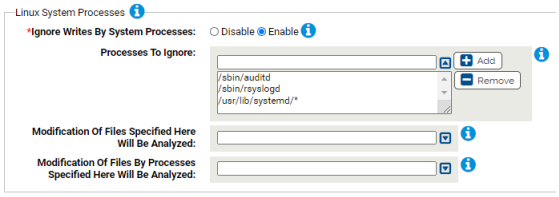
Files To Ignore:
Carbon Black App Control will ignore modification of the specified files. You can add or remove items from this list.

Modification Of Files Specified Here Will Be Analyzed:
Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Modification By The Processes Specified Here Will Be Analyzed:
Carbon Black App Control will analyze modification of files by processes specified here. You can add or remove items from this list.

Linux System Processes

Use this group to specify system processes to be ignored when they modify files.



***Ignore Writes By System Processes:**

Should modification of files by these processes be ignored in order to improve performance?

Processes To Ignore:

Carbon Black App Control will ignore modification of files by the specified processes. You can add or remove items from this list.

- /sbin/auditd
- /sbin/rsyslogd
- /usr/lib/systemd/*

Modification Of Files Specified Here Will Be Analyzed:

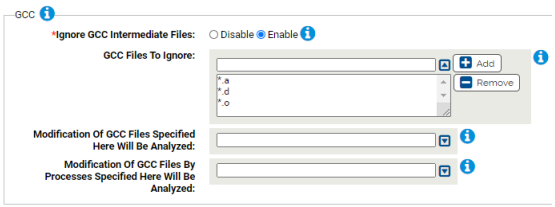
Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Modification Of Files Specified Here Will Be Analyzed:

Carbon Black App Control will analyze modification of files by processes specified here. You can add or remove items from this list.

GCC

Use this group to specify intermediate GCC files that will be ignored.



***Ignore GCC Intermediate Files:**

Should modification of the specified files be ignored in order to improve performance?

GCC Files To Ignore:

Carbon Black App Control will ignore modification of the specified files. You can add or remove items from this list.

- *.a
- *.d
- *.o

Modification Of GCC Files Specified Here Will Be Analyzed:

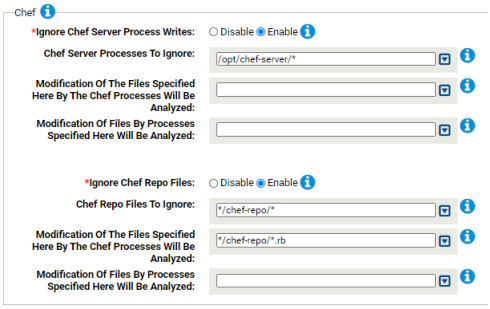
Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Modification Of GCC Files By Processes Specified Here Will Be Analyzed:

Carbon Black App Control will analyze modification of files by processes specified here. You can add or remove items from this list.

Chef

Use this group to specify Chef processes and files to be ignored.



***Ignore Chef Server Process Writes:**

Should modification by Chef server processes be ignored in order to improve performance?

Chef Server Processes To Ignore:

Carbon Black App Control will ignore modifications by the specified files. You can add or remove items from this list. You should verify that the paths match your Chef configuration. Default entry is: /opt/chef-server/*

Modification Of The Files Specified Here By The Chef Processes Will Be Analyzed:

Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Modification Of Files By Processes Specified Here Will Be Analyzed:

Carbon Black App Control will analyze modification of files by processes specified here. You can add or remove items from this list.

***Ignore Chef Repo Files:**

Should modification the specified Chef Repo files be ignored in order to improve performance?

Chef Repo Files To Ignore:

Carbon Black App Control will ignore modifications by the specified files. You can add or remove items from this list. You should verify that the paths match your Chef configuration. The default entry is: */chef-repo/*

Modification Of The Files Specified Here By The Chef Processes Will Be Analyzed:

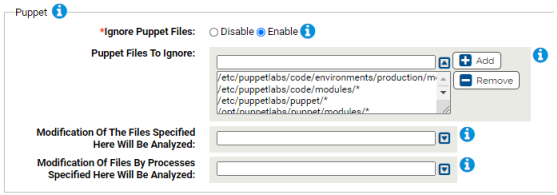
Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list. The default entry is: */chef-repo/*.rb

Modification Of Files By Processes Specified Here Will Be Analyzed:

Carbon Black App Control will analyze modification of files by processes specified here. You can add or remove items from this list.

Puppet

Use this group to specify Puppet files to be ignored.



***Ignore Puppet Files:**

Should modification of the specified Puppet files be ignored in order to improve performance?

Puppet Files To Ignore:

Carbon Black App Control will ignore modifications by the specified files. You can add or remove items from this list. You should verify that the paths match your Puppet configuration. The default file list is as follows:

- /etc/puppetlabs/code/environments/production/modules/*
- /etc/puppetlabs/code/modules/*
- /etc/puppetlabs/puppet/*
- /opt/puppetlabs/puppet/modules/*

Modification Of The Files Specified Here Will Be Analyzed:

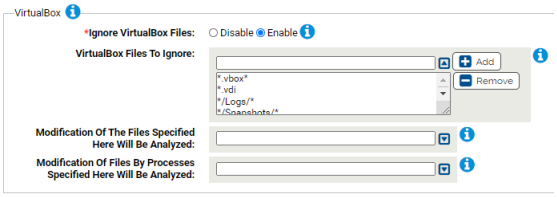
Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Modification Of Files By Processes Specified Here Will Be Analyzed:

Carbon Black App Control will analyze modification of files by processes specified here. You can add or remove items from this list.

VirtualBox

Use this group to specify VirtualBox files to be ignored.



***Ignore VirtualBox Files:**

Should modification of the specified VMWare files be ignored in order to improve performance?

VirtualBox Files To Ignore:

Carbon Black App Control will ignore modifications by the specified files. You can add or remove items from this list. The following are listed by default:

- *.vbox*
- *.vdi*/Logs/*
- */Snapshots/*

Modification Of The Files Specified Here Will Be Analyzed:

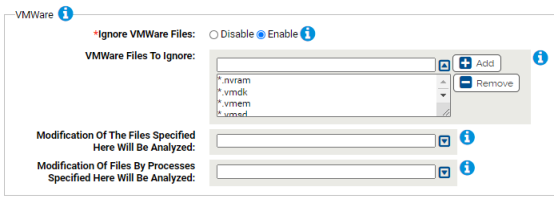
Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Modification Of Files By Processes Specified Here Will Be Analyzed:

Carbon Black App Control will analyze modification of files by processes specified here. You can add or remove items from this list.

VMWare

Use this group to specify VMWare files to be ignored.



***Ignore VMWare Files:**

Should modification of the specified VMWare files be ignored in order to improve performance?

VMWare Files To Ignore:

Carbon Black App Control will ignore modifications by the specified files. You can add or remove items from this list. The following files are listed by default:

- *.nvram
- *.vmdk
- *.vmem
- *.vmsd
- *.vmsn

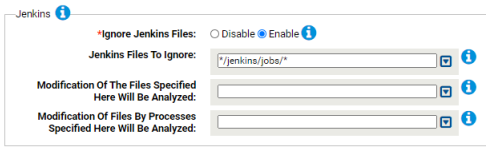
- *.vmss
- *.vmxf

Modification Of The Files Specified Here Will Be Analyzed:
Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Modification Of Files By Processes Specified Here Will Be Analyzed:
Carbon Black App Control will analyze modification of files by processes specified here. You can add or remove items from this list.

Jenkins

Use this group to specify Jenkins files to be ignored.



***Ignore Jenkins Files:**
Should modification of the specified Jenkins files be ignored in order to improve performance?

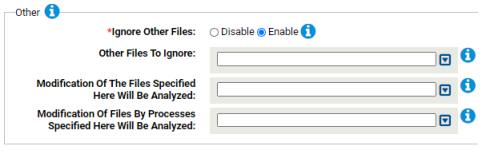
Jenkins Files To Ignore:
Carbon Black App Control will ignore modifications by the specified files. You can add or remove items from this list. The following is listed by default: */jenkins/jobs/*

Modification Of The Files Specified Here Will Be Analyzed:
Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Modification Of Files By Processes Specified Here Will Be Analyzed:
Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Other

Use this group to specify other files to be ignored.



***Ignore Other Files:**
Should modification of the specified files be ignored in order to improve performance?

Other Files To Ignore:

Carbon Black App Control will ignore modifications by the specified files. You can add or remove items from this list.

Modification Of The Files Specified Here Will Be Analyzed:

Carbon Black App Control will analyze modification of files specified here. You can add or remove items from this list.

Modification Of Files By Processes Specified Here Will Be Analyzed:

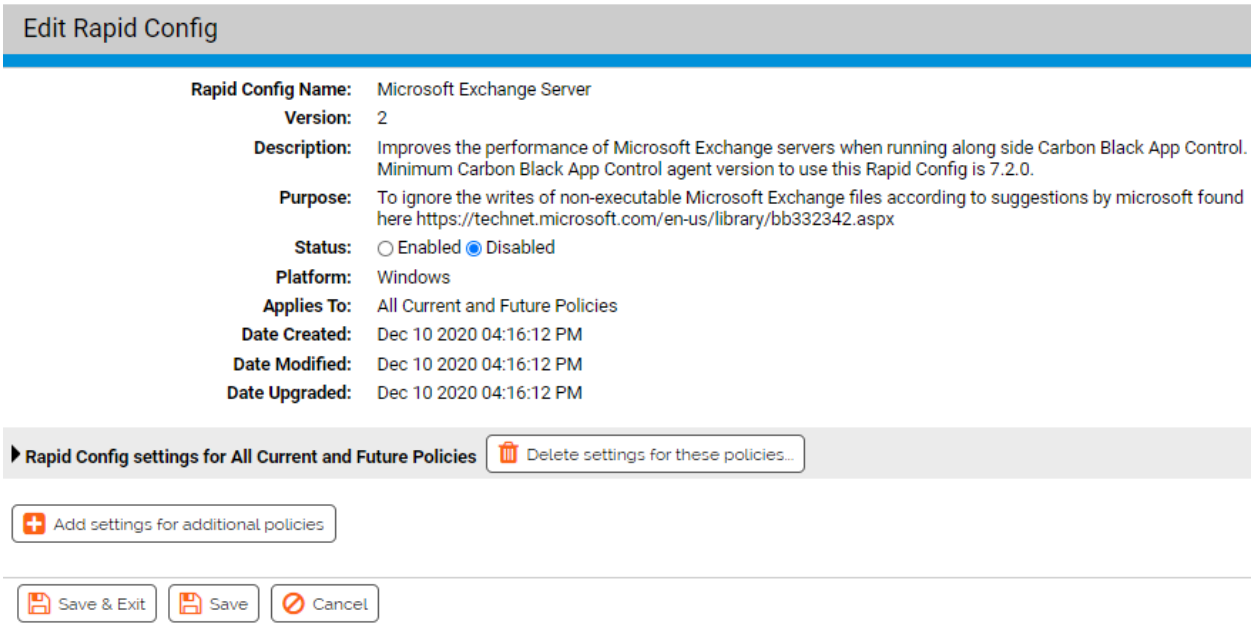
Carbon Black App Control will analyze modification of files by processes specified here. You can add or remove items from this list.

Microsoft Exchange Server Rapid Config

Purpose:To ignore the writes of non-executable Microsoft Exchange files according to suggestions by microsoft found here: https://technet.microsoft.com/en-us/library/bb332342.aspx

Description: Improves the performance of Microsoft Exchange servers when running along side Carbon Black App Control.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



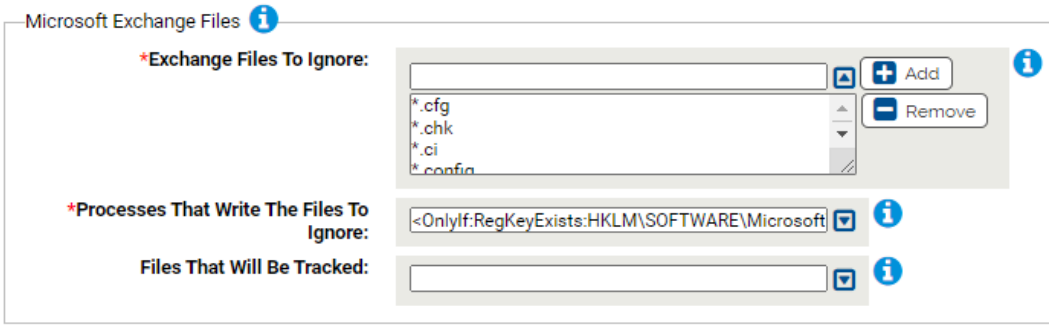
Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

Microsoft Exchange Files

Use this group to specify Microsoft Exchange related files that will be ignored by Carbon Black App Control when they are written by the processes specified below.



***Exchange Files To Ignore:**

Carbon Black App Control will ignore writes of these specified Microsoft Exchange Files. You can add or remove items from this list.

- *.cfg
- *.chk
- *.ci
- *.config
- *.dia
- *.dir
- *.dsc
- *.edb
- *.grxml
- *.jrs
- *.jsl
- *.log
- *.lzx
- *.que
- *.txt
- *.wid
- *.wsb
- *.000
- *.001
- *.002

***Processes That Write The Files To Ignore:**

Carbon Black App Control will ignore writes to the specifed files by these processes. You can add or remove items from this list. Default entry is: <OnlyIf:RegKeyExists:HKLM\SOFTWARE\Microsoft\ExchangeServer><ProgramFiles>\Microsoft\Exchange Server*

Files That Will Be Tracked:

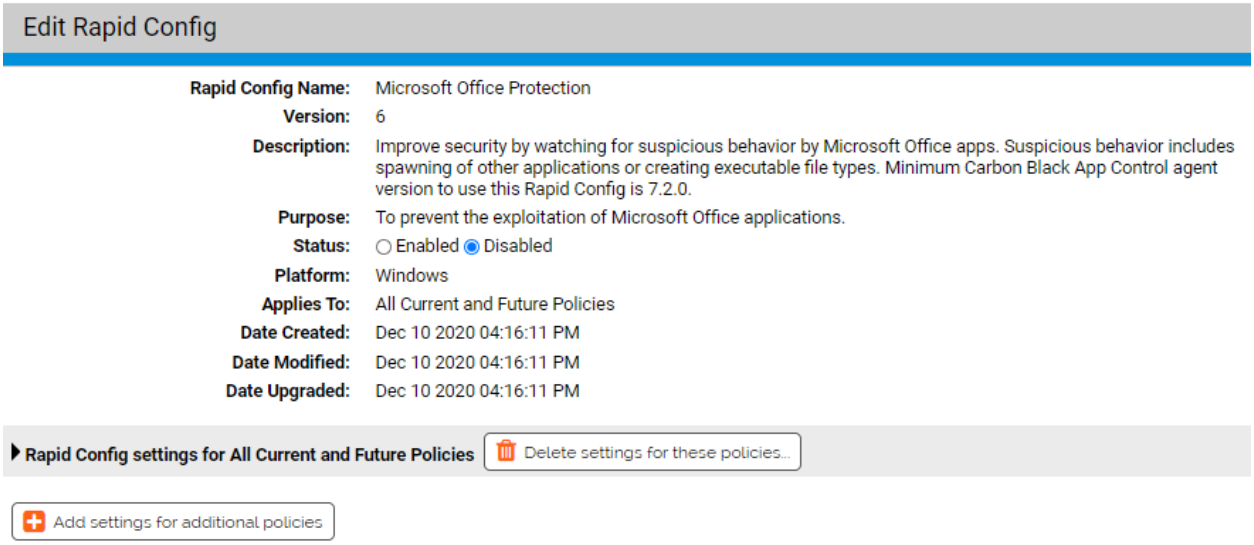
If there are files that are being ignored that should be tracked add them here.

Microsoft Office Protection Rapid Config

Purpose:To prevent the exploitation of Microsoft Office applications.

Description: Improve security by watching for suspicious behavior by Microsoft Office apps. Suspicious behavior includes spawning of other applications or creating executable file types.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



Rapid Config Settings

As with most rapid configs, you can:

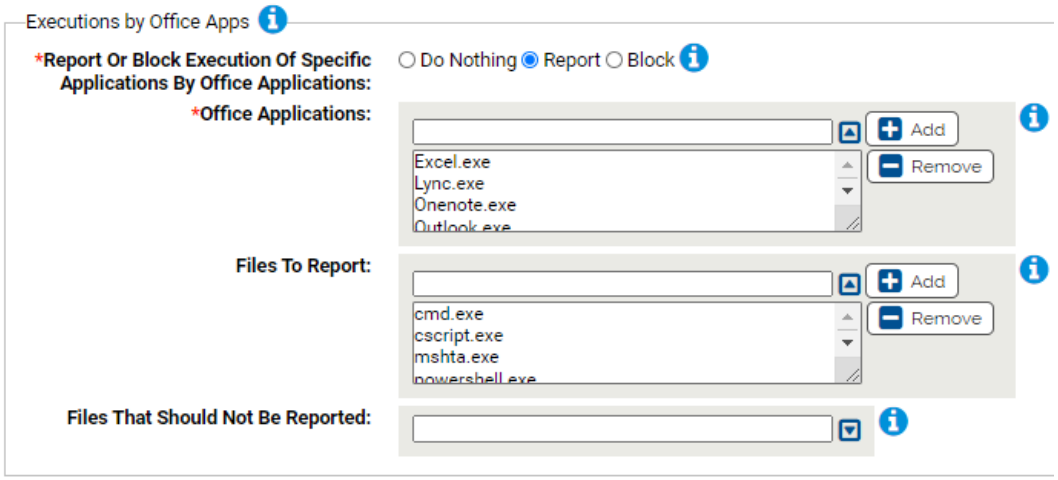
- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors. For each of the following sections, specify what action you require.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

Executions by Office Apps

Use this group to protect against Office Apps running other applications.



***Report Or Block Execution Of Specific Applications By Office Applications:**
Should execution of the specified files by Office applications be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

***Office Applications:**

Carbon Black App Control will report or block execution of specific files by these Microsoft Office applications. You can add or remove items from this list. By default, the list is:

- Excel.exe
- Lync.exe
- Onenote.exe
- Outlook.exe
- Powerpnt.exe
- Winword.exe

Files To Report:

Carbon Black App Control will report or block execution of the specified files by Microsoft Office applications.

In order to prevent the possibility of a malicious process copying, renaming, and executing a script interpreter to bypass the list of filenames here, we recommend enabling the 'Script Processors' Rapid Config. This Rapid Config identifies script interpreters using the Yara detection engine and can prevent the process from running even if the file has been renamed. By default, the list is:

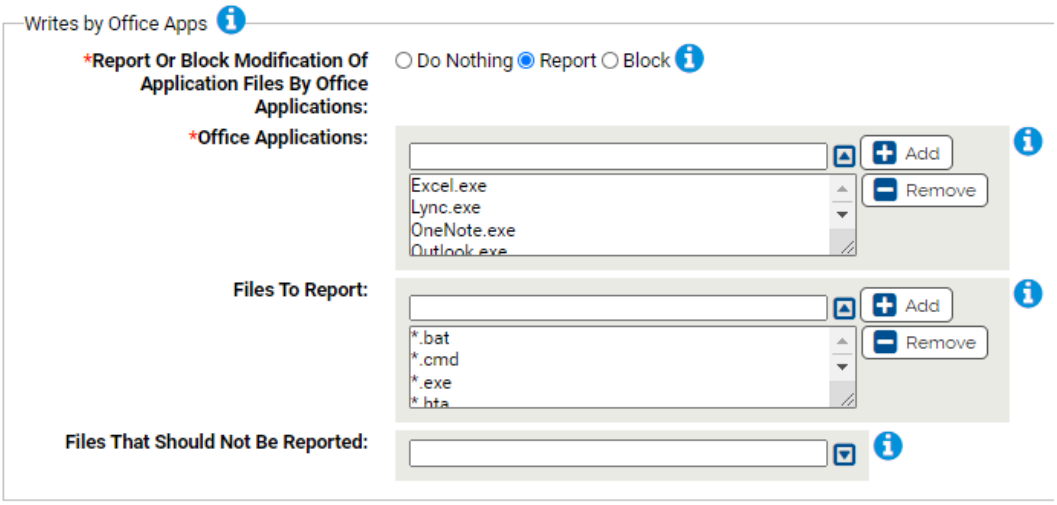
- cmd.exe
- cscript.exe
- mshta.exe
- powershell.exe
- regsvr32.exe
- winrm.exe
- wmic.exe
- wscript.exe

Files That Should Not Be Reported:

Execution of the files specified here will not be reported. You can add or remove items from this list.

Writes by Office Apps

Use this group to protect against Office Apps creating executable files.



***Report Or Block Modification Of Application Files By Office Applications:**

Should modification of the specified files by Microsoft Office applications be reported or blocked? You should validate that legitimate modification will not be blocked before enabling blocking.

***Office Applications:**

Carbon Black App Control will report or block writes of specific files by these Microsoft Office applications. You can add or remove items from this list. By default, the files listed are:

- Excel.exe
- Lync.exe
- OneNote.exe
- Outlook.exe
- Powerpnt.exe
- Winword.exe

Files To Report:

Carbon Black App Control will report or block modifications of the specified files by Microsoft Office applications. You can add or remove items from this list. By default, the files listed are:

- *.bat*.cmd
- *.exe
- *.hta
- *.ps1
- *.psm1
- *.scr
- *.vbe
- *.vbs
- *.wsc
- *.wsf

Files That Should Not Be Reported:

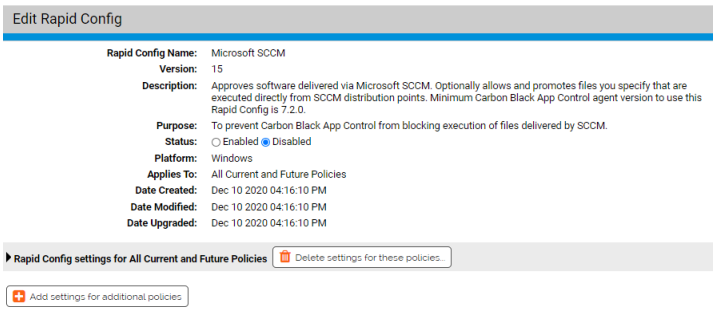
Modifications to the files specified here will not be reported. You can add or remove items from this list.

Microsoft SCCM Rapid Config

Purpose:To prevent Carbon Black App Control from blocking execution of files delivered by SCCM.

Description: Approves software delivered via Microsoft SCCM. Optionally allows and promotes files you specify that are executed directly from SCCM distribution points.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



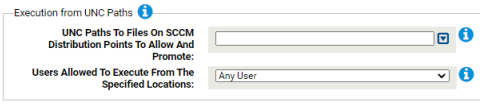
Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

Execution from UNC Paths

Use this group to specify the location of files executed directly from SCCM distribution points and the users allowed to run them. The parameters in this group are optional. They are only necessary in order to allow and promote execution from SCCM distribution points if desired.



UNC Paths To Files On SCCM Distribution Points To Allow And Promote:

Required if any package or part of a package may execute directly from the UNC share path on an SCCM distribution point. Some packages may execute remotely, instead of from the CCM Cache folder on the endpoint. Consult with your SCCM administrator about whether this happens in your environment. You may use wildcards to help represent a naming pattern for the distribution points. DFS aliases are not sufficient, you must enter the individual server names.

Users Allowed To Execute From The Specified Locations:

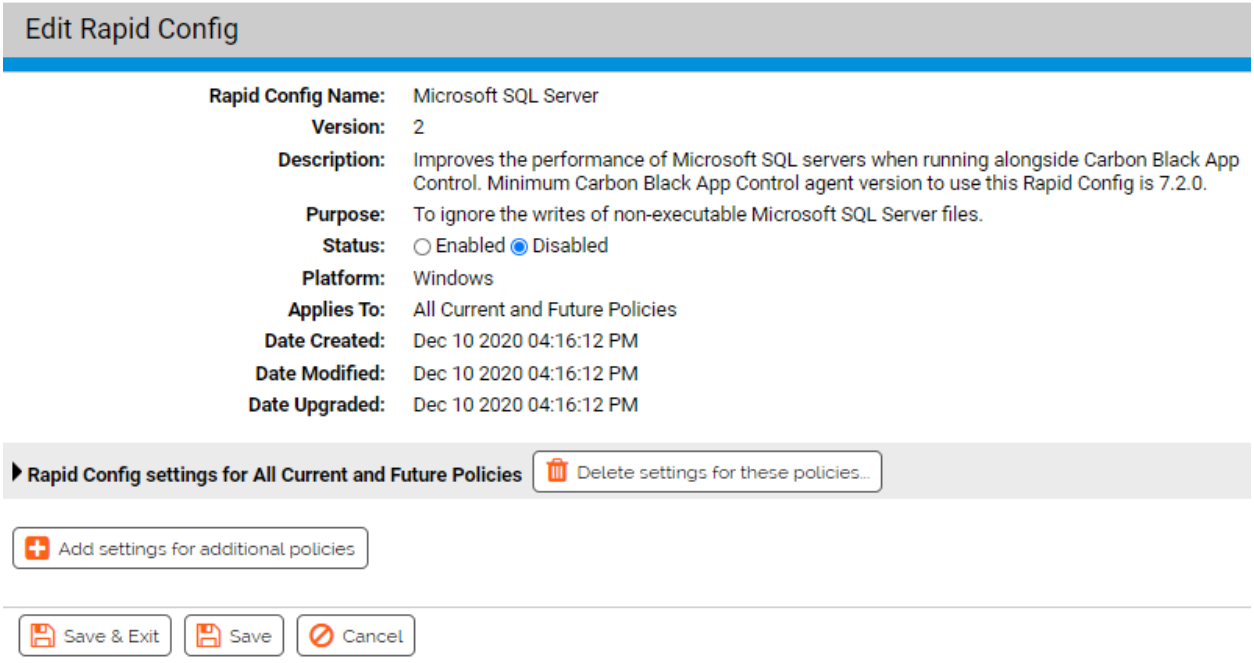
If you specified UNC paths from which files may be execute, you can specify here which users can execute the files.

Microsoft SQL Server Rapid Config

Purpose:To ignore the writes of non-executable Microsoft SQL Server files.

Description: Improves the performance of Microsoft SQL servers when running alongside Carbon Black App Control.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



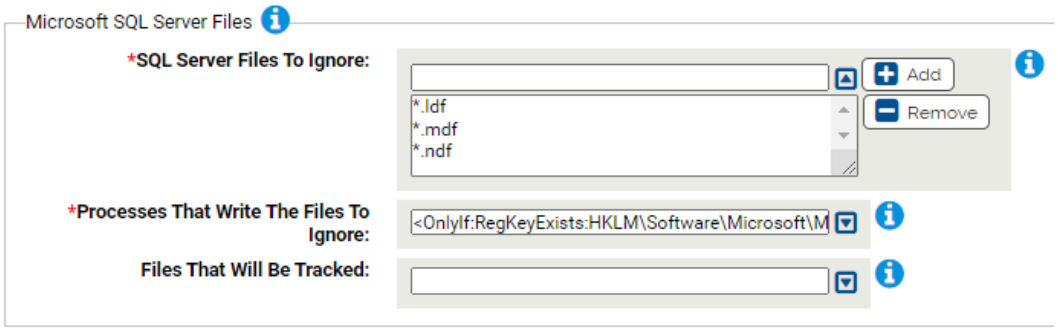
Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

Microsoft SQL Server Files

This group allows you to specify Microsoft SQL Server related files that will be ignored by Carbon Black App Control when they are written by the processes specified below.



***SQL Server Files To Ignore:**

Carbon Black App Control will ignore writes of these specified Microsoft SQL Server Files. You can add or remove items from this list.

- *.ldf
- *.mdf
- *.ndf

***Processes That Write The Files To Ignore:**

Carbon Black App Control will ignore writes to the specifed files by these processes. You can add or remove items from this list. The default entry is as follows: <OnlyIf:RegKeyExists:HKLM\Software\Microsoft\Microsoft SQL Server><ProgramFiles>\Microsoft SQL Server*

Files That Will Be Tracked:

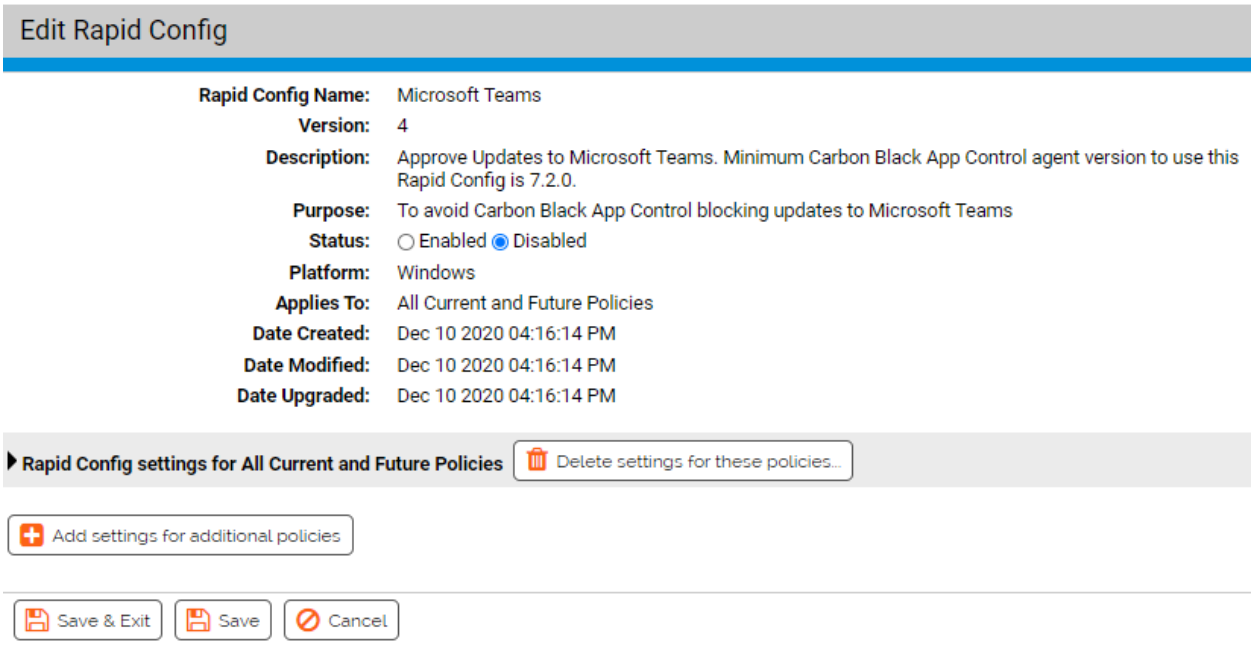
If there are files that are being ignored that should be tracked add them here.

Microsoft Teams Rapid Config

Purpose:To avoid Carbon Black App Control blocking updates to Microsoft Teams

Description: Approve Updates to Microsoft Teams.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



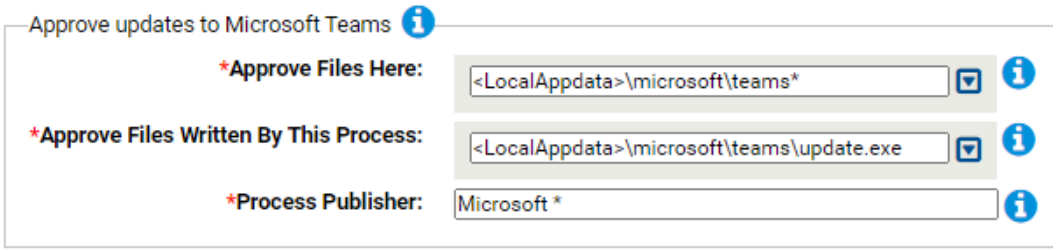
Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

Approve updates to Microsoft Teams

Approve writes to the specified locations by the specified processes if the processes have the specified publisher.



***Approve Files Here:**
Files written here will be approved when written by the specified process.
The default entry is: <LocalAppdata>\microsoft\teams*

***Approve Files Written By This Process:**
Files written by this process to the above location will be approved.
The default entry is: <LocalAppdata>\microsoft\teams\update.exe

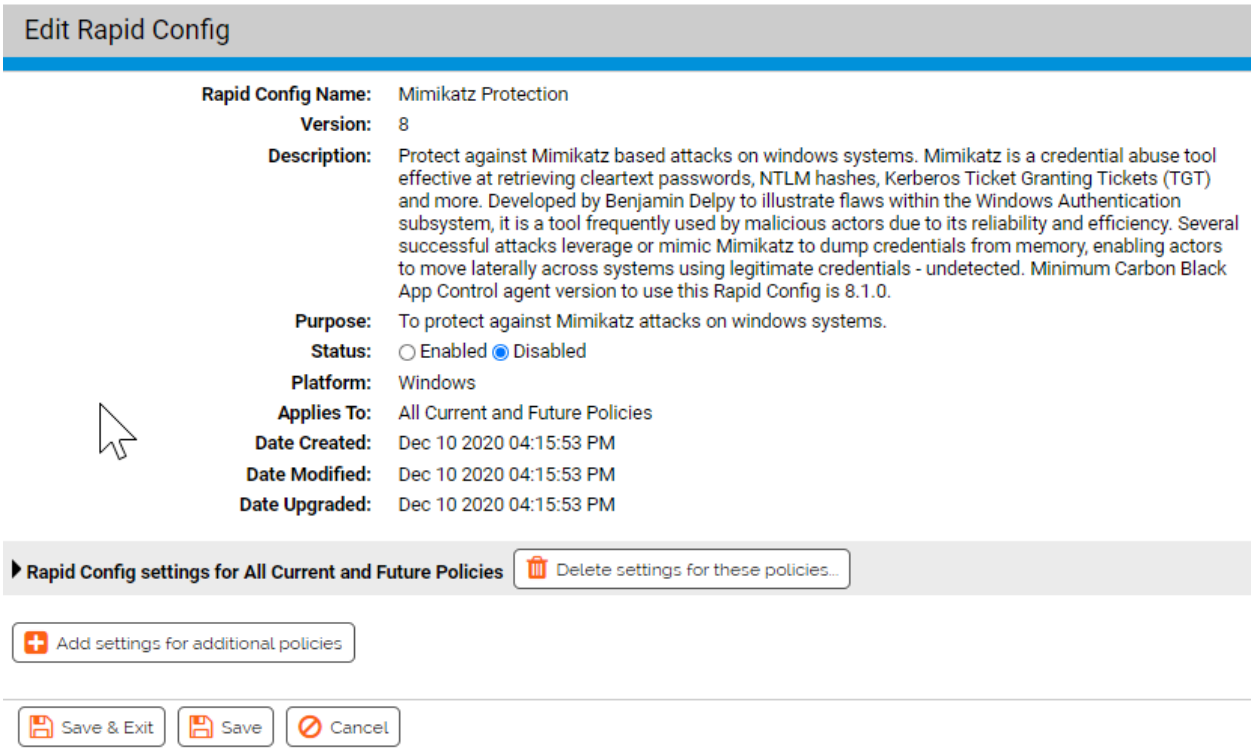
***Process Publisher:**
Files written by the above process to the above location will be approved if the process is signed by this publisher.
This is a single value field. The value can contain wild cards. For example *Microsoft* would mean all publisher names that contain the word Microsoft.
The default entry is: Microsoft *

Mimikatz Rapid Config

Purpose:To protect against Mimikatz attacks on windows systems.

Description: Protect against Mimikatz based attacks on windows systems. Mimikatz is a credential abuse tool effective at retrieving cleartext passwords, NTLM hashes, Kerberos Ticket Granting Tickets (TGT) and more. Developed by Benjamin Delpy to illustrate flaws within the Windows Authentication subsystem, it is a tool frequently used by malicious actors due to its reliability and efficiency. Several successful attacks leverage or mimic Mimikatz to dump credentials from memory, enabling actors to move laterally across systems using legitimate credentials - undetected.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.1.0



What is Mimikatz

Mimikatz started life as a GitHub project by Benjamin Delpy to illustrate flaws within the Windows Authentication subsystem. It is a tool that can extract plain text passwords, NTLM hashes, Kerberos Ticket Granting Tickets (TGT), and more from memory.

Malicious actors have leveraged this technology to infiltrate environments and move laterally across systems using legitimate credentials…undetected.

How can App Control help?

An endpoint in default deny mode (or what we like to call High Enforcement) will be protected from a binary-based Mimikatz attack because the process used to launch the attack will not be approved and therefore blocked.

App Control can protect endpoints in other enforcement levels against binary and memory based attacks with the use of the Mimikatz Protection Rapid Config.

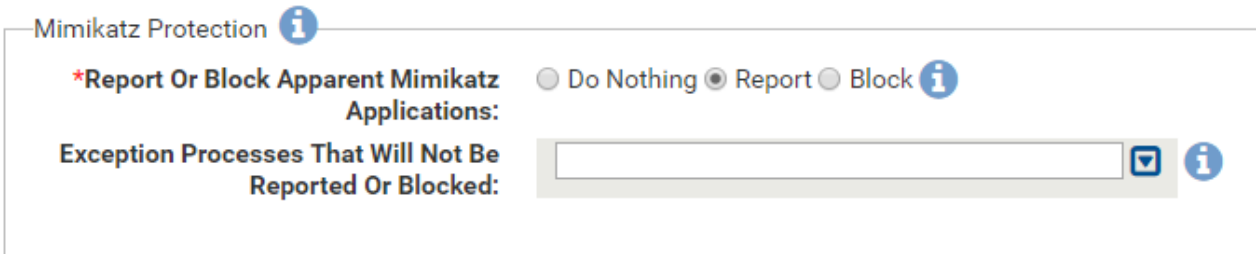
Rapid Config Settings

The Mimikatz Protection Rapid Config has three sections that look for different indicators of compromise.

Report, Block, or Do Nothing

As with most Rapid Configs, you can choose to **Do Nothing**, **Report**, or **Block** the items or behaviors. In this case, you can Report or Block on the detection of a combination of DLLs loading. This particular combination (cryptdll.dll, hid.dll, samlib.dll, vaultcli.dll, and winscard.dll) is a good indication of a Mimikatz process as these are not typically loaded at the same time by other processes.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.



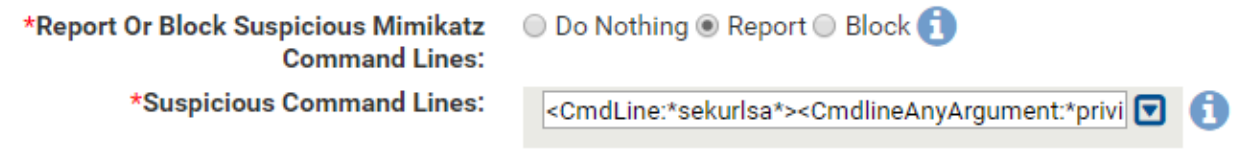
As with all Rapid Configs we recommend setting each section to Report prior to setting to Block. You will want to ensure that the legitimate behavior of these dlls will not be impacted.

Command Lines

The second section of the Rapid Config looks for specific command lines. It will look for:

sekurlsa anywhere within the command line. Sekurlsa is a Mimikatz module that extracts passwords, keys, etc from the memory of lsass.

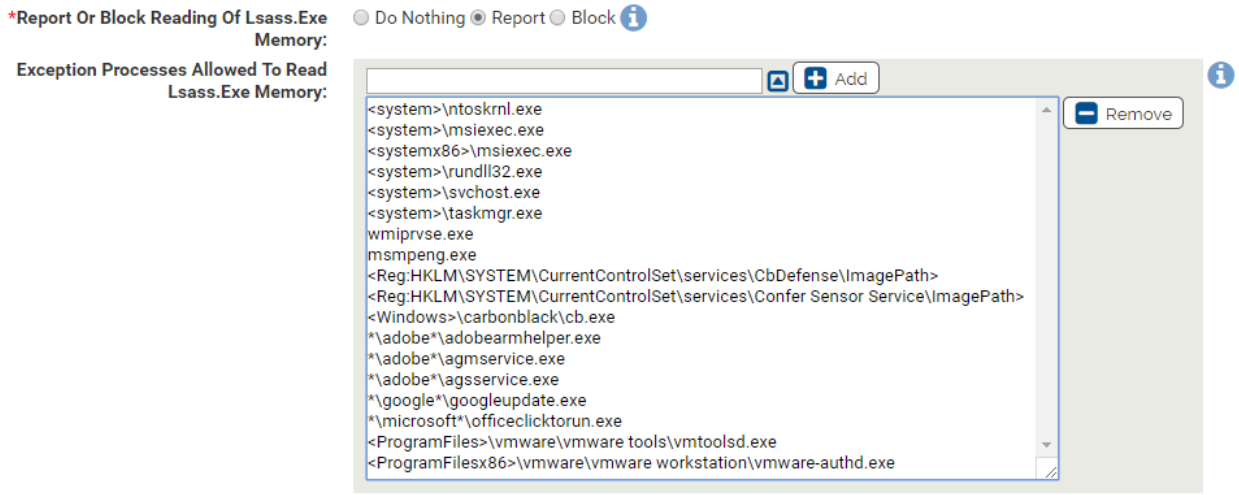
*privilege*debug* in the command line argument. The combination of “privilege” and “debug” within a command line argument is typically used by Mimikatz to get access rights.



*These command line arguments can be changed by a malicious actor, we believe the default arguments will help catch low hanging fruit.

Reading Lsass.exe Memory

The final section of the Rapid Config centers on the reading of Lsass.exe memory.



Most processes should not be reading from lsass memory, however there are executables that legitimately need to do this. Out of the box we’ve included processes like ntoskrnl.exe, msiexec.exe, svchost.exe, and others that should be allowed to read the memory.

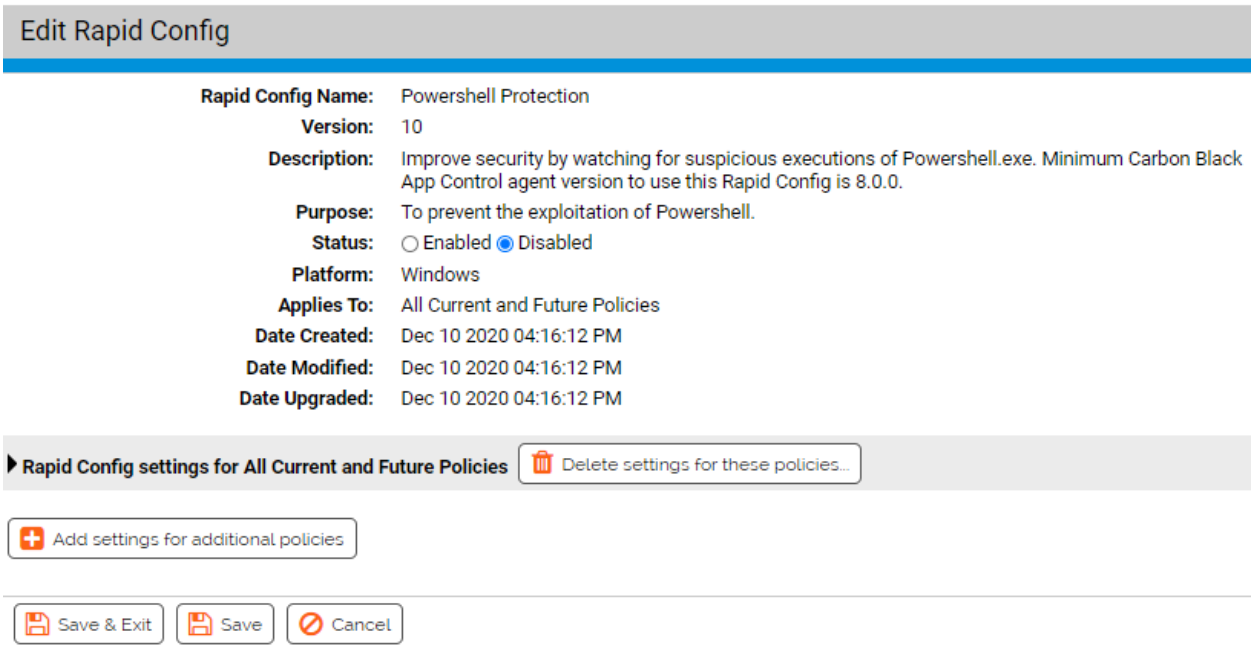
It is crucial to initially set this section to Report so that you can find that approved applications in your environment that legitimately need to read the lsass process memory. After letting the Rapid Config run in Report mode for a few weeks, add any approved processes that access lsass memory to the exception list.

Powershell Protection Rapid Config

Purpose:To prevent the exploitation of Powershell.

Description: Improve security by watching for suspicious executions of Powershell.exe.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

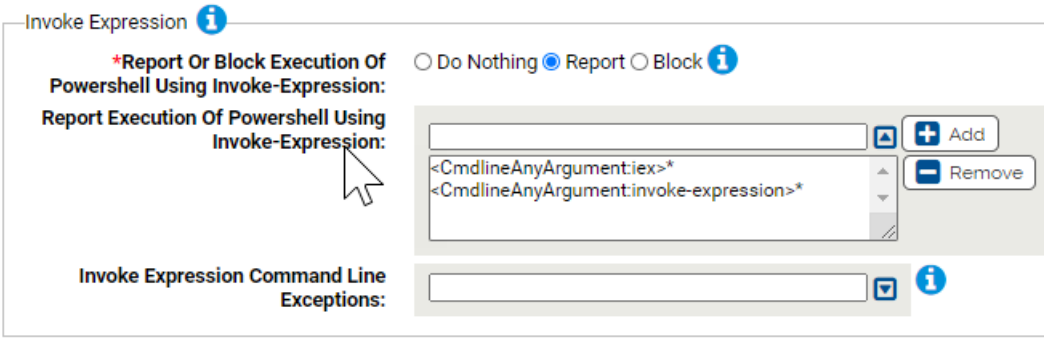
RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

For each of the following sections, specify what action you require.

Invoke Expression

Use this group to protect against execution of powershell using the invoke-expression command line.

Invoke-Expression is sometimes used by attackers to download and dynamically execute content.



***Report Or Block Execution Of Powershell Using Invoke-Expression:**
Should execution of powershell using invoke-expression be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

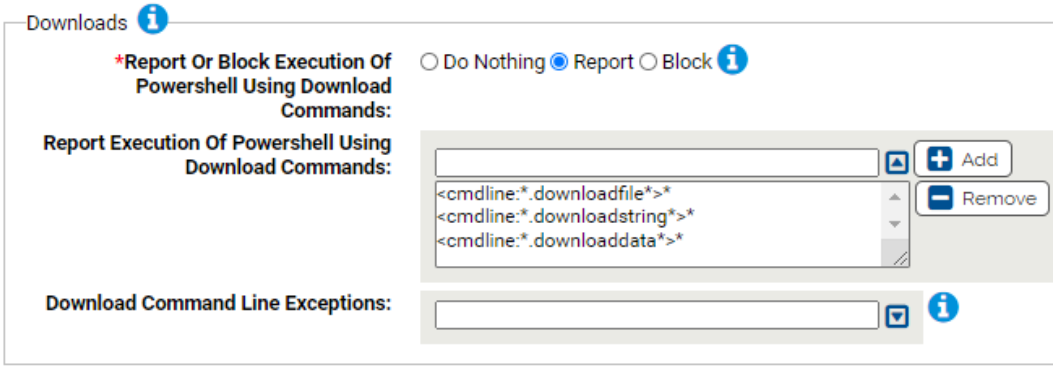
Report Execution Of Powershell Using Invoke-Expression:
Carbon Black App Control will report or block execution of powershell using these command lines. You can add or remove items from this list. By default, the list includes:

- <CmdlineAnyArgument:iex>*
- <CmdlineAnyArgument:invoke-expression>*

Invoke Expression Command Line Exceptions:
Command lines that will not be reported or blocked. You can add or remove items from this list.

Downloads

Use this group to protect against execution of powershell using the download commands to download malicious files.



***Report Or Block Execution Of Powershell Using Download Commands:**
Should execution of powershell using download commands be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

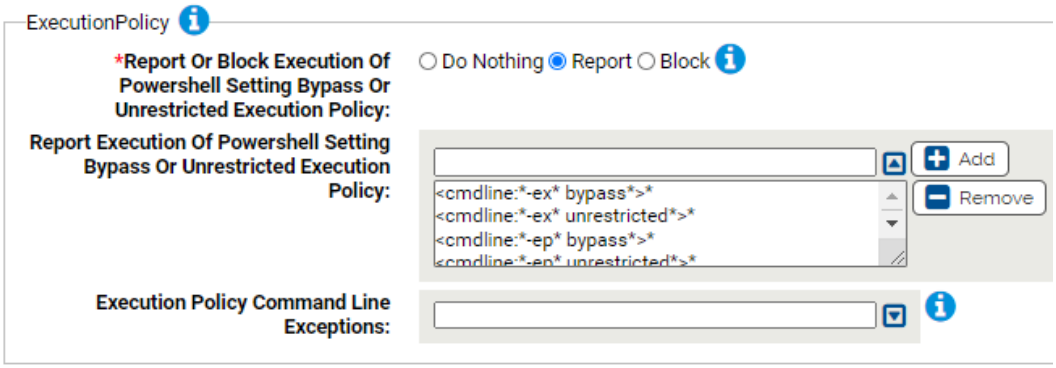
Report Execution Of Powershell Using Download Commands:
Carbon Black App Control will report or block execution of powershell using these command lines. You can add or remove items from this list. By default, the command list is as follows:

- <cmdline:*.downloadfile*>*
- <cmdline:*.downloadstring*>*
- <cmdline:*.downloaddata*>*

Download Command Line Exceptions:
Command lines that will not be reported or blocked. You can add or remove items from this list.

Execution Policy

Use this group to protect against powershell setting the ExecutionPolicy via the command line. The default policy is typically Restricted which only allows interactive powershell sessions and single command execution. Attackers can change the policy with the ExecutionPolicy parameter.



***Report Or Block Execution Of Powershell Setting Bypass Or Unrestricted Execution Policy:**

Should execution of powershell with both the -hidden and -encoded parameters be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Report Execution Of Powershell Setting Bypass Or Unrestricted Execution Policy:

Carbon Black App Control will report or block execution of powershell using these command lines. You can add or remove items from this list. By default, the following commands are listed:

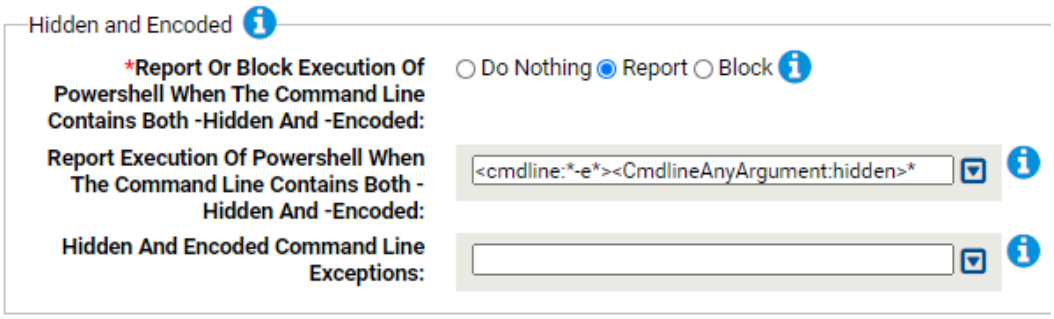
- <cmdline:*-ex* bypass*>*
- <cmdline:*-ex* unrestricted*>*
- <cmdline:*-ep* bypass*>*
- <cmdline:*-ep* unrestricted*>*

Execution Policy Command Line Exceptions:

Command lines that will not be reported or blocked. You can add or remove items from this list.

Hidden and Encoded

Use this group to protect against powershell running in a hidden window and using an encoded command. Powershell attacks will often use the combination of encoded commands and hidden window styles to avoid detection.



***Report Or Block Execution Of Powershell When The Command Line Contains Both -Hidden And -Encoded:**

Should execution of powershell with both the -hidden and -encoded parameters be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Report Execution Of Powershell When The Command Line Contains Both -Hidden And -Encoded:

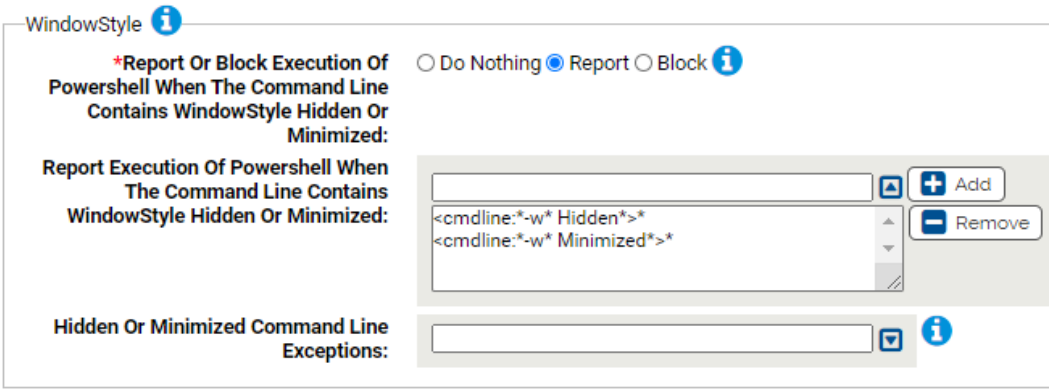
Carbon Black App Control will report or block execution of powershell using these command lines. You can add or remove items from this list. By default, the following is listed: <cmdline:*-e*><CmdlineAnyArgument:hidden>*

Hidden And Encoded Command Line Exceptions:

Command lines that will not be reported or blocked. You can add or remove items from this list.

WindowStyle

Use this group to protect against execution of powershell using -WindowStyle Hidden or WindowStyle -Minimized parameters. This can avoid powershell being hidden or minimized while performing malicious tasks.



***Report Or Block Execution Of Powershell When The Command Line Contains WindowStyle Hidden Or Minimized:**

Should execution of powershell with WindowStyle hidden or minimized be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Report Execution Of Powershell When The Command Line Contains WindowStyle Hidden Or Minimized:

Carbon Black App Control will report or block execution of powershell using these command lines. You can add or remove items from this list. By default, the list includes:

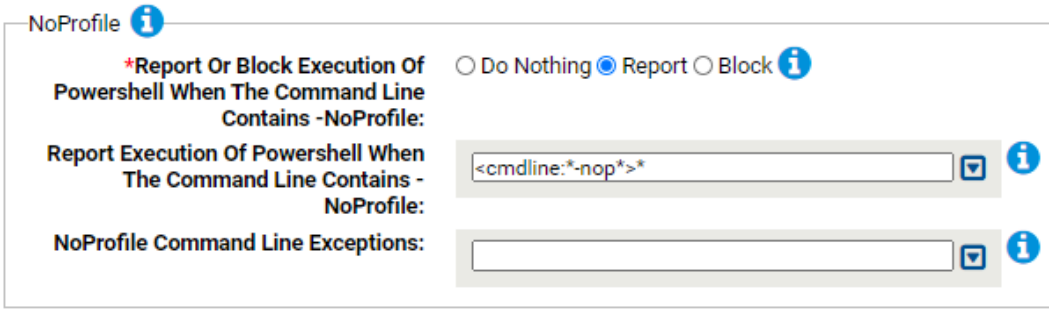
- <cmdline:*-w* Hidden*>*
- <cmdline:*-w* Minimized*>*

Hidden Or Minimized Command Line Exceptions:

Command lines that will not be reported or blocked. You can add or remove items from this list.

NoProfile

Use this group to protect against execution of powershell using the -NoProfile parameter. This can avoid powershell being run without using the profile scripts that have been put in place.



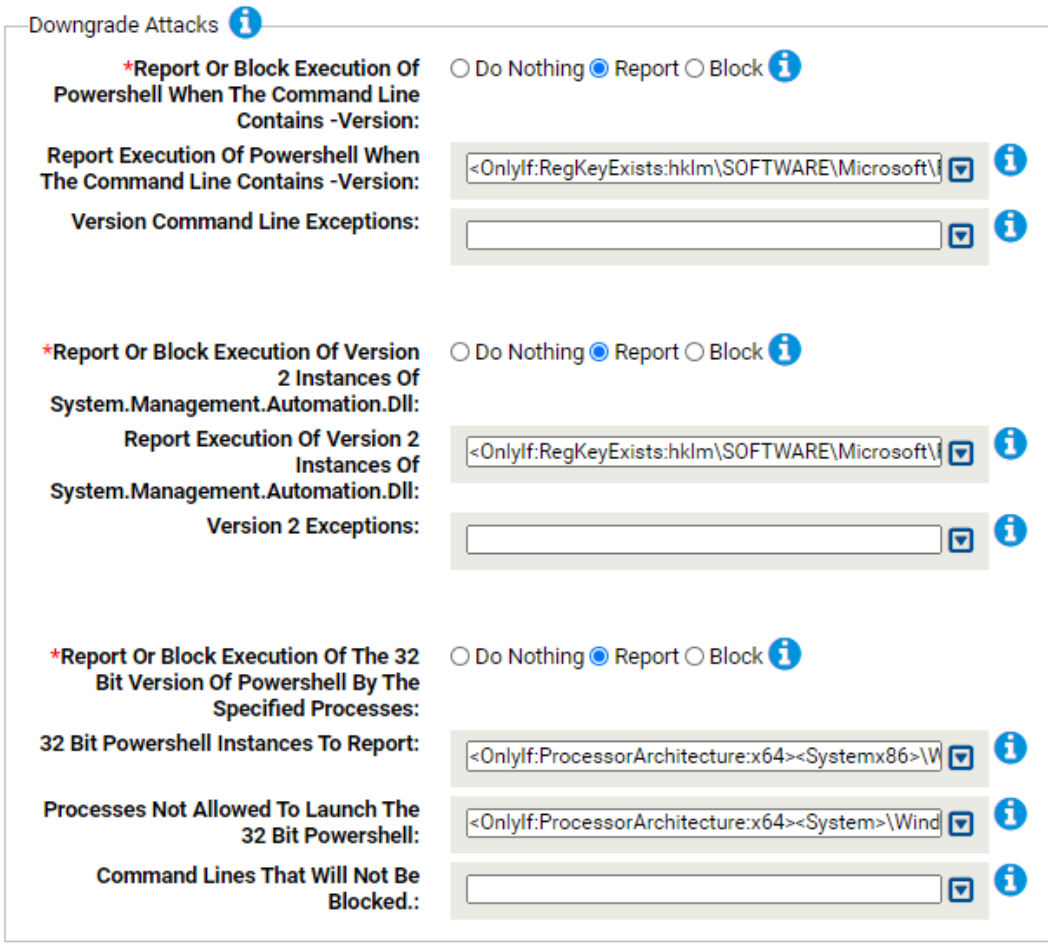
***Report Or Block Execution Of Powershell When The Command Line Contains -NoProfile:**
Should execution of powershell with -NoProfile be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Report Execution Of Powershell When The Command Line Contains -NoProfile:
Carbon Black App Control will report or block execution of powershell using these command lines. You can add or remove items from this list. By default, the following is listed:
<cmdline:*-nop*>*

NoProfile Command Line Exceptions:
Command lines that will not be reported or blocked. You can add or remove items from this list.

Downgrade Attacks

Use this group to protect against powershell downgrade attacks. Downgrade attacks are when the attacker attempts to use an older, more vulnerable version of Powershell.



***Report Or Block Execution Of Powershell When The Command Line Contains -Version:**
Should execution of powershell with -Version be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Report Execution Of Powershell When The Command Line Contains -Version:
Carbon Black App Control will report or block execution of powershell using these command lines. You can add or remove items from this list. By default, the following is listed:
<OnlyIf:RegKeyExists:hklm\SOFTWARE\Microsoft\PowerShell\3><cmdline:*-V*>powershell.exe

Version Command Line Exceptions:
Command lines that will not be reported or blocked. You can add or remove items from this list.

***Report Or Block Execution Of Version 2 Instances Of System.Management.Automation.Dll:**
Should execution of version 2 instances of system.management.automation.dll by powershell be reported or blocked? Carbon Black App Control will block loading the dll by terminating powershell. You should validate that legitimate execution is not blocked before enabling blocking.

Report Execution Of Version 2 Instances Of System.Management.Automation.Dll:
Carbon Black App Control will report or block execution of powershell running older versions of System.Management.Automation*.dll. You can add or remove items from this list. The following listed by default:
<OnlyIf:RegKeyExists:hklm\SOFTWARE\Microsoft\PowerShell\3>*\NativeImages_v2*\System.Management.Automation*.dll

Version 2 Exceptions:
Command lines that will not be reported or blocked. You can add or remove items from this list.

***Report Or Block Execution Of The 32 Bit Version Of Powershell By The Specified Processes:**
Should execution of the 32 bit version of powershell by the specified processes be reported or blocked? Specifically, execution of 32 bit Powershell by 64 bit Powershell can indicate a downgrade attack. You should validate that legitimate execution is not blocked before enabling blocking.

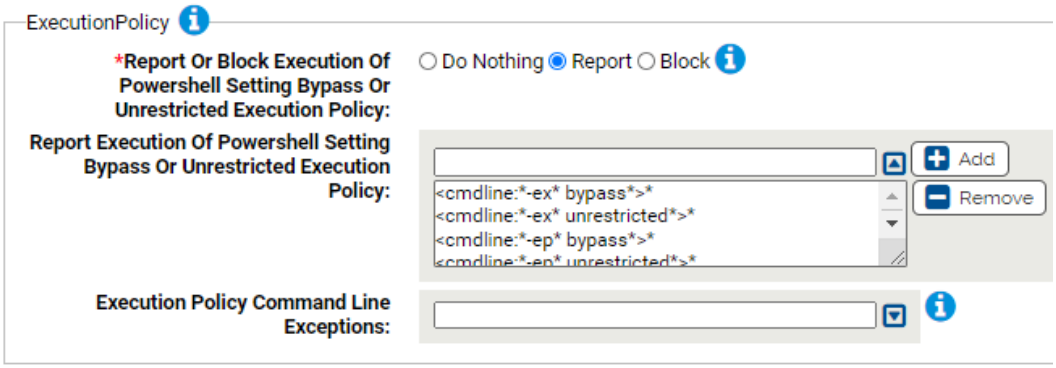
32 Bit Powershell Instances To Report:
Carbon Black App Control will report or block execution of 32 bit powershell instances by the specified processes. By default, the following is listed:
<OnlyIf:ProcessorArchitecture:x64><Systemx86>\WindowsPowerShell*\Powershell.exe

Processes Not Allowed To Launch The 32 Bit Powershell:
Carbon Black App Control will report or block execution of 32 bit powershell instances by the specified processes. By default, the following is listed:
<OnlyIf:ProcessorArchitecture:x64><System>\WindowsPowerShell*\Powershell.exe

Command Lines That Will Not Be Blocked:
Command lines specified here will not be blocked when starting a 32 bit instance of powershell.exe.

Execution Policy Registry Settings

Use this group to protect against modification of Powershell Execution Policy registry settings



***Report Or Block Registry Modification:**

Should modification of the specified Powershell registry settings be reported or blocked? You should validate that legitimate registry modifications are not blocked before enabling blocking.

Report Registry Modification:

Carbon Black App Control will report or block modification of the specified registry settings. You can add or remove items from this list. The default entry is:
HKLM\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy

Processes Allowed To Modify The Specified Registry Settings:

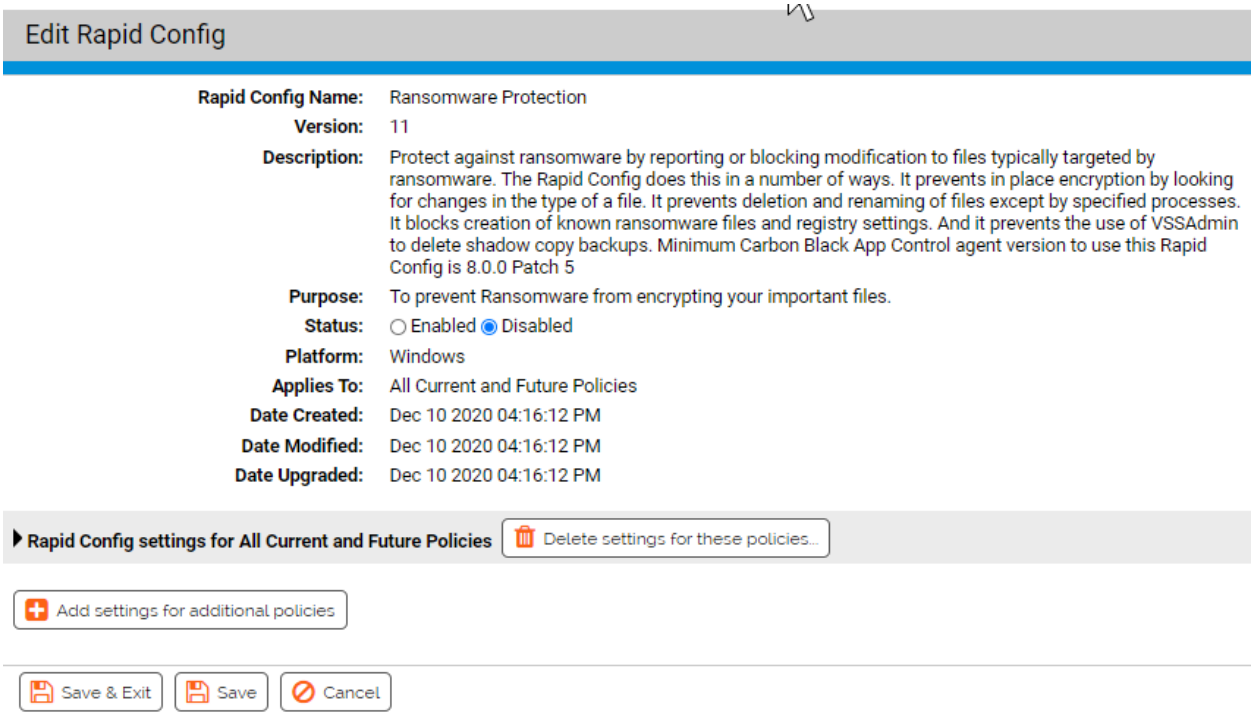
Processes specified here will be allowed to modify the specified registry settings. You can add or remove items from this list. The default entry is:
<windows>\regedit.exe

Ransomware Protection Rapid Config

Purpose:To prevent Ransomware from encrypting your important files.

Description: Protect against ransomware by reporting or blocking modification to files typically targeted by ransomware. The Rapid Config does this in a number of ways. It prevents in place encryption by looking for changes in the type of a file. It prevents deletion and renaming of files except by specified processes. It blocks creation of known ransomware files and registry settings. And it prevents the use of VSSAdmin to delete shadow copy backups.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0 Patch 5



Use Cases:

Out of the box, this Rapid Config is designed to protect all instances of valuable files, such as: *.doc, *.xls, *.gif. Some customers may find that this results in too many false positives that require specific exceptions. For example, application installations and updates often create/remove image and document files that often trigger the protections in the Rapid Config.

Rather than using the out of the box settings and creating a long list of exceptions, you can limit the locations where files are protected. For instance, you could replace the default *.doc setting with *\users\documents*.doc so only doc files under the users' documents folder are protected. This would eliminate the need for most exception cases; however, it limits the protections.

If you take this approach, identify the locations where users create and store their valuable documents and protect those locations.

Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

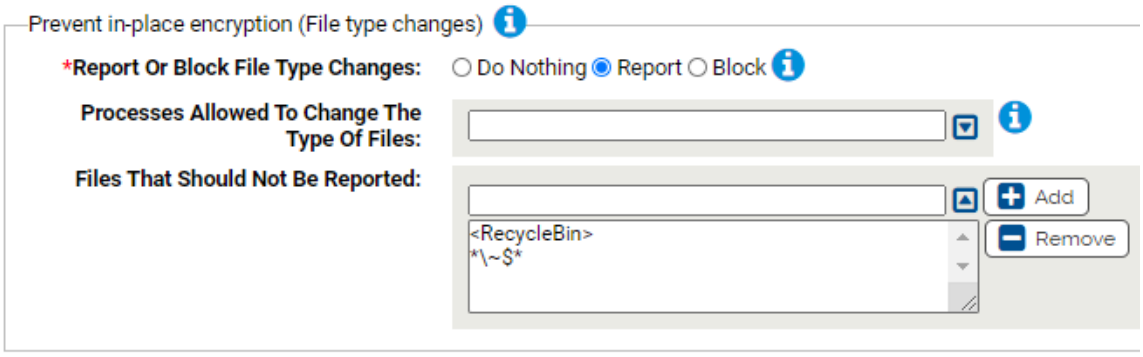
For each of the following sections, specify what action you require.

Prevent in-place encryption (File type changes)

This group allows you to protect files from Ransomware by blocking in place encryption of files. Carbon Black App Control does this by looking for a change in the type of the file.

The protected file types are: doc, docm, docx, xls, xlsm, xlsx, ppt, pptm, pptx, rtf, pdf, png, jpg, jpeg, bmp, giff, and tiff.

In addition to blocking the file type change we will terminate the application attempting the change.



***Report Or Block File Type Changes: Do Nothing Report Block**

This group allows you to protect files from Ransomware by blocking in place encryption of files. Carbon Black App Control does this by looking for a change in the type of the file.

The protected file types are:

doc, docm, docx, xls, xlsm, xlsx, ppt, pptm, pptx, rtf, pdf, png, jpg, jpeg, bmp, giff, and tiff.

In addition to blocking the file type change we will terminate the application attempting the change.

Processes Allowed To Change The Type Of Files:

Processes specified here will be allowed to change the type of the specified files. You can add or remove items from this list.

Files That Should Not Be Reported:

Type changes of files specified here will not be reported. You can add or remove items from this list.

Files listed here must be one of the protected types:

The file types we protect are:

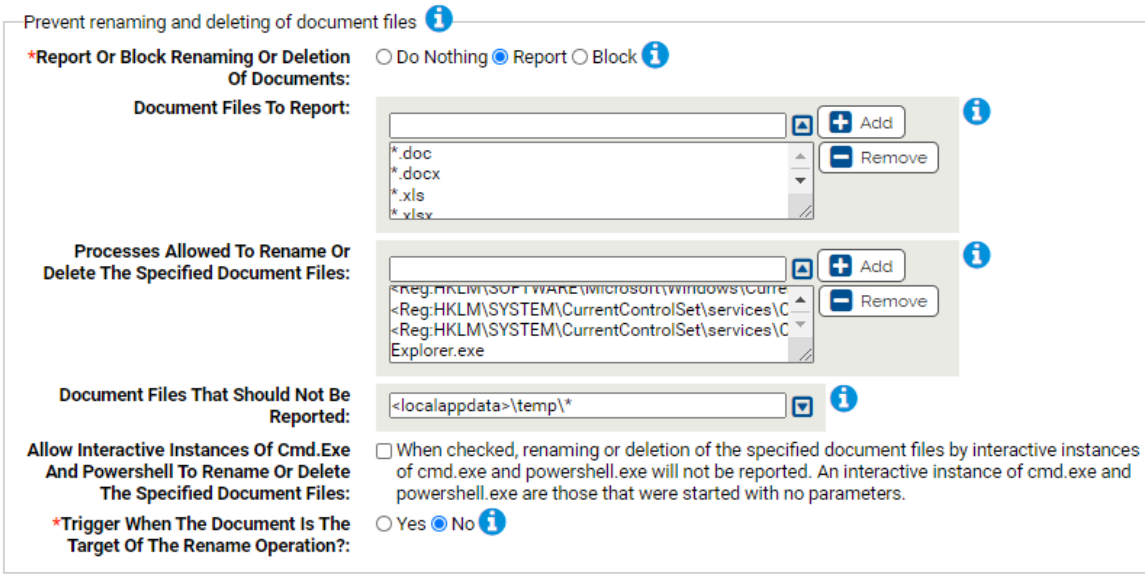
doc, docm, docx, xls, xlsm, xlsx, ppt, pptm, pptx, rtf, pdf, png, jpg, jpeg, bmp, giff, and tiff.

The default exception for *\~$* files is for Microsoft Office owner files. Microsoft uses these files to identify the user that has an office file open in a shared location. The files have the same extensions as Office files but not the same content. By default, the following are listed:

- <RecycleBin>
- *\~$*

Prevent renaming and deleting of document files

This group allows you to protect document files from Ransomware by limiting the processes that are allowed to delete or rename those files.



***Report Or Block Renaming Or Deletion Of Documents:**

Should renaming or deletion of the specified document types be reported or blocked? You should validate that legitimate behavior would not be blocked before enabling blocking.

Document Files To Report:

Carbon Black App Control will report or block renaming or deletion of the specified documents. You can add or remove items from this list. By default, the list is as follows:

- *.doc
- *.docx
- *.xls
- *.xlsx
- *.ppt
- *.pptx
- *.pst*
- .pdf

Processes Allowed To Rename Or Delete The Specified Document Files:

Processes specified here will be allowed to rename or delete the specified documents. You can add or remove items from this list. By default, the following are listed:

- <Reg:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Winword.exe\path>Winword.exe
- <Reg:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\excel.exe\path>excel.exe
- <Reg:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\powerpnt.exe\path>Powerpnt.exe
- <Reg:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\outlook.exe\path>Outlook.exe
- <Reg:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\lync.exe\path>lynchtmlconv.exe
- <Reg:HKLM\SYSTEM\CurrentControlSet\services\CbDefense\ImagePath>
- <Reg:HKLM\SYSTEM\CurrentControlSet\services\Confer Sensor Service\ImagePath>
- Explorer.exe

Document Files That Should Not Be Reported:

Renaming or deletion of files specified here will not be reported. You can add or remove items from this list. The following is listed by default: <localappdata>\temp*

Allow Interactive Instances Of Cmd.Exe And Powershell To Rename Or Delete The Specified Document Files:

When checked, renaming or deletion of the specified document files by interactive instances of cmd.exe and powershell.exe will not be reported. An interactive instance of cmd.exe and powershell.exe are those that were started with no parameters.

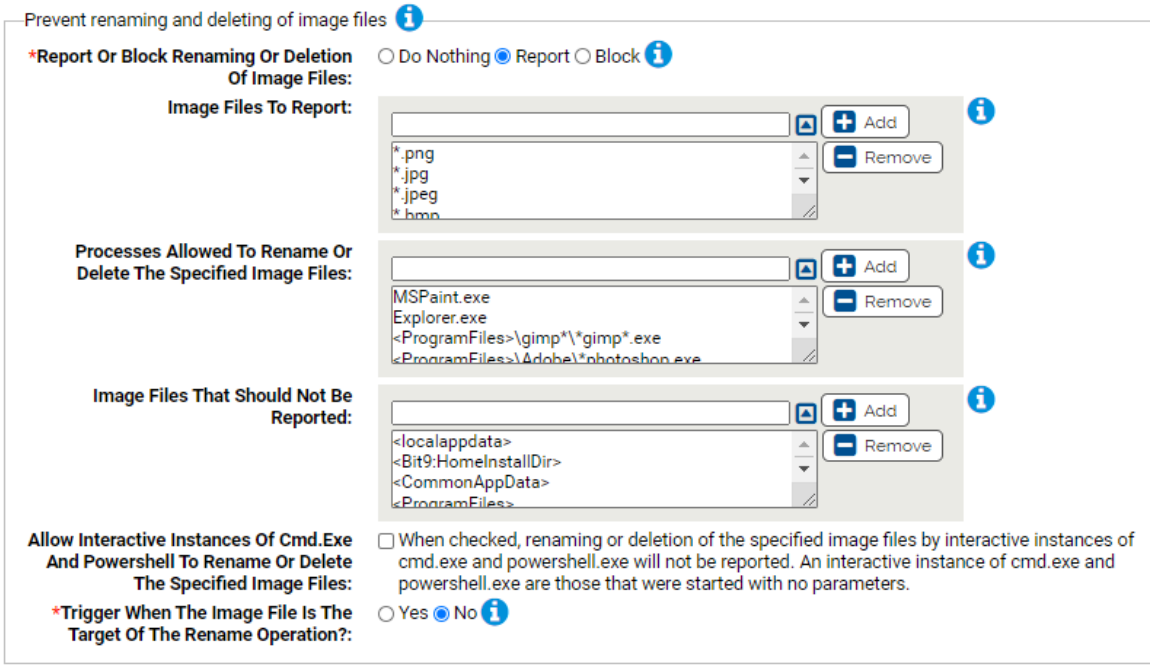
***Trigger When The Document Is The Target Of The Rename Operation?:**

Should the Rapid Config prevent renames when the document is the TARGET of the rename?

Selecting No will cause the rules to only trigger when the document is the source of a rename say from MyFile.Doc to MyFile.Encrypted.
Selecting Yes will also catch when an encrypted file is renamed to a document file. Selecting Yes could result in more false positives but some ransomware variants do use rename when overwriting existing files with encrypted ones.

Prevent renaming and deleting of image files

This group allows you to protect Image files from ransomware by limiting the process that are allowed to delete or rename the files.



***Report Or Block Renaming Or Deletion Of Image Files:**

Should renaming or deletion of the specified image file types be reported or blocked? You should validate that legitimate behavior would not be blocked before enabling blocking.

Image Files To Report:

Carbon Black App Control will report or block renaming or deletion of the specified image files. You can add or remove items from this list. The following are listed by default:

- *.png
- *.jpg
- *.jpeg
- *.bmp
- *.gif

- *.tif
- *.xcf

Processes Allowed To Rename Or Delete The Specified Image Files:

Processes specified here will be allowed to rename or delete the specified Image files. You can add or remove items from this list. The following are listed by default:

- MSPaint.exe
- Explorer.exe
- <ProgramFiles>\gimp**gimp*.exe
- <ProgramFiles>\Adobe*photoshop.exe
- <Reg:HKLM\SYSTEM\CurrentControlSet\services\CbDefense\ImagePath>
- <Reg:HKLM\SYSTEM\CurrentControlSet\services\Confer Sensor Service\ImagePath>

Image Files That Should Not Be Reported:

Renaming or deletion of files specified here will not be reported. You can add or remove items from this list. The following are listed by default:

- <localappdata>
- <Bit9:HomeInstallDir>
- <CommonAppData>
- <ProgramFiles>
- <ProgramFilesX86>

Allow Interactive Instances Of Cmd.Exe And Powershell To Rename Or Delete The Specified Image Files:

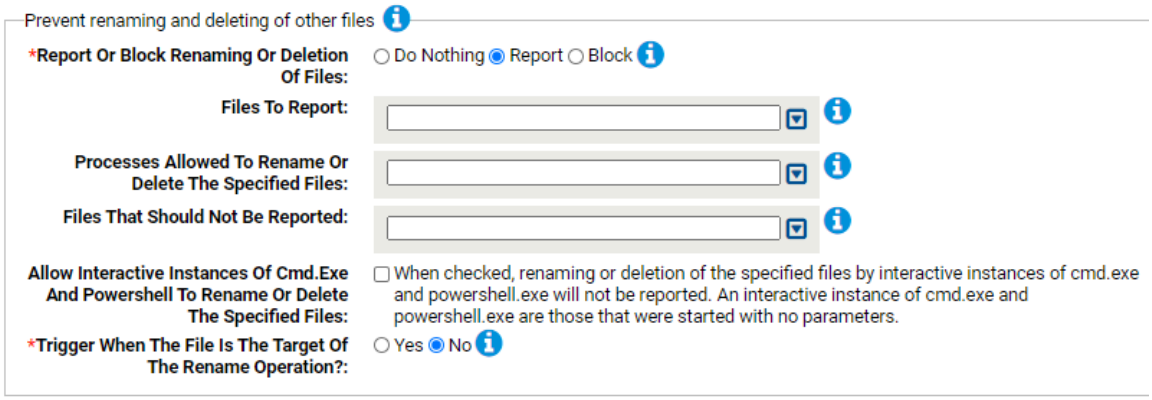
When checked, renaming or deletion of the specified image files by interactive instances of cmd.exe and powershell.exe will not be reported. An interactive instance of cmd.exe and powershell.exe are those that were started with no parameters.

***Trigger When The Image File Is The Target Of The Rename Operation?:**

Should the Rapid Config prevent renames when the image file is the TARGET of the rename?
Selecting No will cause the rules to only trigger when the image file is the source of a rename say from MyFile.Png to MyFile.Encrypted.
Selecting Yes will also catch when an encrypted file is renamed to an image file. Selecting Yes could result in more false positives but some ransomware variants do use rename when overwriting existing files with encrypted ones.

Prevent renaming and deleting of other files

This group allows you to specify any additional files you would like to protect. You can specify the files and the processes that should be allowed to delete or rename them.



Report Or Block Renaming Or Deletion Of Files:
Should renaming or deletion of the specified files be reported or blocked? You should validate that legitimate behavior would not be blocked before enabling blocking.

Files To Report:
Carbon Black App Control will report or block renaming or deletion of the specified files. You can add or remove items from this list.

Processes Allowed To Rename Or Delete The Specified Files:
Processes specified here will be allowed to rename or delete the specified files. You can add or remove items from this list.

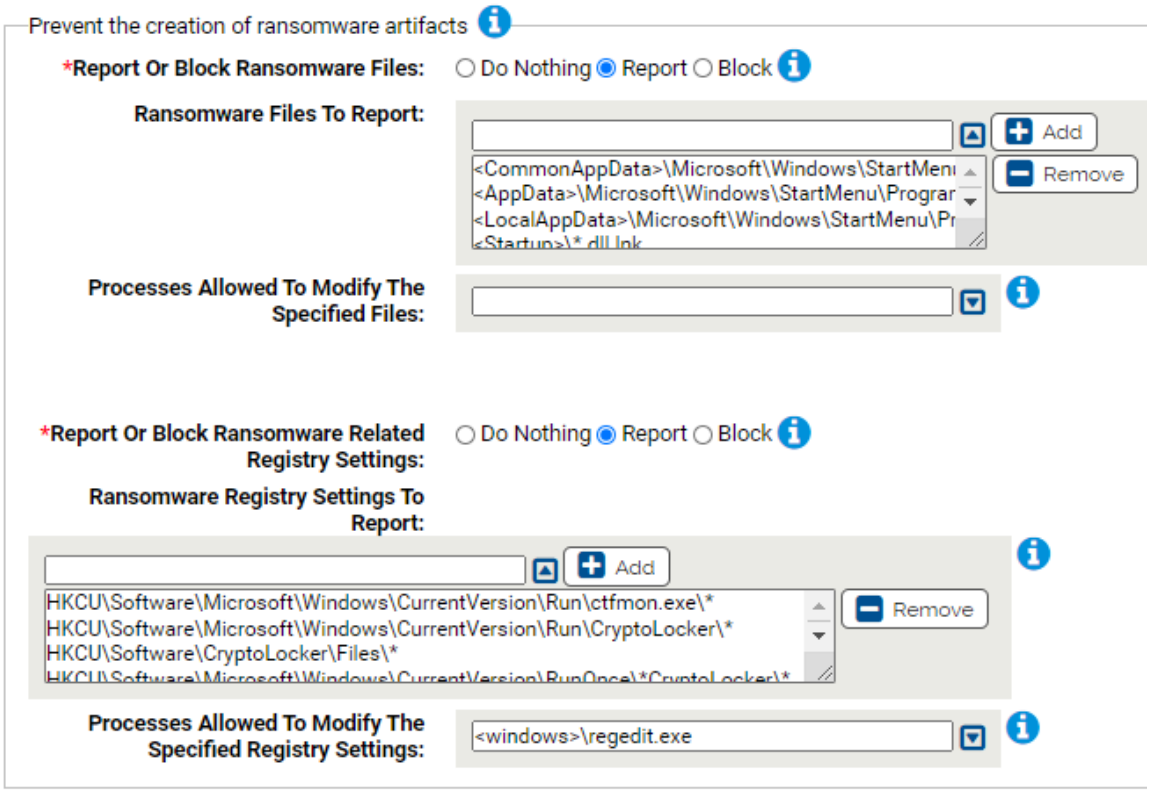
Files That Should Not Be Reported:
Renaming or deletion of files specified here will not be reported. You can add or remove items from this list.

Allow Interactive Instances Of Cmd.Exe And Powershell To Rename Or Delete The Specified Files:
When checked, renaming or deletion of the specified files by interactive instances of cmd.exe and powershell.exe will not be reported. An interactive instance of cmd.exe and powershell.exe are those that were started with no parameters.

***Trigger When The File Is The Target Of The Rename Operation?:**
Should the Rapid Config prevent renames when the file is the TARGET of the rename?
Selecting No will cause the rules to only trigger when the file is the source of a rename say from MyFile.Doc to MyFile.Encrypted.
Selecting Yes will also catch when an encrypted file is renamed to a protected file. Selecting Yes could result in more false positives but some ransomware variants do use rename when overwriting existing files with encrypted ones.

Prevent the creation of ransomware artifacts

This group allows you to watch for and optionally block file and registry changes that indicate ransomware activity. For example you can block files with extensions known to be used by ransomware.



***Report Or Block Ransomware Files:**

Should modification of the specified files be reported or blocked? You should validate that legitimate modification is not blocked before enabling blocking.

Ransomware Files To Report:

Carbon Black App Control will report or block modifications of the specified files. Typically listed here are files or extensions known to be used by ransomware. You can add or remove items from this list. By default, the following are listed:

- <CommonAppData>\Microsoft\Windows\StartMenu\Programs\Startup*.dll.lnk
- <AppData>\Microsoft\Windows\StartMenu\Programs\Startup*.dll.lnk
- <LocalAppData>\Microsoft\Windows\StartMenu\Programs\Startup*.dll.lnk
- <Startup>*.dll.lnk

Processes Allowed To Modify The Specified Files:

Processes specified here will be allowed to modify the specified files. You can add or remove items from this list.

***Report Or Block Ransomware Related Registry Settings:**

Should modification of the specified registry settings be reported or blocked? You should validate that legitimate modification is not blocked before enabling blocking.

Ransomware Registry Settings To Report:

Carbon Black App Control will report or block modification of the specified registry settings. You can add or remove items from this list. By default, the following are listed:

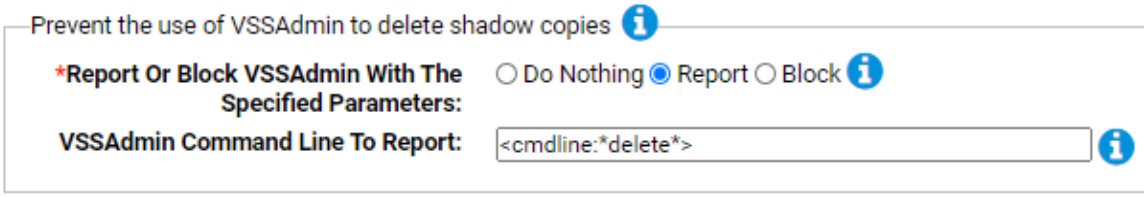
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ctfmon.exe*
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker*
- HKCU\Software\CryptoLocker\Files*
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker*

Processes Allowed To Modify The Specified Registry Settings:

Processes specified here will be allowed to modify the specified registry settings. You can add or remove items from this list.

Prevent the use of VSSAdmin to delete shadow copies

This group allows you to report or block VSSAdmin execution when using the specified command line options. Ransomware will often delete shadow copies using VSSAdmin in order to hinder restoring systems from backup.



***Report Or Block VSSAdmin With The Specified Parameters:**

Should execution of VSSAdmin using the delete command be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

VSSAdmin Command Line To Report:

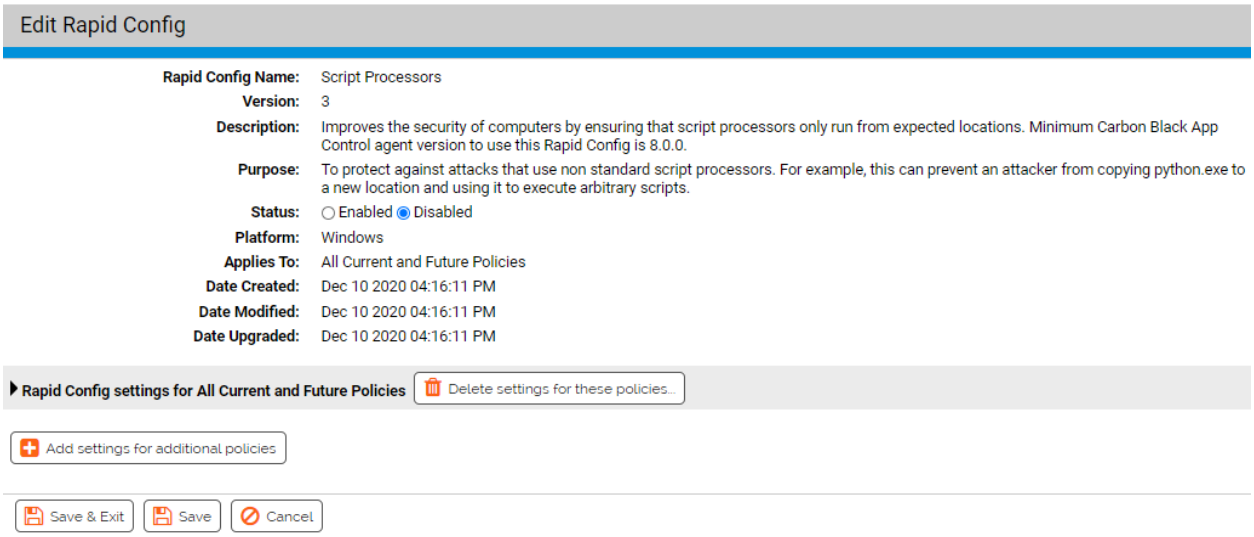
Carbon Black App Control will report or block execution of VSSAdmin.exe with the specified command line.

Script Processors Rapid Config

Purpose:To protect against attacks that use non standard script processors. For example, this can prevent an attacker from copying python.exe to a new location and using it to execute arbitrary scripts.

Description: Improves the security of computers by ensuring that script processors only run from expected locations.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

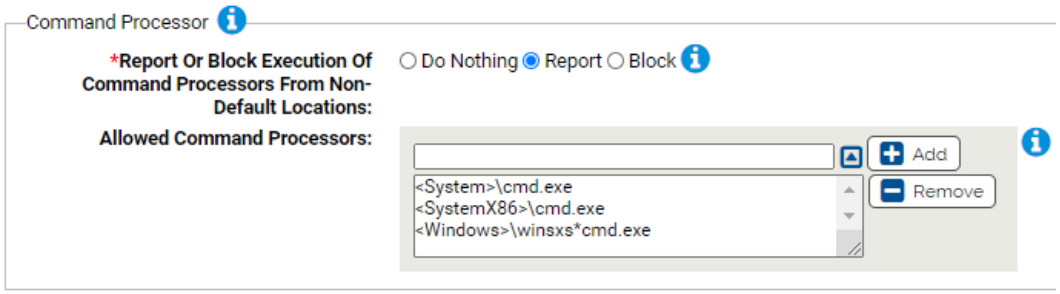
In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

For each of the following sections, specify what action you require.

Command Processor

Use this group to report or block command processors run from non-default locations.



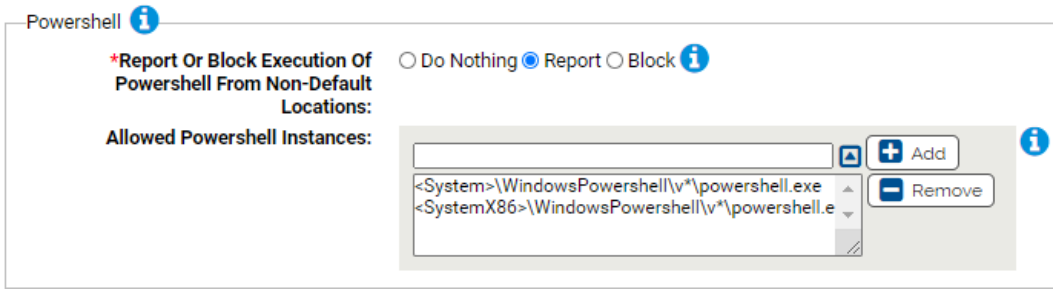
***Report Or Block Execution Of Command Processors From Non-Default Locations:**
Should execution of command processors from non-default locations be reported or blocked? You should validate that legitimate executions are not blocked before enabling blocking.

Allowed Command Processors:
Execution of command processors specified here will not be blocked (if approved). You can add or remove items from this list. By default, the list includes:

- <System>\cmd.exe
- <SystemX86>\cmd.exe
- <Windows>\winsxs*cmd.exe

Powershell

Use this group to report or block powershell run from non-default locations.



***Report Or Block Execution Of Powershell From Non-Default Locations:**

Should execution of powershell from non-default locations be reported or blocked? You should validate that legitimate executions are not blocked before enabling blocking.

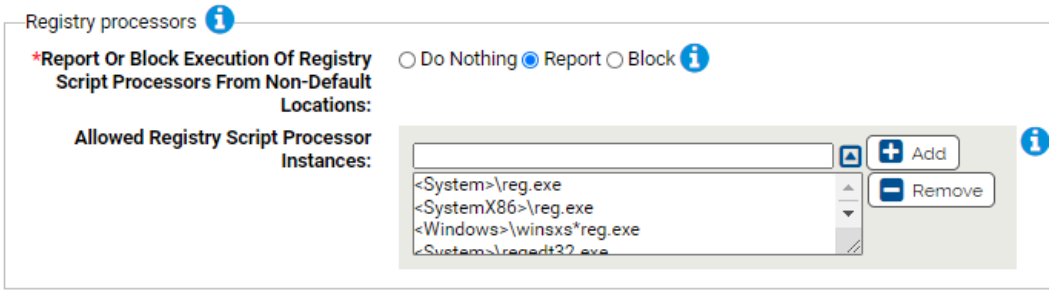
Allowed Powershell Instances:

Execution of these instances of powershell will not be blocked (if approved). You can add or remove items from this list. By default, the list includes:

- <System>\WindowsPowershell\v*\powershell.exe
- <SystemX86>\WindowsPowershell\v*\powershell.exe

Registry processors

Use this group to report or block registry processors run from non-default locations.



***Report Or Block Execution Of Registry Script Processors From Non-Default Locations:**

Should execution of registry script processors from non-default locations be reported or blocked? You should validate that legitimate executions are not blocked before enabling blocking.

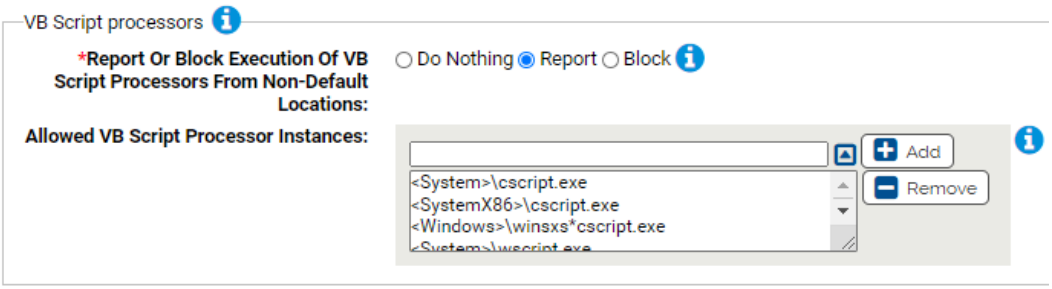
Allowed Command Processors:

Execution of these instances of registry script processors will not be blocked (if approved). You can add or remove items from this list. By default, the list includes:

- <System>\reg.exe
- <SystemX86>\reg.exe
- <Windows>\winsxs*reg.exe
- <System>\regedt32.exe
- <SystemX86>\regedt32.exe
- <Windows>\winsxs*regedt32.exe
- <windows>\regedit.exe
- <System>\regedit.exe
- <SystemX86>\regedit.exe
- <Windows>\winsxs*regedit.exe

VB Script processors

Use this group to report or block VB Script processors run from non-default locations.



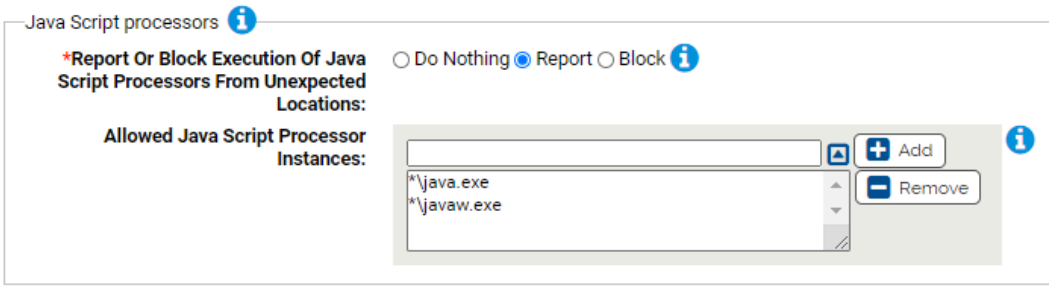
***Report Or Block Execution Of VB Script Processors From Non-Default Locations:**
Should execution of VB Script processors from non-default locations be reported or blocked? You should validate that legitimate executions are not blocked before enabling blocking.

Allowed VB ScriptProcessors:
Execution of these instances of VB Script processors will not be blocked (if approved). You can add or remove items from this list. By default, the list includes:

- <System>\cscript.exe
- <SystemX86>\cscript.exe
- <Windows>\winsxs*cscript.exe
- <System>\wscript.exe
- <SystemX86>\wscript.exe
- <Windows>\winsxs*wscript.exe

Java Script processors

Use this group to report or block Java Script processors run from unexpected locations.



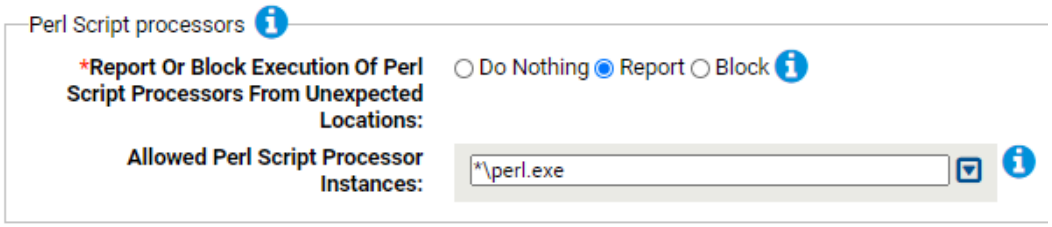
***Report Or Block Execution Of Java Script Processors From Unexpected Locations:**
Should execution of Java Script processors from non-default unexpected be reported or blocked? You should validate that legitimate executions are not blocked before enabling blocking.

Allowed Java Script Processors:
Execution of these instances of Java Script processors will not be blocked (if approved). You can add or remove items from this list. By default, the list includes:

- *\java.exe
- *\javaw.exe

Perl Script processors

Use this group to report or block Perl Script processors run from unexpected locations.



***Report Or Block Execution Of Perl Script Processors From Unexpected Locations:**
Should execution of Perl Script processors from unexpected locations be reported or blocked? You should validate that legitimate executions are not blocked before enabling blocking.

Allowed Perl Script Processors:
Execution of these instances of Perl Script processors will not be blocked (if approved). You can add or remove items from this list. By default, the list includes:

- *\perl.exe

Python Script processors

Use this group to report or block Python Script processors run from unexpected locations.

***Report Or Block Execution Of Python Script Processors From Unexpected Locations:**

Should execution of Python Script processors from unexpected locations be reported or blocked? You should validate that legitimate executions are not blocked before enabling blocking.

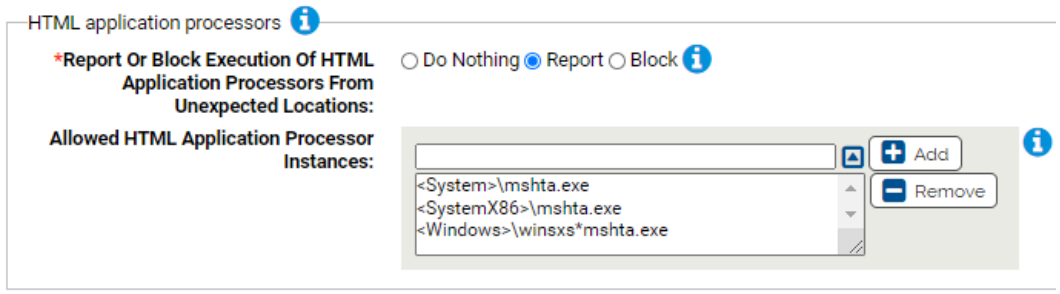
Allowed Python Script Processors:

Execution of theses instances of Python Script processors will not be blocked (if approved). You can add or remove items from this list. By default, the list includes:

- *\python.exe
- *\pythonw.exe

HTML application processors

Use this group to report or block HTML application processors run from unexpected locations.



***Report Or Block Execution Of HTML Application Processors From Unexpected Locations:**

Should execution of HTML Application processors from unexpected locations be reported or blocked? You should validate that legitimate executions are not blocked before enabling blocking.

Allowed HTML Application Processors:

Execution of these instances of HTML Application will not be blocked (if approved). You can add or remove items from this list. By default, the list includes:

- <System>\cmd.exe
- <SystemX86>\cmd.exe
- <Windows>\winsxs*cmd.exe

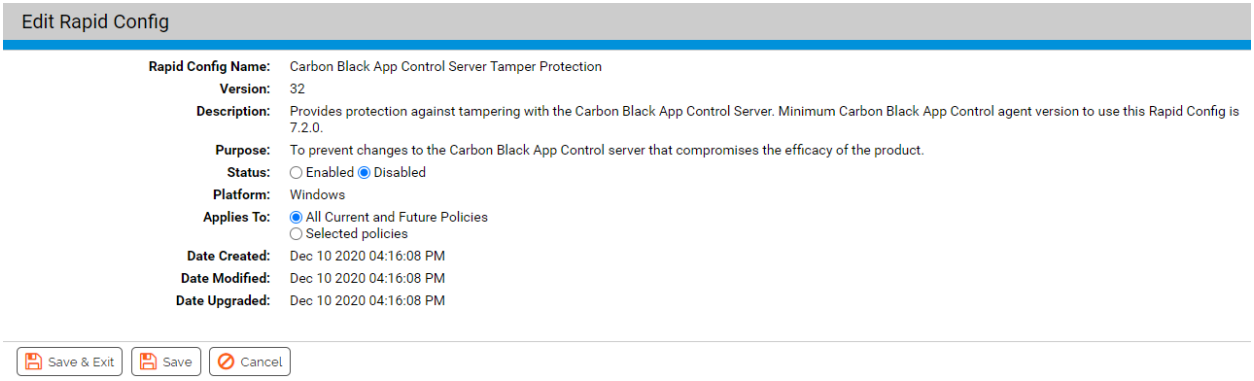
Self-Service Approvals Rapid Config

Purpose:To provide a mechanism for achieving High Enforcement in dynamic environments, which enables normal end-users to install software under certain conditions, by prompting them before executing certain files.

Description: Provides a folder from which normal end-users can approve the execution of unapproved files even when in high enforcement.

For more details on the benefits of this Rapid Config, see: https://community.carbonblack.com/docs/DOC-4162.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



Rapid Config Settings

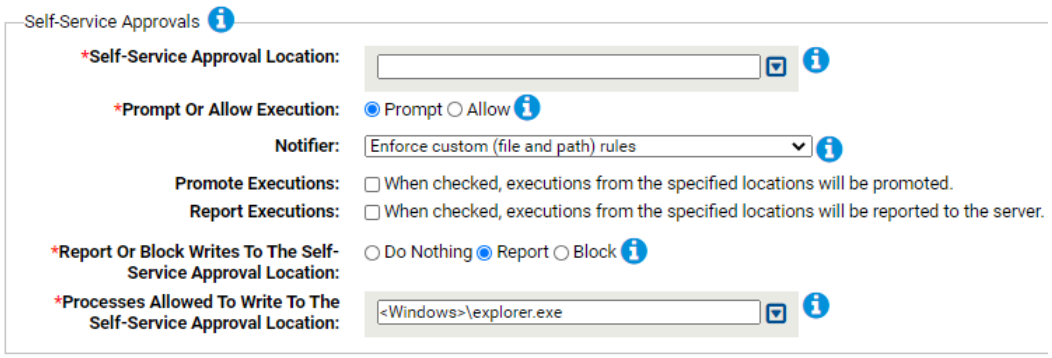
As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

For each of the following sections, specify what action you require.

Self-Service Approvals

Use this group to specify the location of files that will be either prompted for or allowed to run even if they are unapproved. You can also choose to promote the executions or report the executions to the server.



***Self-Service Approval Location:**
Execution of unapproved files from the locations specified here will be prompted for or allowed depending on subsequent parameter settings.

Prompt Or Allow Execution:
Should execution of unapproved files from the specified locations generate a prompt or be allowed without prompting.

Notifier:
Notifier to show when prompting for execution of files from the specified location. Select option from drop-down list. By default, selection is: *Enforce custom (file and path) rules*.

Promote Executions:
When checked, executions from the specified locations will be promoted.

Report Executions:
When checked, executions from the specified locations will be reported to the server.

***Report Or Block Writes To The Self-Service Approval Location:**

Should writing of files to the the self-service approval location be reported or blocked. This allows you to easily monitor or control processes that can write to your Self-Service Approval location.

***Processes Allowed To Write To The Self-Service Approval Location:**

Processes specified here will be allowed to write to the Self Service Approval Location. You can add or remove items from the list. By default, the list includes:

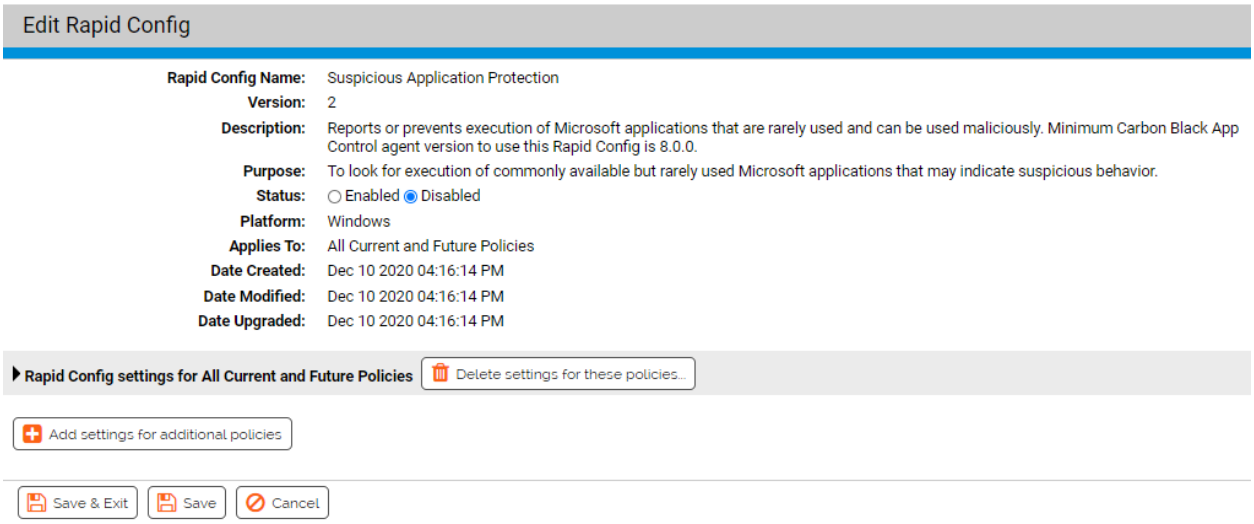
- <Windows>\explorer.exe

Suspicious Application Protection Rapid Config

Purpose: To look for execution of commonly available but rarely used Microsoft applications that may indicate suspicious behavior.

Description: Reports or prevents execution of Microsoft applications that are rarely used and can be used maliciously.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

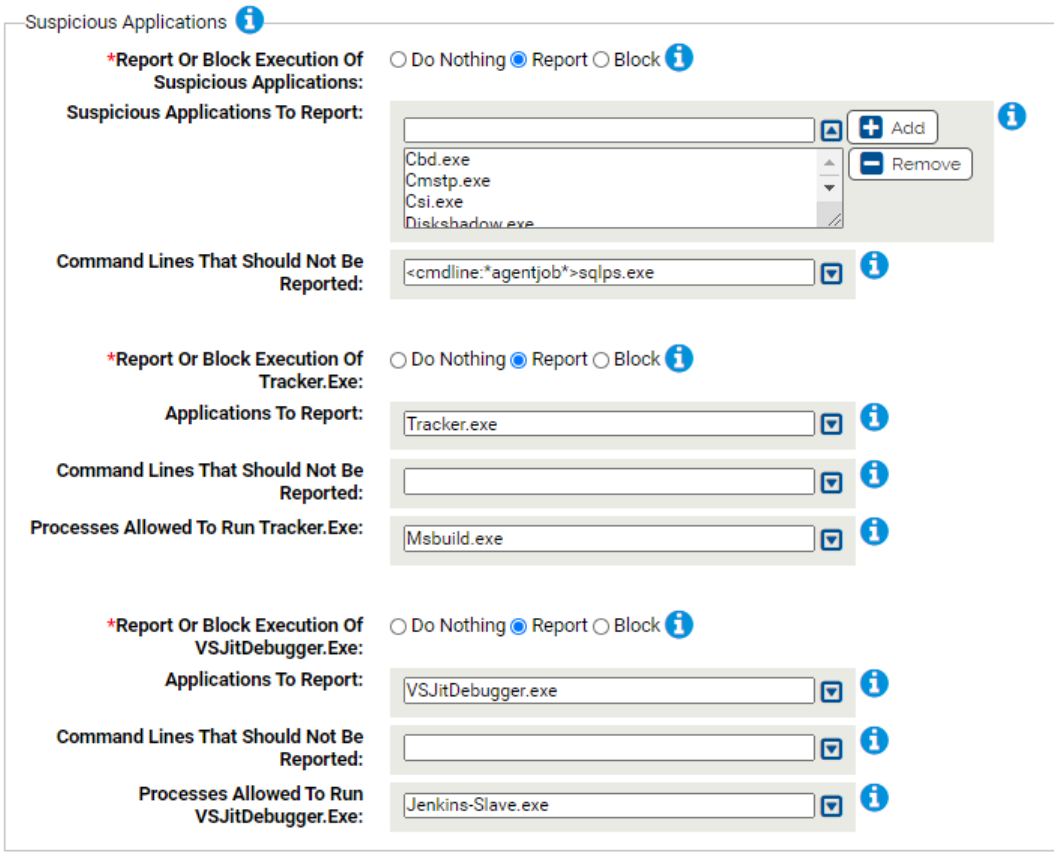
In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

For each of the following sections, specify what action you require.

Suspicious Applications

Use this group to specify suspicious applications that should be blocked from running.



***Report Or Block Execution Of Suspicious Applications:**

Should execution of suspicious applications be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Suspicious Applications To Report:

Carbon Black App Control will report or block execution of the specified applications. You can add or remove items from this list. By default, the list includes:

- Cbd.exe
- Cmstp.exe
- Csi.exe
- Diskshadow.exe
- Dnx.exe
- Dxcap.exe
- Extexport.exe
- Forfiles.exe
- Hh.exe
- Ieexec.exe
- Ie4uinit.exe
- infdefaultinstall.exe
- installutil.exe
- Mftrace.exe
- Msdeploy.exe
- Msdt.exe
- Msxsl.exe
- Presentationhost.exe
- Rcsi.exe
- Regasm.exe
- Regsvcs.exe
- Runscripthelper.exe
- Sqlps.exe
- Sqltoolsps.exe
- Te.exe

Command Lines That Should Not Be Reported:

Carbon Black App Control will report or block execution of the specified applications. You can add or remove items from this list. By default, the list includes:

- <cmdline:*agentjob*>sqlps.exe

***Report Or Block Execution Of Tracker.Exe:**

Should execution of Tracker.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Applications To Report:

Carbon Black App Control will report or block execution of the specified applications. You can add or remove items from this list. By default, the list includes:

- Tracker.exe

Command Lines That Should Not Be Reported:

Execution of these command lines will not be reported or blocked.

Processes Allowed To Run Tracker.Exe:

Tracker will not be reported or blocked when run by these processes. By default, the list includes:

- Msbuild.exe

***Report Or Block Execution Of VSJitDebugger.Exe:**

Should execution of VSJitDebugger.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Applications To Report:

Carbon Black App Control will report or block execution of the specified applications. You can add or remove items from this list. By default, the list includes:

- VSJitDebugger.exe

Command Lines That Should Not Be Reported:

Execution of these command lines will not be reported or blocked.

Processes Allowed To Run VSJitDebugger.Exe:

VSJitDebugger will not be reported or blocked when run by these processes. By default, the list includes:

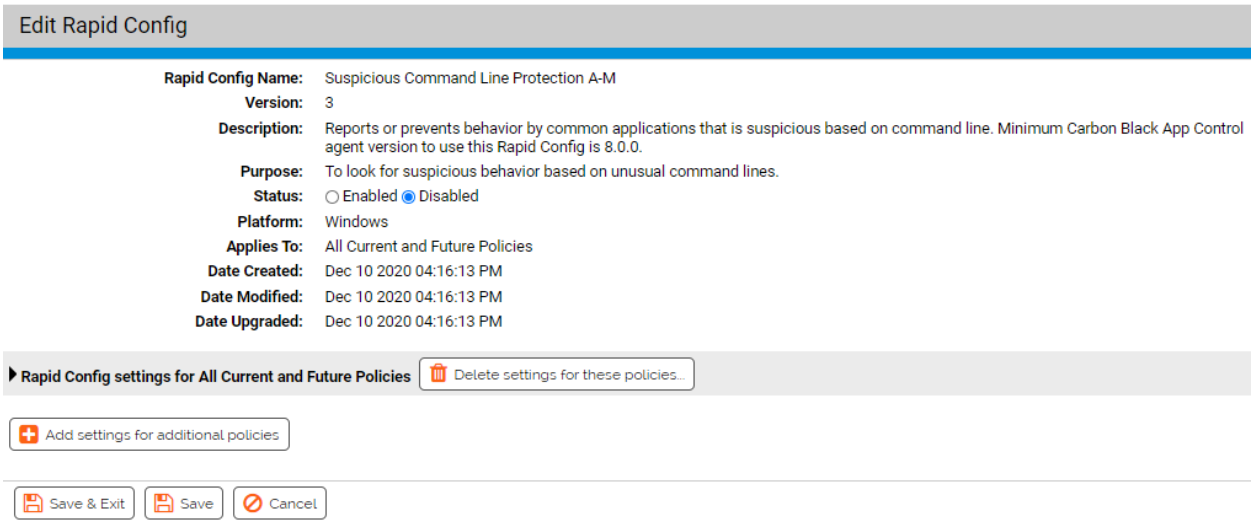
- Jenkins-Slave.exe

Suspicious Command Line Protection A-M Rapid Config

Purpose:To look for suspicious behavior based on unusual command lines.

Description: Reports or prevents behavior by common applications that is suspicious based on command line.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

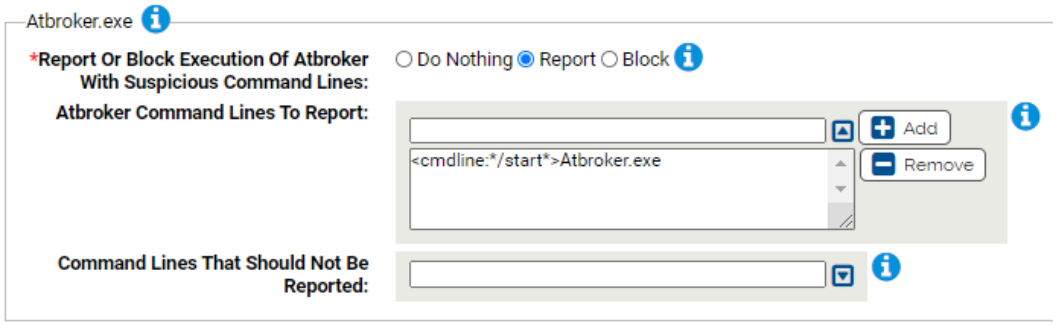
In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

For each of the following sections, specify what action you require.

Atbroker.exe

Use this group to specify how to handle suspicious Atbroker command lines. Atbroker is part of the Windows Assistive Technology Manager.



Report Or Block Execution Of Atbroker With Suspicious Command Lines:
Should execution of Atbroker with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

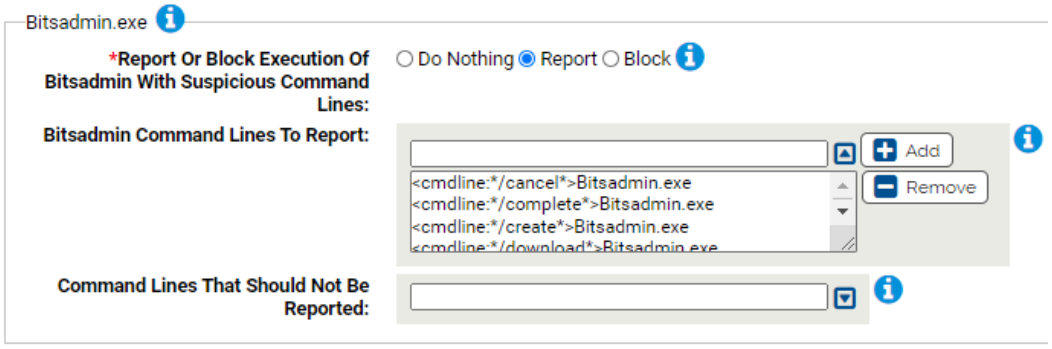
Atbroker Command Lines To Report:
Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the list includes:

- <cmdline:*/start*>Atbroker.exe

Command Lines That Should Not Be Reported:
Execution of command lines specified here will not be reported or blocked.

Bitsadmin.exe

Use this group to specify how to handle suspicious Bitsadmin command lines. Bitsadmin is part of the Background Intelligent Transfer Service



***Report Or Block Execution Of Bitsadmin With Suspicious Command Lines:**
Should execution of Bitsadmin with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

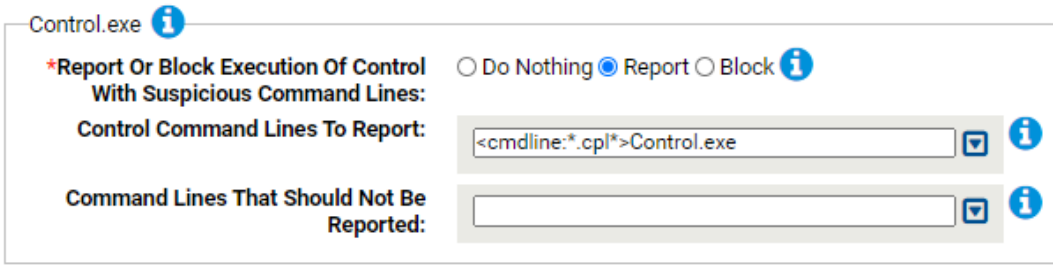
Bitsadmin Command Lines To Report:
Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list.

- <cmdline:*/cancel*>Bitsadmin.exe
- <cmdline:*/complete*>Bitsadmin.exe
- <cmdline:*/create*>Bitsadmin.exe
- <cmdline:*/download*>Bitsadmin.exe
- <cmdline:*/resume*>Bitsadmin.exe
- <cmdline:*/transfer*>Bitsadmin.exe

Command Lines That Should Not Be Reported:
Execution of command lines specified here will not be reported or blocked.

Control.exe

Use this group to specify how to handle suspicious Control command lines. Control.exe runs the Control Panel application.



***Report Or Block Execution Of Control With Suspicious Command Lines:**

Should execution of Control with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Control Command Lines To Report:

Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the list includes:

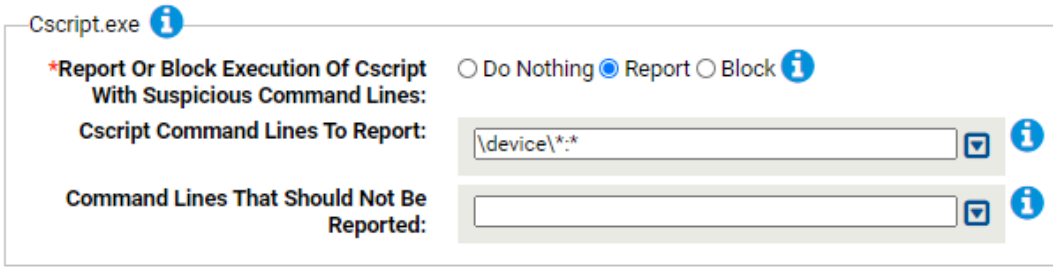
- <cmdline:*.cpl*>Control.exe

Command Lines That Should Not Be Reported:

Execution of command lines specified here will not be reported or blocked.

Cscript.exe

Use this group to specify how to handle suspicious Cscript command lines. Cscript is the Windows Script Host.



***Report Or Block Execution Of Cscript With Suspicious Command Lines:**

Should execution of Cscript with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Cscript Command Lines To Report:

Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the list includes:

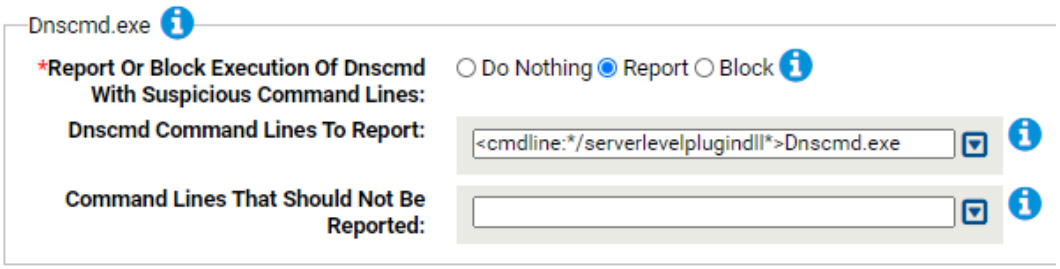
- \device*:*

Command Lines That Should Not Be Reported:

Execution of command lines specified here will not be reported or blocked.

Dnscmd.exe

Use this group to specify how to handle suspicious Dnscmd command lines. Dnscmd is a command line tool for managing DNS servers



***Report Or Block Execution Of Dnscmd With Suspicious Command Lines:**
Should execution of Dnscmd with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

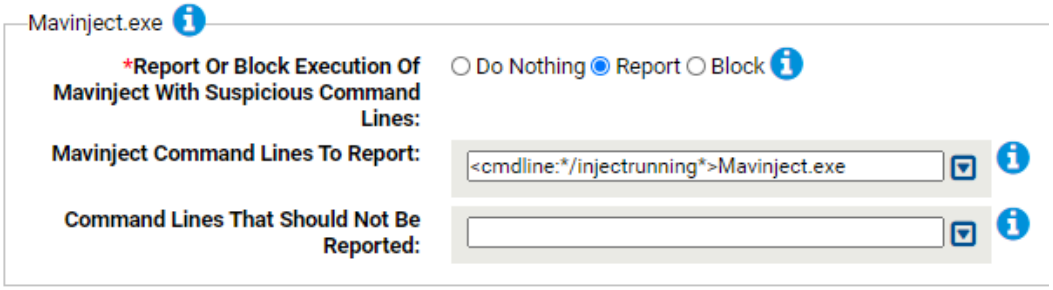
Dnscmd Command Lines To Report:
Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the list includes:

- <cmdline:*/serverlevelplugindll*>Dnscmd.exe

Command Lines That Should Not Be Reported:
Execution of command lines specified here will not be reported or blocked.

Mavinject.exe

Use this group to specify how to handle suspicious Mavinject command lines. Mavinject is part of Microsoft Application Virtualization.



***Report Or Block Execution Of Mavinject With Suspicious Command Lines:**
Should execution of Mavinject with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Mavinject Command Lines To Report:

Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the list includes:

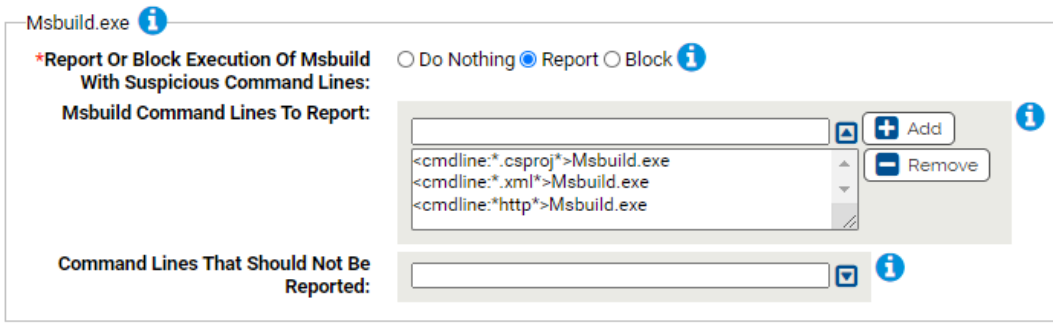
- <cmdline:*/injectrunning*>Mavinject.exe

Command Lines That Should Not Be Reported:

Execution of command lines specified here will not be reported or blocked.

Msbuild.exe

Use this group to specify how to handle suspicious Msbuild command lines. Msbuild is the Microsoft Build Engine.



***Report Or Block Execution Of MSbuild With Suspicious Command Lines:**

Should execution of MSbuild with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

MSbuild Command Lines To Report:

Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the list includes:

- <cmdline:*.csproj*>Msbuild.exe
- <cmdline:*.xml*>Msbuild.exe
- <cmdline:*http*>Msbuild.exe

Command Lines That Should Not Be Reported:

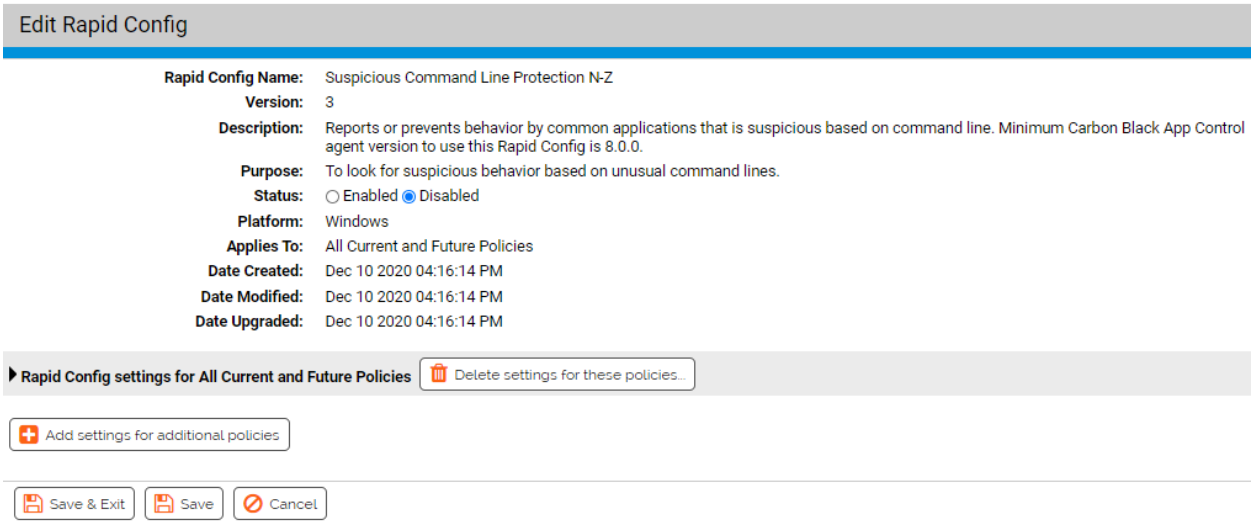
Execution of command lines specified here will not be reported or blocked.

Suspicious Command Line Protection N-Z Rapid Config

Purpose:To look for suspicious behavior based on unusual command lines.

Description: Reports or prevents behavior by common applications that is suspicious based on command line.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

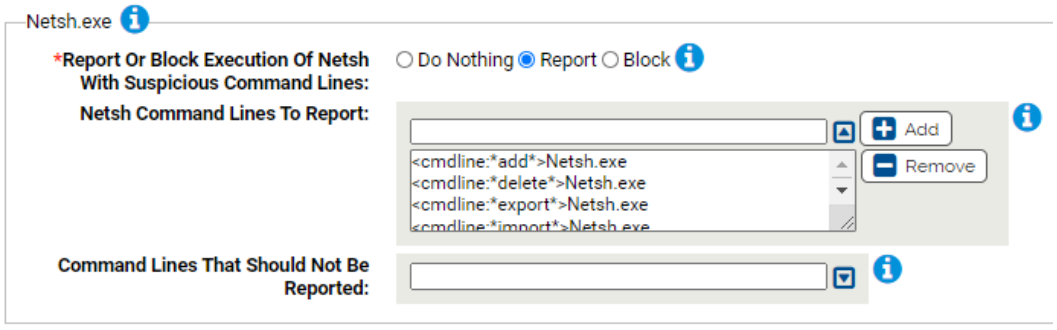
In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

For each of the following sections, specify what action you require.

Netsh.exe

Use this group to specify how to handle suspicious Netsh command lines. Netsh is the Network shell command line utility.



***Report Or Block Execution Of Netsh With Suspicious Command Lines:**
Should execution of Netsh with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Netsh Command Lines To Report:
Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the following are listed:

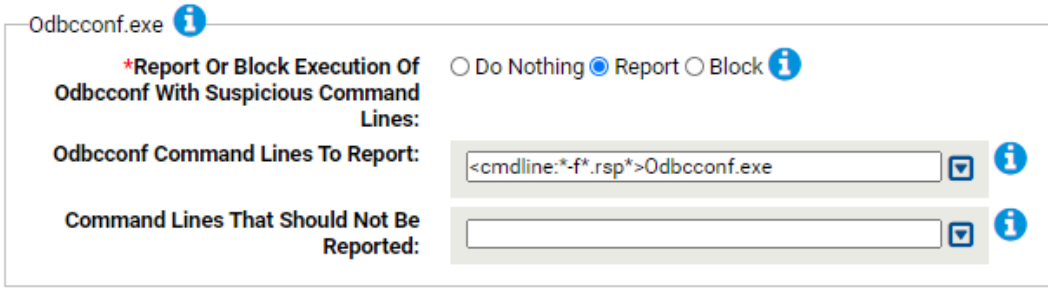
- <cmdline:*add*>Netsh.exe
- <cmdline:*delete*>Netsh.exe

- <cmdline:*export*>Netsh.exe
- <cmdline:*import*>Netsh.exe
- <cmdline:*off*>Netsh.exe
- <cmdline:*portproxy*>Netsh.exe
- <cmdline:*show*>Netsh.exe
- <cmdline:*trace*>Netsh.exe

Command Lines That Should Not Be Reported:
Execution of command lines specified here will not be reported or blocked.

Odbcconf.exe

Use this group to specify how to handle suspicious Odbcconf command lines. Odbcconf is a utility for configuring ODBC drivers.



***Report Or Block Execution Of Odbcconf With Suspicious Command Lines:**
Should execution of Odbcconf with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

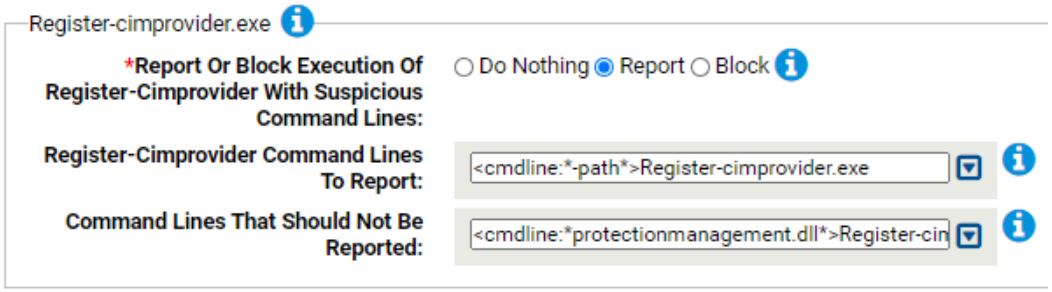
Odbcconf Command Lines To Report:
Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the following is listed:

- <cmdline:*-f*.rsp*>Odbcconf.exe

Command Lines That Should Not Be Reported:
Execution of command lines specified here will not be reported or blocked.

Register-cimprovider.exe

Use this group to specify how to handle suspicious Register-cimprovider command lines. Register-cimprovider is a utility for registering Windows Management Infrastructure providers.



***Report Or Block Execution Of Register-cimprovider With Suspicious Command Lines:**

Should execution of Register-cimprovider with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Register-cimprovider Command Lines To Report:

Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the following is listed:

- <cmdline:*-path*>Register-cimprovider.exe

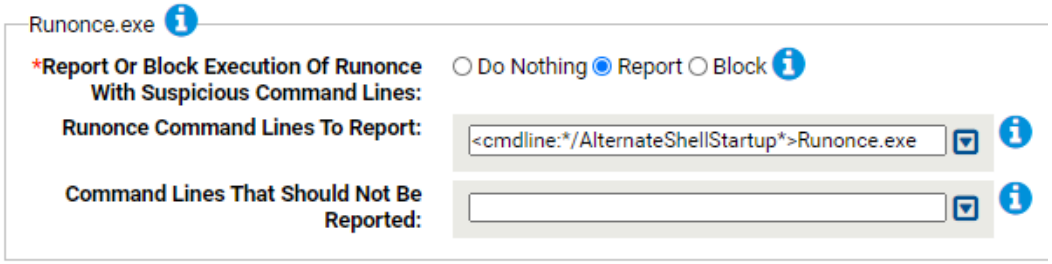
Command Lines That Should Not Be Reported:

Execution of command lines specified here will not be reported or blocked. You can add or remove items from this list. By default, the following is listed:

- <cmdline:*protectionmanagement.dll*>Register-cimprovider.exe

Runonce.exe

Use this group to specify how to handle suspicious Runonce command lines. Runonce is an application typically used to install drivers and services at startup.



***Report Or Block Execution Of Runonce With Suspicious Command Lines:**

Should execution of Runonce with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Runonce Command Lines To Report:

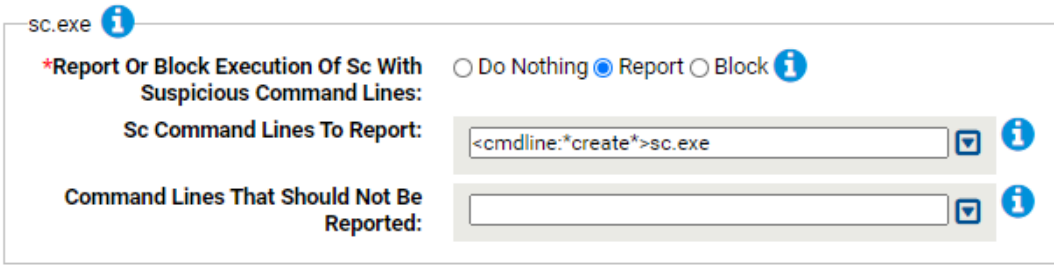
Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the following is listed:

- <cmdline:*/AlternateShellStartup*>Runonce.exe

Command Lines That Should Not Be Reported:
Execution of command lines specified here will not be reported or blocked.

sc.exe

Use this group to specify how to handle suspicious sc command lines. sc is the Service Control Manager.



***Report Or Block Execution Of Sc With Suspicious Command Lines:**
Should execution of Sc with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

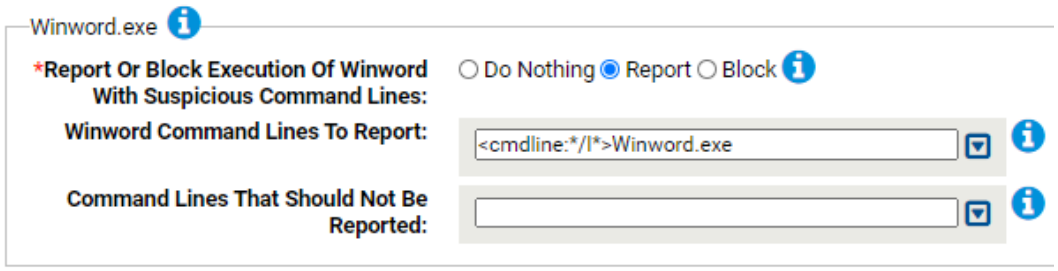
Sc Command Lines To Report:
Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the following is listed:

- <cmdline:*create*>sc.exe

Command Lines That Should Not Be Reported:
Execution of command lines specified here will not be reported or blocked.

Winword.exe

Use this group to specify how to handle suspicious Winword command lines. Winword is the Micorosoft Office Word application.



***Report Or Block Execution Of Winword With Suspicious Command Lines:**

Should execution of Winword with suspicious command lines be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Winword Command Lines To Report:

Carbon Black App Control will report or block execution of the specified command lines. You can add or remove items from this list. By default, the following is listed:

- <cmdline:*/I*>Winword.exe

Command Lines That Should Not Be Reported:

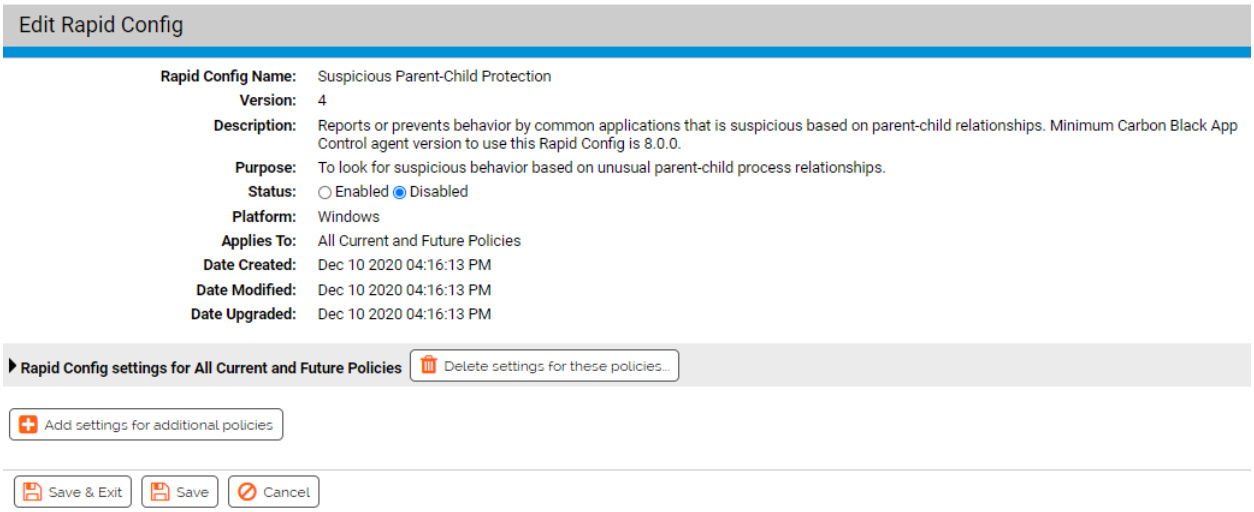
Execution of command lines specified here will not be reported or blocked.

Suspicious Parent-Child Protection Rapid Config

Purpose:To look for suspicious behavior based on unusual parent-child process relationships.

Description: Reports or prevents behavior by common applications that is suspicious based on parent-child relationships.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

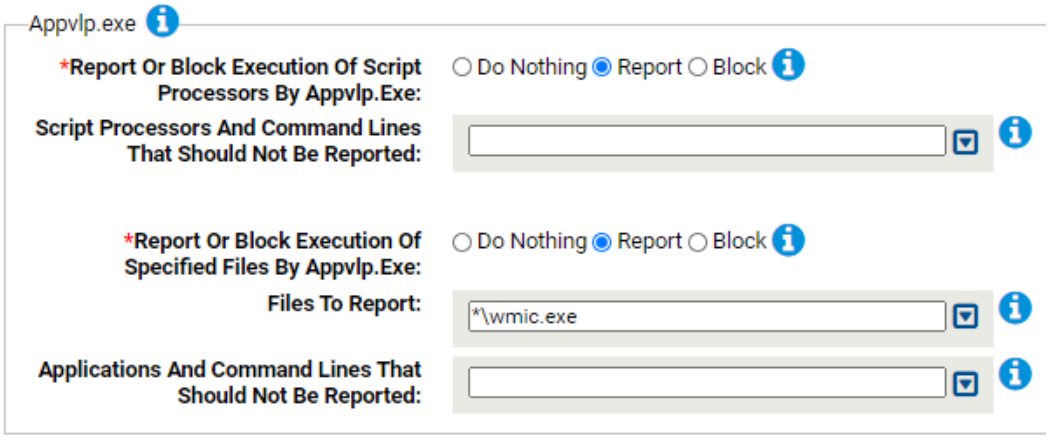
In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

For each of the following sections, specify what action you require.

Appvlp.exe

Use this group to specify how to handle suspicious behavior by Appvlp.exe.



***Report Or Block Execution Of Script Processors By Appvlp.Exe:**
Should execution of script processors by Appvlp.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Script Processors And Command Lines That Should Not Be Reported:
Execution of these files by Appvlp.exe will not be reported or blocked.

***Report Or Block Execution Of Specified Files By Appvlp.Exe:**

Should execution of the specified files by Appvlp.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Files To Report:

Carbon Black App Control will report or block execution of the specified files by Appvlp.exe. You can add or remove items from this list. By default, the following is listed:

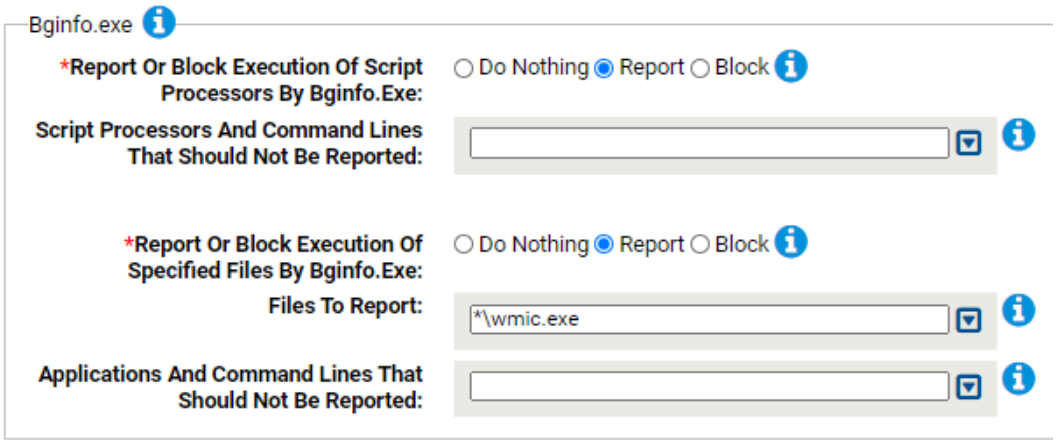
- *\wmic.exe

Applications And Command Lines That Should Not Be Reported:

Execution of these files by Appvlp.exe will not be reported or blocked.

Bginfo.exe

Use this group to specify how to handle suspicious behavior by Bginfo.exe.



***Report Or Block Execution Of Script Processors By Bginfo.Exe:**

Should execution of script processors by Bginfo.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Script Processors And Command Lines That Should Not Be Reported:

Execution of these files by Bginfo.exe will not be reported or blocked.

***Report Or Block Execution Of Specified Files By Bginfo.Exe:**

Should execution of the specified files by Bginfo.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Files To Report:

Carbon Black App Control will report or block execution of the specified files by Bginfo.exe. You can add or remove items from this list. By default, the following is listed:

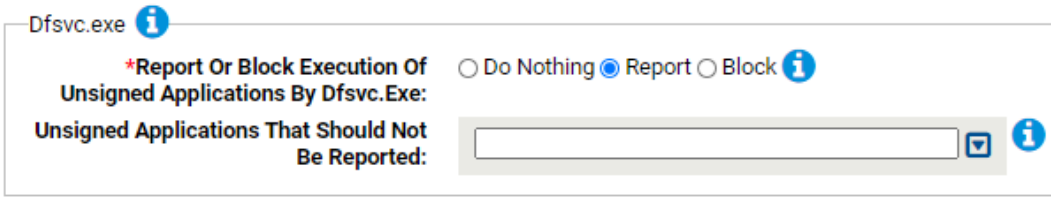
- *\wmic.exe

Applications And Command Lines That Should Not Be Reported:

Execution of these files by Bginfo.exe will not be reported or blocked.

Dfsvc.exe

Use this group to specify how to handle suspicious behavior by Dfsvc.exe.

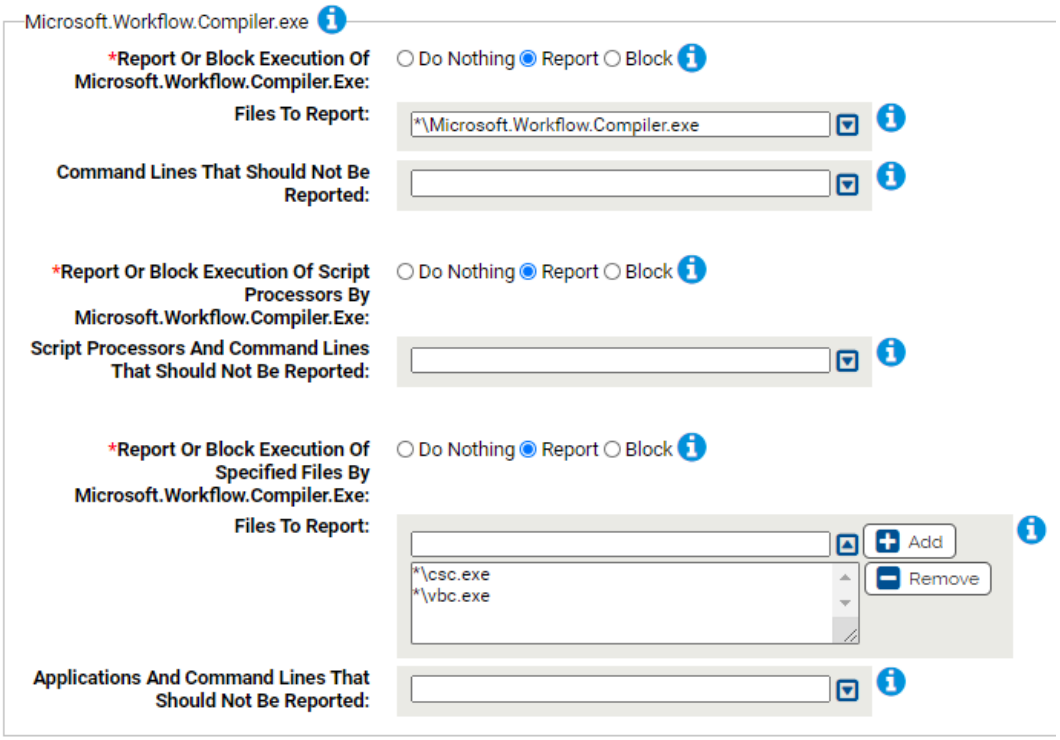


***Report Or Block Execution Of Unsigned Applications By Dfsvc.Exe:**
Should execution of unsigned applications by dfsvc.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Unsigned Applications That Should Not Be Reported:
Execution of applications specified here will not be reported or blocked.

Microsoft.Workflow.Compiler.exe

Use this group to specify how to handle suspicious behavior by Microsoft.Workflow.Compiler.exe.



***Report Or Block Execution Of Microsoft.Workflow.Compiler.Exe:**
Should execution of the Microsoft.Workflow.Compiler.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Files To Report:
Carbon Black App Control will report or block execution of the specified files. You can add or remove items from this list. By default, the following is listed:

- *\Microsoft.Workflow.Compiler.exe

Command Lines That Should Not Be Reported:
Execution of Microsoft.Workflow.compiler.exe command lines specified here will not be reported or blocked.

***Report Or Block Execution Of Script Processors By Microsoft.Workflow.Compiler.Exe:**
Should execution of script processors by Microsoft.Workflow.Compiler.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Script Processors And Command Lines That Should Not Be Reported:
Execution of these files by Microsoft.Workflow.Compiler.exe will not be reported or blocked.

***Report Or Block Execution Of Specified Files By Microsoft.Workflow.Compiler.Exe:**
Should execution of the specified files by Microsoft.Workflow.Compiler.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

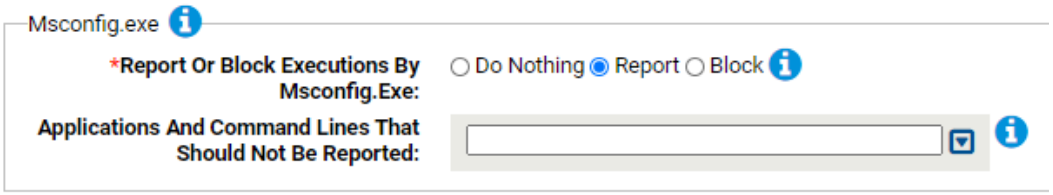
Files To Report:
Should execution of the specified files by Microsoft.Workflow.Compiler.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking. You can add or remove items from this list. By default, the following is listed:

- *\csc.exe*\vbc.exe

Applications And Command Lines That Should Not Be Reported:
Execution of these files by Microsoft.Workflow.Compiler.exe will not be reported or blocked.

Msconfig.exe

Use this group to specify how to handle suspicious behavior by Msconfig.exe. Note that if msconfig.exe is started by Task Manager subsequent executions by msconfig.exe will not be reported/blocked.

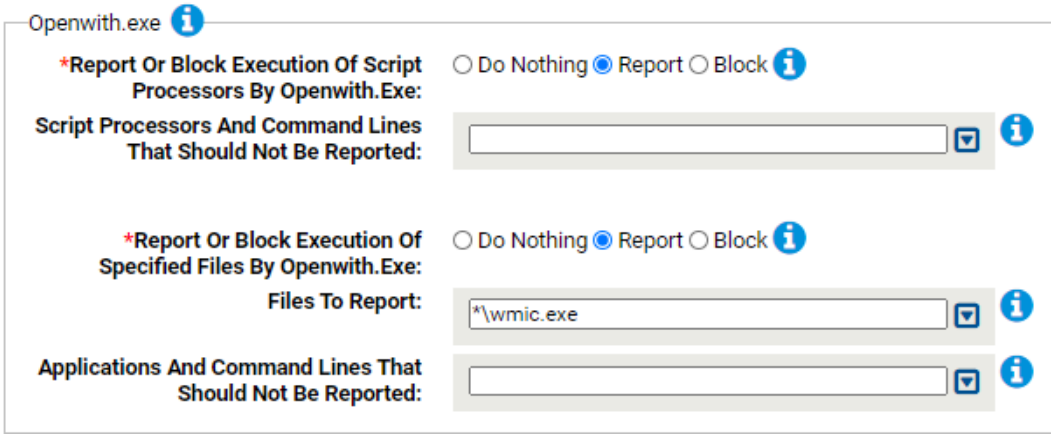


***Report Or Block Execution By Msconfig.Exe:**
Should execution of applications by msconfig.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking. Note that if msconfig.exe is started by Task Manager subsequent executions by msconfig.exe will not be reported/blocked.

Applications And Command Lines That Should Not Be Reported:
Execution of applications or command lines specified here will not be reported or blocked.

Openwith.exe

Use this group to specify how to handle suspicious behavior by Openwith.exe.



***Report Or Block Execution Of Script Processors By Openwith.Exe:**
Should execution of script processors by Openwith.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Script Processors And Command Lines That Should Not Be Reported:
Execution of these files by Openwith.exe will not be reported or blocked.

***Report Or Block Execution Of Specified Files By Openwith.Exe:**
Should execution of the specified files by Openwith.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

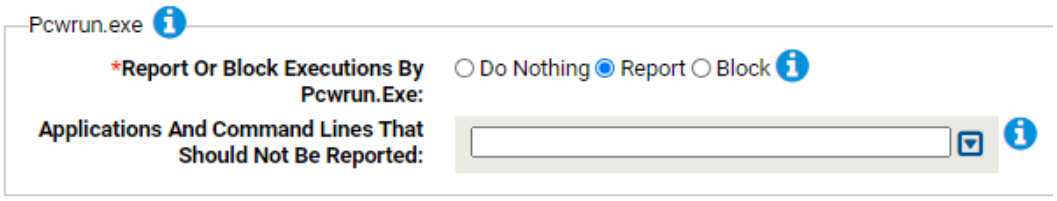
Files To Report:
Carbon Black App Control will report or block execution of the specified files by Openwith.exe. You can add or remove items from this list. By default, the following is listed:

- *\wmic.exe

Applications And Command Lines That Should Not Be Reported:
Execution of these files by Openwith.exe will not be reported or blocked.

Pcwrun.exe

Use this group to specify how to handle suspicious behavior by Pcwrun.exe.

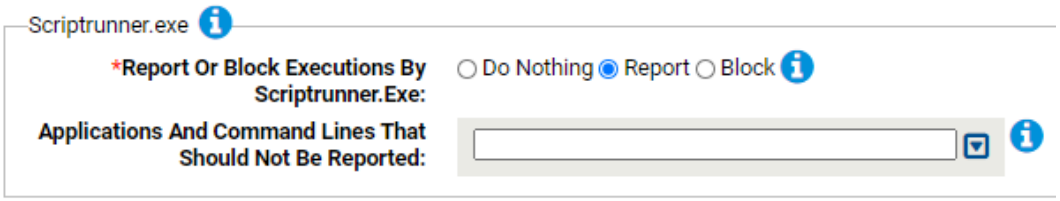


***Report Or Block Execution By Pcwrun.Exe:**
Should execution of applications by Pcwrun.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

Applications And Command Lines That Should Not Be Reported:
Execution of applications or command lines specified here will not be reported or blocked.

Scriptrunner.exe

Use this group to specify how to handle suspicious behavior by Scriptrunner.exe.



***Report Or Block Execution By Scriptrunner.Exe:**
Should execution of applications by Scriptrunner.exe be reported or blocked? You should validate that legitimate execution is not blocked before enabling blocking.

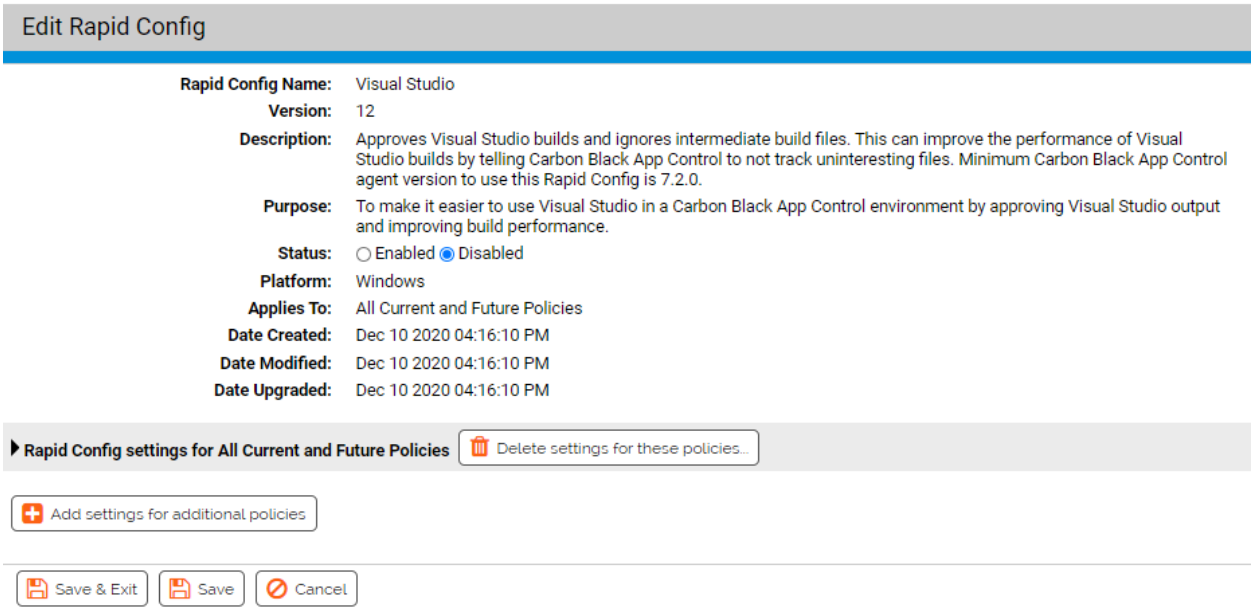
Applications And Command Lines That Should Not Be Reported:
Execution of applications or command lines specified here will not be reported or blocked.

Visual Studio Rapid Config

Purpose:To make it easier to use Visual Studio in a Carbon Black App Control environment by approving Visual Studio output and improving build performance.

Description: Approves Visual Studio builds and ignores intermediate build files. This can improve the performance of Visual Studio builds by telling Carbon Black App Control to not track uninteresting files.

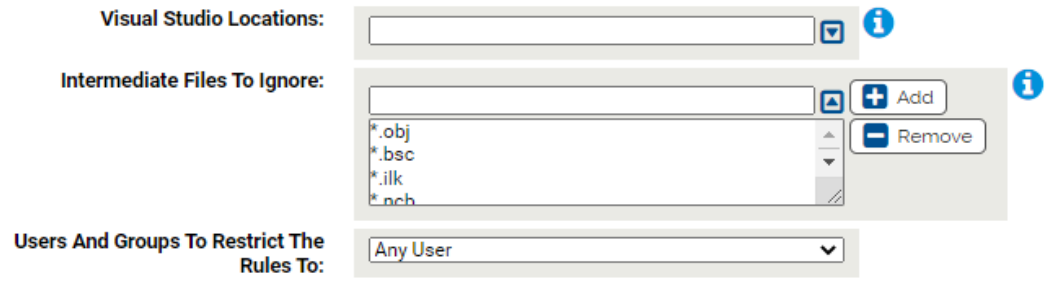
Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.



Visual Studio Locations:

Visual Studio installation locations will be identified using well known registry keys. If there are additional installation locations for Visual Studio please enter them here.

Intermediate Files To Ignore:

Ignore writes of the following file types by Visual Studio. You can add and remove items from this list.

- *.obj
- *.bsc
- *.ilk
- *.ncb
- *.sbr
- *.idb
- *.pdb
- *.pch
- *.manifest
- *.res
- *.dbx
- *.idx
- <LocalAppData>\temp_CL_*

Users And Groups To Restrict The Rules To:

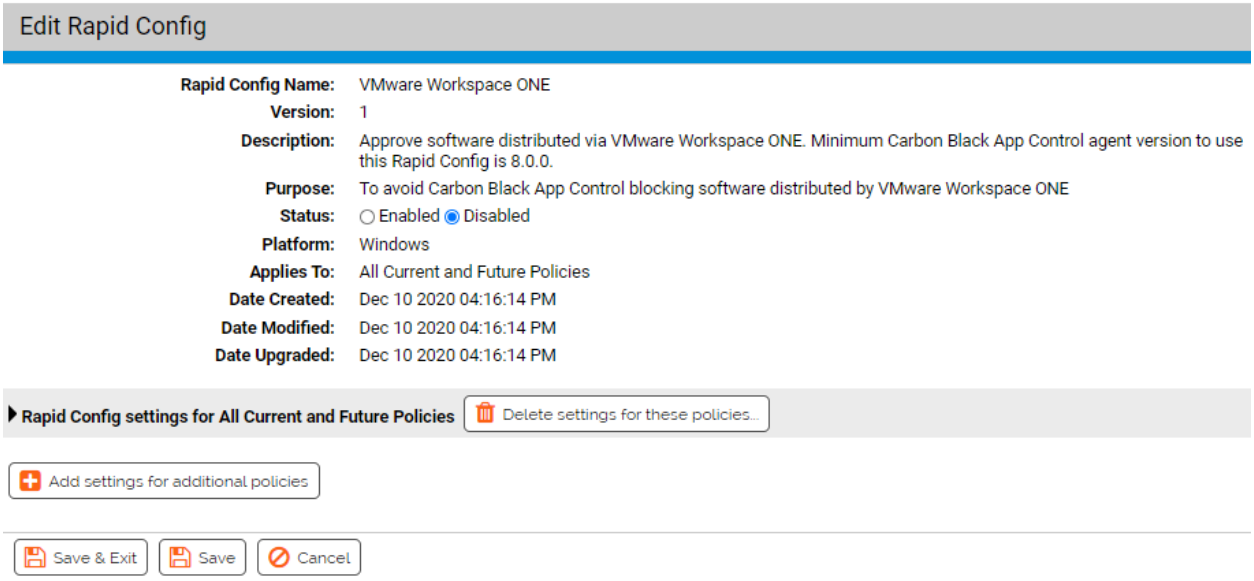
Defines specific users or groups to apply the rule to. By default, selection is Any User.

VMware Workspace ONE Rapid Config

Purpose:To avoid Carbon Black App Control blocking software distributed by VMware Workspace ONE.

Description: Approves software distributed via VMware Workspace ONE.

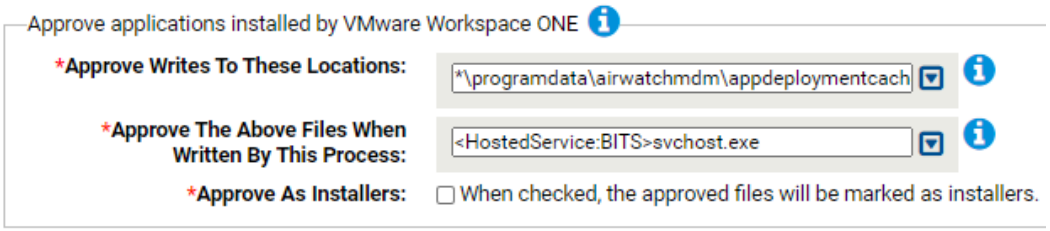
CDC Push Date:	
Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.



Approve applications installed by VMware Workspace ONE

Use this group to approve writes by the specified files by the specified processes to the specified locations by the specified users.

***Approve Writes To These Locations:**

Files written to these locations will be approved. You can add and remove locations. By default this list includes:

- *\programdata\airwatchmdm\appdeploymentcache*

***Approve The Above Files When Written By This Process:**

Files written to these locations will be approved. You can add and remove locations. By default this list includes:

- <HostedService:BITS>svchost.exe

***Approve As Installers:**

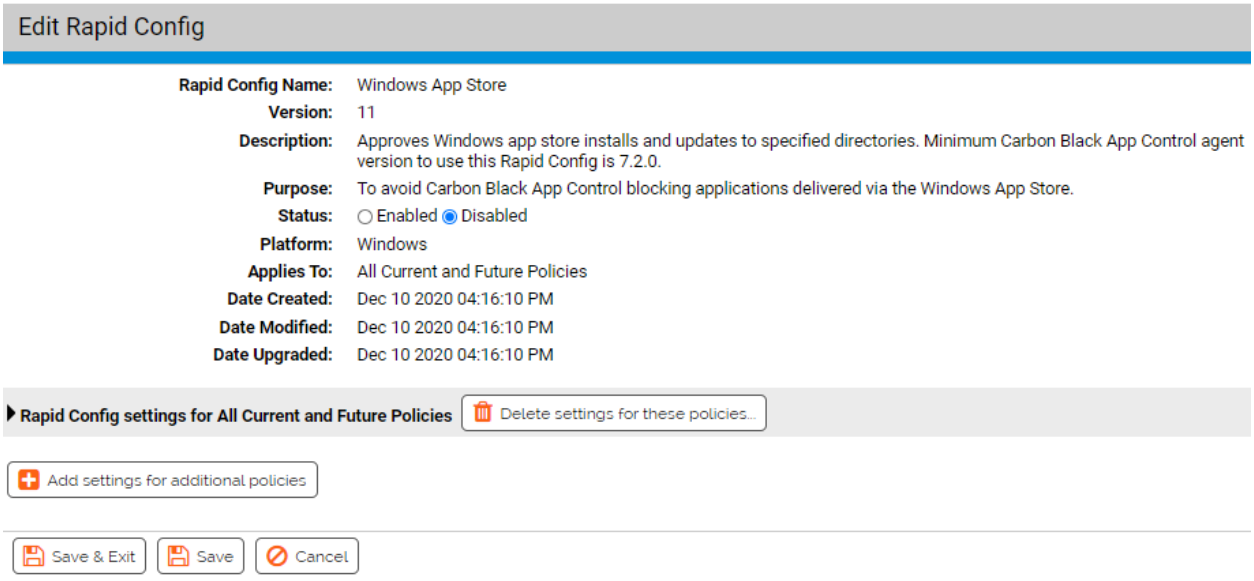
When checked, the approved files will be marked as installers.

Windows App Store Rapid Config

Purpose:To avoid Carbon Black App Control blocking applications delivered via the Windows App Store.

Description: Approves Windows app store installs and updates to specified directories.

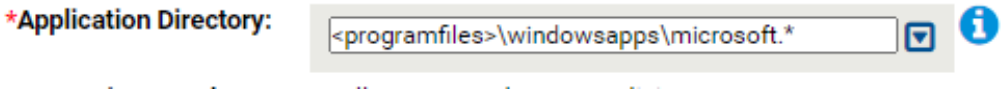
Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.



***Application Directory:**

Windows App Store applications typically download to unique subdirectories under program files\windowsapps. You can control which Windows App Store applications are approved based on their directories specified here. By default, the following directory is specified:

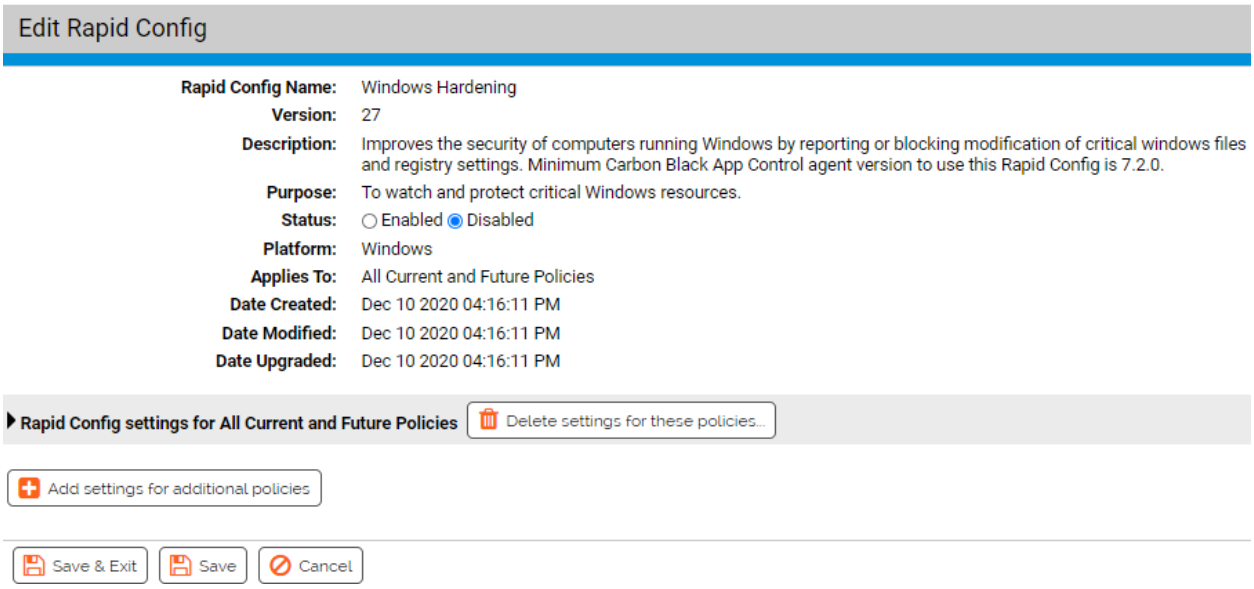
- <programfiles>\windowsapps\microsoft.*

Windows Hardening Rapid Config

Purpose: To watch and protect critical Windows resources.

Description: Improves the security of computers running Windows by reporting or blocking modification of critical windows files and registry settings.

CDC Push Date:	
Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	7.2.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

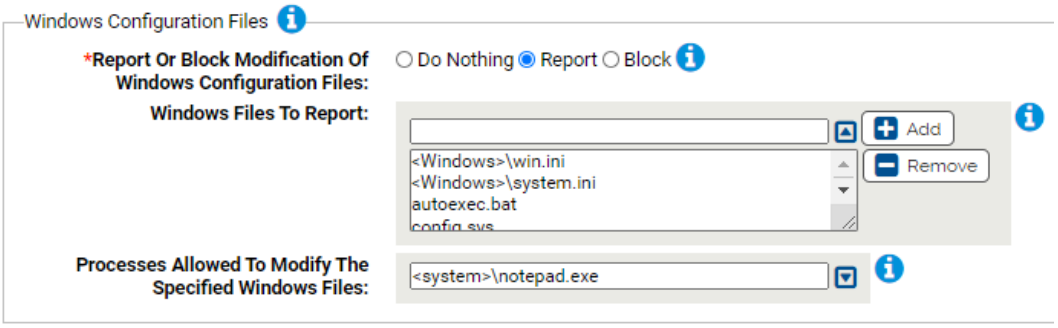
In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

For each of the following sections, specify what action you require.

Windows Configuration Files

Use this group to protect Windows configuration files.



***Report Or Block Modification Of Windows Configuration Files:**
Should modification of the specified files be reported or blocked? You should validate that legitimate modification is not blocked before enabling blocking.

Windows Files To Report:
Carbon Black App Control will report or block modifications of the specified files. You can add or remove items from this list. By default, the list includes:

- <Windows>\win.ini
- <Windows>\system.ini

- autoexec.bat
- config.sysboot.ini

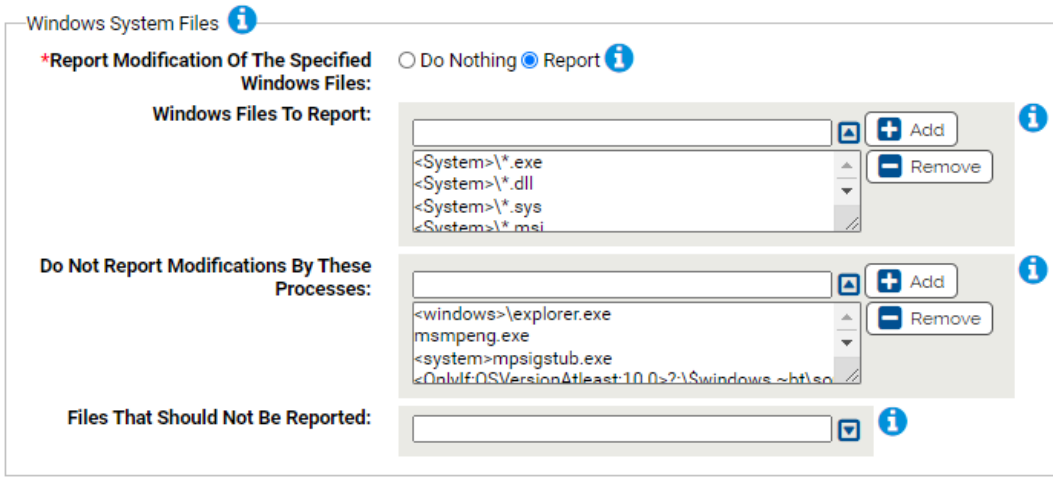
Processes Allowed To Modify The Specified Windows Files:

Processes specified here will be allowed to modify the specified Windows files. You can add or remove items from this list. By default, the list includes:

- <system>\notepad.exe

Windows System Files

Use this group to protect Windows system files.



***Report Modification Of The Specified Windows Files:**

Should modification of the specified Windows files be reported?

Windows Files To Report:

Carbon Black App Control will report modifications of the specified Windows files. You can add or remove items from this list. By default, the list includes:

- <System>*.exe
- <System>*.dll
- <System>*.sys
- <System>*.msi<System>*.drv
- <System>*.ocx<System>*.scr
- <SystemX86>*.exe
- <SystemX86>*.dll
- <SystemX86>*.sys
- <SystemX86>*.msi
- <SystemX86>*.drv
- <SystemX86>*.ocx
- <SystemX86>*.scr

Do Not Report Modifications By These Processes:

Processes listed here will be allowed to modify the specified Windows files. You can add or remove items from this list. By default, the list includes:

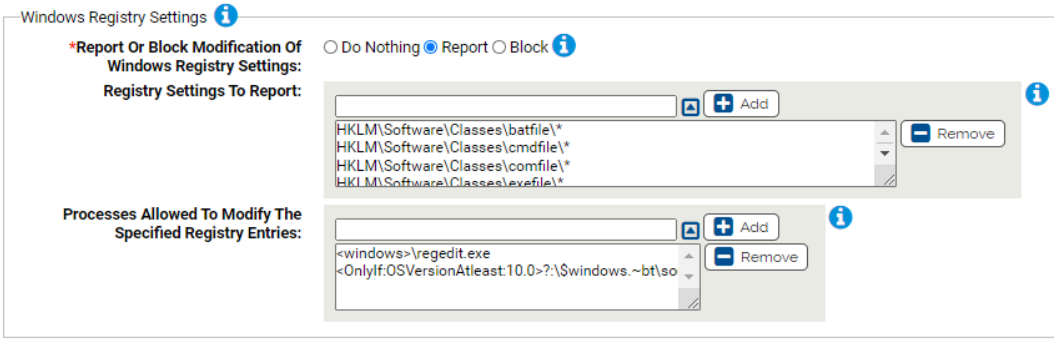
- <windows>\explorer.exe
- msmpeng.exe
- <system>mpsigstub.exe
- <OnlyIf:OSVersionAtleast:10.0>?:\$windows.~bt\sources\setuphost.exe

Files That Should Not Be Reported:

Modifications to files specified here will not be reported. You can add or remove items from this list.

Windows Registry Settings

Use this group to protect Windows registry settings.



***Report Or Block Modification Of Windows Registry Settings:**

Should modification of the specified registry settings be reported or blocked? You should validate that legitimate registry modifications are not blocked before enabling blocking.

Registry Settings To Report:

Carbon Black App Control will report or block modification of the specified registry settings. You can add or remove items from this list. By default, the list includes:

- HKLM\Software\Classes\batfile*
- HKLM\Software\Classes\cmdfile*
- HKLM\Software\Classes\comfile*
- HKLM\Software\Classes\exefile*
- HKLM\Software\Classes\piffile*
- HKLM\Software\Classes\AllFilesystemObjects*
- HKLM\Software\Classes\Directory*
- HKLM\Software\Classes\Folder*
- HKLM\Software\Classes\Protocols
- HKLM\System\CurrentControlSet\Control\Session Manager\KnownDLLs*
- HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg*

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run*
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce*
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx*
- HKLM\Software\Microsoft\Windows\CurrentVersion\URL*
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies*
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows*
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon*
- HKLM\Software\Microsoft\Active Setup\Installed Components*

Processes Allowed To Modify The Specified Registry Entries:

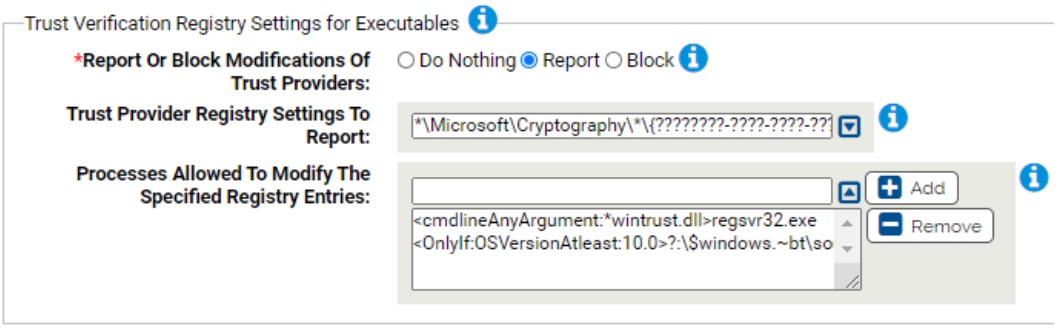
Processes specified here will be allowed to modify the specified registry entries. You can add or remove items from this list. By default, the list includes:

- <windows>\regedit.exe
- <OnlyIf:OSVersionAtleast:10.0>?:\$windows.~bt\sources\setuphost.exe

Trust Verification Registry Settings for Executables

Use this group to protect registry settings that affect verifying security certificates for executable files - exes, dlls, etc. We expect minimal false positives for these keys. Allowing modification of these keys enables a malicious user to make a file appear to have a valid digital signature even though it does not. Windows updates will be allowed to make modifications to the registry settings, other processes will be blocked or reported.

For more information, see: https://community.carbonblack.com/docs/DOC-9225



***Report Or Block Modifications Of Trust Providers:**

Should modification of the specified registry settings be reported or blocked? You should validate that legitimate registry modifications are not blocked before enabling blocking.

Trust Provider Registry Settings To Report:

Carbon Black App Control will report or block modification of the specified registry settings. You can add or remove items from this list. By default, the list includes:

- *\Microsoft\Cryptography*\{????????-????-????-????-00C04FC295EE}*

Processes Allowed To Modify The Specified Registry Entries:

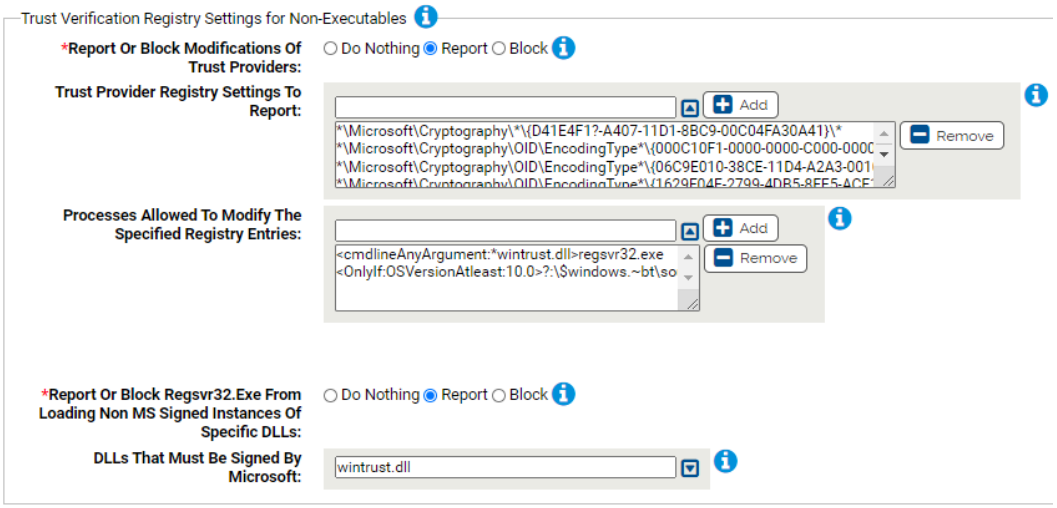
Processes specified here will be allowed to modify the specified registry entries. You can add or remove items from this list. By default, the list includes:

- <cmdlineAnyArgument:*wintrust.dll>regsvr32.exe<OnlyIf:OSVersionAtleast:10.0>?:\$windows .~bt\sources\setuphost.exe

Trust Verification Registry Settings for Non-Executables

Use this group to protect registry settings that affect verifying security certificates for non executables such as scripts, .net assemblies, etc. Allowing modification of these keys enables a malicious user to make a file appear to have a valid digital signature even though it does not. Windows updates will be allowed to make modifications to the registry settings, other processes will be blocked or reported.

For more information, see: https://community.carbonblack.com/docs/DOC-9225



***Report Or Block Modifications Of Trust Providers:**

Should modification of the specified registry settings be reported or blocked? You should validate that legitimate registry modifications are not blocked before enabling blocking.

Trust Provider Registry Settings To Report:

Carbon Black App Control will report or block modification of the specified registry settings. You can add or remove items from this list. By default, the list includes:

- *\Microsoft\Cryptography*\{D41E4F1?-A407-11D1-8BC9-00C04FA30A41}*
- *\Microsoft\Cryptography\OID\EncodingType*\{000C10F1-0000-0000-C000-000000000046}*
- *\Microsoft\Cryptography\OID\EncodingType*\{06C9E010-38CE-11D4-A2A3-00104BD35090}*
- *\Microsoft\Cryptography\OID\EncodingType*\{1629F04E-2799-4DB5-8FE5-ACE10F17EBAB}*
- *\Microsoft\Cryptography\OID\EncodingType*\{1A610570-38CE-11D4-A2A3-00104BD35090}*
- *\Microsoft\Cryptography\OID\EncodingType*\{0AC5DF4B-CE07-4DE2-B76E-23C839A09FD1}*
- *\Microsoft\Cryptography\OID\EncodingType*\{0F5F58B3-AADE-4B9A-A434-95742D92ECEB}*
- *\Microsoft\Cryptography\OID\EncodingType*\{5598CFF1-68DB-4340-B57F-1CACF88C9A51}*
- *\Microsoft\Cryptography\OID\EncodingType*\{9F3053C5-439D-4BF7-8A77-04F0450A1D9F}*
- *\Microsoft\Cryptography\OID\EncodingType*\{CF78C6DE-64A2-4799-B506-89ADFF5D16D6}*
- *\Microsoft\Cryptography\OID\EncodingType*\{D1D04F0C-9ABA-430D-B0E4-D7E96ACCE66C}*
- *\Microsoft\Cryptography\OID\EncodingType*\{603BCC1F-4B59-4E08-B724-D2C6297EF351}*
- *\Microsoft\Cryptography\Providers\Trust*\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}*
- *\Microsoft\Cryptography\Providers\Trust*\{6078065b-8f22-4b13-bd9b-5b762776f386}*
- *\Microsoft\Cryptography\Providers\Trust*\{64B9D180-8DA2-11CF-8736-00AA00A485EB}*
- *\Microsoft\Cryptography\Providers\Trust*\{7801EBD0-CF4B-11D0-851F-0060979387EA}*
- *\Microsoft\Cryptography\Providers\Trust*\{C6B2E8D0-E005-11CF-A134-00C04FD7BF43}*
- *\Microsoft\Cryptography\Providers\Trust*\{FC451C16-AC75-11D1-B4B8-00C04FB66EA0}*

Processes Allowed To Modify The Specified Registry Entries:

Processes specified here will be allowed to modify the specified registry entries. You can add or remove items from this list. By default, the list includes:

- <cmdlineAnyArgument:*wintrust.dll>regsvr32.exe
- <OnlyIf:OSVersionAtleast:10.0>?:\$windows.~bt\sources\setuphost.exe

***Report Or Block Regsvr32.Exe From Loading Non MS Signed Instances Of Specific DLLs:**

Should regsvr32.exe loading the specified DLLs be reported or blocked when the DLLs are NOT signed by Microsoft? You should validate that legitimate DLL loading is not blocked before enabling blocking.

DLLs That Must Be Signed By Microsoft:

DLLs listed here that are not signed by Microsoft will be reported or blocked from being loaded by regsvr32.exe. You can add or remove items from this list. By default, the list includes:

- wintrust.dll

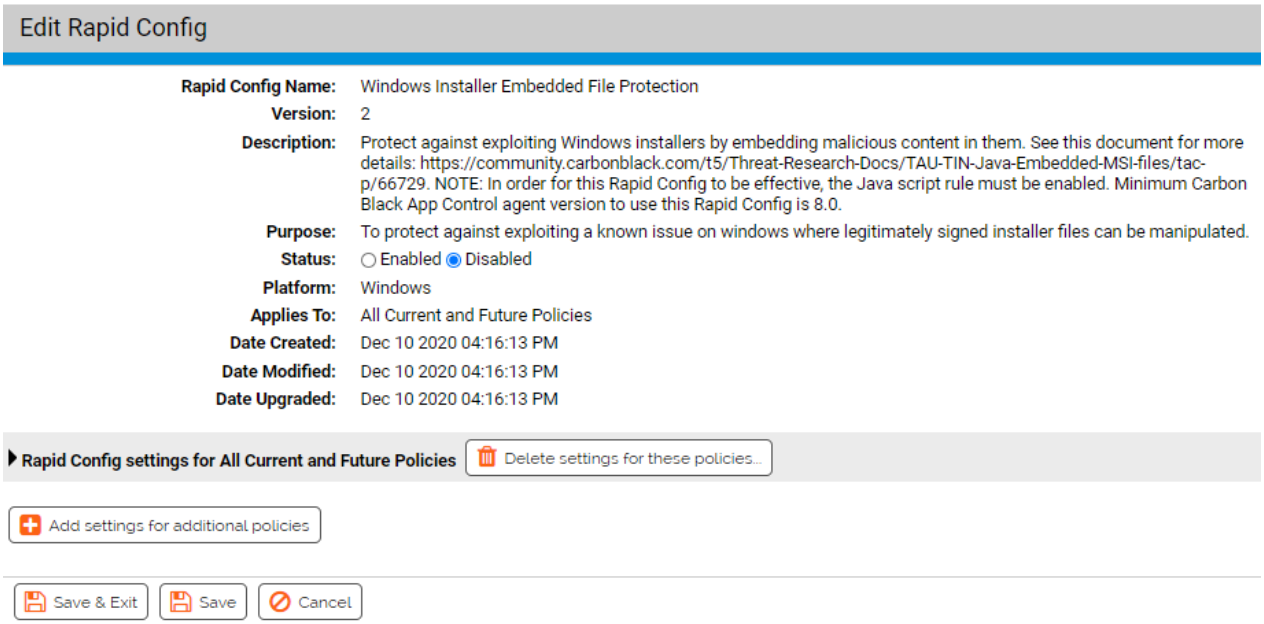
Windows Installer Embedded File Protection Rapid Config

Purpose:To protect against exploiting a known issue on windows where legitimately signed installer files can be manipulated.

Description: Protect against exploiting Windows installers by embedding malicious content in them.

See this document for more details: https://community.carbonblack.com/t5/Threat-Research-Docs/TAU-TIN-Java-Embedded-MSI-files/tac-p/66729.

Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0, patch 7



What are Embedded MSI files?

In February of 2019, our threat team posted about a feature in Windows that when abused could lead to unauthorized code execution bypassing code signing checks. This is done by appending malicious jar files to msi files.

To read more about what our threat team found, please see this UeX post, TAU-TIN - Java Embedded MSI files.

How can CB Protection help?

The Windows Installer Embedded File Protection Rapid Config focuses on blocking or reporting jar files that are appended to msi files and other related Microsoft installer formats.

Requirements

NOTE: Prior to v8.5.0, App Control was known as CB Protection.

- The java.exe script rule needs to be enabled.
- App Control Server version 8.0 Patch 7 and above.
- If you are running a version of App Control Server 8.0 prior to 8.0.Patch 7, you are able to import a rule to provide this coverage. You should follow the instructions in this link. There is no support for versions prior to 8.X.
- If your environment prevents you from receiving this Rapid Config via the CDC, please contact support for instructions for manual installation.

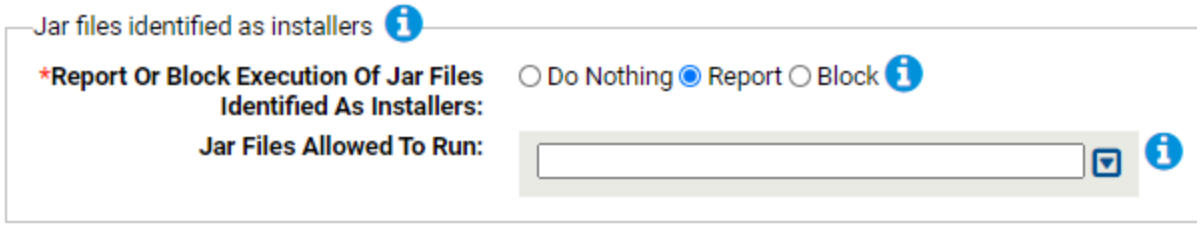
Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors. In this case, you can Report or Block the execution of Jar files identified as installers. It is unusual for jar files to be identified as installers by App Control.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.



Report Or Block Execution Of Jar Files Identified As Installers:
Should execution of jar files identified as installers be reported or blocked? You should validate that legitimate behavior is not blocked before enabling blocking.

Jar Files Allowed To Run:
Approved jar files specified here will be allowed to run even if identified as installers. You can add or remove items from this list.

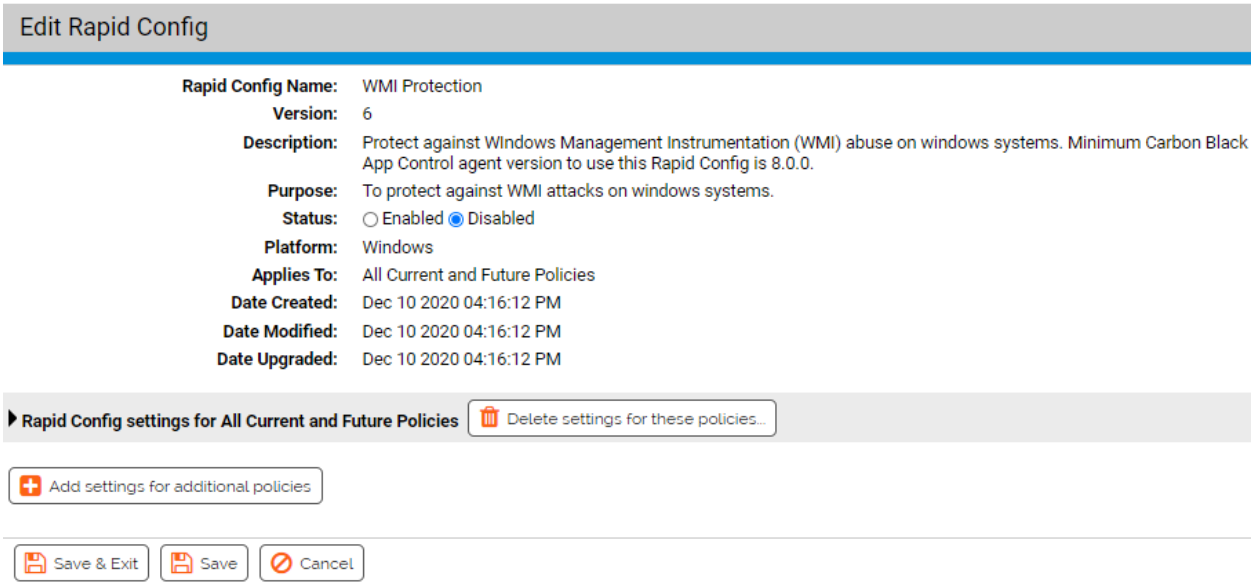
EXAMPLE: If you have a jar file named foo.jar that is tagged as an installer, and you still want to be able to execute it, you could specify that here.

WMI Protection Rapid Config

Purpose:To protect against WMI attacks on windows systems.

Description: Protect against WIndows Management Instrumentation (WMI) abuse on windows systems.

CDC Push Date:	
Enabled by Default:	No
Platform:	Windows
Minimum Agent Version Required:	8.0.0



Rapid Config Settings

As with most rapid configs, you can:

- Enable or disable the rapid config.
- Specify what policies the rapid config applies to.

In addition, you can choose to **Do Nothing**, **Report**, or **Block** the specific items or behaviors.

RECOMMENDATION: We recommend setting each section to **Report** prior to setting to **Block**. Use the resulting events to ensure that legitimate behavior will not be impacted.

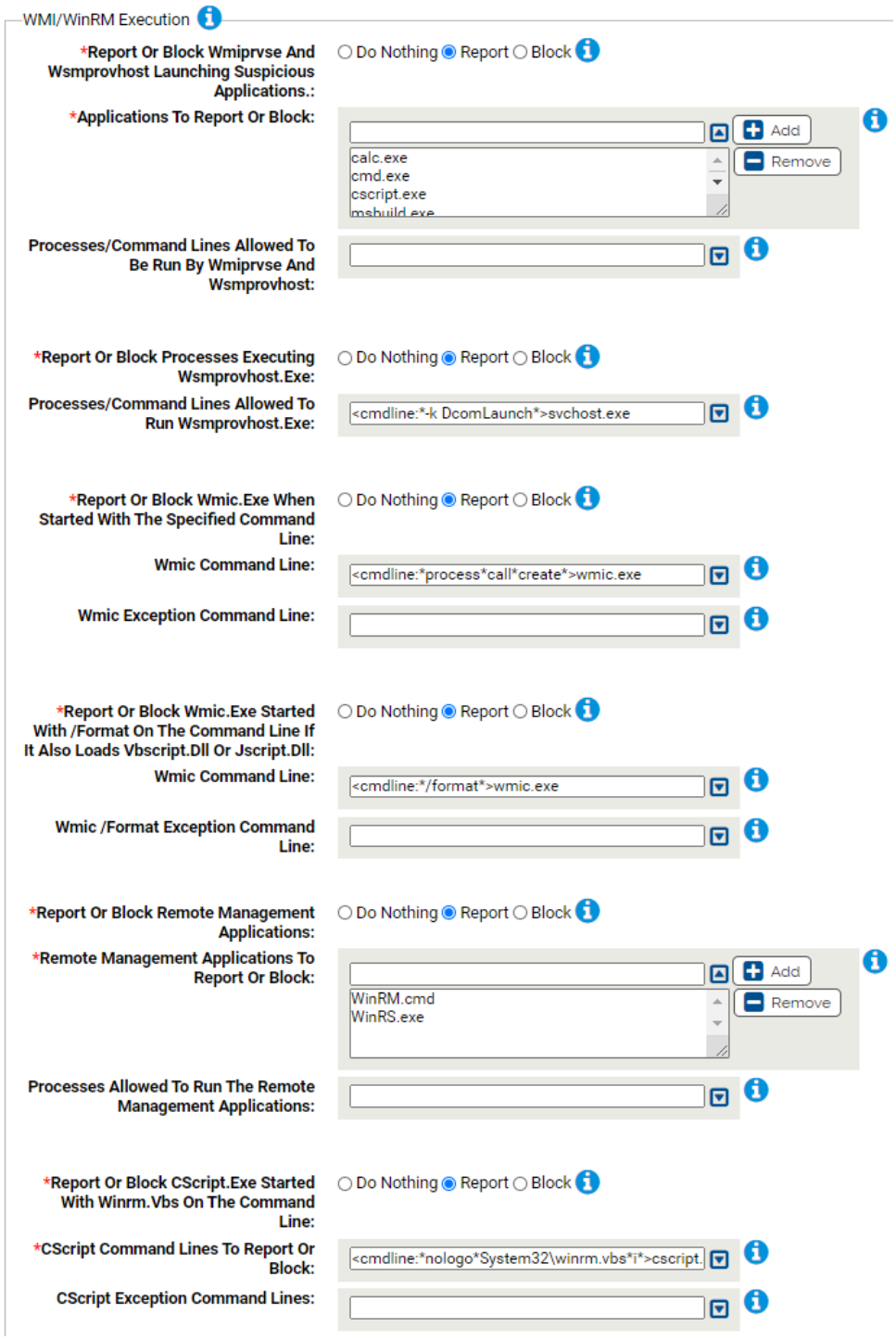
For each of the following sections, specify what action you require.

WMI/WinRM Execution

Use this group to protect against attacks using Windows Management Instrumentation (WMI)

Windows Management Instrumentation is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB) and Remote Procedure Call Service (RPCS) for remote access.

FOR MORE INFORMATION: https://attack.mitre.org/wiki/Technique/T1047


WMI/WinRM Execution
*Report Or Block Wmiprvse And Wsmprovhost Launching Suspicious Applications.:
Do Nothing Report Block
*Applications To Report Or Block:
Add
Remove
calc.exe
cmd.exe
cscript.exe
msbuild.exe
Processes/Command Lines Allowed To Be Run By Wmiprvse And Wsmprovhost:
*Report Or Block Processes Executing Wsmprovhost.Exe:
Do Nothing Report Block
Processes/Command Lines Allowed To Run Wsmprovhost.Exe:
<cmdline:*-k DcomLaunch*>svchost.exe
*Report Or Block Wmic.Exe When Started With The Specified Command Line:
Do Nothing Report Block
Wmic Command Line:
<cmdline:*process*call*create*>wmic.exe
Wmic Exception Command Line:
*Report Or Block Wmic.Exe Started With /Format On The Command Line If It Also Loads Vbscript.Dll Or Jscript.Dll:
Do Nothing Report Block
Wmic Command Line:
<cmdline:*/format*>wmic.exe
Wmic /Format Exception Command Line:
*Report Or Block Remote Management Applications:
Do Nothing Report Block
*Remote Management Applications To Report Or Block:
Add
Remove
WinRM.cmd
WinRS.exe
Processes Allowed To Run The Remote Management Applications:
*Report Or Block CScript.Exe Started With Winrm.Vbs On The Command Line:
Do Nothing Report Block
*CScript Command Lines To Report Or Block:
<cmdline:*nologo*System32\winrm.vbs*i*>cscript.
CScript Exception Command Lines:

***Report Or Block Wmiprvse And Wsmprovhost Launching Suspicious Applications:**

Should execution of the specified applications by wmiprvse or wsmprovhost be reported or blocked? You should validate that legitimate behavior is not blocked before enabling blocking.
These child processes are common living-off-the-land binaries adversaries leverage to gain code execution or spread laterally via WMI/WinRM

***Applications To Report Or Block:**

Carbon Black App Control will report or block execution of the specified applications by wmiprvse.exe or wsmprovhost.exe. You can add or remove files from this list. By default, the list includes:

- calc.exe
- cmd.exe
- cscript.exe
- msbuild.exe
- mshta.exe
- notepad.exe
- powershell.exe
- vssadmin.exe
- wscript.exe

Processes/Command Lines Allowed To Be Run By Wmiprvse And Wsmprovhost:

Processes and command lines listed here will not be blocked.

***Report Or Block Processes Executing Wsmprovhost.Exe:**

Should execution of wsmprovhost.exe be reported or blocked. Wsmprovhost is the process responsible for powershell remoting. You should validate that legitimate behavior is not blocked before enabling blocking.

Processes/Command Lines Allowed To Run Wsmprovhost.Exe:

Processes/command lines listed here will not be reported or blocked when they run wsmprovhost.exe. You can add or remove lines from this list. By default, the list includes:

- <cmdline:*-k DcomLaunch*>svchost.exe

***Report Or Block Wmic.Exe When Started With The Specified Command Line:**

Should execution of wmic.exe be reported or blocked when started with the potentially supcicious command line. The process call create command is often used for lateral movement/code execution. You should validate that legitimate behavior is not blocked before enabling blocking.

Wmic Command Line:

Carbon Black App Control will report or block execution of wmic.exe using the specified command line. You can add or remove items from this list. By default, the list includes:

- <cmdline:*process*call*create*>wmic.exe

Wmic Exception Command Line:

Command lines specified here will not be blocked. You can add or remove items from this list.

***Report Or Block Wmic.Exe Started With /Format On The Command Line If It Also Loads Vbscript.Dll Or Jscript.Dll:**

Should execution of wmic.exe be reported or blocked when started with /format on the command line and wmic loads either vbscript.dll or jscript.dll.
This technique, discovered by security researcher Casey Smith, enables an adversary to execute code within XSL cripts either locally or from a URL bypassing application whitelisting
You should validate that legitimate behavior is not blocked before enabling blocking.

Wmic Command Line:

Carbon Black App Control will report or block execution of wmic.exe using the specified command line if it also loads vbscript.dll or jscript.dll. You can add or remove items from this list. By default, the list includes:

- <cmdline:*/format*>wmic.exe

Wmic /Format Exception Command Line:

Command lines specified here will not be blocked. You can add or remove items from this list.

***Report Or Block Remote Management Applications:**

Should execution of the specified remote management applications be blocked? You should validate that legitimate behavior is not blocked before enabling blocking.
These binaries are used by adversaries to interact with WMI/winRM to spread laterally or execute code on local or remote systems.

***Remote Management Applications To Report Or Block:**

Carbon Black App Control will report or block execution of the remote management applications. You can add or remove files from this list. By default, the list includes:

- WinRM.cmd
- WinRS.exe

Processes Allowed To Run The Remote Management Applications:

The remote management applications will not be blocked when run by processes listed here.

***Report Or Block CScript.Exe Started With Winrm.Vbs On The Command Line:**

Should execution of Cscript.exe using the specified command lines be blocked? You should validate that legitimate behavior is not blocked before enabling blocking.
This rule protects against execution of WinRM.cmd or WinRM.vbs with the invoke parameter, which can be leveraged to execute code on a remote system.

***CScript Command Lines To Report Or Block:**

Carbon Black App Control will report or block execution of CScript.exe started with the specified command lines. You can add or remove files from this list. By default, the list includes:

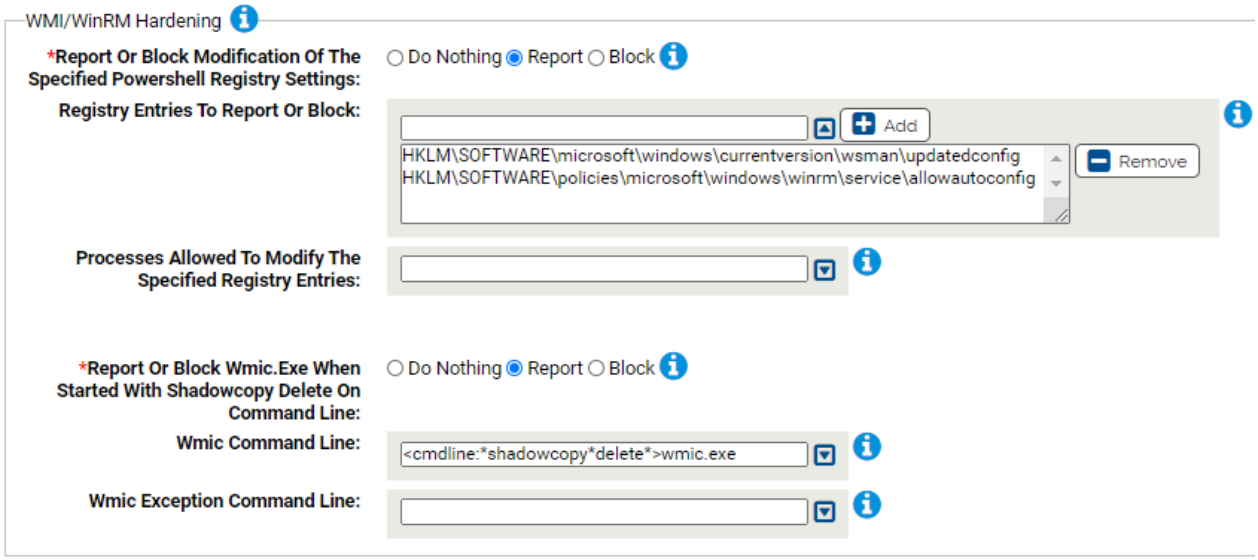
- <cmdline:*nologo*System32\winrm.vbs*i*>cscript.exe

CScript Exception Command Lines:

CScript Command lines specified here will not be reported or blocked.

WMI/WinRM Hardening

Use this group to provide miscellaneous rules for WMI hardening



***Report Or Block Modification Of The Specified Powershell Registry Settings:**

Should modification of the specified powershell registry entries be reported or blocked. You should validate that legitimate behavior is not blocked before enabling blocking.

This rule detects modifications to registry keys responsible for maintaining the state of WinRM, which can be leveraged to execute code on a remote system.

Registry Entries To Report Or Block:

Carbon Black App Control will report or block modification of the specified registry entries. You can add or remove items from this list. By default, the list includes:

- HKLM\SOFTWARE\microsoft\windows\currentversion\wsman\updatedconfig
- HKLM\SOFTWARE\policies\microsoft\windows\winrm\service\allowautoconfig

Processes Allowed To Modify The Specified Registry Entries:

Processes specified here will be allowed to modify the specified registry entries. You can add or remove items from this list.

***Report Or Block Wmic.Exe When Started With Shadowcopy Delete On Command Line:**

Should execution of wmic.exe be reported or blocked when started with shadowcopy delete on the command line. You should validate that legitimate behavior is not blocked before enabling blocking.

Wmic Command Line:

Carbon Black App Control will report or block execution of wmic.exe using the specified command line. You can add or remove items from this list. By default, the list includes:

- <cmdline:*shadowcopy*delete*>wmic.exe

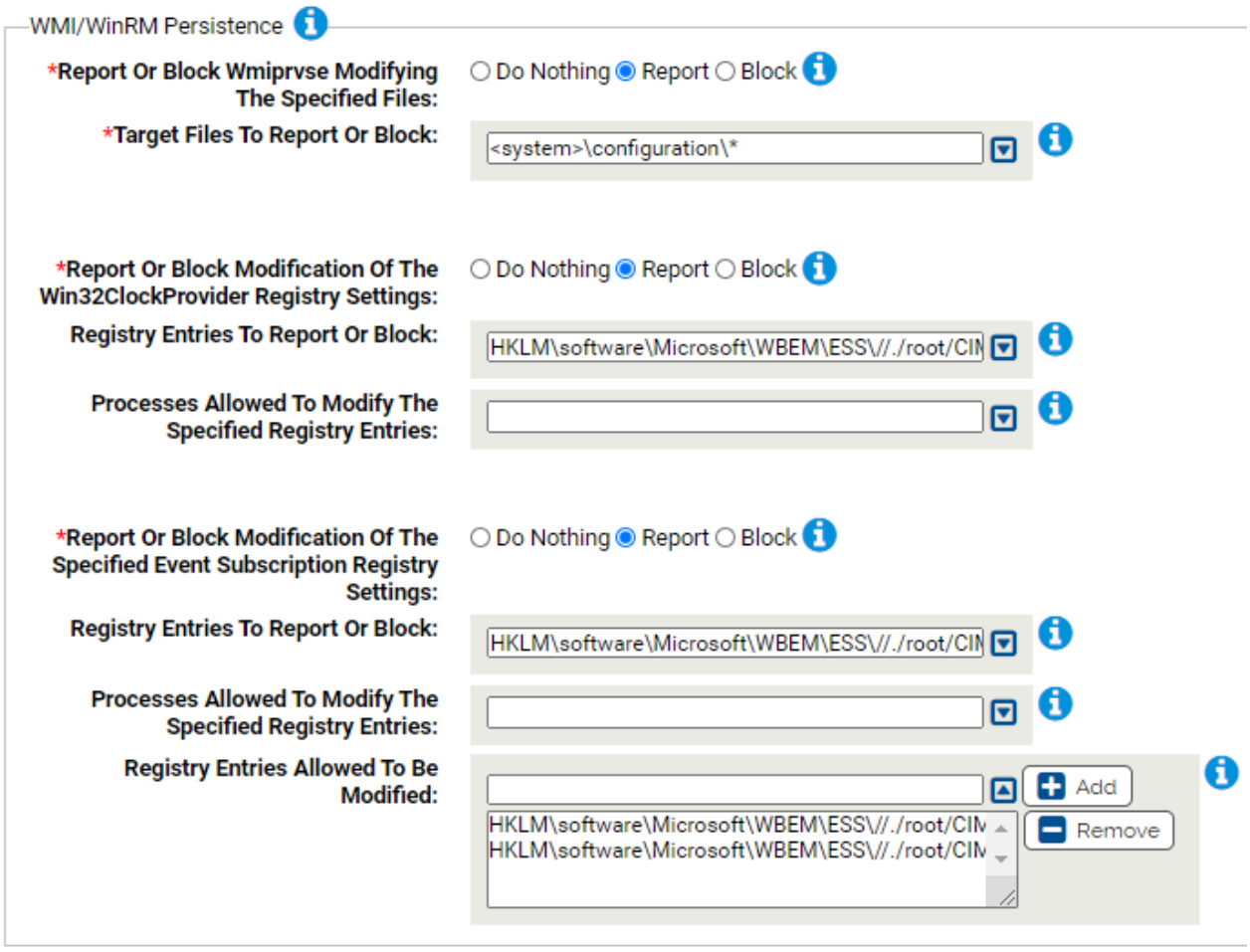
Wmic Exception Command Line:

Command lines specified here will not be blocked. You can add or remove items from this list.

WMI/WinRM Persistence

Windows Management Instrumentation (WMI) can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system.

FOR MORE INFORMATION: https://attack.mitre.org/wiki/Technique/T1084



***Report Or Block Wmiprvse Modifying The Specified Files:**

Should writing of the specified files by wmiprvse.exe be reported or blocked. You should validate that legitimate behavior is not blocked before enabling blocking.

This technique, discovered by Security Researchers Matt Hastings and Ryan Kazanciyan (with an honorary mention to Matt Graeber for his POC), enables an adversary to persist and move laterally within a network via Desired State Configuration, a Microsoft configuration management platform.

***Target Files To Report Or Block:**

Carbon Black App Control will report or block modification of the specified files by WMIPrvse.exe. You can add or remove items from this list. By default, the list includes:

- <system>\configuration*

***Report Or Block Modification Of The Win32ClockProvider Registry Settings:**

Should modification of the specified registry entries be reported or blocked. You should validate that legitimate behavior is not blocked before enabling blocking.

This rule protects against common WMI event filter persistence techniques leveraging a Win32_ LocalTime trigger. This may or may not be suspicious, but it is uncommon for this registry key to be modified.

Registry Entries To Report Or Block:

Carbon Black App Control will report or block modification of the specified registry entries. You can add or remove items from this list. By default, the list includes:

- HKLM\software\Microsoft\WBEM\ESS\//./root/CIMV2\Win32ClockProvider*

Processes Allowed To Modify The Specified Registry Entries:

Processes specified here will be allowed to modify the specified registry entries. You can add or remove items from this list.

***Report Or Block Modification Of The Specified Event Subscription Registry Settings:**

Should modification of the specified Event Subscription registry entries be reported or blocked. You should validate that legitimate behavior is not blocked before enabling blocking.

This rule protects against other forms of WMI Event Subscription persistence techniques not covered by the Win32ClockProvider rule above. The SCM Event Provider exclusion is provided to reduce false positives.

Registry Entries To Report Or Block:

Carbon Black App Control will report or block modification of the specified registry entries. You can add or remove items from this list. By default, the list includes:

- HKLM\software\Microsoft\WBEM\ESS\//./root/CIMV2*

Processes Allowed To Modify The Specified Registry Entries:

Processes specified here will be allowed to modify the specified registry entries. You can add or remove items from this list.

Registry Entries Allowed To Be Modified:

Modification of the registry entries specified here will be allowed. You can add or remove items from this list. By default, the list includes:

- HKLM\software\Microsoft\WBEM\ESS\//./root/CIMV2\Win32ClockProvider*
- HKLM\software\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider*