

Policies Page Content Updates

This document contains embedded help and text updates to several pieces of the Cb Defense Settings and Local Scan Settings pages.

General section: Check box title and tool tip edits

The top right section of Cb Defense Settings has checkboxes with question mark tool tips. The question mark tool tips stay as is for now, but here are edits to some of the tool tip titles and entries.

Current	Change	New
Allow Executable Uploads for Scans	capitalization	Allow executable uploads for scans
Show Sensor UI	full edit	Show sensor user interface
Allow User to Disable Protection	capitalization	Allow user to disable protection
Private Logging Level	full edit and capitalization	Enable private logging level
Run background scan	No change	n/a
Scan files on network drives	No change	n/a
Scan execute on network drives	No change	n/a
Delay Execute for Cloud Scan	capitalization	Delay execute for cloud scan
Hash MD5	No change	n/a
Use Windows Security Center	No change	n/a
Allow user to override policy enforcement	No change	n/a
Require Code to Uninstall Sensor	capitalization	Require code to uninstall sensor
Enable Live Response	No change	n/a
Submit unknown binaries for analysis	No change	n/a
Auto delete known malware hashes after	hyphenation	Auto-delete known malware hashes after
Rate Limit (KB/hr)	full edit and capitalization	Rate limit (KB/hour)
Connection Limit (connections/hr)	full edit and capitalization	Connection limit per hour
Keep sensor in bypass after login (minutes)	full edit	Bypass sensor after login
Keep sensor in bypass after restart (minutes)	full edit	Bypass sensor after restart

Tool tip edits

Allow User to Disable Protection

Sensor includes a Protection on/off toggle to set bypass mode. Applies to sensor versions 1.2 and later.

Enable Private Logging Level (current reads as Private Logging Level)

Logged events protect sensitive details. Redacts command line arguments, obfuscates document file names, IP addresses unresolved to domain names.

Scan execute on network drives

Applies to sensor versions 2.x and later. Sensor versions 1.x always scan network drives on execute.

Delay execute for cloud scan

Applies to sensor versions 2.x and later.

Create MD5 Hash (current reads as Hash MD5)

For best performance, uncheck this setting. Applies to sensor versions 2.x and later. Sensor versions 1.x always create MD5 hashes.

Enable Live Response

Enable Live Response on sensors. Default is disabled.

Target Value field

Add instructional text below the field label.

Target Value

Multiplier when calculating the threat level for detected issues and resulting alerts. Medium is the baseline/default.

New descriptions for each section

Permissions

PERMISSIONS Allow specific operations or bypass application activity entirely. Takes precedence over blocking and isolation settings below.

Blocking and Isolation

BLOCKING AND ISOLATION Deny or terminate processes and applications.








Uploads


UPLOADS Deny or allow upload paths.

Permissions section: Help Off / Show Tips








Note: Use Process instead of Application as first column header


Note: Fix “comma-separated” to be hyphenated

PROCESS	OPERATION ATTEMPT	ACTION		
Application(s) at path:		Allow	Allow & Log	Bypass
<input type="text" value="Add comma-separated paths"/>	Performs any operation			<input type="checkbox"/>
	Performs any API operation			<input type="checkbox"/>
	Runs or is running	<input type="checkbox"/>	<input type="checkbox"/>	
	Communicates over the network 	<input type="checkbox"/>	<input type="checkbox"/>	
	Scrapes memory of another process 	<input type="checkbox"/>	<input type="checkbox"/>	
	Executes code from memory 	<input type="checkbox"/>	<input type="checkbox"/>	
	Invokes a command interpreter 	<input type="checkbox"/>	<input type="checkbox"/>	
	Performs ransomware-like behavior 		<input type="checkbox"/>	
	Executes a fileless script 	<input type="checkbox"/>	<input type="checkbox"/>	
	Injects code or modifies memory of another process 	<input type="checkbox"/>	<input type="checkbox"/>	


[SHOW TIPS ?](#) 

Permissions section: Help On / Hide Tips










PROCESS	OPERATION ATTEMPT	ACTION		
Application(s) at path:		Allow	Allow & Log	Bypass
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <i>Add comma-separated paths</i> </div> <p>* matches 1 or multiple characters within the same directory ** matches 1 or multiple directories</p> <p>Examples Windows: **\powershell.exe Mac: /Users/*/Downloads/**</p>	Performs any operation <small>Bypass and ignore all activity at the application path.</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Performs any API operation <small>Bypass and ignore API activity at the application path.</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Runs or is running <small>Application operating on the endpoint</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Communicates over the network  <small>Network activity caused by the application</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Scrapes memory of another process  <small>Targeted attempt to read memory of processes such as lsass.exe</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Executes code from memory  <small>Untargeted attempt to run code from dynamic memory</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Invokes a command interpreter  <small>Attempt to use a shell / command line tool</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Performs ransomware-like behavior  <small>Access Cb Defense decoy files, attempt to write to the master boot record, attempt to access Volume Shadow Copy Service (VSS)</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Executes a fileless script  <small>Use trusted process for malicious use. Also called non-malware or "living off the land."</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Injects code or modifies memory of another process  <small>Trusted application injects code, or any use of process hollowing</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

HIDE TIPS 

CONFIRM
CANCEL



Blocking and Isolation section: Help Off / Show Tips

PROCESS	OPERATION ATTEMPT	ACTION	
Known malware	Runs or is running	<input type="checkbox"/>	<input type="checkbox"/>
	Communicates over the network 	<input type="checkbox"/>	<input type="checkbox"/>
	Scrapes memory of another process 	<input type="checkbox"/>	<input type="checkbox"/>
	Executes code from memory 	<input type="checkbox"/>	<input type="checkbox"/>
	Invokes a process not on the whitelist	<input type="checkbox"/>	<input type="checkbox"/>
	Invokes a command interpreter 	<input type="checkbox"/>	<input type="checkbox"/>
	Performs ransomware-like behavior 	<input type="checkbox"/>	<input type="checkbox"/>
	Executes a fileless script 	<input type="checkbox"/>	<input type="checkbox"/>
	Injects code or modifies memory of another process 	<input type="checkbox"/>	<input type="checkbox"/>
SHOW TIPS 	CONFIRM	CANCEL	

Blocking and Isolation section: Help On / Hide Tips

Note: Slightly different text for “Performs ransomware-like behavior”

PROCESS	OPERATION ATTEMPT	ACTION	
Known malware Reputation determined by Cb Defense analytics with hash set to Known Malware	Runs or is running Process operating on the endpoint	<input type="checkbox"/>	<input type="checkbox"/>
	Communicates over the network ⓘ Network activity caused by the process	<input type="checkbox"/>	<input type="checkbox"/>
	Scrapes memory of another process ⓘ Targeted attempt to read memory of processes such as lsass.exe	<input type="checkbox"/>	<input type="checkbox"/>
	Executes code from memory ⓘ Untargeted attempt to run code from dynamic memory	<input type="checkbox"/>	<input type="checkbox"/>
	Invokes a process not on the whitelist Untrusted application or process is accessed	<input type="checkbox"/>	<input type="checkbox"/>
	Invokes a command interpreter ⓘ Attempt to use a shell / command line tool	<input type="checkbox"/>	<input type="checkbox"/>
	Performs ransomware-like behavior ⓘ Access Cb Defense decoy files, attempt to write to the master boot record, attempt to access Volume Shadow Copy Service (VSS). Terminate is only option because denying ransomware does not prevent further encryption.	<input type="checkbox"/>	<input type="checkbox"/>
	Executes a fileless script ⓘ Uses trusted process for malicious use. Also called non-malware or “living off the land.”	<input type="checkbox"/>	<input type="checkbox"/>
	Injects code or modifies memory of another process ⓘ Trusted application injects code, or any use of process hollowing	<input type="checkbox"/>	<input type="checkbox"/>

[HIDE TIPS ?](#)

Blocking and Isolation sections

Note: Edit to “Unknown application or process” label

Note: Edit to “Adware” label

Note: Edit to “Not listed application” label

Known malware

Reputation determined by Cb Defense analytics with hash set to Known Malware

Application on the company blacklist

Application added to your organization’s blacklist in Cb Defense

Unknown application or process

Application reputation set to Unknown, for example, a new application added when the sensor was offline or unable to connect

Adware or PUP

Reputation determined by Cb Defense analytics with hash set to a PUP (potentially unwanted program) status of adware or popups

Suspected malware

Reputation determined by Cb Defense analytics with hash set to Suspected Malware

Not listed application

No reputation information to supply to the sensor; typically means the hash is new. Helps protect against zero-day malware and is frequently assigned to new hashes/updated applications.

Uploads

Note: Fix “comma-separated” to be hyphenated

Note: Change “Upload” column header to “Action”

Note: Edits to text in third column

PATH	ACTION	
<input type="text" value="Add comma-separated paths"/>	NO UPLOAD	<i>Prevent the sensor from sending uploads from the specified paths</i>
<input type="text" value="Add comma-separated paths"/>	UPLOAD	<i>If needed, allow the sensor to send uploads from the specified paths</i>

Local Scan Settings

Updates to the Local Scan Settings tab.

Target Value field

Add instructional text below the field label.

Target Value

Multiplier when calculating the threat level for detected issues and resulting alerts. Medium is the baseline/default.

Update Servers

Note: Add general “Upload Servers” section in the same style as other fields on the page, to allow us to add descriptive text.

Note: Add “for internal devices” to column header for first table

Note: The table width below isn’t prescriptive – I think the current table on dev01 is too small but I don’t know what the width is supposed to be. Screen shots in the user guide and on UeX show much wider tables.

Update Servers

Specify one or more update servers for local scanning signatures. Use the default from Carbon Black alone, or add your own signature mirror URLs. For internal devices, select the Master to specify which update server is checked first. Other update servers are checked if the master is not available.

UPDATE SERVERS FOR INTERNAL DEVICES		MASTER
<input type="text" value="Enter signature mirror URL"/>	<input type="button" value="ADD"/>	
<hr/>		
http://updates.cdc.carbonblack.io/update	<input type="checkbox"/>	<input type="checkbox"/>
<hr/>		

UPDATE SERVERS FOR OFFSITE DEVICES		
<input type="text" value="Enter signature mirror URL"/>	<input type="button" value="ADD"/>	
<hr/>		
http://updates.cdc.carbonblack.io/update		<input type="checkbox"/>
<hr/>		