General Notes

Cb Defense Sensor version 3.2.0 is a release for the Windows operating system only.

New Features

This section lists features introduced in the 3.2.0 version of Cb Defense Sensor. (For a more thorough description of the new features in this release, see the User's Guide.)

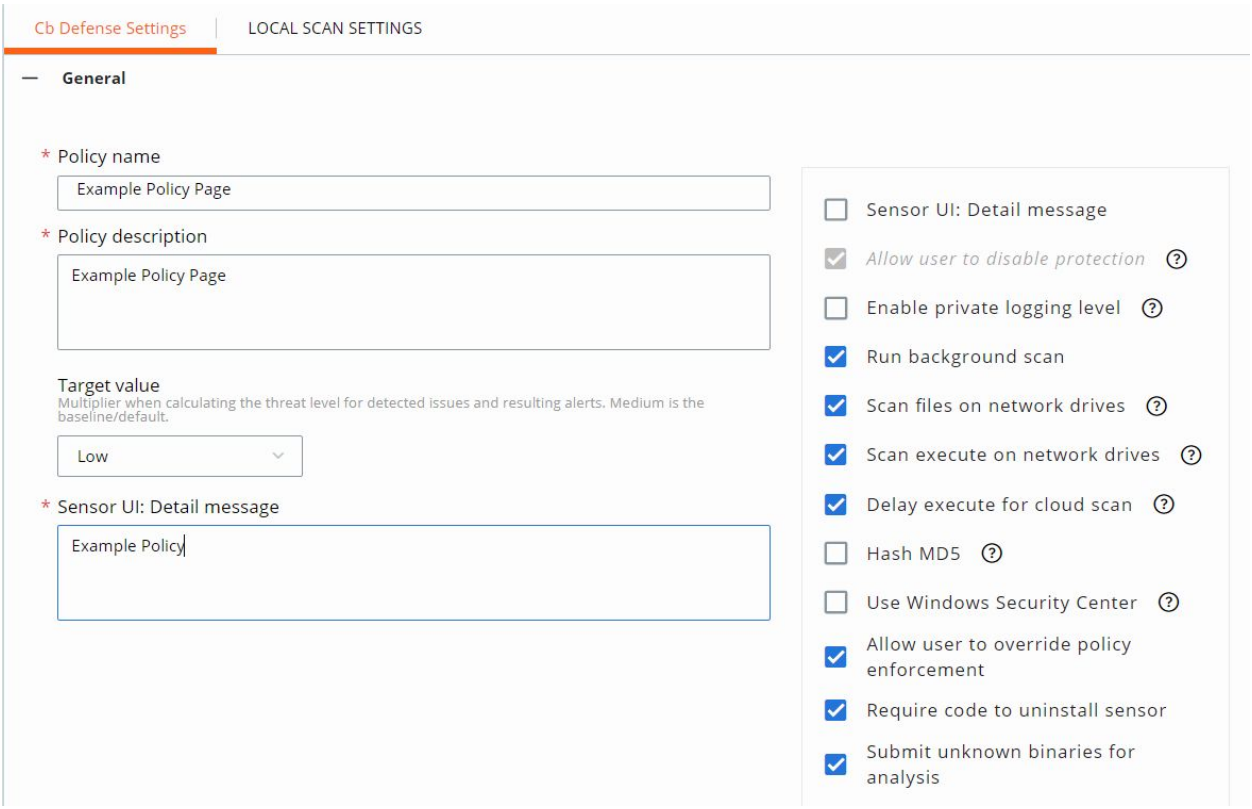
Improved Cloud Binary Analysis

The 3.2 Cb Defense sensor provides the ability to submit unknown binaries for additional cloud analysis. A check box on the "Policies" page, enables users to "opt in" to this feature, and thereby consent to share data with Carbon Black and our third-party partner detailed below. This feature will only be functional for users that have also enabled their local scanner.

DATA COLLECTION NOTICE: If you opt in to this functionality, the binary files (including the content of the files) are uploaded to Carbon Black for analysis. Carbon Black uses a third-party vendor, Avira Operations GmbH & Co. KG ("Avira"), as a sub-processor to assist with the threat analysis. The binary files are sent to Avira's network. Avira only processes the data to meet Carbon Black's obligations under the applicable agreement and for no other purpose. Avira has implemented appropriate security and operational methods that are designed to secure the data, and will comply with all applicable data privacy laws when processing the data. The information will be processed by Avira in their US or EU data centers.

In the course of using the services, you shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use and transfer to Carbon Black all such data. You can view Carbon Black's privacy policy at https://www.carbonblack.com/privacy-policy/ (which is modified by Carbon Black from time to time).

This feature is disabled by default. To enable this improved binary analysis, log into the Cb Defense Console → click on **Settings** icon in the top-right corner → click **Policies** and then, on the CB Defense Settings page, check **Submit Unknown Binaries for Analysis** for the specific policies to enable.



To read more about this security improvement, please see the User's Guide.

Enhanced sensor installer

The 3.2 Cb Defense sensor provides a redesigned Windows sensor installer. This improved installer significantly improves the reliability of new installs and sensor upgrades, especially for mass sensor installs through Group Policy Objects (GPO), upgrades, and software distribution tools such as SCCM.

The enhanced installer has a number of quality improvements, and keeps the upgrade and install methods the same as prior releases. This new installer as been tested on upgrades for all supported sensor versions (2.1.0 and above) to our latest 3.2 sensor.

To read more about which install paths are supported in this sensor please see: https://community.carbonblack.com/docs/DOC-13622

To read more about the methods in which you can install and upgrade sensors, please see the User's Guide.

Carbon Black.

Issues Resolved in 3.2.0

Description
If you have already run into any of the two Sensor Install issues described in the Knowledge Base articles below, the sensor clean up tool is still required to cleanup the device state. However, going forward the Enhanced Sensor Installer will prevent these issues from occurring since we no longer allow third party applications to re-add the the Cb Defense registry key in HKEY_CLASSES_ROOT\Installer\Products\ https://community.carbonblack.com/docs/DOC-10328 https://community.carbonblack.com/docs/DOC-10643 **Introduced additional checks to ensure that GPO is configured to allow upgrades manually or from the Cb Defense Console. See https://community.carbonblack.com/docs/DOC-13411 for details.**
Resolved an issue where duplicate BLOCK or TERMINATE notifications are not sent to the Sensor UI for a period of 30 minutes.
Resolved a a potential product bypass found internally, by making improvements to the product's tamper protection.
Resolved an issue where Permission Rules were intermittently not working
Resolved an interoperability issue when BitDefender was enabled, that resulted in ctiuser.dll missing from computer.
Resolved a latency issue that some users were experiencing when copying files to a shared drive.
Resolved an issue where applications were crashing because of ctiuser.dll.
Resolved an issue where Internet Explorer and Microsoft Edge could not load internal web applications with Defense enabled.
Resolved an issue that prevented users from accessing Windows 7 EFS encrypted files with Defense enabled.
Resolved an issue with the agent denying/terminating processes associated with Microsoft office applications, and no notification appearing in the console/UI.

Resolved an issue where applications that "attempted to modify the next instruction to execute in the process" are being blocked\terminated
Resolved an issue where sensors immediately install in bypass mode if Kaspersky Encryption software is installed.
Resolved an issue where Ivanti RES One Workspace immediately errors out and logs the user out of Windows if the sensor is installed.
Resolved an issue where the Sensor was unable to remove a file marked for deletion if we lacked permissions, there are open handles, or the file currently running. In the first two cases the sensor will delete the file immediately, but files already running will be deleted on reboot.

Known Issues and Caveats

The following section lists known issues in this version of Cb Defense Sensor.

ID	Description
DSEN-1740	When upgrading Windows 10 to the 1709 update, with Windows Security Center integration enabled, the WSC integration service sometimes fails to start until the system has been rebooted following the update 1709 update.
DSEN-1180	When using Live Response, users can kill the PID for repmgr32, and the Live Response UI session ends; however, the sensor does not recover until after a reboot.
DSEN-1293	When trying to delete a registry key (that contains subkeys) by using Live Response, keys are not deleted; however, no error message displays.
DSEN-1554	Network file access slow or fails when "Scan execute on network drives" is enabled. Refer to https://community.carbonblack.com/docs/DOC-11994
DSEN-1387	Background Scan Remains Disabled On Devices Where VDI=1 Was Used. Refer to https://community.carbonblack.com/docs/DOC-12001
EA-11954	Sensor Installation Hangs if Virtual Machine Uses VirtIO Network Driver. Refer to https://community.carbonblack.com/docs/DOC-13166

Carbon Black.

DSER-7265	VDI Master Image Sensor Keeps Uninstalling Itself. Refer to https://community.carbonblack.com/docs/DOC-13540
EA-11628	Sensor is locking PDF files if Local Scanner is enabled.
DSEN-1987	False Positive Alert when the [application name] attempted to access the raw disk on the device. Refer to https://community.carbonblack.com/docs/DOC-10730
DSEN-1463	False Positive Alert when the [application name] attempted to modify a user data file. Refer to https://community.carbonblack.com/docs/DOC-10730.
DSEN-2687	An issue was identified in 3.2.0 that could cause the agent to not block a script file the first time its accessed. Subsequent access was blocked properly. The issue is currently aimed to be resolved in August.