General Notes

Cb Defense Sensor version 3.3 is a GA (General Availability) for Windows only.

New Features

LiveQuery

LiveQuery is a new component to Carbon Black's LiveOps product, part of the Predictive Security Cloud product suite. LiveOps consists of Live Response and LiveQuery. To enable a device to return LiveQuery results, your organization must have purchased LiveOps and must have a 3.3 sensor present on an endpoint. To read more about how to use LiveQuery, see: https://community.carbonblack.com/community/resources/cb-predictive-security-cloud/cb-liveops/live-query.

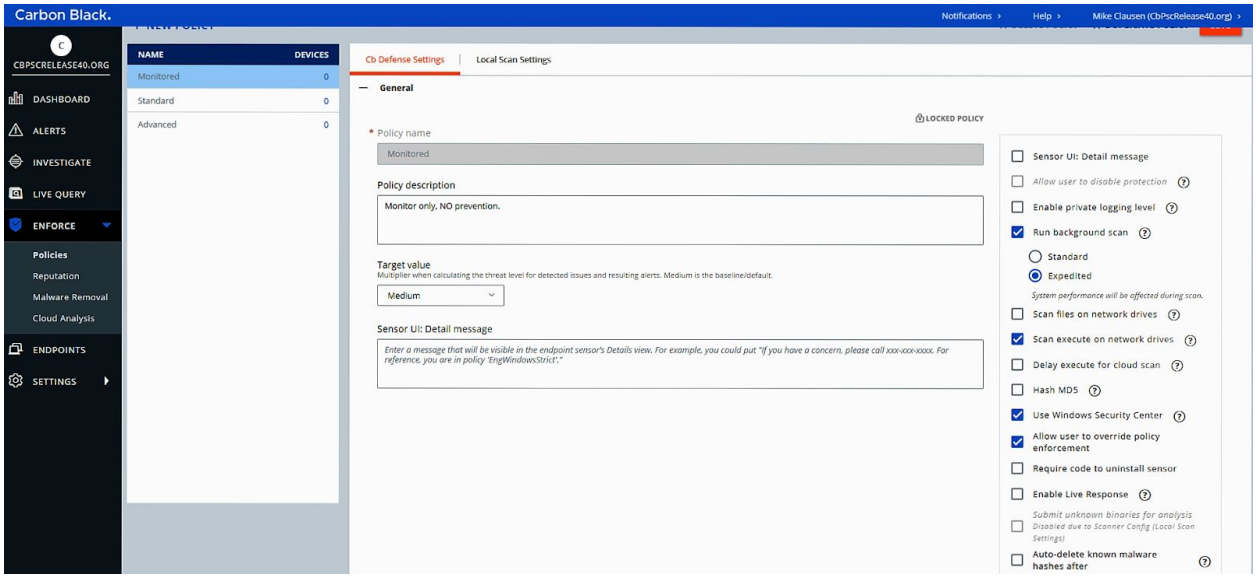
Enabling the RepCLI Supportability Tool - User Groups

RepCLI is a command line tool that can be used as a way to locally manage the sensor without using the backend. It can be used by support for troubleshooting and repairing.

RepCLI is authenticated by userSid. To enable the RepCLI tool, the user should specify the field <CLI_USERS>= <sid> during an unattended sensor installation. Any member in that user group can use the authenticated RepCLI commands. Users should identify the subset of users who administer CbDefense and authenticate them using this field. A dedicated user account for RepCLI can also be used. Carbon Black recommends creating a new AD user group and specifying its user SID on the installer command line even if you don't initially plan to use RepCLI capabilities. This way, should you find a problematic sensor that can't connect to backend, you can add an authenticated IT or helpdesk user to the AD group who can run authenticated RepCLI commands to repair the sensor.

Quick Scan

Quick scan is a policy setting that enables an expedited scan of an endpoint. The setting, shown below, accelerates the scan so that it runs 3x faster than the previous normal scan would run. Keep in mind this will increase the CPU and Disk I/O. Currently, there is no indication in the UI for when the scan is completed. However, the command `RepCLI.exe status` will show the current state of the background scan.



Issues Resolved in Sensor version 3.3

ID	Description
EA-11628/DSEN-3170	The issue noted in https://community.carbonblack.com/thread/9746 will be resolved in the 3.3 release and behavioral rules will not be required to block files such as docs and PDFs.
DSEN-2994	The issue where sensor does not terminate org blacklisted applications that began running before the sensor install has been resolved.
DSEN-2914	The issue causing the Citrix receiver to occasionally crash and require a restart has been resolved.
EA-12598, DSEN-1554	Some customers have reported that the scan execute on network drives has caused latency on the order of 10-15 minutes. This issue is resolved in 3.3
DSEN-3986, EA-13205	Customers may have experienced a hang on their machine post-install of the original 3.3 sensor (v3.3.0.953). This issue is resolved.
DSEN-2792, EA-13169	Customers may have experienced crashes on the original 3.3 sensor. (v.3.3.0.953). This issue is resolved.

DSEN-4237, EA-13407	This fix resolves a race condition previously identified on 3.3 sensors which result in a BSOD.
DSEN-3894	This fix resolves a pre-existing issue in which the sensor may whitelist invalidly signed certificates that were defined in the certificate whitelisting module in the Reputation page in the cloud console. More information is here: https://community.carbonblack.com/t5/Documentation-Downloads/CB18-1218-Cb-Defense-Improper-Reputation-Whitelisting-Windows/ta-p/63937

Known Issues & Caveats

ID	Description
DSEN-1987	False positive alert when the [application name] attempted to access the raw disk on the file. Refer to: https://community.carbonblack.com/docs/DOC-10730.
DSEN-1180, DSEN-3065	When using Live Response, users can kill the pid for repmgr32, and the Live Response session ends. However, the sensor does not recover until after a reboot. Users can also delete certain files within the confer directory. Users should be advised to use caution during Live Response sessions.
DSEN-2877	Some sensors can be caught in an infinite loop upon system crash or hard reset. In this case, an uninstall/reinstall is required to resolve the issue. This issue will be resolved in the 3.4 release.
DSEN-2378	During an attended install, Windows installer shows blank error dialogue when attempting to install on an unsupported OS.
DSEN-1387	Background Scan remains disabled on devices where VDI=1 was used. See https://community.carbonblack.com/docs/DOC-12001.
DSEN-3061	Sensor does not whitelist files by certificate if it is signed with multi-byte characters.
DSEN-2484, DSEN-3047	When uninstalling the Cb Defense sensor, a warning dialog box appears with the following message: **Warning 1910. Could not remove Shortcut Cb Defense.lnk.**

	Verify that the shortcut file exists and that you can access it. The referenced shortcut Cb Defense.lnk is located under the Defense install folder and attempts to remove the shortcut occur prior to the Defense service shutdown. Bypass prevents this error message from occurring.
DSEN-3088	When the sensor is removed from an AD domain, the sensor will still be reflected as within that domain in the endpoints page and will remain in an endpoint group. The sensor must be taken out of auto-assignment to make policy updates to that sensor and endpoint. This issue is resolved in the upcoming 3.4 release.
DSEN-2990	Major Windows updates occasionally fail. This has only been observed during upgrades from Redstone 3 to Redstone 4. Users must place the sensor in bypass mode to upgrade major operating systems, and then re-enable the sensor.
DSEN-3716	RepCli.exe status command does not show the correct state of slow (standard) or fast (expedited) scan.
DSEN-3848	If a user inputs an incorrect registration code during an attended install, the user may not be notified of a failure. The installer UI will indicate that cloud connectivity can not be established. The UI will remain responsive and the user can input the correct code and proceed with installation.
DSEN-3610	Uninstall.exe exits almost immediately with error code -1073741510 (0xC000013A) on Windows x86, but eventually will complete. This issue is resolved in the upcoming 3.4 sensor.
DSEN-3854	If Windows Security Center integration is enabled in the CbD policy, and a 3.2.x or later sensor is installed on a Windows Server OS (which does not have Security Center), protection cannot be enabled within 1 minute of restarting the CbDefense service.
DSEN-3866	Windows sensor 3.3, while compatible with Windows Server 2019 results in Windows Server 2019 devices being showed as Windows Server 2016 devices.
DSEN-3134	GPO upgrades from 3.2 to 3.3 occasionally fail.
DSEN-4004	Service Pack version is not reported for Windows 7 devices. This only impacts 3.3 sensors.
DSEN-4054	The LiveResponse memdump command may cause crashes. It is disabled by default on 3.3 and above. Instructions on enabling the command can be provided.
DSEN-4091	Users may experience latency associated with the execution of script files.
DSEN-3052	Users may experience latency associated with Cb-triggered file deletes.

DSEN-4520	Users may not be able to execute application deletions from the cloud console, and LiveQuery executions may not return results against endpoints behind a proxy. This issue was identified on 1/16/19 and will be resolved in the 3.4 GA sensor release.