Carbon Black.

Cb Defense Sensor 3.1.0 for Windows

Release Notes

January 29th, 2018

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

General Notes

Cb Defense Sensor version 3.1 is a release for the Windows operating system only.

New Features

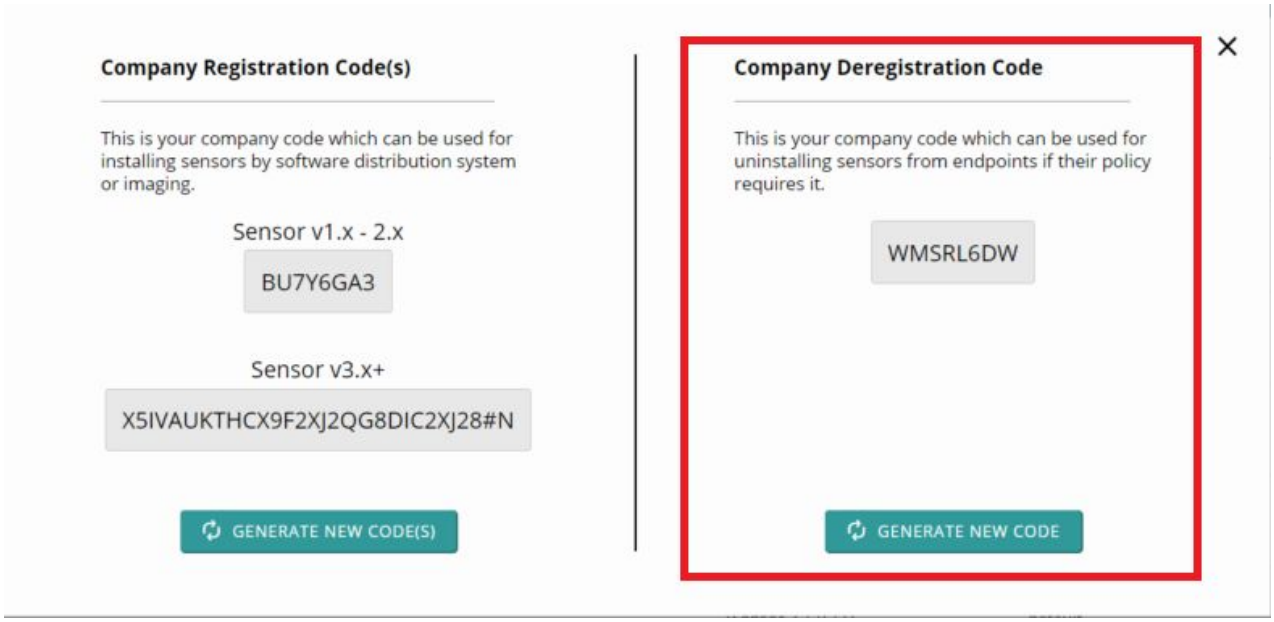
This section lists features introduced in the 3.1 version of Cb Defense Sensor. (For a more thorough description of the new features in this release, see the User's Guide.)

Protected Uninstall

The 3.1 Cb Defense sensor provides admins additional control and protection of their endpoints by allowing them to require a code to uninstall sensors. Admins can now enable a policy setting that protects the action of uninstalling an endpoint by requiring a unique, randomly-generated code.

After this policy setting is enabled, admins will have the flexibility to uninstall a group of sensors by using a company deregistration code, or uninstalling sensors on a per-device basis by using an individual device uninstall code.

Company Deregistration Code:



Per Device Code:

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

Mass Sensor Management

This release allows admins to manage a group of sensors for automatic policy group assignments. Admins can now create sensor groups to manage sensors in bulk. After they are in a group, all the sensors in that group receive an automatic assignment to a policy group based on the metadata that is associated with the sensor and the criteria that the admin defines. This allows admins to save time in managing a large number of sensors.

Metadata for Cb Defense sensors v3.1 and above includes:

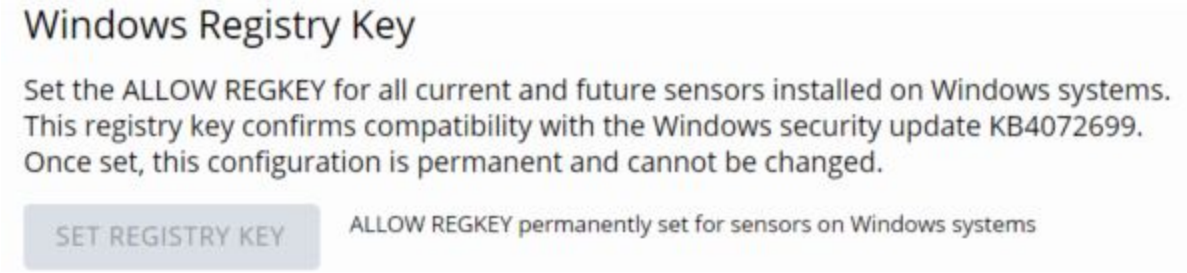
- Operating system (Windows, macOS)
- Active Directory organizational unit (Windows only)
- Active Directory domain (Windows only)
- Active Directory distinguished name (Windows only)
- Device host name
- Subnet (The subnet filtering is applied to the internal IP address of the sensor.)

To read more about this feature and how to configure these groups, see the User's Guide.

Set Windows Registry Key

This release offers a way to download the required registry key for compatibility with the Windows update addressing Meltdown and Spectre.

This setting is disabled by default, and once enabled, will set the registry key for all current and future sensors installed on Windows systems.



To read more about this feature and how to configure this setting, see the User's Guide.

Issues Resolved in 3.1.0

Description
Resolved additional False Positives associated with the Ransomware prevention improvements in the 3.0.1 (and 3.0.2.2) sensor
Resolved a bug that resulted in BSOD (Blue Screen of Death) related to ctifile.sys.
Resolved a bug that caused Microsoft Office documents, .tmp files to be created and not deleted when the file was closed or saved.
Added back support for Windows Server 2008, which was unintentionally removed with the 3.0 sensor.
Added Anti-Spyware integration for Win7 and Win8 users that never properly appeared in UI of the Windows Security Center/Action Center in prior versions.

Known Issues and Caveats

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

ID	Description
N/A	Upgrade issues have been observed when upgrading from sensor 2.0.3 to any newer version. Please reference the below Knowledge Base articles for more detail on these issues: https://community.carbonblack.com/docs/DOC-10328 https://community.carbonblack.com/docs/DOC-10643 For additional issues or concerns please contact Carbon Black Support.

EA-8575 CIT-10882	Duplicate BLOCK or TERMINATE notifications are not sent to the Sensor UI for a period of 30 minutes.
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.