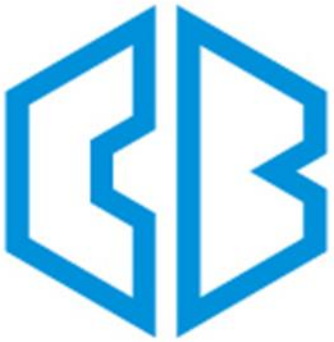


VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Supplemental Administrative Guidance for Common Criteria

Version 1.1
June 24, 2021

VMware Carbon Black
1100 Winter Street
Waltham, M.A. 02451

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Table of Contents

List of Tables

1 Introduction

The TOE is the VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 application, also referred to as the TOE from this point forward. The VMware CB EDR Windows Sensor is an enterprise software application whose primary purpose is to gather event data on the endpoints and invoke the OS to securely transmit this information to the operating environment's management server for centralized storage and indexing. The evaluated TOE scope is comprised of only those functions identified by the security functional requirements in the VMware CB EDR Windows Sensor v7.2 Security Target.

The Protection Profile for Application Software Version 1.3 (APP_PP) defines an application as "software that runs on a platform and performs tasks on behalf of the user or owner of the platform, as well as its supporting documentation."

As a Common Criteria evaluated product, this guidance serves to define the 'evaluated configuration' in which the evaluation was performed and to summarize how to perform the security functions that were tested as part of the evaluation.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating VMware CB EDR Windows Sensor 7.2. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is also expected to be familiar with the "*VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Security Target*" and the general CC terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions for how to perform the security functions that are defined by these SFRs. The VMware CB EDR Windows Sensor product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the claimed PP are discussed here. Any functionality that is not described here or in the "*VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Security Target*" was not evaluated and should be exercised at the user's risk.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below. These terms are also described in the "*VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Security Target.*"

CC: stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

SFR: stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: stands for Target of Evaluation. This refers to the aspects of the VMware CB EDR Windows Sensor product that contain the security functions that were tested as part of the CC evaluation process.

Local Administrator: The Windows OS administrator who has system permissions to access sensitive data and perform management functionality on the endpoint system.

Management Server: Management of the Sensors by an enterprise administrator using the operational environment's VMware Carbon Black EDR Server. The VMware CB EDR Sever application was separately evaluated.

Endpoint System: A device or set of devices, such as a laptop or desktop, with the Windows operating system that hosts the VMware CB EDR Windows Sensor (TOE).

Endpoint User: An individual who has access to the TOE but is not able to manage its behavior.

Sensor Group: Each sensor is associated with a sensor group that defines its configuration and security characteristics. A sensor group must contain at least one sensor and can contain many sensors. However, a single sensor can only belong to one sensor group. Sensor groups can be based on the security and organizational requirements. For example, one could base sensor groups on functional groupings/departments (such as marketing, customer service, or IT) or location.

4 References

The following security-relevant documents are included with the TOE.

[1] VMware Carbon Black EDR User Guide, "VMware Carbon Black EDR User Guide VMware Carbon Black EDR 7.5", [standard documentation for VMware Carbon Black EDR product].

[2] VMware Carbon Black EDR Supplemental Guide for the server, "VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Supplemental Administrative Guidance for Common Criteria", [See Common Criteria VID11156 VMware Carbon Black EDR Server]

[3] Microsoft Windows Common Criteria Evaluation Microsoft Windows 10 version 1903 (May 2019 Update) Microsoft Windows Server version 1903 (May 2019 Update) Security Target Version 0.04 July 19, 2019

The following document was created in support of the VMware CB EDR Windows Sensor CC evaluation:

[4] VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Security Target, v1.5, June 24, 2021

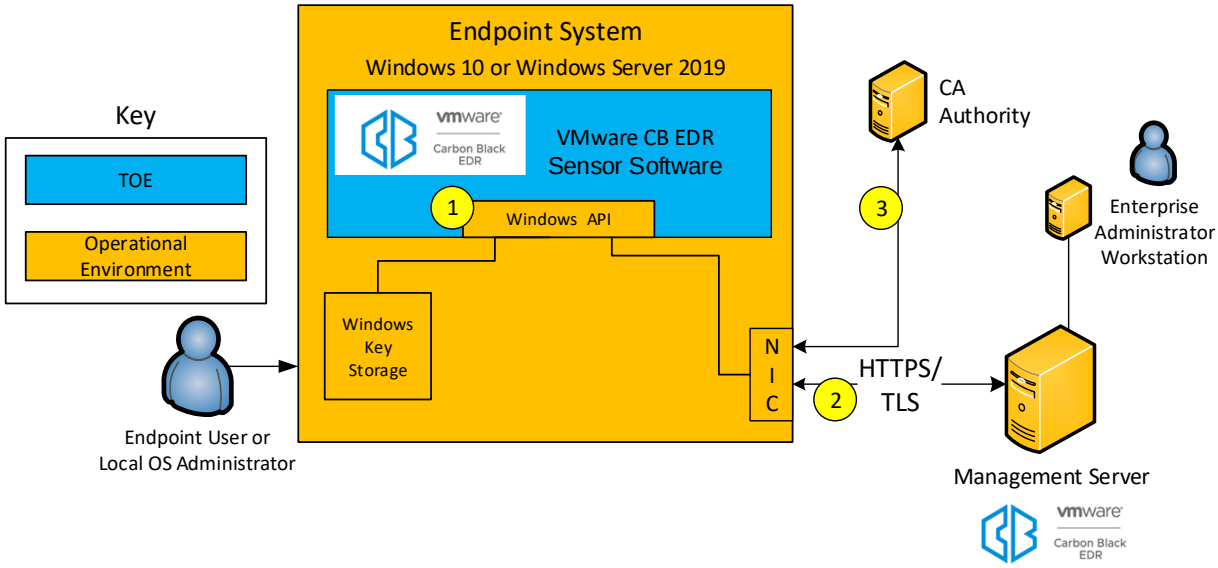
5 Evaluated Configuration of the TOE

This section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself, environmental components that support the security behavior of the TOE,

or non-interfering environmental components that were present during testing but are not associated with any security claims.

5.1 TOE Components

The TOE is the VMware Carbon Black EDR Windows Sensor 7.2 application, referred to as VMware CB EDR Windows Sensor or TOE. The VMware CB EDR Windows Sensor is an enterprise software application that gathers event data on the endpoints and reports it back to the VMware Carbon Black EDR Server (referred to as the management server from this point forward), which is part of the operational environment, for storage and indexing.



The following table describes the TOE components in the evaluated configuration:

Component	Definition
VMware CB EDR Windows Sensor (TOE)	An application that is installed on a Windows 10 platform, which collects event data from this host endpoint platform and invokes the OS to securely transmit this collected information back to the management server in the Operating Environment. The TOE maintains the configuration settings in the Windows registry and on the local file system. The TOE does not provide an interactive user interface for creating or storing data on the endpoint system.

Table 1: Evaluated Components of the TOE

5.2 Supporting Environmental Components

The following table lists components and applications in the operating environment that the TOE relies upon in order to function properly:

Component	Definition
Endpoint system with Microsoft Windows 10 (Windows)	The host platform along with the operating system installed that the TOE application is installed on.**

Management Server platform with the VMware CB EDR Server* software installed *evaluated independently	The management server is used in the evaluated configuration to deploy the TOE, collect the system data from these sensors, perform configuration updates, and deploy software updates. However, it is used to the extent that it can assist in the evaluation of the TOE software and no security claims for its functionality are made in this evaluation.
Administration Workstation	Any general-purpose computer that is used by an enterprise administrator to operate the Management Server remotely via a web browser.
Certificate Authority	The server deployed within the Operational Environment which confirms the validity and revocation status of certificates. This is only required for the TOE to validate TOE server certificate.

Table 2: Components in the Operational Environment

**NOTE: It is expected that the TOE is operating on a Common Criteria certified operating system and platform based on the Microsoft Windows 10 and Server 2019 version 1903 (May 2019 Update) evaluation. The TOE software that is installed on the Windows based OS, is identical (installation, executables, functionality, and features) no matter which variation of the Windows 10 (May 2019 Update) is used. For testing, the TOE was installed and fully tested on the Windows 10 Enterprise 2019 variant.

5.3 Resource Access Requirements

By installing the VMware CB EDR Windows Sensor and agreeing to the End User Licensing Agreement (EULA), the end user agrees to allow the TOE to access the following resources:

Hardware Resources Access

- Network Connectivity
  - The TOE invokes the OS to establish a trusted channel to the management server for polling cycles which includes:
    - sending collected host platform system information
    - receiving configuration updates and software updates

Sensitive Information Repositories Access

- The VMware CB EDR Windows Sensor collects system events and information from:
  - system log files
  - memory dumps

  Note: These files themselves are considered sensitive as they have the potential to contain user information such as password credentials that were erroneously typed into the username field.

5.4 Assumptions

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile:

- **Platform:** The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- **Proper administrator:** The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

- **Proper user:** The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.

6 Secure Installation and Configuration

Documentation for how to order and acquire the TOE is described under the Contact Us link on the VMware Carbon Black website www.carbonblack.com. Section 5.1 of this document lists the properties that are associated with the TOE. When downloading the TOE, this documentation should be checked as part of the acceptance procedures so that the correctness of the software application can be verified.

Physical installation and first-time setup of the TOE can be accomplished by following the steps outlined in [1] (see "Getting Started" and "Installing, Upgrading, and Uninstalling Sensors: Installing Sensors on Windows") by an administrator through the management server, or manually by a Local Administrator on the endpoint device (see Section 6.1). Once the application is installed on the endpoint, it boots automatically and operates immediately with no user action required.

The TOE does not have an interactive user interface and does not require user credentials (default or otherwise) to operate. The TOE operates as a Windows service. In the evaluated configuration, the only credentials used are the certificates used to support HTTPS/TLS mutual authentication communication between the TOE and the management server. These certificates are created on the management server and packaged with the installation package and installed on the host endpoint system, which is described in Section 6.1.

The TOE software is automatically installed with the appropriate file permissions to prevent unauthorized access to the binaries, configuration settings, and data.

6.1 Initial Out-Of-The-Box Setup

Before the VMware CB EDR Windows Sensor is installed on the endpoint device, there are a several pre-requisite configurations that need to be performed by the administrator on the management server and the local administrator to ensure the VMware CB EDR Windows Sensor is operating efficiently.

6.1.1 Pre-requisites on the Endpoint System:

1. Modify the C:\Windows\system32\drivers\etc\hosts file to include the management server so that it matches the certificate. For example: 10.0.0.9.
2. Import the management server's certificate chain onto the host platform.
    - All intermediate CA certificates need to be installed in the Local Computer "Intermediate Certification Authorities > Certificates" store.
    - And then the Root CA certificate needs to be installed in the Local Computer "Trusted Root Certification Authorities > Certificates" store.
3. Execute the following steps to import the certificate to the endpoint system certificate store:
    a. In the Windows search bar, type: mmc

b. Click on link to the “mmc” program. (Click “Yes” to the warning banner, if displayed.)

c. File → Add/Remove Snap-in

d. Select “Certificates,” then click “Add” in the middle of the window.

e. Select “Computer Account” and click “Next.”

f. Select “Local Computer” and click “Finish.”

g. Click “OK.”

h. Double click on “Certificates.”

NOTE: All intermediate CA certificates need to be installed in the Local Computer “Intermediate Certification Authorities > Certificates” store.

NOTE: The Root CA certificate needs to be installed in the Local Computer “Trusted Root Certification Authorities > Certificates” store.

i. Double click on “Intermediate Certification Authorities”

j. Select “Certificates”

k. Right click and select “All Tasks” with “import”. This will start the import wizard. Following the wizards prompts import the Intermediate CA certificates

l. Select the “Trusted Root Certification Authorities”

m. Select “Certificates”

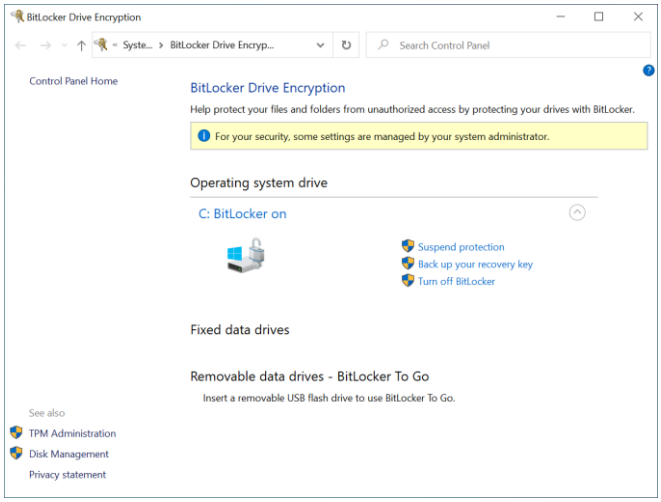
n. Right click and select “All Tasks” with “import”. This will start the import wizard. Following the wizards prompts import the Root CA certificate

4. Verify that BitLocker is turned on.

a. In the Windows search bar, type: bitlocker

b. Click on link to the “Manage BitLocker” program. (Click “Yes” to the warning banner, if displayed.)

c. A new window will open and display the BitLocker status. It should display as “on”:



d. If BitLocker is off, select the "Turn on BitLocker" link and follow the instructions.

5. Modify Windows Defender Exploit Settings

    a. In the Windows search bar, type: Windows Defender Settings

    b. Click on link to "Exploit Protection Settings." (Click "Yes" to the warning banner, if displayed.)

    c. Select "Program Settings."

    d. Click "Add Program to Customize."

    e. Select "Add by Program Name."

    f. Type: cb.exe

    g. Scroll down through the options and select:

        – Control flow guard (CFG)

        – Data Execution Prevention (DEP)

        – Export address filtering (EAF)

        – Import address filtering (IAF)

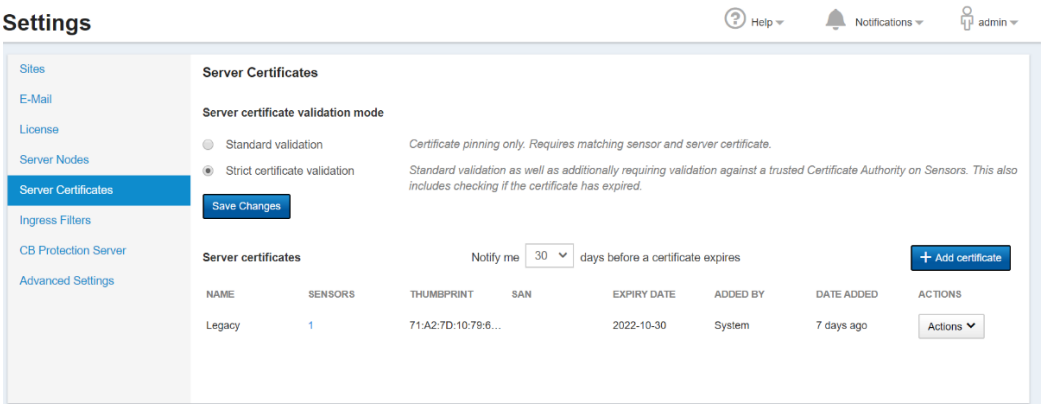
        – Randomize memory allocations (Bottom-up ASLR)

    h. Click "Apply."

6.1.2 Pre-requisite on the Management Server

1. Installation of management server (VMware CB EDR Server) is assumed complete (See reference [2]).

2. Full validation of the server certificate is required. As part of assigning the cbserver certificate, the 'Server certificate validation mode' must be set to 'Strict certificate validation'.



3. Verify that the URL for the management server is using HTTPS (i.e., https://cbserver.cctest.local:443) from a sensor platform.

4. Log into the management server console as an administrator of the management server.

6.1.2.1 Create/Edit Sensor Groups

An administrator on the management server can create Sensor Groups before or after installing sensors. When an administrator edits a Sensor Group, the settings are the same as creating the Sensor Group.

To create or edit a Sensor Group:

1. In the navigation bar of the management server console, click “Sensors.” The Sensors page appears.

2. In the Groups panel of the Sensors page, do one of the following:

   a. To create a new group, click “NEW” at the top of the Groups panel. The Create Group panel appears to the right of the Groups panel.

   b. To edit an existing group, do one of the following:

      - Select a group and at the top of the Sensors page click “Edit.”
      - Next to a group name, click the gear icon. The Edit Group panel appears.

   In the Create or Edit Group panel, sensor group settings are organized in sections that can expand or collapse as needed.

   NOTE: To quickly open or close all sections of sensor group settings at once, click “Display All Sections” or “Collapse All Sections” at the top right of the Create Group or Edit Group page.

3. Navigate the “Sensor Groups: Create or Edit a Sensor Group” section in [1] to complete settings in the following categories:

   - General – See “General Settings”
   - Sharing – See “Sharing Settings”
   - Advanced – See “Advanced Settings”
   - Permissions – See “Permissions Settings”

- Event Collection – See “Event Collection Settings”
- Isolation Exclusions – See “Isolation Exclusions”
- Upgrade Policy – See “Upgrade Policy Settings”

While viewing settings for one sensor group, the display settings can be switched for a different group by clicking the gear icon next to the other group. The Edit Group page refreshes to show settings for the newly selected group.

4. When all configurations of the sensor group settings are completed, do one of the following:
   a. Click “Create Group” to create a new group.
   b. Click “Save Group” to save the changes. Sensor Group changes take effect after the next time the sensors report to the management server.

   NOTE: If any errors are introduced in the management server URL (in the General section of the Edit Group page), communication will be lost with the deployed sensors.

6.1.3 Installing the VMware CB EDR Windows Sensor

There are two ways to install VMware CB EDR Windows Sensors:

- Windows .EXE – Installs a sensor onto a single host. This option is useful for bringing a new host online in your network.
- Windows MSI for GPO Installation – Deploys sensors to multiple hosts over the network using Microsoft's Group Policy Objects (GPO). This option is also appropriate for deploying sensors remotely with third-party software deployment applications using standard **msiexec** commands.

  For information about Windows MSI for GPO, see https://technet.microsoft.com/enus/library/hh147307(v=ws.10).aspx.

After the installation is complete, the VMware CB EDR Windows Sensor is installed and running.

NOTE: Only Local OS Administrators can install or uninstall VMware CB EDR Windows Sensors on Windows endpoint devices. There is no local configuration that a Local OS Administrator is required to accomplish. All configuration of the TOE is performed on the management server via the Enterprise Manager.

6.1.3.1 Obtaining Windows Standalone Installer

For the standalone installation of the VMware CB EDR Windows Sensor, do the following:

1. Using a web browser on the endpoint system, login to the management server by typing: https://<ip address or FQDN> into the address bar.
2. Login with administrator credential.
3. On the left-hand side, select the screen icon. Hovering over the icon will display “Sensors.”
4. Select the correct Sensor Group.
5. Click on “Download Sensor Installer.”

6. Select the appropriate installer: “Windows Standalone EXE – Latest Version” or “Windows MSI for GPO Installation – Latest Version”
7. The file will download to the endpoint system.

6.1.3.2 Executing Windows Standalone Installer

1. On the endpoint system, copy the downloaded `<install package name>.zip` to desired location.
2. Extract the contents of the `<install package name>.zip` file to a temporary folder. Do not skip this step.
3. If .EXE file: Double-click to run the file `CarbonBlackClientSetup.exe`, and then follow the installation prompts.
4. If MSI for GPO installation, follow the instructions in the `GPO_README.txt` file, which is included in the downloaded `<install package name>.zip` file.
5. After installation, verify that the application was installed correctly by performing the steps in section 6.1.4.

6.1.4 Verification of Installed Version

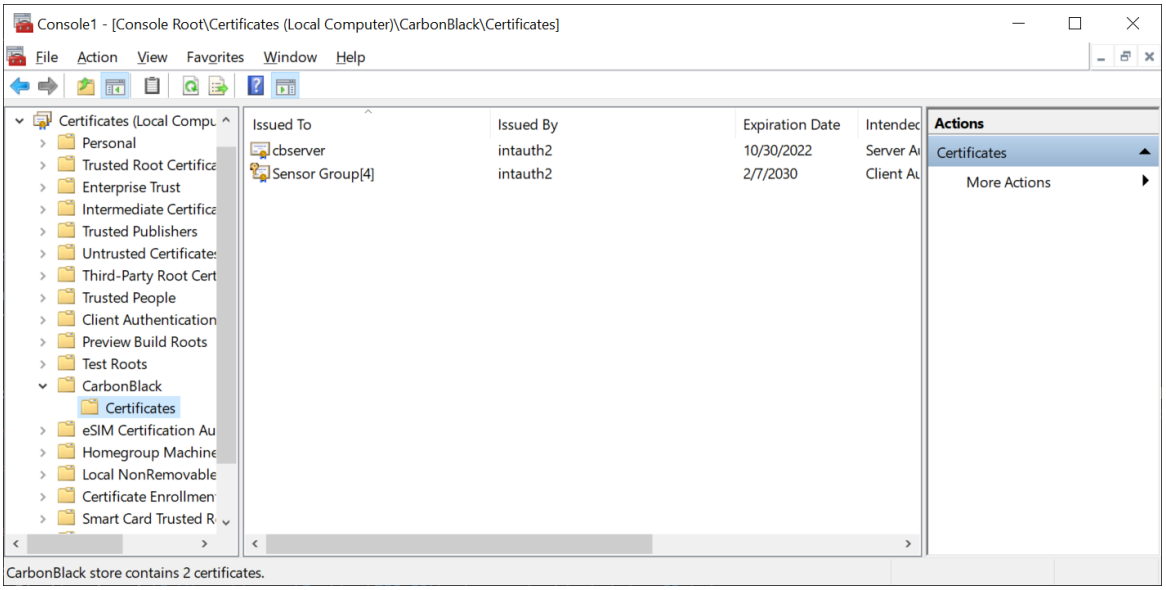
Windows application wizard:

1. In the Windows Search Bar type: add or remove
2. Click on link to the “Add or Remove Programs” program. (Click “Yes” to the warning banner, if displayed.)
3. Scroll down to the list of Apps and select “Carbon Black Sensor.”
4. The software version will be displayed under the icon in the form of major.minor.patch.build (i.e., 7.2.0.17354).

6.1.5 Verification of Sensor Group Certificate Installation

1. In the Windows search bar type: mmc
2. Click on link to the “mmc” program. (Click “Yes” to the warning banner, if displayed.)
3. File → Add/Remove Snap-in
4. Select “Certificates” then click “Add” in the middle of window.
5. Select “Computer Account” and click “Next.”
6. Select “Local Computer” and click “Finish.”
7. Click “OK.”
8. Double-click on “Certificates.”
9. Double-click on “CarbonBlack.”
10. Double-click on “Certificates.”

11. A certificate called “cbserver” should display.
12. A certificate called “Sensor Group[#]” should display.



6.2 Cryptographic Configuration

There is no TOE-required configuration for cryptography. The TOE does not perform any asymmetric key generation. Sensor Group certificates are installed as part of the installation and are not on the TOE’s host endpoint system. The Sensor Group certificates are generated on the management server.

The TOE invokes the underlying platform (Windows OS) to perform all cryptographic services including required to support the HTTPS/TLS trusted communications (client only), and sensitive data encryption storage. The OS calls on the DRBG services required.

NOTE: The TOE was installed on a certified Windows OS and platform based on the “*Microsoft Windows Common Criteria Evaluation Microsoft Windows 10 version 1903 (May 2019 Update) Microsoft Windows Server version 1903 (May 2019 Update) Security Target Version 0.04 July 19, 2019*” in order to have assurance of correct cryptographic implementation. Cryptographic Algorithm Verification Program (CAVP) certificate numbers are contained in the referenced Windows evaluation documentation.

NOTE: The use of other cryptographic engines and cryptographic settings were not evaluated nor tested during the Common Criteria evaluation of the TOE.

6.3 Secure VMware CB EDR Windows Sensor Communications

The TOE requires network access to communicate with the operational environment’s management server. During startup, the TOE invokes the platform to establish a persistent HTTPS/TLS connection to the management server for the purpose of periodically transmitting the collected information about the endpoint system and retrieve configuration updates. This periodic polling is approximately every 30 seconds. If the HTTPS/TLS connection is interrupted the TOE will automatically invoke the platform to re-establish the connection.

During a polling cycle, the VMware CB EDR Windows Sensor:

- collects configuration updates and data requests from the management server
- transmits endpoint host OS telemetry data (processes/threads being created, filesystem activity, registry activity, etc.), system logs, and/or memory dumps in response to the data request received from the management server.

NOTE: System logs and memory dumps can contain data that the operational environment could consider sensitive, credentials from failed login attempts, keys that are in memory that are written out to the system or process crashes. Therefore, system logs and memory dumps are considered sensitive data in the eyes of Common Criteria evaluations.

7 Secure Management of the TOE

The following sections provide information on managing TOE functionality that is relevant to the claimed Protection Profile. Note that this information is largely derived from [1] but summarized here to discuss only actions that are required as part of the 'evaluated configuration'. The Security Administrator is encouraged to reference this document in full in order to have in-depth awareness of the security functionality of the VMware CB EDR Windows Sensor, including functions that may be beyond the scope of this evaluation.

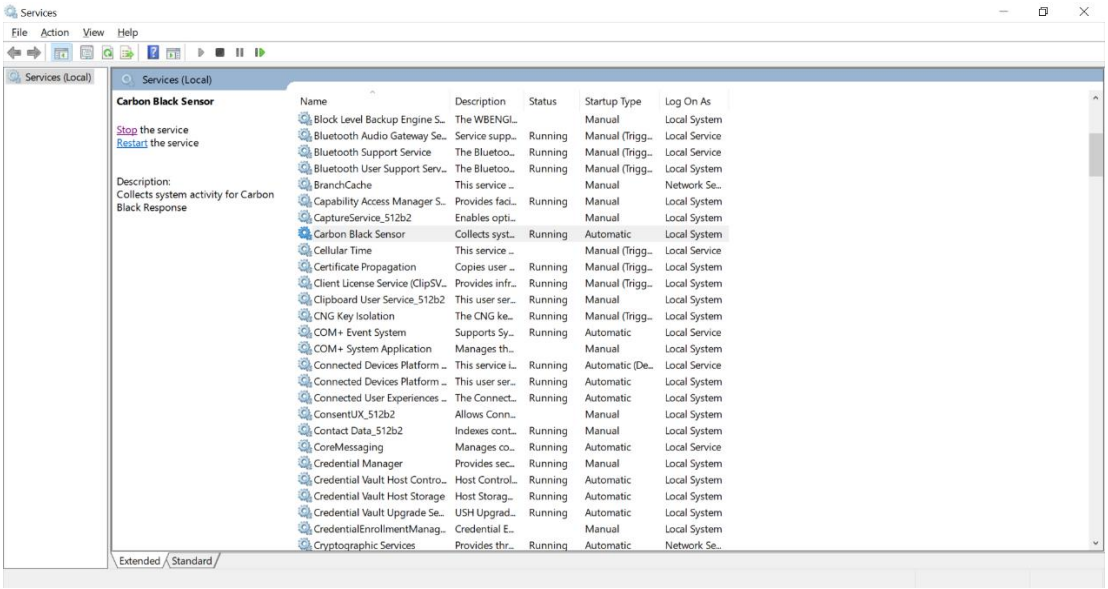
7.1 Administrator Functionality

Both the local administrator and endpoint user are considered the owner or user of the endpoint device for which the TOE is installed. A typical endpoint user does not have any management functionality. However, the local administrator (Windows OS administrator) can start and stop the "CarbonBlack" service (hard stopping all transmissions), verifying version, enable/disable system information from being transmitted, and uninstall the application.

7.1.1 Starting VMware CB EDR Window Sensor Service

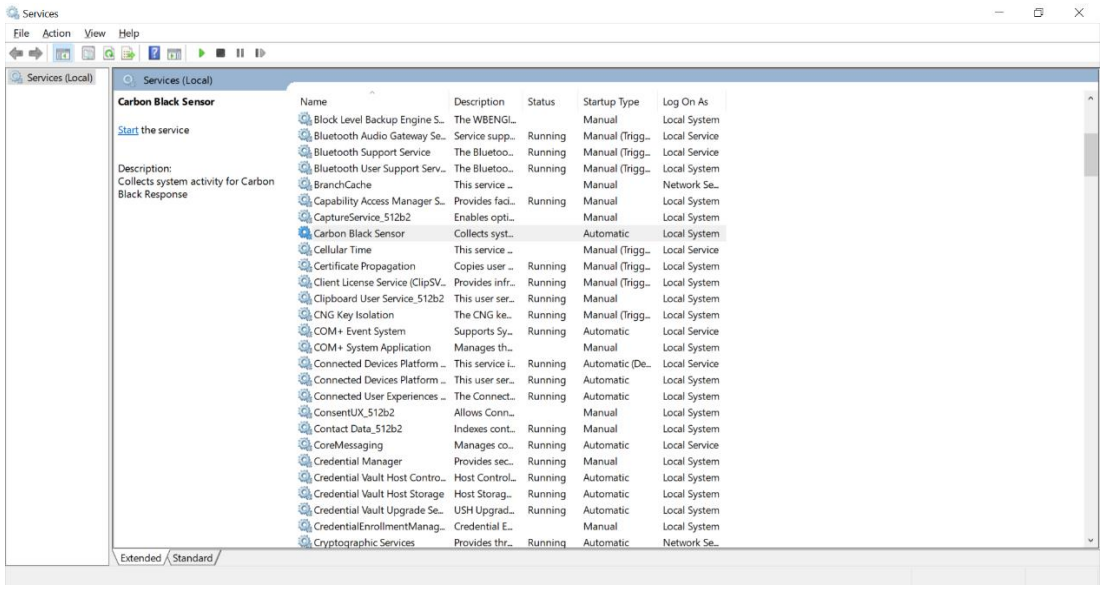
To turn on the VMware CB EDR Windows Sensor:

1. In the Windows search bar type: services
2. Click on link to the "Services" app.
3. Find "Carbon Black Sensor" in the list and select it.
4. In the right-hand column, click "Restart" to restart the service.



7.1.2 Stopping VMware CB EDR Window Sensor Service

1. In the Windows search bar type: services
2. Click on link to the “Services” app.
3. Find “Carbon Black Sensor” in the list and select it.
4. In the right-hand column, click “Stop” to stop the service.



7.1.3 Version Verification

There are several methods that an OS administrator can verify the version of the TOE.

Windows application wizard:

1. In the Windows Search Bar type: add or remove

2. Click on link to the “Add or Remove Programs” program. (Click “Yes” to the warning banner, if displayed.)
3. Scroll down to the list of Apps and select “VMware Carbon Black EDR Sensor.”
4. The software version will be displayed under the icon in the form of major.minor.patch.build (i.e., 7.2.0.17354).

Properties information on executables:

1. Right click on cb.exe and select ‘Properties’. The version will be displayed next to the Product version label.

Issuing cb.exe command:

1. Open a cmd window with administrative permissions.
2. Execute the following: c:\Windows\CarbonBlack\cb.exe -v

7.1.4 Uninstall VMware CB EDR Windows Sensor

To uninstall VMware CB EDR Windows Sensors, an administrator on the management server can follow [1] in “Installing, Upgrading, and Uninstalling Sensors: Uninstalling Sensors via the Console,” or the local administrator can manually uninstall them by using the following procedure:

Either:

- Launch the uninstall file in the `%windir%/CarbonBlack/` directory, or
- Navigate to **Control Panel > Add/Remove Programs** and use the Windows application uninstall feature.
    1. In the Windows search bar type: add or remove
    2. Click on link to the “Add or Remove Programs” program.
    3. Scroll down to the list of Apps and select “VMware Carbon Black Sensor.”
    4. Select “Uninstall.”
    5. The program should be removed from list.

Note: The uninstall will not remove the original folder that the installation was executed from. However, the uninstall removes all other remnants of the product that it installed by Carbon Black (registry keys, drivers, directory, binaries, and data files).

7.1.5 Enable/Disable System Information from Being Transmitted

There are two means in which host platform system information can be enabled/disabled. The first, which is a hard stop is starting and stopping the service as described in Sections 7.1.1 and 7.1.2 of this document. This hard stop will prevent transmission of data entirely. However, it does not change the event collection policy so upon restarting of TOE the same level of information is transmitted.

The second method is to change the collection policy at the management server. Once the changes have been completed at the management server, the TOE will receive this information during the next polling cycle. The TOE will automatically enforce the updated collection policy and only collect and transmit the

system event information based on the new collection policy. The change in collection policy effectively and gracefully enables/disables the transmission of system's hardware, software and configuration information. There is no Windows OS administrator intervention required.

7.2 Secure Updates

To maintain security throughout its lifecycle, the TOE provides a mechanism to apply software updates. In the evaluated configuration, updates were performed manually and automatically where the TOE obtained the update from the management server. High severity issues can result in a patch release as soon as remediation is available. Lower severity issues will be incorporated into the next monthly release. Security fixes will be released as new packages in the same manner as any feature updates. The TOE contains third-party components that VMware Carbon Black does not have control over the implementation of. Any implementation flaws are expected to be addressed within 90 days of reporting. Customers are notified of security-related fixes on the VMware Carbon Black customer portal.

The enterprise administrator has to obtain the update and import the file onto the management server manually by following the section entitled "Installing, Upgrading, and Uninstalling Sensors: Obtaining New Sensor Installation Packages" in [1]. Once the upgrade has been imported the enterprise administrator must assign the update to the sensor group via the Sensor→Edit functionality and assign the upgrade policy (automatic or manual).

If the TOE has been configured for automatic updates:

> During each periodic polling cycle the TOE application checks the management server's check-in response for the upgrade request object to see if there is a new update available. That object carries the information to upgrade including the sensor package (binary) to use.
>
> If the management server has set the upgrade request object, the TOE will download the specified sensor package (binary) and execute the update package. The update package invokes the OS APIs to validate the certificate chain (WinVerifyTrust) and install the update correctly.
>
> If the management server has not set the upgrade request object, then there is no further upgrade action accomplished by the TOE.

If the TOE has been configured for manual updates:

> The OS administrator must navigate to the management server and authenticate as an enterprise administrator and manually select the update package for downloading to the endpoint machine. The management server will only show allowed versions available for download. The list of available update packages contains the version number as part of the displayed filename. Once the update package has been downloaded, the OS administrator can execute the update package. The update package invokes the OS APIs to validate the certificate chain (WinVerifyTrust) and install the update correctly.

After the successful installation of the update package, the TOE will report that it is operating with updated version during the next polling cycle to the management server. The management server will then reset the upgrade request object to show that there is no update available

7.2.1 Upgrade Policy Options

The administrator on the management server can set an upgrade policy to perform sensor updates. The Upgrade Policy section of the Create or Edit Group panel on the Sensors page contains options to set the policy for upgrading installed sensors in the group, for the Windows platforms.

Upgrade policy options are as follows:

- No automatic updates – Manually decide when to upgrade sensors. VMware CB EDR Windows Sensor OS administrator action is required.
- Automatically install the latest version – Automatically upgrades the sensors to the latest version. No VMware CB EDR Windows Sensor OS administrator action is required.
- Automatically install a specific version – Install a specific version for all sensors in a group. This keeps all sensors at the selected version. Select a version number using the drop-down list. Selecting the upgrade policy of a specific version is useful when sensor versions must be tested or vetted. No VMware CB EDR Windows Sensor OS administrator action is required.

7.2.2 Perform a manual update

1. Using a web browser on the endpoint system, login to the management server by typing: https://<ip address or FQDN> into the address bar.
2. Login with administrator credential.
3. On the left-hand side, select the screen icon. Hovering over the icon will display “Sensors.”
4. Select the correct Sensor Group.
5. Click on “Download Sensor Installer.”
6. Select the appropriate installer: “Windows Standalone EXE – Latest Version” or “Windows MSI for GPO Installation – Latest Version”
7. Then follow the instructions in Section 6.1.3.2 Executing Windows Standalone Installer.
8. Verify which sensors have been upgraded by refreshing this same page. As the Sensors check-in through the polling intervals the upgrade will be reported if successful.

8 Operational Modes

The TOE does not have operational modes. When the TOE is first installed, it is considered to be in its evaluated operational mode provided the pre-requisites outlined in Section 6.1.1 of this document have been accomplished. If the pre-requisites where not performed in the initial set-up of the Sensor, the local administrator can still accomplish these steps after the Sensor installation. Once these steps have been completed, the TOE will be able to communicate with the management server and will be considered to be in its normal operational mode to perform the functions as described in the Security Target.

There is no separate error mode or other degraded mode of operation. If the VMware CB EDR Windows Sensor fails, the endpoint system will need to be rebooted. If the TOE has been corrupted or the

application has failed such that rebooting will not resolve the issue, an administrator will need to contact VMware Carbon Black support per the guidance in Section 10.

9 Additional Support

VMware Carbon Black provides technical support for its products, if needed, on their Support website https://www.carbonblack.com/support/. Customers can register for a User Exchange account to open a support case at by clicking on 'User Exchange' at the bottom of the Support website. Additionally, customers can open a ticket with a VMware Carbon Black representative by calling (877) 248-9098 (toll free) or (617) 393-7400 (choose option 2), or by emailing support@carbonblack.com.