FORTINET FORTISANDBOX AND CARBON BLACK CB PROTECTION INTEGRATION GUIDE
DEPLOYMENT GUIDE: FORTINET FORTISANDBOX AND CARBON BLACK CBPROTECT

FORTINET FORTISANDBOX AND CARBON BLACK CBPROTECT

Overview ......................................................... 3
Deployment Prerequisites ................................. 3
Architecture Overview ................................. 3

Deployment ..................................................... 4
Cb Protection Configuration ....................... 4
FortiSandbox Configuration ....................... 5

Client Configuration .................................. 6
Verifying configuration ................................. 6
FortiSandbox Adapter verification ................. 6
Cb Protection Connector verification .............. 7

Testing the Integration ................................. 7

Summary ....................................................... 9
OVERVIEW

This document is a guide on the Security Fabric Partner integration between Carbon Black Cb Protection, previously known as Bit9, and the FortiSandbox.

The integration allows customers who already have Cb Protection in their environment to tap into Fortinet’s Advanced Threat Prevention capabilities over the Security Fabric. Cb Protection takes on the role of arming the endpoints with application control, while the FortiSandbox analyzes for potentially unknown malware within files submitted to it by Cb Protection.

This guide will focus on the required components, the architectural overview and the configurations on the respective products. This guide also assumes an environment of Carbon Black Cb Protection v7.2.1+ and FortiSandbox v2.2+.

NOTE: This guide is pertinent to the integration between Carbon Black Cb Protection and FortiSandbox only. For integration details on Cb Response, please refer to the relevant guide available on FUSE.

ARCHITECTURE OVERVIEW

This is a simple example of what an enterprise network may look like with Carbon Black Cb Protection and FortiSandbox, where the Cb Protection and the FortiSandbox are located in the Datacenter and the Endpoints are located behind an Access Layer FortiGate ISFW, with the FortiGate NGFW at the core of the network.

![Diagram](image.png)

The communication between the Cb Protection server and the FortiSandbox occurs via the means of an adapter within the FortiSandbox.

DEPLOYMENT PREREQUISITES

1. FortiSandbox
2. Carbon Black Cb Protection server
3. Clients with Carbon Black Cb Protection agent
4. FortiGate NGFW
5. Optional:
   a. Windows AD Server
   b. ISFW

For licenses to Carbon Black Cb Protection, please contact Carbon Black’s respective sales team.
DEPLOYMENT

This guide assumes that the installations of the Carbon Black Protection server, the FortiSandbox, the FortiGate(s) and Windows AD server (optional) are complete. Fort deployment and installations instructions, please refer to the respective guides.

CB PROTECTION CONFIGURATION

The configuration on the Cb Protection side requires a special Administrator user to be created for the integration component that has an API toke associated with it.

1. Verify License.

Firstly, verify that your Cb Protection server has the appropriate licensing for the integration. The Cb Protection server must be licensed for “Connectors”.

   → Go to the Administrator tab -> System Configuration -> Licensing.

2. Create New User.

A new user needs to be created specifically to allow the communication for the integration to take place.

   → Go to the Administration tab -> Login Accounts -> click on “Add User”.

   → Set the “Group” to “Administrator” and enable the “Show API Token” option at the bottom of the page. Click on “Generate” and note the API Token generated – this will be used for the FortiSandbox configuration later in the process.

   → Click Save.
FORTISANDBOX CONFIGURATION

1. Go to Scan Input -> Adapter.
2. Add new Adapter
3. Insert details, along with the Name, IP address of the Cb Protection server, the API Token generated from Cb Protection server and the serial number of the Cb Protection server.
CLIENT CONFIGURATION

To install the Carbon Black Cb Protection agent on the clients, download the Install Package for the clients from the Cb Protection server page, typically located at https://carbon-black-server-hostname-or-ip/hostpkg. The downloaded client package contains all the relevant information required for the client to communicate with the Cb Protection server.

Please download and install the required Windows or Mac Client install packages on the endpoints, following the instructions as prompted.

VERIFYING CONFIGURATION

To verify that the configuration is correct and that the communication between the FortiSandbox and the Cb Protection server is active, you may verify the following way.

FORTISANDBOX ADAPTER VERIFICATION

Verify that the Cb Protection adapter on the FortiSandbox is up.

   — Go to Scan Unit -> Adapter.

   — Verify that the green arrow is displayed for the Cb Protection adapter that was added.
CB PROTECTION CONNECTOR VERIFICATION

Verify that the FortiSandBox Connector on the Cb Protection server is Enabled.

— Go to Administration -> System Configuration -> Connectors -> FortiSandbox.
— Ensure that the checkboxes next to the “Integration Enabled” and the “File Analysis Enabled” fields are checked.

![Image of System Configuration page]

TESTING THE INTEGRATION

To test your Integration and ensure that it is working as expected, please follow the steps outlined:

1. Download or copy a new file over to one of your endpoints with the Cb Protection agent on it.
2. Log in to the Carbon Black Protection server and go to the “Assets” tab and click on “Files”.
3. This should show you a list view of ‘New Unapproved Files’. The file you just copied to one of the clients should appear close to the top of the list. In this example, the file in question is `fsa_downloader_1dd6fa.exe`.

![Image of file list]

4. To test the integration, we will select this line of the file, and click on “Action” -> “Analyze with FortiSandbox”, per the screenshot below. This will force the file to be sent over to the FortiSandbox for Analysis.

NOTE: Depending on the configuration and policy, all new file submission from Carbon Black agents may automatically be sent to FortiSandbox for analysis as well.
5. Still within the Carbon Black Protect console, click on the details of the file to go to the Details view.

6. Towards the bottom, under the “External Analysis Results”, it should say that the file’s Analysis is pending by the FortiSandbox.

7. Log on to FortiSandbox and notice the Scanning Statistics Widget on the dashboard. You will see at least one in the “Adapter” section. In this case, we see one entry in the “Suspicious – High Risk” section. Click on the number will take us to all the list of all the files submitted by 3rd party Adapters, in this case, the Carbon Black Protect Server.
8. Now, you should see the same file submitted from the Carbon Black Protect server with its respecting rating from FortiSandBox analysis.

9. Moving back to the Carbon Black Protect server, open the details of the same file, and you should now see that the FortiSandbox section shows the corresponding rating from within the Carbon Black Protect server.

Please note that the rating with in the Carbon Black Protect server may not reflect the exact same rating as shown from within the FortiSandbox. For example, a file with the rating “Suspicious: High Risk” or “Suspicious: Low Risk” in the FortiSandbox console, may only show as “Suspicious” within the Carbon Black Protect server. This is due to Cb Protection’s categorization conventions.

**SUMMARY**

Access to FortiSandbox demo: [https://fortisandbox.fortidemo.com](https://fortisandbox.fortidemo.com)

How to get help

- FortiSandbox Administration Guide - [http://docs.fortinet.com/fortisandbox/admin-guides](http://docs.fortinet.com/fortisandbox/admin-guides)
- FUSE: [https://fuse.fortinet.com/p/fo/si/topic=471](https://fuse.fortinet.com/p/fo/si/topic=471)
- Carbon Black Cb Protection - [https://www.carbonblack.com/resources/resource-library/](https://www.carbonblack.com/resources/resource-library/)