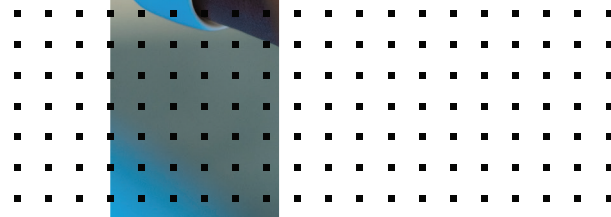
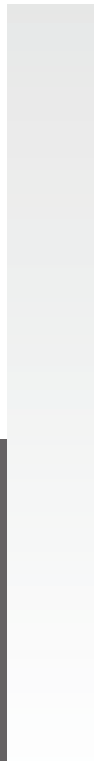
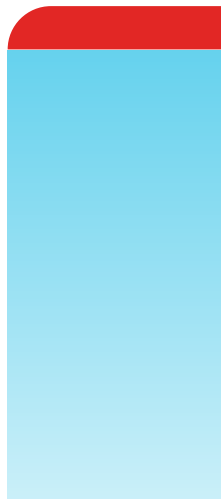


DEPLOYMENT GUIDE

# Fortinet FortiSandbox and Carbon Black CB Protection Integration Guide



# Fortinet FortiSandbox and Carbon Black CB Protection Integration Guide

- Overview ..... 3
  - Deployment Prerequisites ..... 3
  - Architecture Overview ..... 3
- Deployment ..... 4
- CB Protection Configuration ..... 4
- FortiSandbox Configuration ..... 5
- Client Configuration ..... 5
- Verifying Configuration ..... 5
  - FortiSandbox Adapter Verification ..... 5
  - CB Protection Connector Verification ..... 6
- Testing the Integration ..... 6
- 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+.

### Deployment Prerequisites

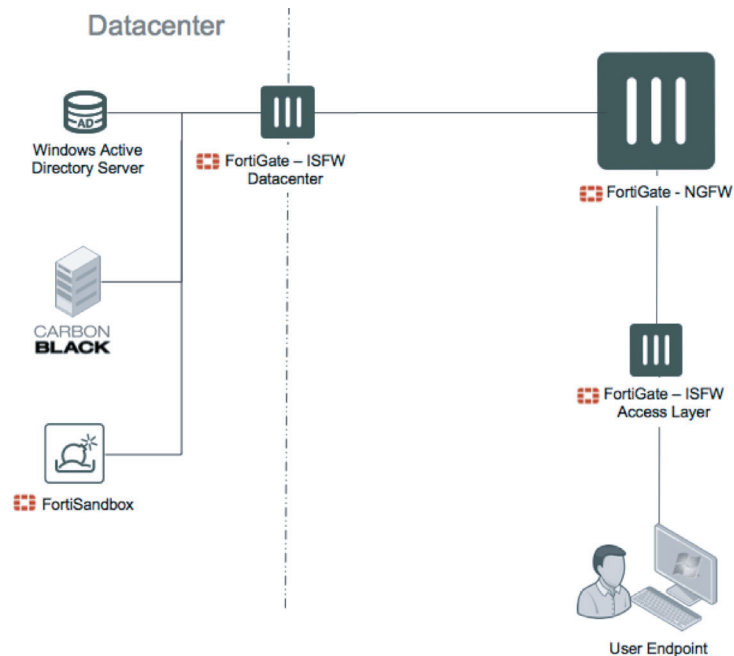
1. FortiSandbox
2. Carbon Black CB Protection server
3. Clients with Carbon Black CB Protection agent
4. FortiGate NGFW
5. Optional
  - Windows AD Server
  - ISFW

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

**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.



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

## 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. For deployment and installations instructions, please refer to the respective guides.

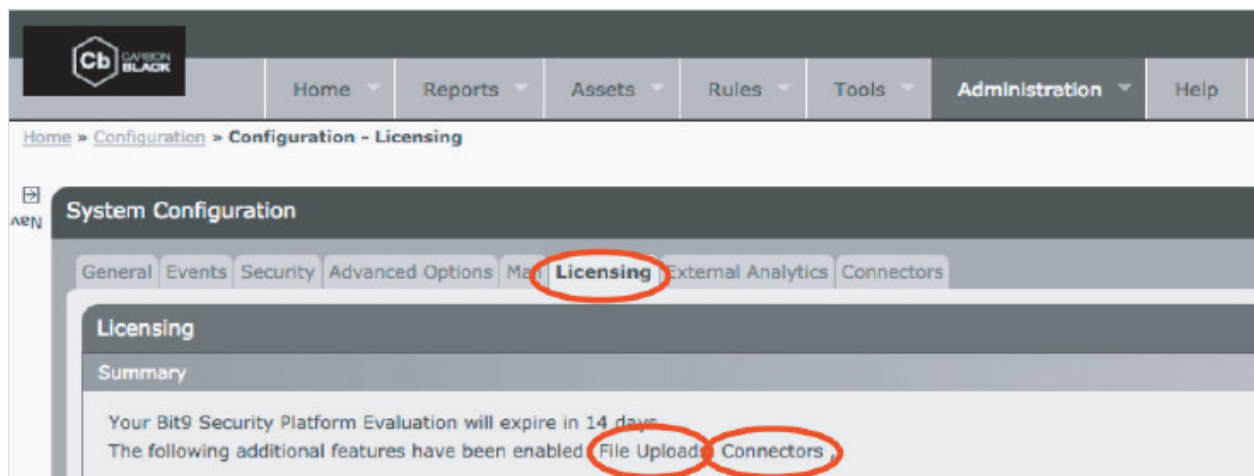
## CB Protection Configuration

The configuration on the CB Protection side requires a special Administrator user to be created for the integration component that has an API token 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.



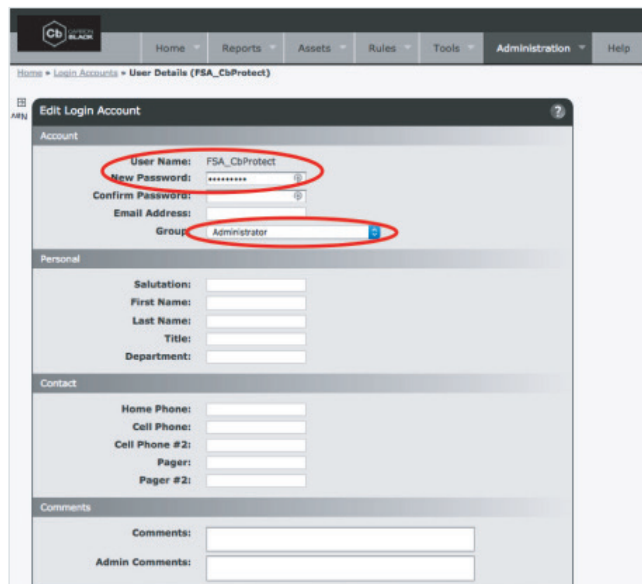
### 2. Create New User.

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.

The screenshot shows the FortiSandbox 3000D interface. On the left sidebar, the 'Scan Input' menu item is circled in red. At the bottom of the sidebar, the 'Adapter' menu item is also circled in red. The main content area is titled 'Edit Adapter' and contains the following configuration fields:

- Vendor Name: Bit9 + CARBON BLACK
- Adapter Name: CbProtect\_Server
- FQDN/IP: 101
- Token: 738AF
- Timeout (Seconds): 500
- Serial: 3202

At the bottom right of the configuration area, there are 'OK' and 'Cancel' buttons.

## 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.

The screenshot shows the Carbon Black web interface. The page title is 'Download Bit9 Agent Install Packages'. Below the title, there are instructions for installing the Bit9 Agent software. Below the instructions, there is a table titled 'Bit9 Installation Setup Files'.

Policy Name	Install Package		Date Created s	Date Modified
EntLabHW	Windows, Mac	Policy for EntLabHW clients	Sep 26 2016 02:44:33 PM	Mar 20 2017 10:30:50 PM
Low Enforcement Policy	Windows, Mac	Default-allow but can blacklist/ban malicious (e.g. from FortiSandbox analysis).	Jan 9 2017 11:50:51 AM	Mar 20 2017 10:30:50 PM
Medium Enforcement Policy	Windows, Mac	Default-deny untrusted files BUT end-user can self-allow or self-block an untrusted file.	Jan 9 2017 11:51:57 AM	Mar 20 2017 10:30:50 PM
High Enforcement Policy	Windows, Mac	Default-deny of untrusted files but user can submit approval request to administrator, and approvals/denials can be manual or automated e.g. from FortiSandbox analysis.	Jan 9 2017 11:53:45 AM	Mar 20 2017 10:30:50 PM

4 items Page 1/1

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.

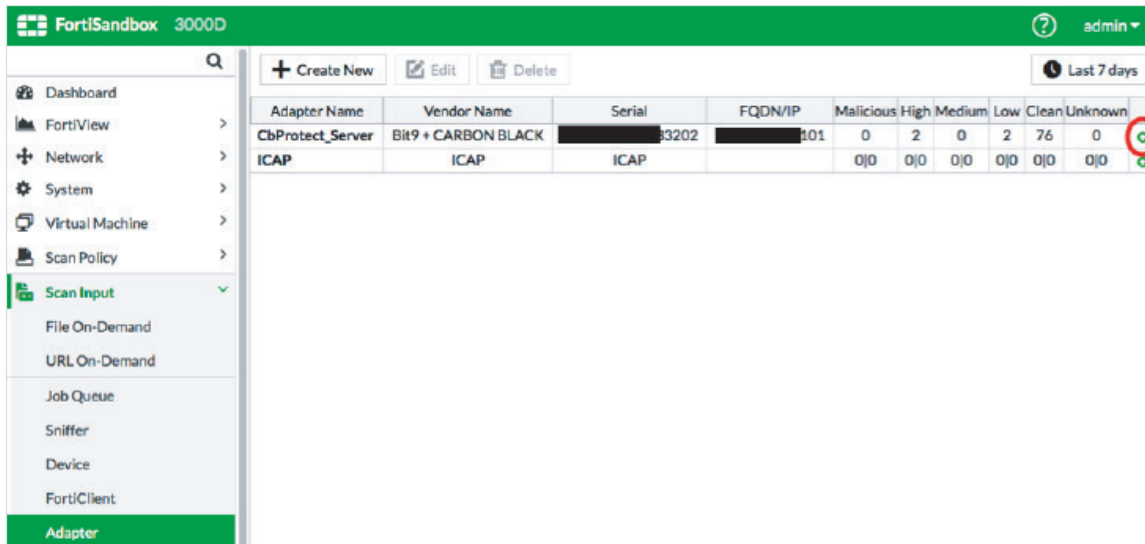


## FortiSandbox Adapter Verification

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.



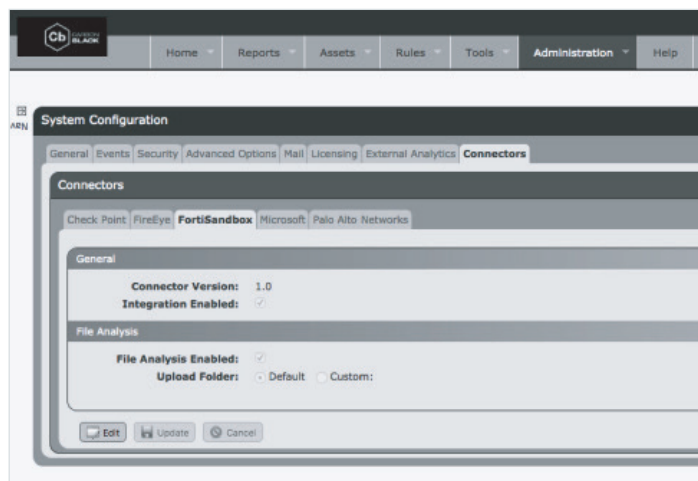
Adapter Name	Vendor Name	Serial	FQDN/IP	Malicious	High	Medium	Low	Clean	Unknown	
CbProtect_Server	Bit9 + CARBON BLACK	33202	:01	0	2	0	2	76	0	0
ICAP	ICAP	ICAP		0 0	0 0	0 0	0 0	0 0	0 0	0 0

## 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.

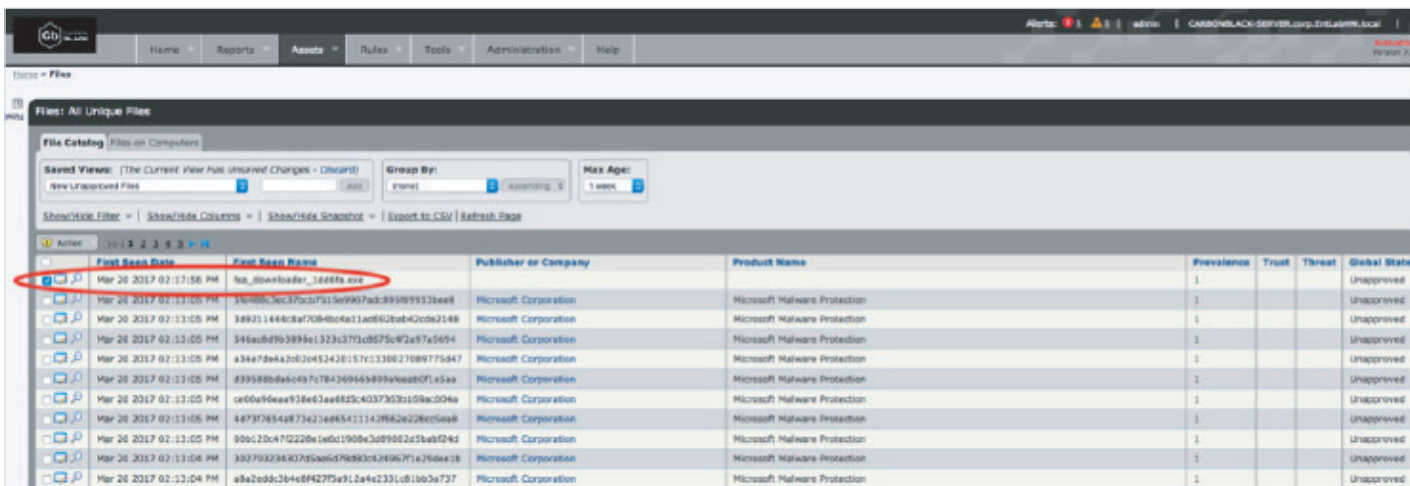


## Testing the Integration

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

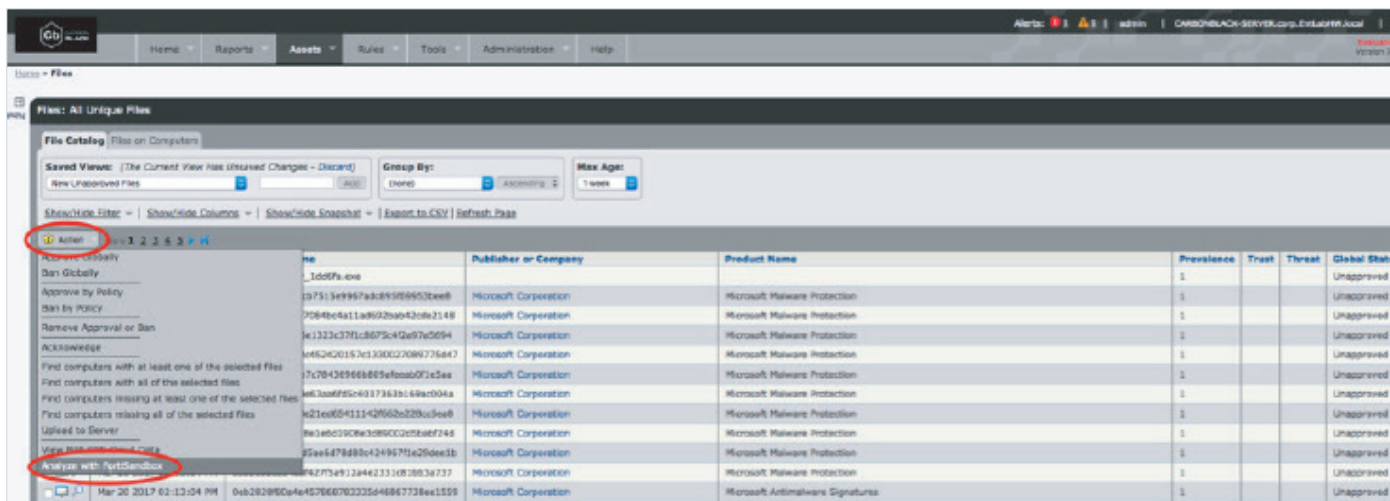
1. Download or copy a new file over to one of your endpoints with the CB Protection agent on it.
2. Log in to the Carbon Black Protection server and go to the “Assets” tab and click on “Files”.
3. This should show you a list view of ‘New Unapproved Files’. The file you just copied to one of the clients should appear close to the top of the list. In this example, the file in question is fsa\_downloader\_1dd6fa.exe.





- 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.

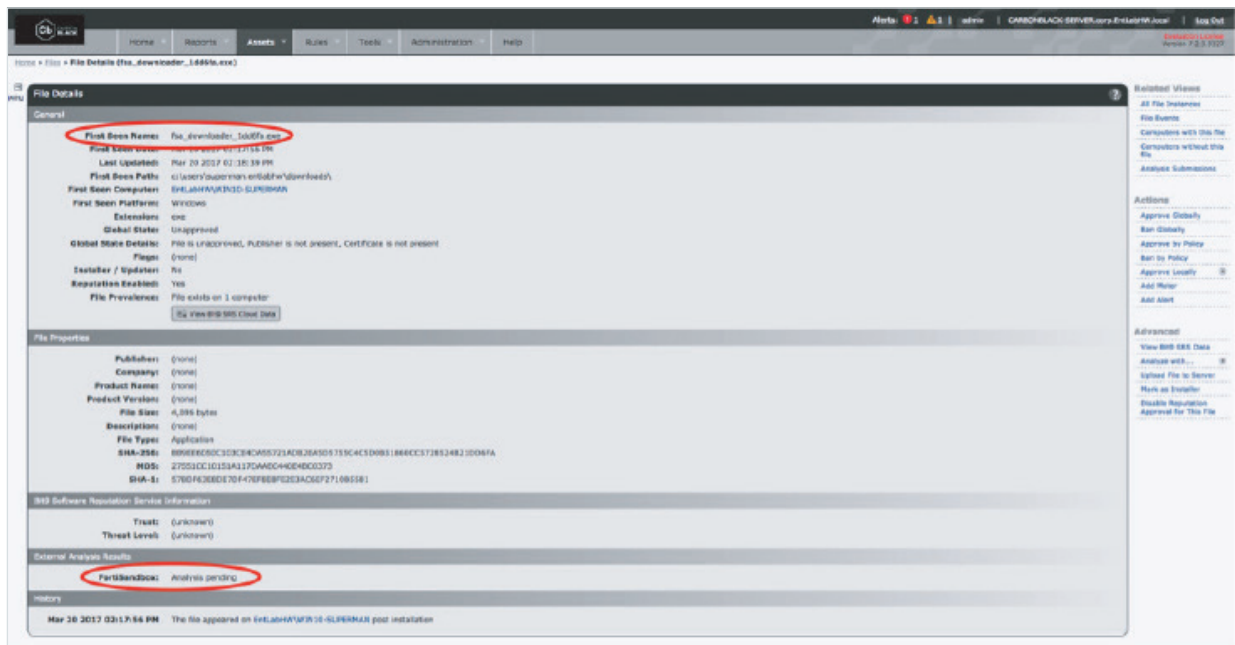
**NOTE: Depending on the configuration and policy, all new file submission from Carbon Black agents may automatically be sent to FortiSandbox for analysis as well.**



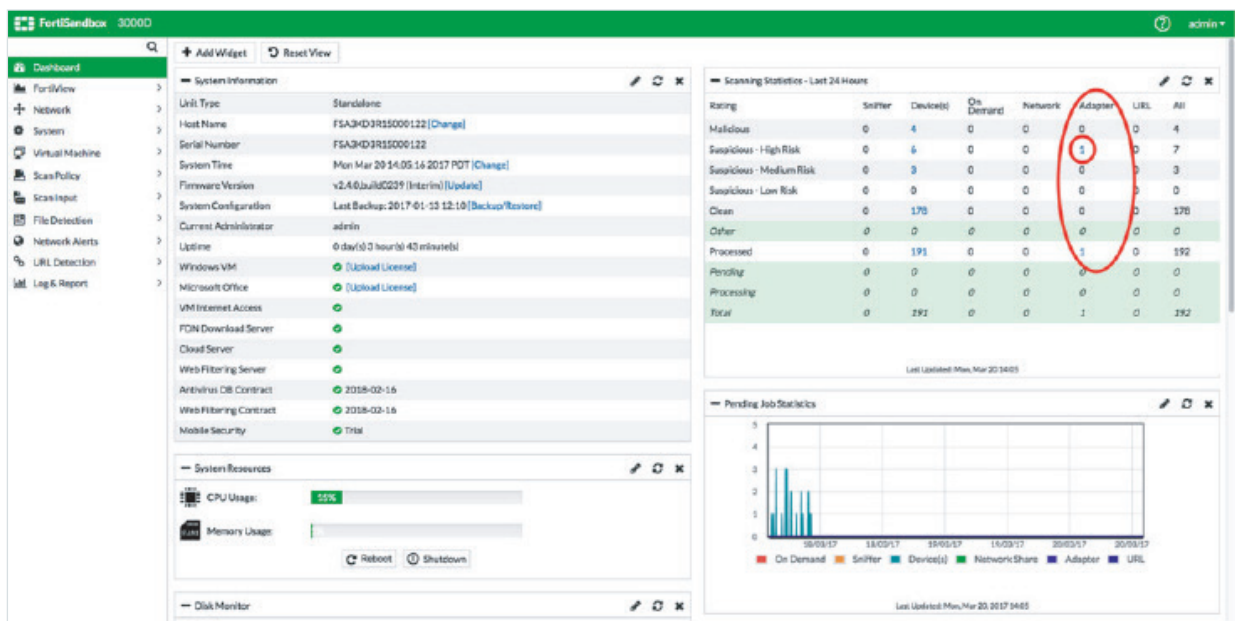
- Still within the Carbon Black Protect console, click on the details of the file to go to the Details view.







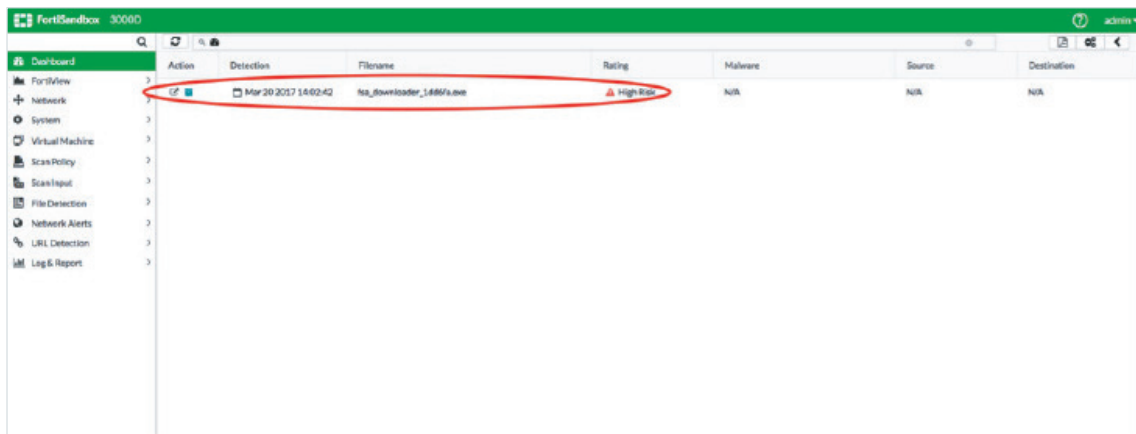
6. Towards the bottom, under the “External Analysis Results”, it should say that the file’s Analysis is pending by the FortiSandbox.
7. Log on to FortiSandbox and notice the Scanning Statistics Widget on the dashboard. You will see at least one in the “Adapter” section. In this case, we see one entry 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.

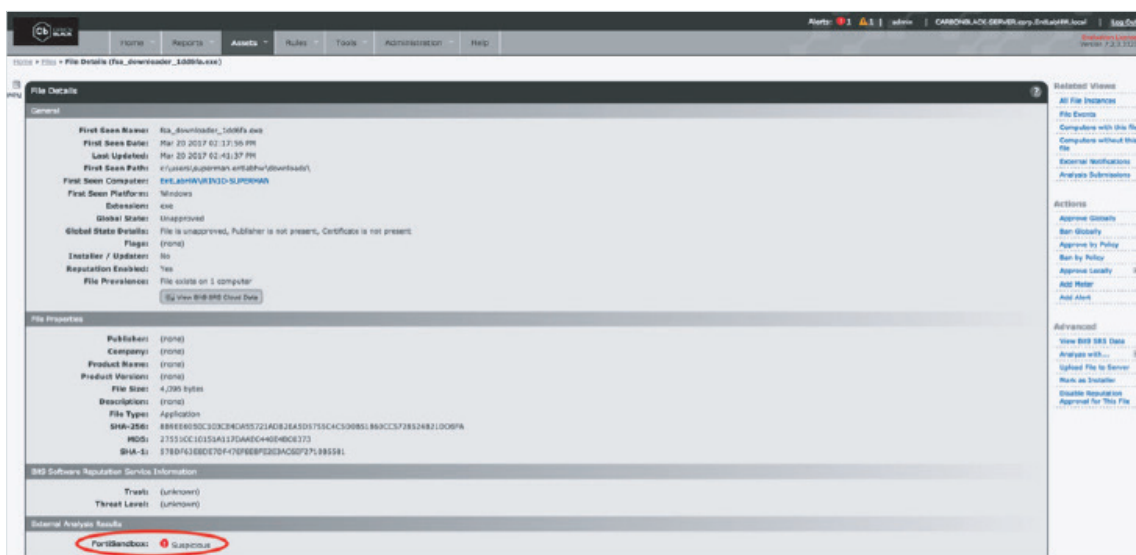






9. Moving back to the Carbon Black Protect server, open the details of the same file, and you should now see that the FortiSandbox section shows the corresponding rating from within the Carbon Black Protect server.

Please note that the rating with in the Carbon Black Protect server may not reflect the exact same rating as Destination 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>

How to get help:

- FortiSandbox Administration Guide - <http://docs.fortinet.com/fortisandbox/admin-guides>
- FUSE: <https://fuse.fortinet.com/p/fo/si/topic=471>
- Carbon Black CB Protection - <https://www.carbonblack.com/resources/resource-library/>



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.