구성: 클라우드 파일 평판 서비스 연동

개요

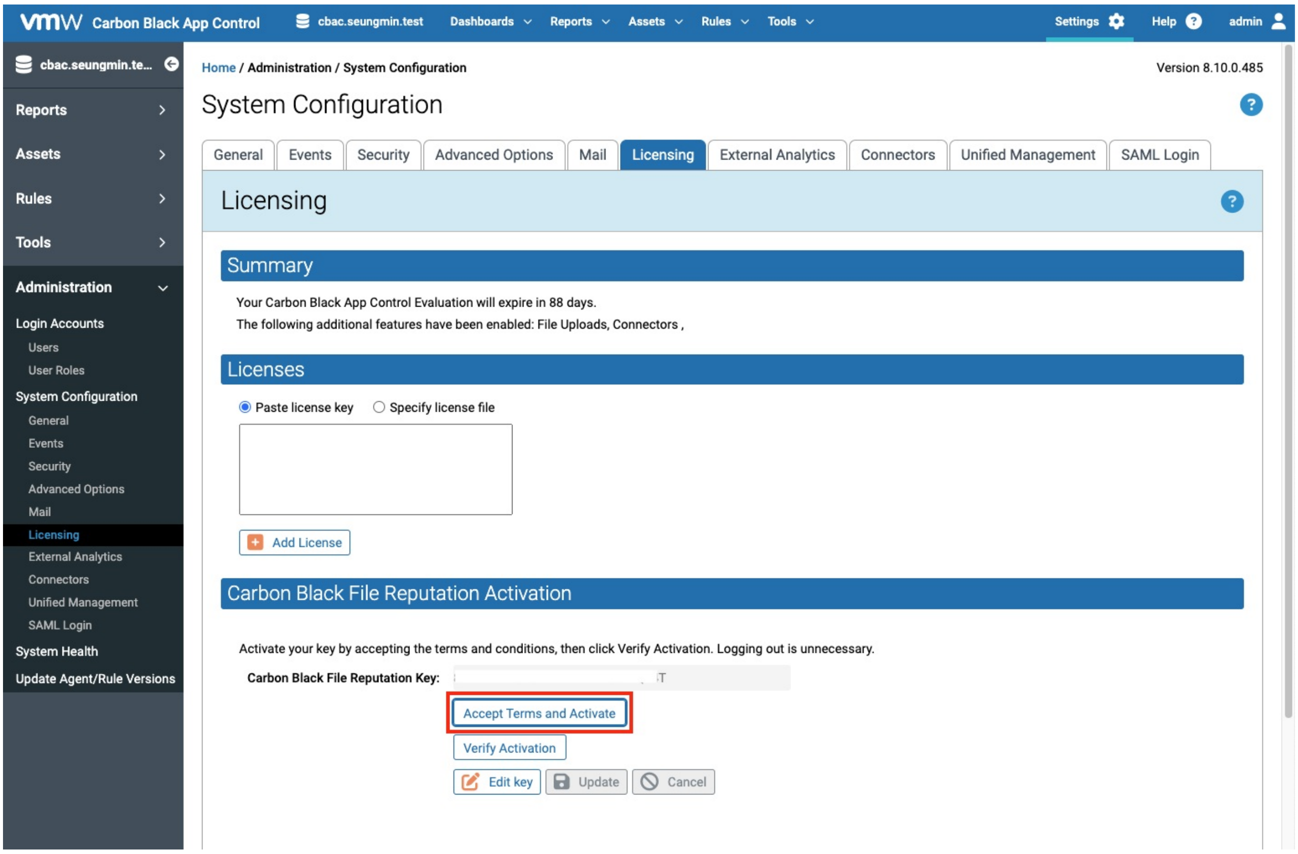
Carbon Black App Control 파일 평판 서비스와 연동하는 방법을 작성한 가이드 문서입니다.

진행 방법

1. Reputation Approval Rules 활성화

1.1 Reputation 활성화 (App Control 서버)

- [App Control 웹] 접속 > 오른쪽 상단의 [Settings] 'System Configuration' 클릭 > [Licensing] 탭 선택 > 'File Reputation Activation' 설정



System Configuration

Licensing

Summary

Your Carbon Black App Control Evaluation will expire in 88 days.
The following additional features have been enabled: File Uploads, Connectors ,

Licenses

● Paste license key ○ Specify license file

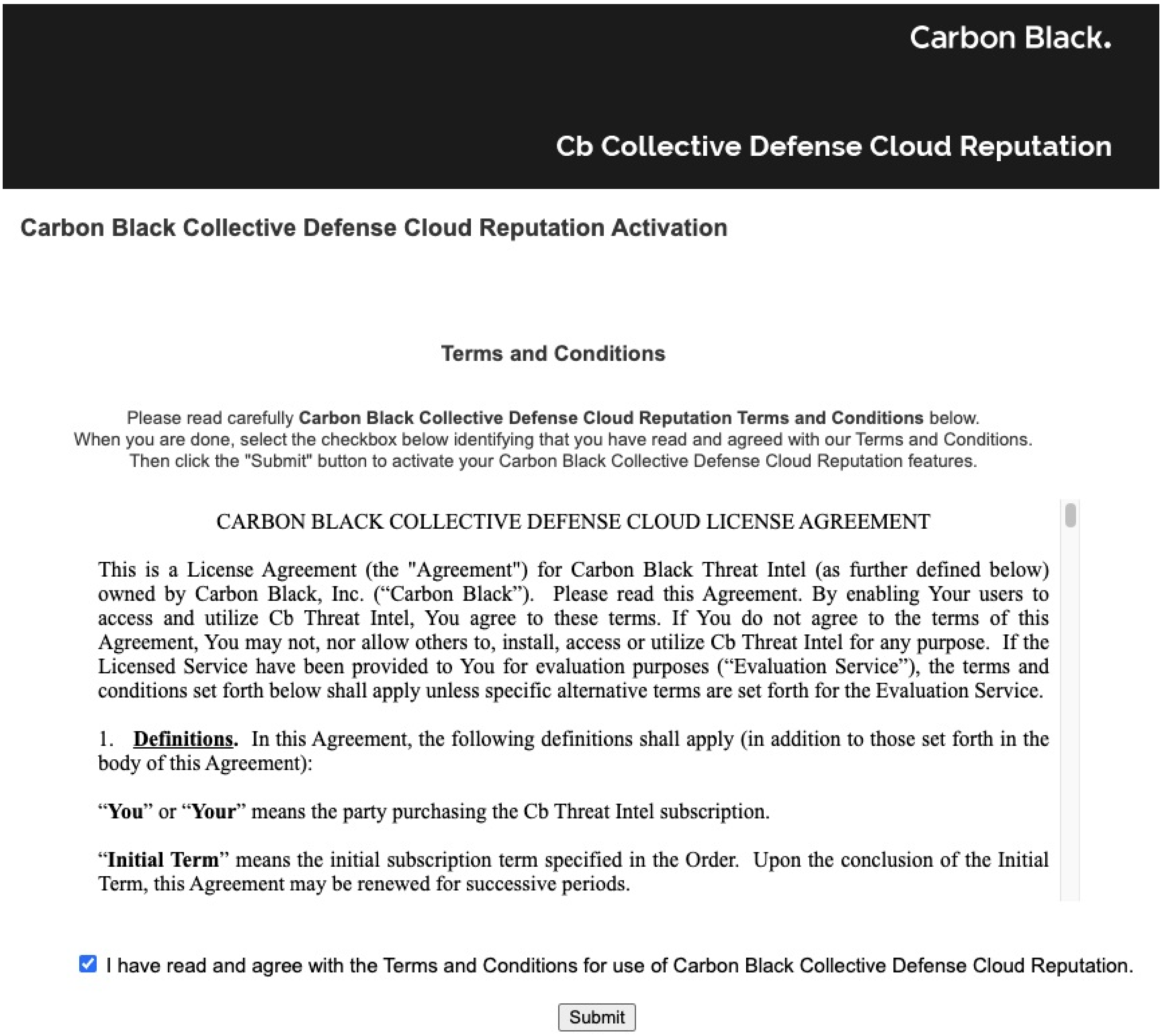
Carbon Black File Reputation Activation

Activate your key by accepting the terms and conditions, then click Verify Activation. Logging out is unnecessary.

Carbon Black File Reputation Key: [redacted]

- [Accept Terms and Activate] 버튼을 클릭하여 Carbon Black File Reputation 사이트 '약관 동의' 진행

-


Carbon Black.

Cb Collective Defense Cloud Reputation

Carbon Black Collective Defense Cloud Reputation Activation

Terms and Conditions

Please read carefully **Carbon Black Collective Defense Cloud Reputation Terms and Conditions** below.
When you are done, select the checkbox below identifying that you have read and agreed with our Terms and Conditions.
Then click the "Submit" button to activate your Carbon Black Collective Defense Cloud Reputation features.

CARBON BLACK COLLECTIVE DEFENSE CLOUD LICENSE AGREEMENT

This is a License Agreement (the "Agreement") for Carbon Black Threat Intel (as further defined below) owned by Carbon Black, Inc. ("Carbon Black"). Please read this Agreement. By enabling Your users to access and utilize Cb Threat Intel, You agree to these terms. If You do not agree to the terms of this Agreement, You may not, nor allow others to, install, access or utilize Cb Threat Intel for any purpose. If the Licensed Service have been provided to You for evaluation purposes ("Evaluation Service"), the terms and conditions set forth below shall apply unless specific alternative terms are set forth for the Evaluation Service.

1. **Definitions.** In this Agreement, the following definitions shall apply (in addition to those set forth in the body of this Agreement):

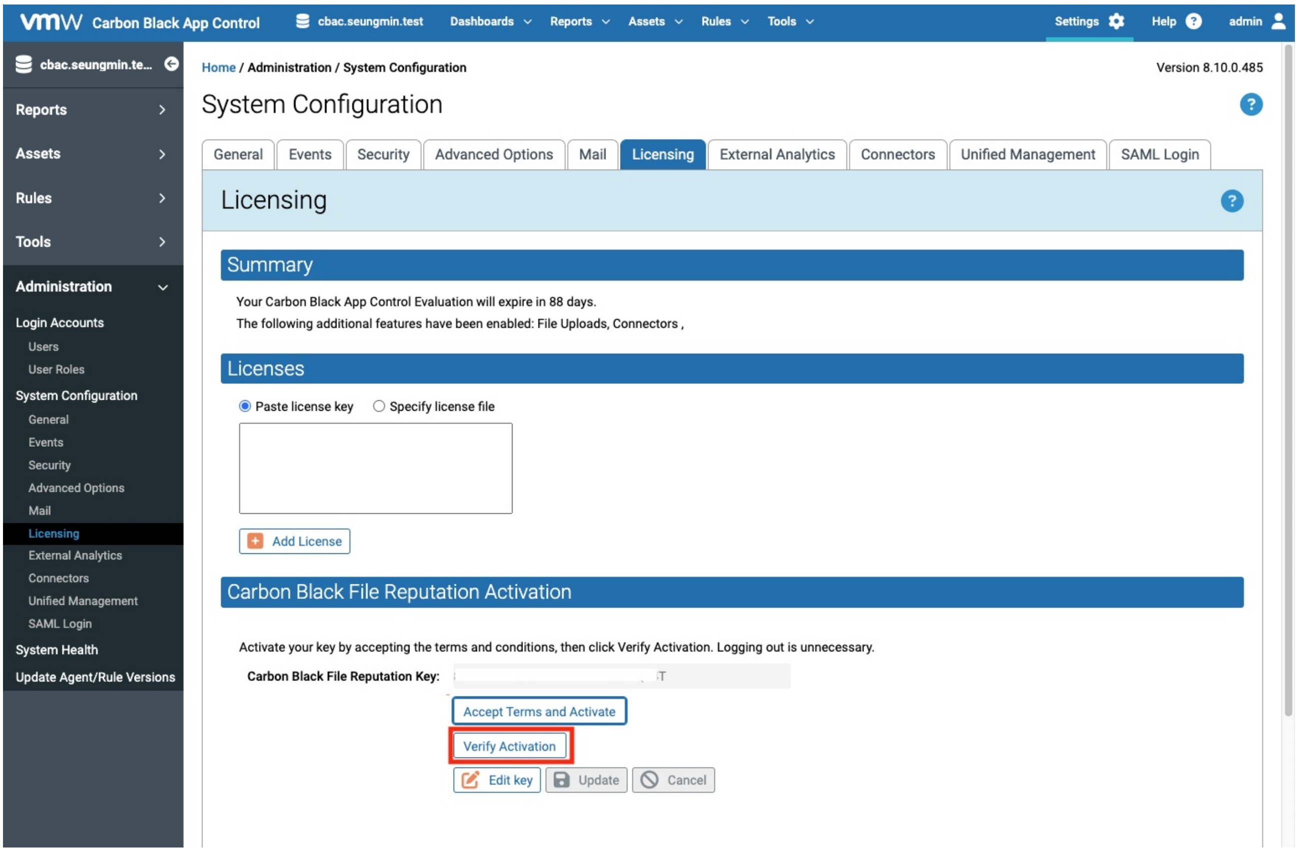
"**You**" or "**Your**" means the party purchasing the Cb Threat Intel subscription.

"**Initial Term**" means the initial subscription term specified in the Order. Upon the conclusion of the Initial Term, this Agreement may be renewed for successive periods.

☑ I have read and agree with the Terms and Conditions for use of Carbon Black Collective Defense Cloud Reputation.

- Carbon Black File Reputation 사이트로 이동되며, 이용 약관 확인 및 제출

https://services.bit9.com/services/signup.aspx?ak=989f0414ef1da7d704b6fa170189760f&sg=de1b18a8b6d6ccb9b4486001da912697&v=8.10.0.485 로 이동됨



Home / Administration / System Configuration

Version 8.10.0.485

System Configuration

Licensing

Summary

Your Carbon Black App Control Evaluation will expire in 88 days.

The following additional features have been enabled: File Uploads, Connectors ,

Licenses

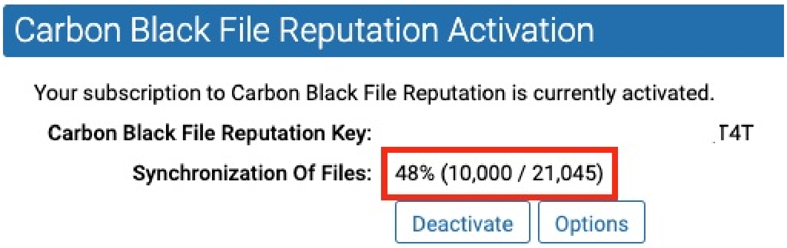
● Paste license key ○ Specify license file

Carbon Black File Reputation Activation

Activate your key by accepting the terms and conditions, then click Verify Activation. Logging out is unnecessary.

Carbon Black File Reputation Key: [redacted]T

- [Verify Activation] 버튼을 선택하여 Carbon Black File Reputation 사이트와의 연동 진행



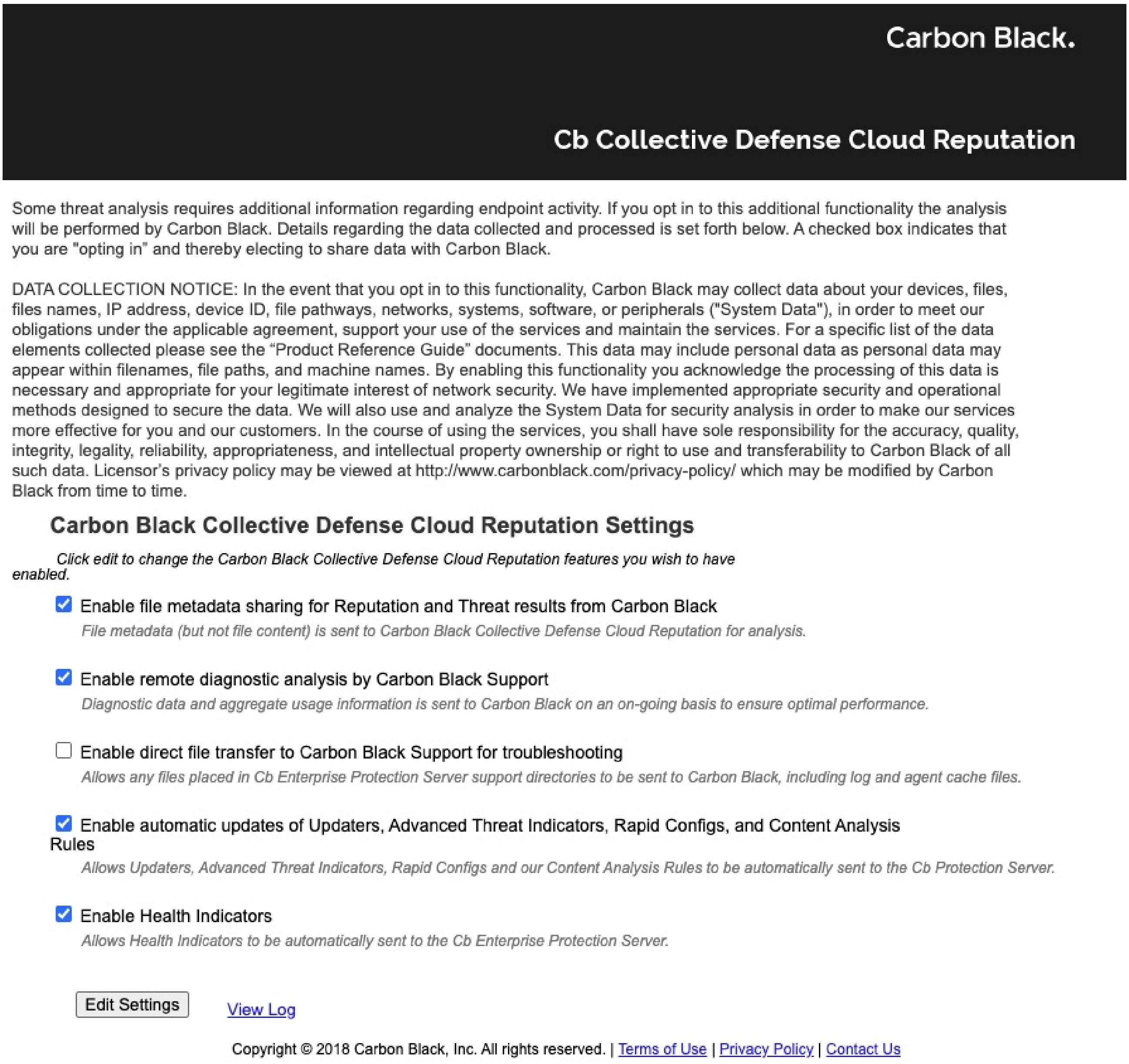
Carbon Black File Reputation Activation

Your subscription to Carbon Black File Reputation is currently activated.

Carbon Black File Reputation Key: [redacted]T4T

Synchronization Of Files: 48% (10,000 / 21,045)

- Carbon Black File Reputation 데이터 다운로드 현황 확인



Carbon Black.

Cb Collective Defense Cloud Reputation

Some threat analysis requires additional information regarding endpoint activity. If you opt in to this additional functionality the analysis will be performed by Carbon Black. Details regarding the data collected and processed is set forth below. A checked box indicates that you are "opting in" and thereby electing to share data with Carbon Black.

DATA COLLECTION NOTICE: In the event that you opt in to this functionality, Carbon Black may collect data about your devices, files, files names, IP address, device ID, file pathways, networks, systems, software, or peripherals ("System Data"), in order to meet our obligations under the applicable agreement, support your use of the services and maintain the services. For a specific list of the data elements collected please see the "Product Reference Guide" documents. This data may include personal data as personal data may appear within filenames, file paths, and machine names. By enabling this functionality you acknowledge the processing of this data is necessary and appropriate for your legitimate interest of network security. We have implemented appropriate security and operational methods designed to secure the data. We will also use and analyze the System Data for security analysis in order to make our services more effective for you and our customers. In the course of using the services, you shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use and transferability to Carbon Black of all such data. Licensor's privacy policy may be viewed at http://www.carbonblack.com/privacy-policy/ which may be modified by Carbon Black from time to time.

Carbon Black Collective Defense Cloud Reputation Settings

Click edit to change the Carbon Black Collective Defense Cloud Reputation features you wish to have enabled.

☑ Enable file metadata sharing for Reputation and Threat results from Carbon Black
File metadata (but not file content) is sent to Carbon Black Collective Defense Cloud Reputation for analysis.

☑ Enable remote diagnostic analysis by Carbon Black Support
Diagnostic data and aggregate usage information is sent to Carbon Black on an on-going basis to ensure optimal performance.

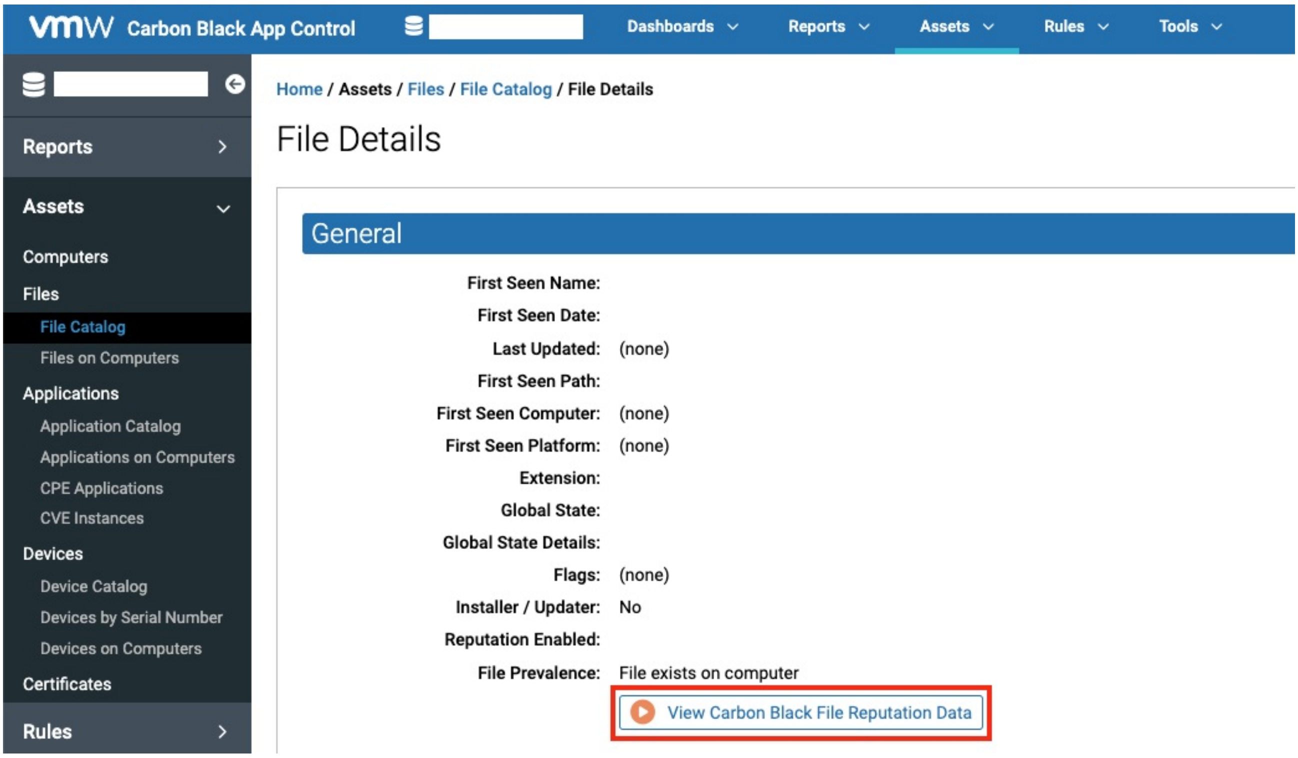
□ Enable direct file transfer to Carbon Black Support for troubleshooting
Allows any files placed in Cb Enterprise Protection Server support directories to be sent to Carbon Black, including log and agent cache files.

☑ Enable automatic updates of Updaters, Advanced Threat Indicators, Rapid Configs, and Content Analysis Rules
Allows Updaters, Advanced Threat Indicators, Rapid Configs and our Content Analysis Rules to be automatically sent to the Cb Protection Server.

☑ Enable Health Indicators
Allows Health Indicators to be automatically sent to the Cb Enterprise Protection Server.

Copyright © 2018 Carbon Black, Inc. All rights reserved. | Terms of Use | Privacy Policy | Contact Us

- [Options] 버튼 선택 시, Carbon Black File Reputation 사이트로 이동되며, 옵션 설정 가능

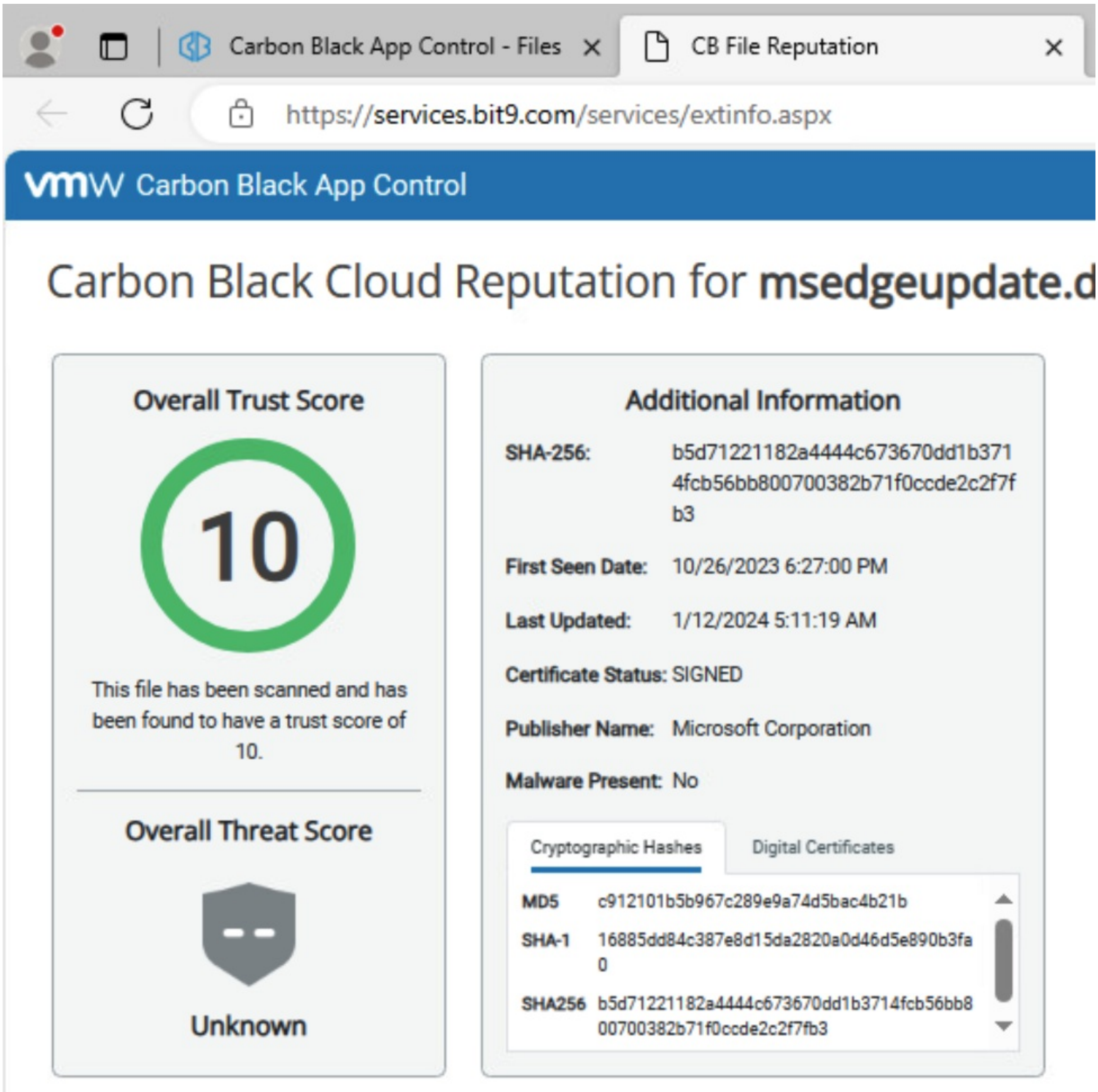


File Details

General

First Seen Name:
First Seen Date:
Last Updated: (none)
First Seen Path:
First Seen Computer: (none)
First Seen Platform: (none)
Extension:
Global State:
Global State Details:
Flags: (none)
Installer / Updater: No
Reputation Enabled:
File Prevalence: File exists on computer

- [View Carbon Black File Reputation Data] 를 선택하여 파일에 대한 평판 확인



Carbon Black App Control - Files
CB File Reputation
https://services.bit9.com/services/extinfo.aspx
vmw Carbon Black App Control

Carbon Black Cloud Reputation for **msedgeupdate.d**

Overall Trust Score

10

This file has been scanned and has been found to have a trust score of 10.

Overall Threat Score

Unknown

Additional Information

SHA-256:	b5d71221182a4444c673670dd1b3714fcb56bb800700382b71f0ccde2c2f7fb3
First Seen Date:	10/26/2023 6:27:00 PM
Last Updated:	1/12/2024 5:11:19 AM
Certificate Status:	SIGNED
Publisher Name:	Microsoft Corporation
Malware Present:	No

MD5	c912101b5b967c289e9a74d5bac4b21b
SHA-1	16885dd84c387e8d15da2820a0d46d5e890b3fa0
SHA256	b5d71221182a4444c673670dd1b3714fcb56bb800700382b71f0ccde2c2f7fb3

- 'service.bit9.com' 도메인으로 리다이렉트 후 파일 평판 확인 가능

⏲버전 #4
★생성 15 1월 2024 14:54:30
✎수정 18 4월 2025 17:06:16