

# 구성: Cloud 및 EDR 간 연동

## 개요

App Control 제품과 EDR 및 Cloud 간의 연동 구성 방법입니다.

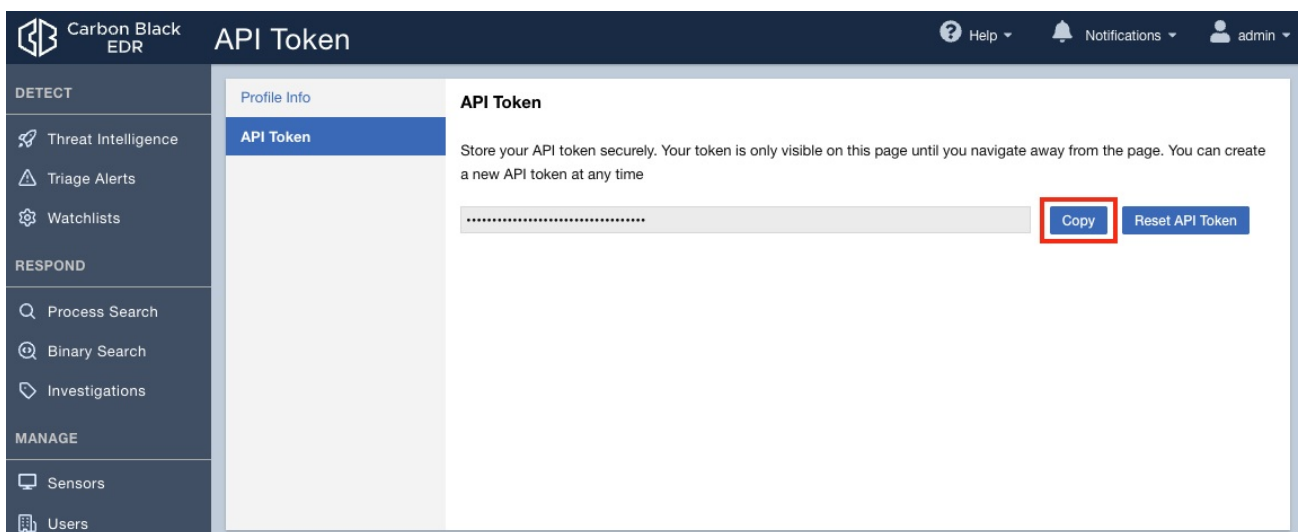
## 진행 방법

### 1. App Control - EDR 간 연동

참고 문서 : <https://community.carbonblack.com/t5/Knowledge-Base/EDR-How-to-Integrate-with-App-Control/ta-p/82936>

#### 1.1 EDR API Token 복사 (EDR 서버)

- [EDR 웹 콘솔] 접속 > 오른쪽 상단의 [사용자 이름] My Profile 클릭 > [API Token] 탭 > API Token [Copy] 버튼 선택하여 API 토큰 값 복사



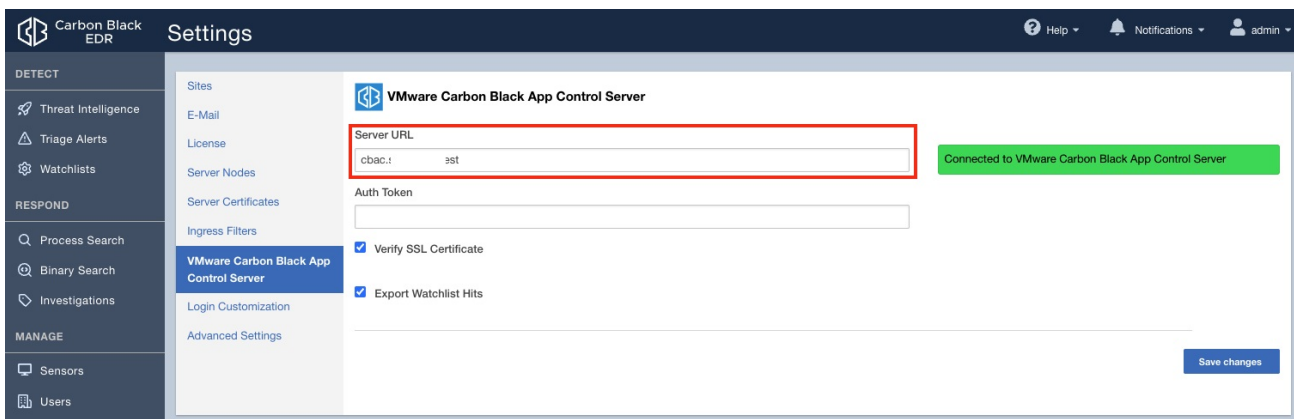
#### 1.2 EDR 서버 연동 (App Control 서버)

- [App Control 웹 콘솔] 접속 > 오른쪽 상단의 [Settings] 'System Configuration' 클릭 > [Licensing] 탭 선택 > 'Carbon Black EDR' 설정

- EDR 서버로부터 Watchlist Event 발생 이력에 대해 수신 받을 수 있음
  - URL : EDR 서버의 도메인 정보 입력 (ex : https://FQDN or IP)
  - **SSL Certificate : SSL 인증서 사용 여부 선택**
  - API Token : EDR 서버에서 복사한 API 토큰 입력
  - Receive Watchlist Events : EDR 서버로부터 Watchlist Event 수신 여부 선택
    - 체크 선택 시 : Watchlist 데이터 수신 및 센서 status 및 디바이스 정보 확인 가능
    - 체크 해제 시 : Watchlist 데이터 미수신 및 센서 status 및 디바이스 정보 확인 가능
  - **Force Strong SSL : SSL 강제 적용 여부 선택 (?)**

### 1.3 App Control 연동 여부 확인 (EDR 서버)

- [EDR 웹 콘솔] 접속 > 오른쪽 상단의 [사용자 이름] 의 Settings 클릭 > [VMware Carbon Black App Control Server] 탭 선택



- 정상 연동이 이루어진 경우, 'Connected to VMware Carbon Black App Control Server' 메시지가 확인되며, 또한 'Server URL' 정보에 App Control 서버 URL 이 자동으로 기입됨

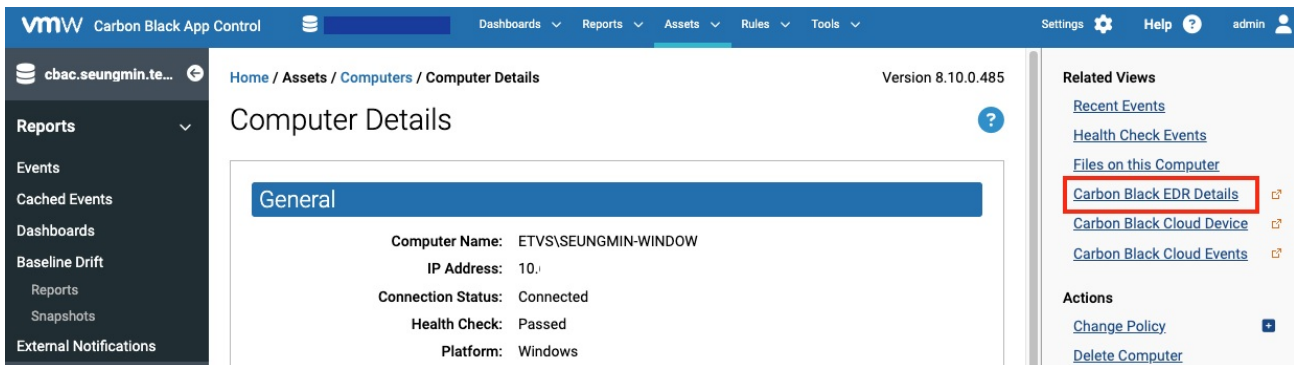
## 1.4 EDR 연동 정보 확인 (App Control)

- [App Control 웹 콘솔] 접속 > [Reports] 의 [Event] 메뉴 선택

Timestamp	Severity	Description	Source	Process Name
Jan 10 2024 01:30:38 PM	Notice	Carbon Black EDR process Watchlist 'seungmin-test' hit for process 'chrome.exe' [A9DD2...4D2E8] on computer 'ETVS\SEUNGMIN-WINDOW'.	ETVS\SEUNGMIN-WINDOW	chrome.exe
Jan 10 2024 01:30:38 PM	Notice	Carbon Black EDR process Watchlist 'seungmin-test' hit for process 'chrome.exe' [A9DD2...4D2E8] on computer 'ETVS\SEUNGMIN-WINDOW'.	ETVS\SEUNGMIN-WINDOW	chrome.exe
Jan 10 2024 01:30:38 PM	Notice	Carbon Black EDR process Watchlist 'seungmin-test' hit for process 'chrome.exe' [A9DD2...4D2E8] on computer 'ETVS\SEUNGMIN-WINDOW'.	ETVS\SEUNGMIN-WINDOW	chrome.exe
Jan 10 2024 01:30:38 PM	Notice	Carbon Black EDR process Watchlist 'seungmin-test' hit for process 'chrome.exe' [A9DD2...4D2E8] on computer 'ETVS\SEUNGMIN-WINDOW'.	ETVS\SEUNGMIN-WINDOW	chrome.exe

- Watchlist 에서 생성된 정보를 수신하여 App Control 콘솔에서 확인 가능
- Event 프로세스에 대한 세부 정보 확인 가능
- EDR 에이전트에 대한 상태 정보 확인 가능
- [EDR 버튼]을 선택하면 EDR 웹 콘솔로 이동하여, EDR 웹 콘솔 통한 디테일 정보 확인 가능

- [App Control 웹 콘솔] 접속 > [Assets] 의 [Devices on Computers] 메뉴 선택



- [EDR 버튼]을 선택하면 EDR 웹 콘솔로 이동하여, EDR 웹 콘솔 통한 디테일 정보 확인 가능

## 2. App Control - Cloud 간 연동

참고 문서 : <https://community.carbonblack.com/t5/Knowledge-Base/App-Control-How-to-enable-VMware-Carbon-Black-Cloud-Integration/ta-p/103396>

### 2.1 Cloud 서버 연동 (App Control 서버)

- [App Control 웹 콘솔] 접속 > 오른쪽 상단의 [Settings] 'System Configuration' 클릭 > [Connectors] 탭 선택 > 'Carbon Black Cloud' 설정

- Cloud 웹 콘솔 정보를 입력하여, Cloud 콘솔로 다이렉트 이동 지원
  - Enable Carbon Black Cloud Integration : Carbon Black Cloud와의 통합 여부
  - Do You Have Carbon Black Cloud Enterprise EDR : Enterprise EDR 사용 여부 (미사용 시, 이벤트/장치 정보만 수집 가능)
  - Automatic : 기본 URL 주소 입력하여, 각 필드 URL에 적용
  - File Event URL, Computer/Device Event URL, Device URL : 수집할 Carbon Black Cloud URL 정보 입력

## 2.2 Cloud 연동 정보 확인 (App Control)

- [App Control 웹 콘솔] 접속 > [Reports]의 [Event] 메뉴 선택

Timestamp	Severity	Description	Source	Process Name
Jan 10 2024 01:30:38 PM	Notice	Carbon Black EDR process Watchlist 'seungmin-test' hit for process 'chrome.exe' [A9DD2...4D2E8] on computer 'ETVS\SEUNGMIN-WINDOW'.	ETVS\SEUNGMIN-WINDOW	chrome.exe
Jan 10 2024 01:30:38 PM	Notice	Carbon Black EDR process Watchlist 'seungmin-test' hit for process 'chrome.exe' [A9DD2...4D2E8] on computer 'ETVS\SEUNGMIN-WINDOW'.	ETVS\SEUNGMIN-WINDOW	chrome.exe
Jan 10 2024 01:30:38 PM	Notice	Carbon Black EDR process Watchlist 'seungmin-test' hit for process 'chrome.exe' [A9DD2...4D2E8] on computer 'ETVS\SEUNGMIN-WINDOW'.	ETVS\SEUNGMIN-WINDOW	chrome.exe
Jan 10 2024 01:30:38 PM	Notice	Carbon Black EDR process Watchlist 'seungmin-test' hit for process 'chrome.exe' [A9DD2...4D2E8] on computer 'ETVS\SEUNGMIN-WINDOW'.	ETVS\SEUNGMIN-WINDOW	chrome.exe

- [App Control 웹 콘솔] 접속 > [Assets]의 [Devices on Computers] 메뉴 선택

- [Cloud 버튼]을 선택하면 Cloud 웹 콘솔로 이동하여, Cloud 웹 콘솔 통한 디테일 정보 확인 가능

## 3. Reputation Approval Rules 활성화

### 3.1 Reputation 활성화 (App Control 서버)

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

vmw Carbon Black App Control    cbac.seungmin.test    Dashboards   Reports   Assets   Rules   Tools   Settings   Help   admin

Home / Administration / System Configuration    Version 8.10.0.485

### System Configuration

General   Events   Security   Advanced Options   Mail   **Licensing**   External Analytics   Connectors   Unified Management   SAML Login

#### 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

[Add License](#)

##### Carbon Black File Reputation Activation

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

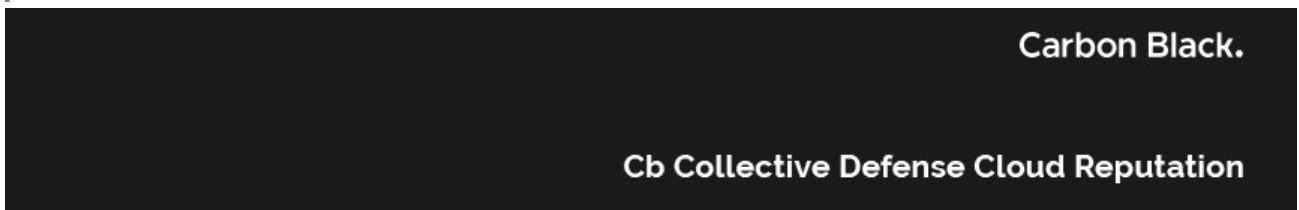
Carbon Black File Reputation Key:

[Accept Terms and Activate](#)

[Verify Activation](#)

[Edit key](#)   [Update](#)   [Cancel](#)

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



## 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.

[Submit](#)

- 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

vmw Carbon Black App Control cbac.seungmin.test Dashboards Reports Assets Rules Tools Settings Help admin

Home / Administration / System Configuration Version 8.10.0.485

## System Configuration

General Events Security Advanced Options Mail **Licensing** External Analytics Connectors Unified Management SAML Login

### 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

[Add License](#)

**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:

[Accept Terms and Activate](#)

[Verify Activation](#)

[Edit key](#) [Update](#) [Cancel](#)

- [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:** T4T

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

[Deactivate](#) [Options](#)

- Carbon Black File Reputation 데이터 다운로드 현황 확인

## 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.*

[Edit Settings](#)

[View Log](#)

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

The screenshot displays the Carbon Black App Control web interface. The top navigation bar includes 'vmW Carbon Black App Control' and several dropdown menus: Dashboards, Reports, Assets, Rules, and Tools. The left sidebar lists various sections: Reports, Assets (expanded), Computers, Files, Applications, Devices, Certificates, and Rules. The main content area is titled 'File Details' and shows the 'General' tab. Key information displayed includes: 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, and File Prevalence (File exists on computer). A red rectangular box highlights a button labeled 'View Carbon Black File Reputation Data' with a play icon, located at the bottom right of the file details section.

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

🔄버전 #16  
★생성 10 1월 2024 09:26:59  
✍수정 18 4월 2025 17:06:16