설치

설치: 서버 요구사항

개요

App Control 서버 구성 전, 환경 요구사항을 확인하기 위한 문서입니다.

요구 사항

> 단일 환경 구성 기준으로 작성되었습니다.

1. 서버 환경

참고 문서 : https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/8.10/cb-ac-oer/GUID-16E1F2A8-7B5D-4F1E-8F6B-937B4677814A.html

1.1 서버 운영 체제

> 운영체제의 경우, 영어 버전으로 설치 필수

운영 체제	아키텍처 버전	서비스 팩	비고
Windows Server 2012 R2	x64	최신 버전 사용	가상 환경일 경우, HVM 만 해당
Windows Server 2016	x64	최신 버전 사용	
Windows Server 2019	x64	최신 버전 사용	
Windows Server 2022	x64	최신 버전 사용	

1.2 서버 스펙

1.2.1 베어메탈

엔드포인트 수	Logical Processors	RAM (GB)	DISK (TB)
Up to 40,000	2	12	2
40,001 to 70,000	6	32	4
70,001 to 90,000	8	48	8
90,001 to 110,000	16	64	8

1.2.1 VMware vSphere

엔드포인트 수	Logical Processors	RAM (GB)	DISK (TB)
Up to 40,000	2	16	2
40,001 to 60,000	6	32	4
60,001 to 70,000	8	48	4

1.3 네트워크

서비스 명	출발지	목적지	포트	비고
App Control 클라우드 서비스	App Control 서버	services.bit9.com	TCP / 443	프록시 연결 지원
	App Control 서버	Reputation.threatintel.carbonblack.io	TCP / 443	프록시 연결 지원
엔드포인트 통신	에이전트	App Control 서버	TCP / 41001	
로그 송신	App Control 서버	Syslog / SIEM	TCP / 514	선택 사항
App Control 웹 콘솔	사용자	App Control 서버 (FQDN or IP)	TCP / 443	

2. Database 환경

2.1 SQL Server 버전

데이터베이스 시스템	아키텍처 버전	서비스 팩	비고
SQL Server 2012	x64	최신 버전 사용	
SQL Server 2014	x64	최신 버전 사용	
SQL Server 2016	x64	최신 버전 사용	
SQL Server 2017	x64	최신 버전 사용	
SQL Server 2019	x64	최신 버전 사용	최신 누적 업데이트 진행 필수
SQL Server 2022	x64	최신 버전 사용	최신 누적 업데이트 진행 필수

3. 환경 구성

3.1 IIS 설치 구성

- Common HTTP Features:
  - Static Content
  - Default Document
  - HTTP Errors
  - HTTP Redirection
- Application development:
  - ASP.NET (version 4.8)
  - .NET Extensibility (version 4.8)
  - CGI
  - ISAPI Extensions
  - ISAPI Filters
- Health and Diagnostics:
  - HTTP Logging
  - Logging Tools
  - Request Monitor
  - Tracing
- Security:
  - Request Filtering
- Performance: None
- Management Tools:
  - IIS Management Console
  - IIS Management Scripts and Tools
- FTP Publishing Service: None

2.2 Database 설정

- 기본적으로 SQL 서버는 시스템에 할당된 RAM을 모두 사용하므로 시스템 메모리 부족 이슈 발생 가능
  - 메모리 상한 설정 필요 (ex: 16GB 메모리가 할당된 경우, 메모리 상한을 12GB 로 설정)

설치: 서버

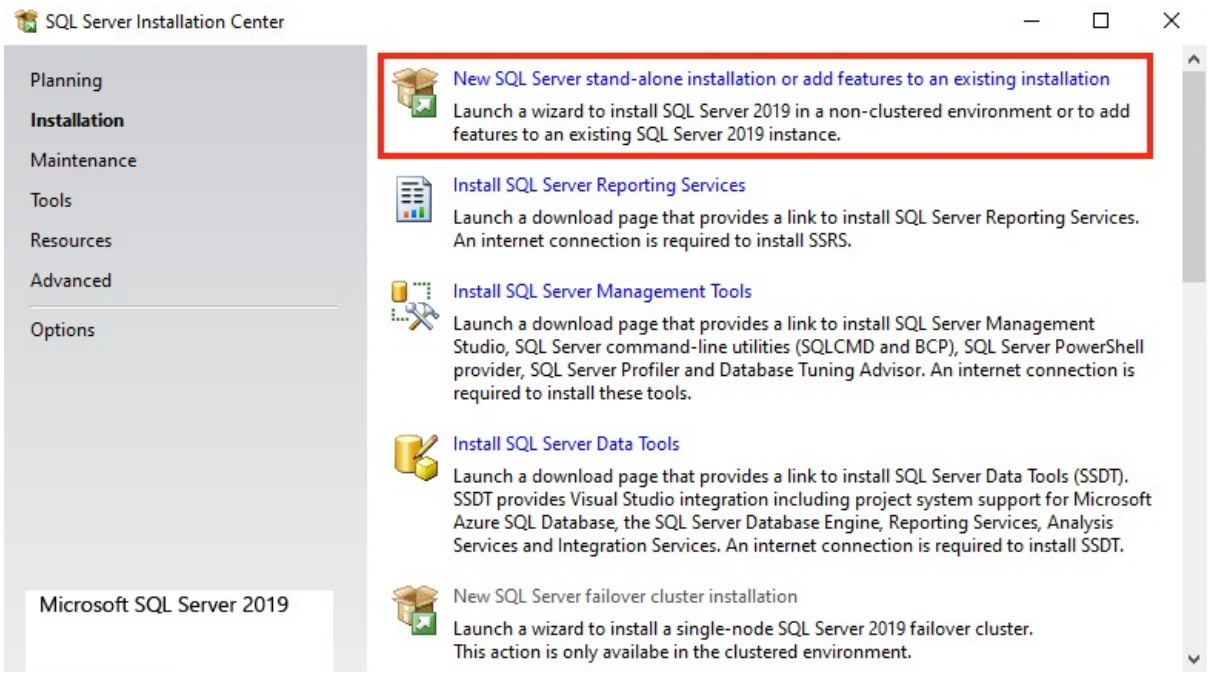
개요

App Control 서버 설치 방법 가이드 문서 입니다.

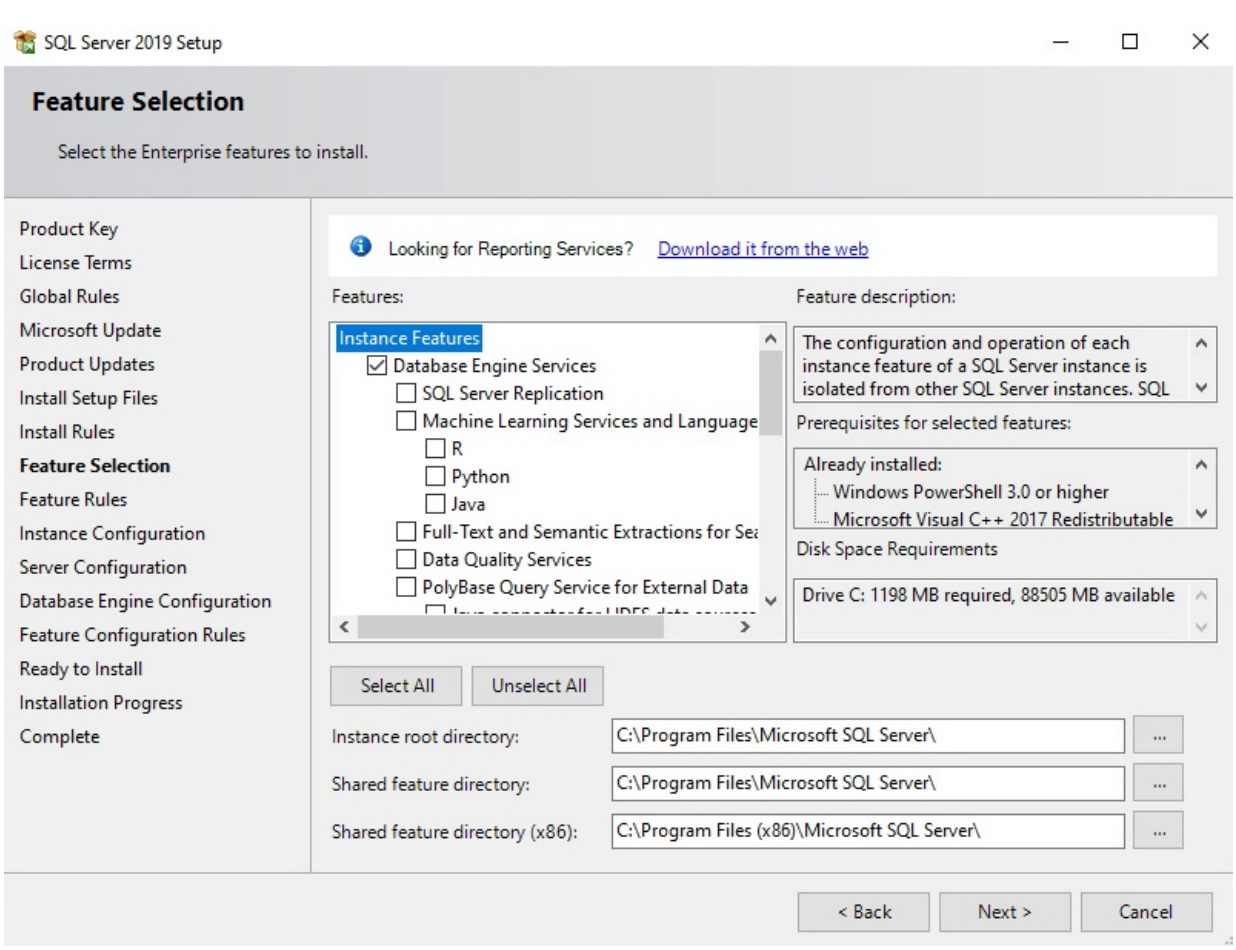
진행 방법

1. SQL Server 설치

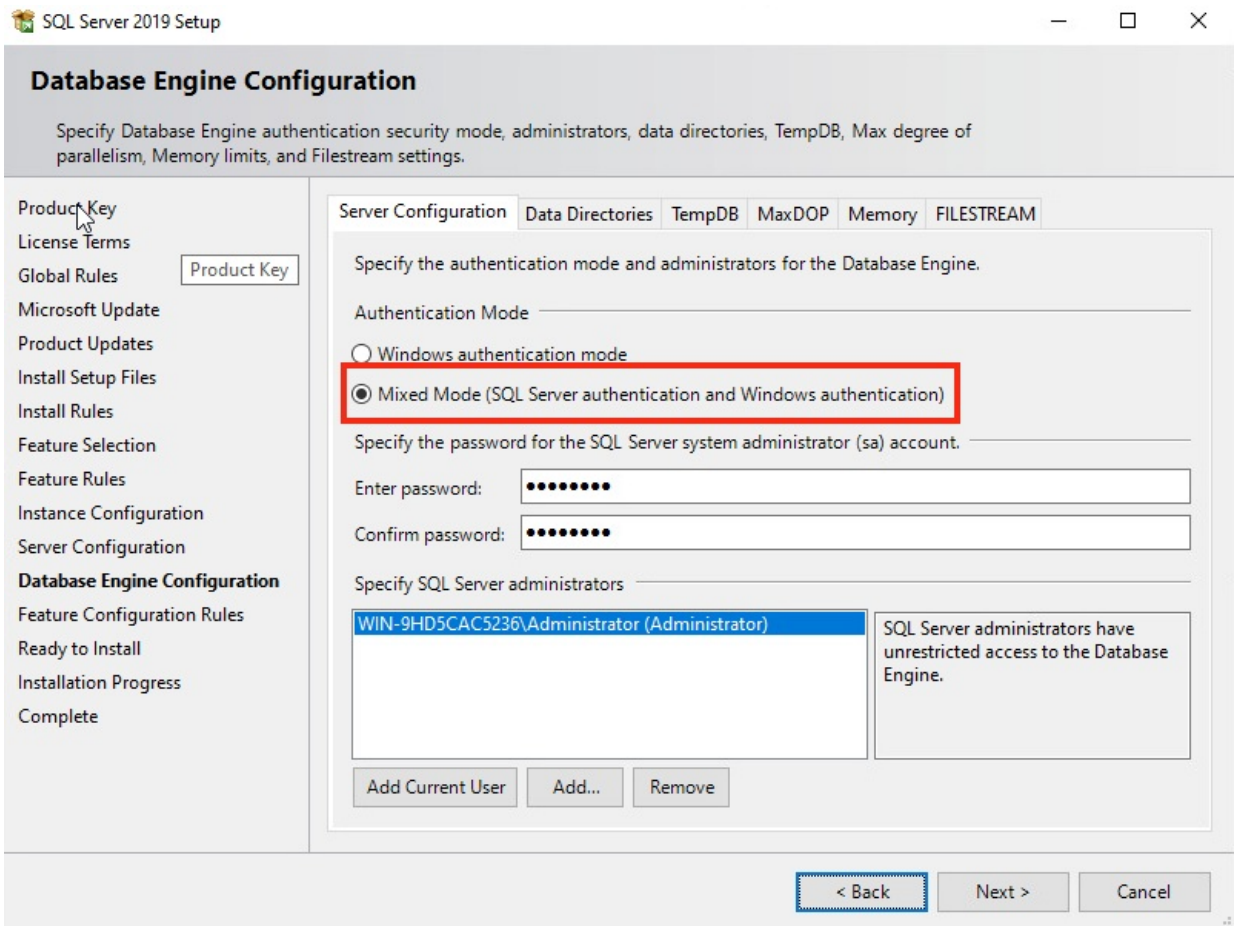
> App control 서버 설치 전, SQL 설치가 선행되어야 합니다.



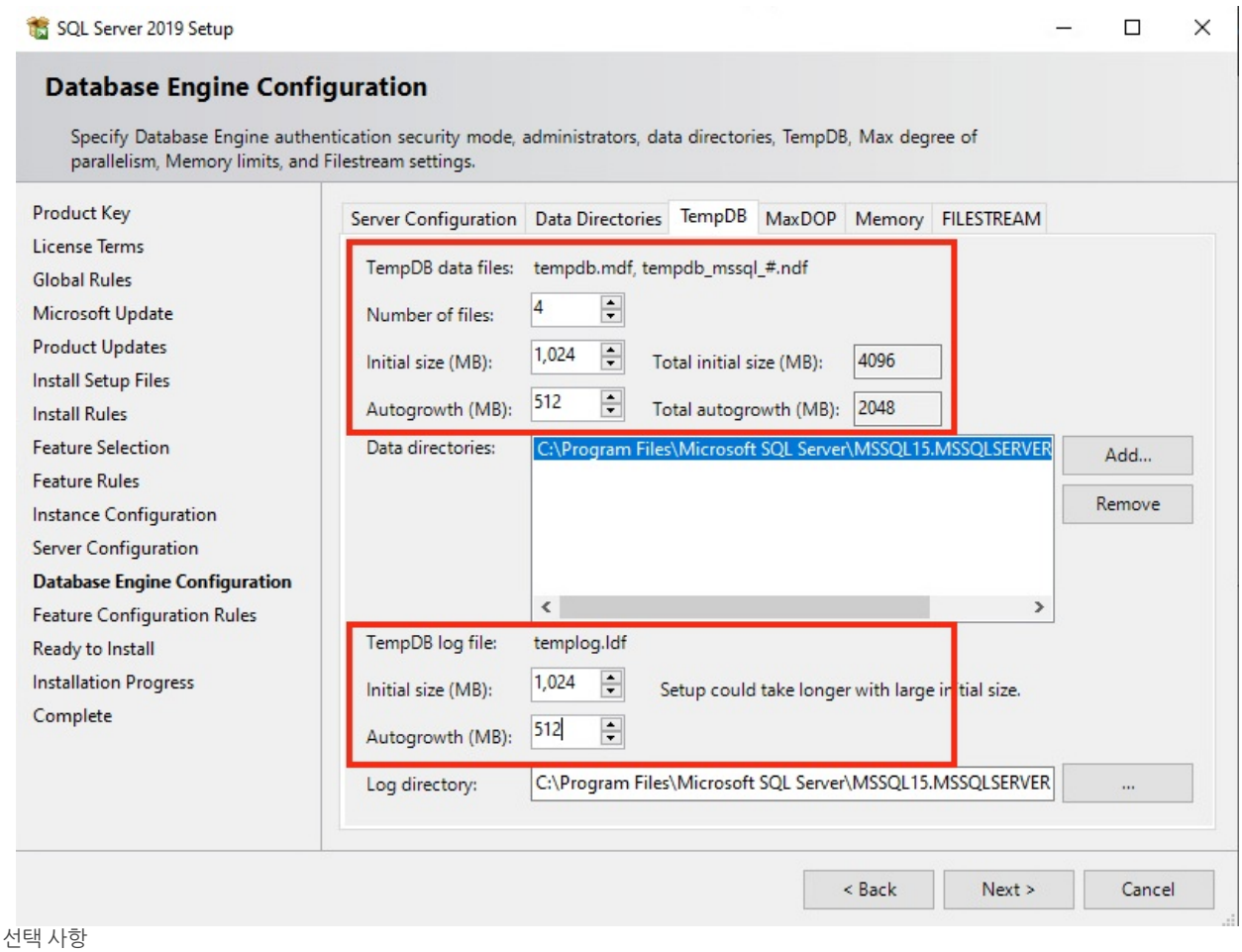
- 'SQL Server Installation Center' 실행 > 'New SQL Server stand-alone Installation' 버튼을 클릭하여 설치 진행



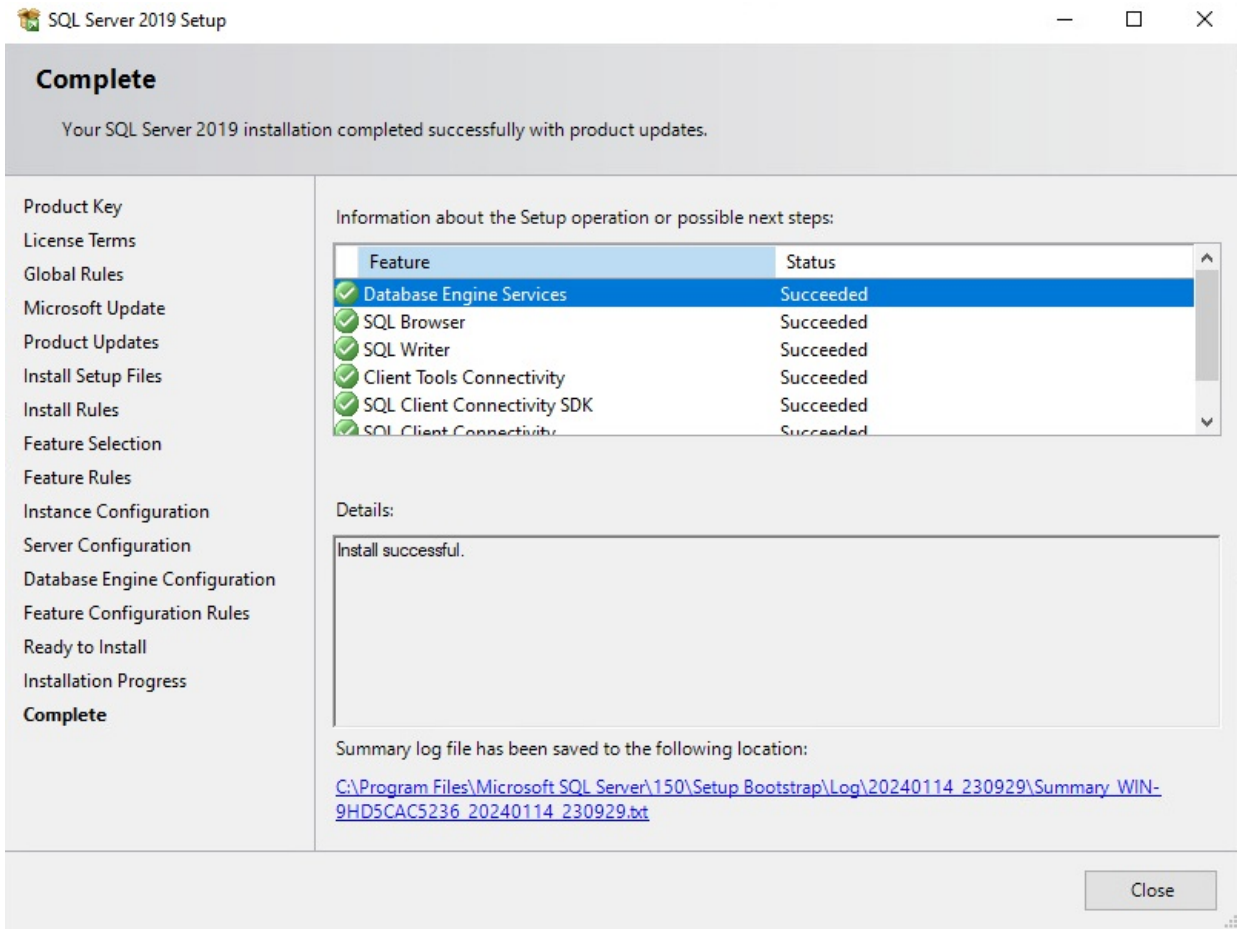
- 'Database Engine Servies' 및 'Client Tools Connectivity' 체크박스 선택



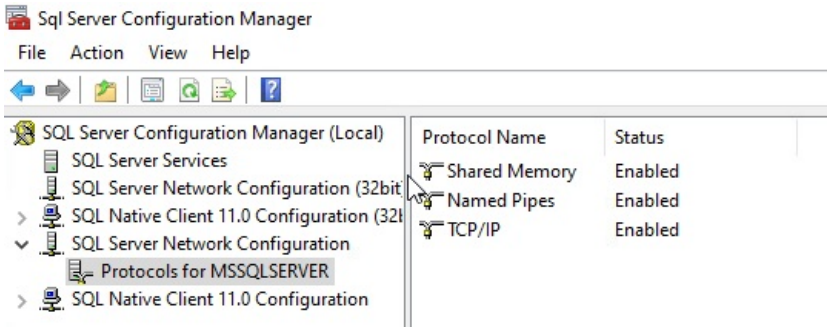
- 'Mixed Mode' 를 선택하고, SQL Server administrator 계정에서 사용할 패스워드 입력
- [Add Current User] 선택하여 사용할 Windows 계정 추가



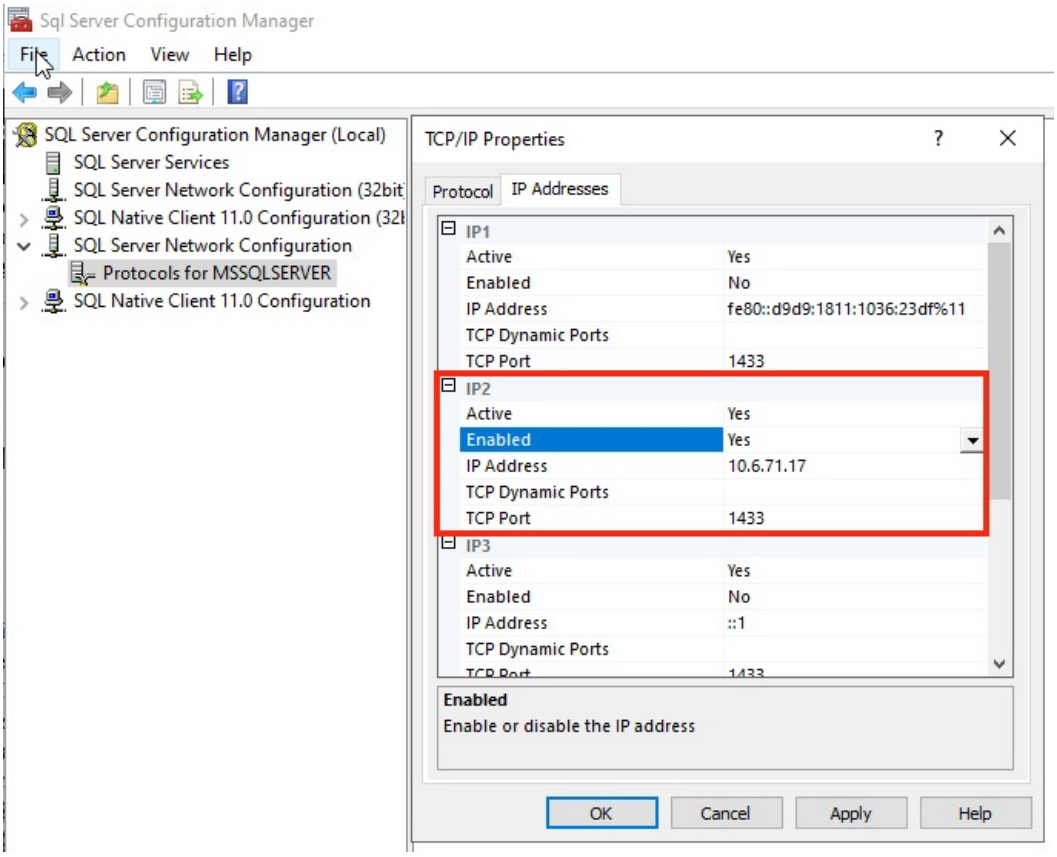
* 선택 사항
- TempDB 선택하여 'data files' 및 'log flie' 크기 사이즈 지정



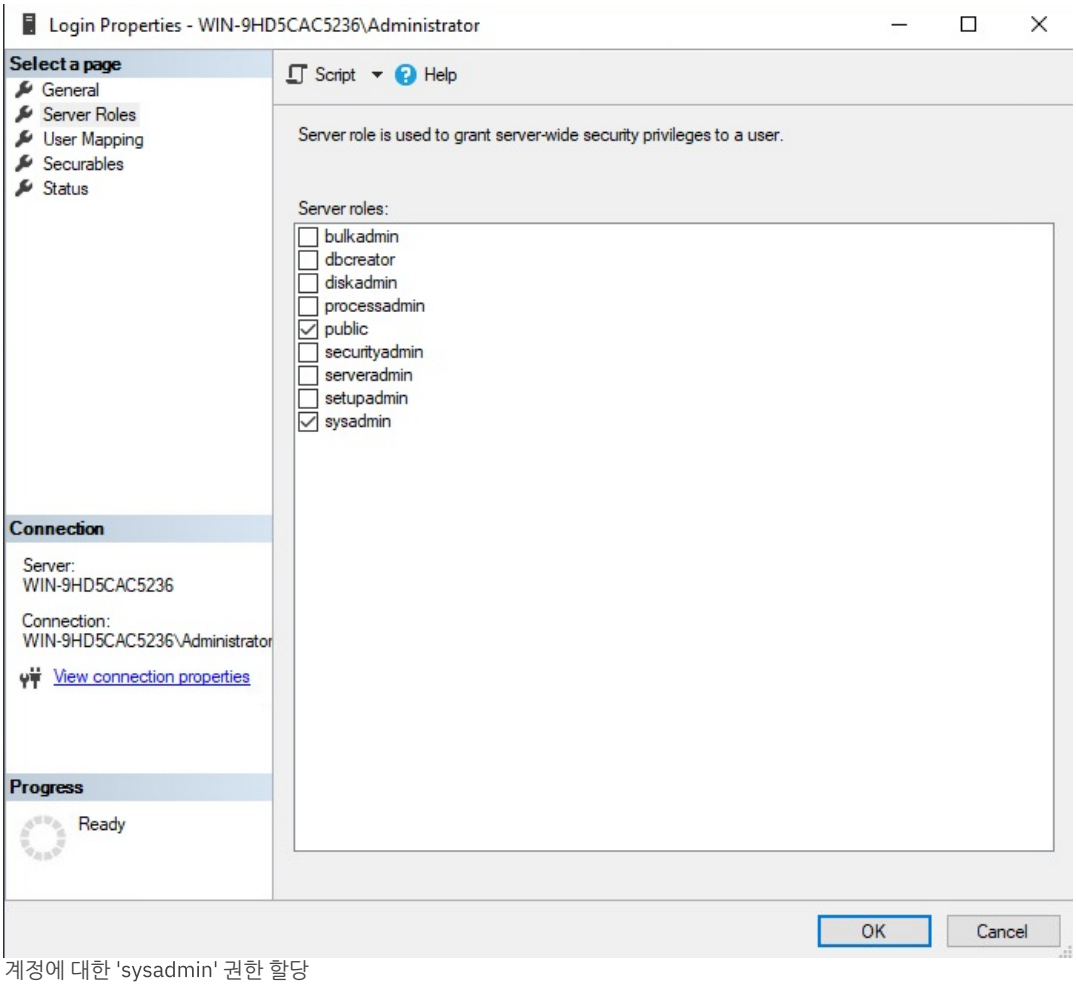
- MS SQL Server 설치 완료 확인



- 'Sql Server Configuration Manager' 실행하여 DB 접속에 사용할 프로토콜 확인



- TCP/IP 사용의 경우, 'TCP/IP' 활성화 설정 진행
- 활성화 작업 완료 후 SQL Server 서비스 재실행



- DB 엑세스 계정에 대한 'sysadmin' 권한 할당

2. App Control Server 설치

참고 문서 : https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/8.10/cb-ac-server-installation-guide/GUID-17F7BE89-2E6F-4F69-92F8-0FA8F562E454.html

8.9.x Server

8.9.6, Released 10 April 2023

- Announcement
- Release Notes
- Installer Download Link

8.8.x Server

8.8.6, Released 21 February 2023

- Announcement
- Release Notes
- Installer Download Link

8.7.x Server

8.7.8 Released 21 February 2023

- Announcement
- Release Notes
- Installer Download Link

Rules Installer

1.22, Released 14 September 2023

- Announcement
- Release Notes
- Installer Download Link

Certificate Installer

21 February 2023

- Announcement
- Certificate Installer Download Link

Agent Information & Downloads

Windows Agent

8.9.2, Released: 6 November 2023

- Announcement
- Release Notes
- Installer Download Link

Linux Agent

8.7.20, Released: 14 December 2023

- Announcement
- Release Notes
- Installer Download Link

macOS Agent

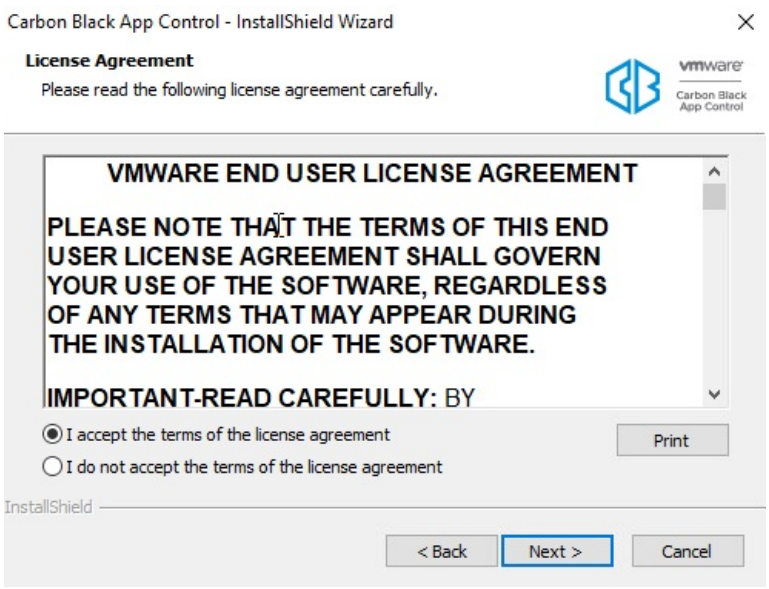
8.9.0, Released: 27 July 2023

- Announcement
- Release Notes
- Installer Download Link

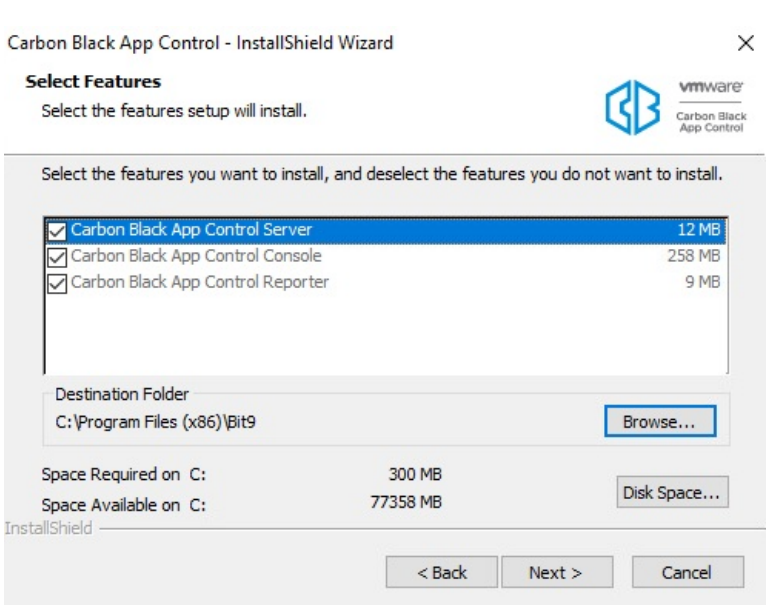
- App Control 인스톨러 다운로드

- Server Installer 다운로드
- Rules Installer 다운로드
- Certificate Installer 다운로드
- Agent Installer 다운로드 (MAC, Windows, Linux)

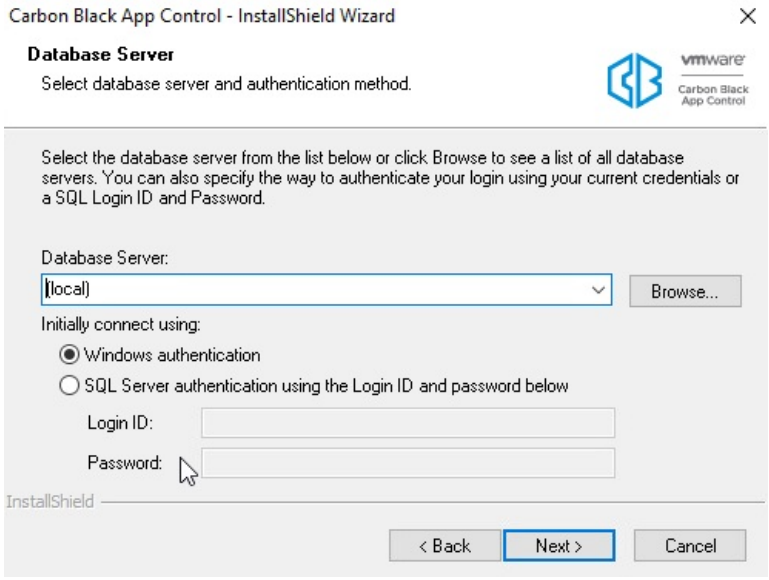
> 다운로드 : https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-appc-release-info/GUID-97815946-2AA4-4488-BC12-B8DCABEBFE56.html



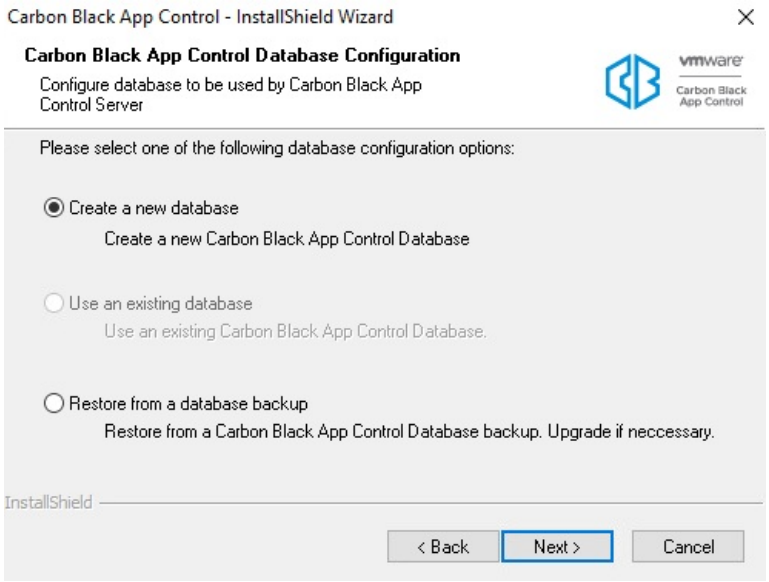
- ParityServerSetup.exe 프로그램 실행 및 라이선스 동의



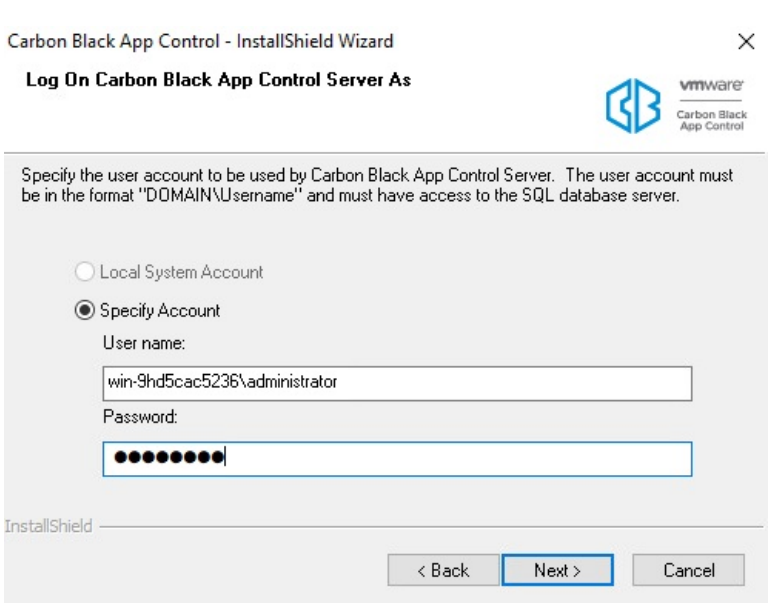
- 설치 진행할 기능 및 설치 위치, 용량 확인



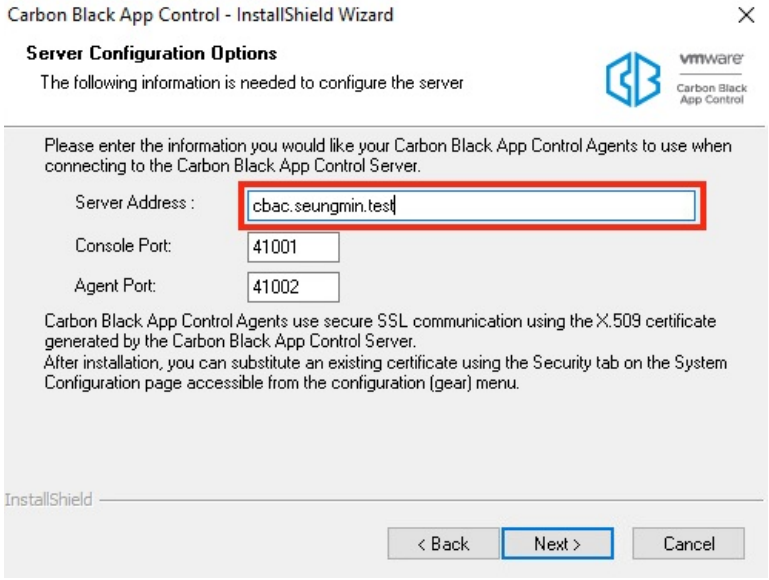
- (동일 환경에 DB가 설치된 경우) Database 서버 위치 '(local)' 선택 및 인증 방법 선택
- (외부 환경에 DB가 설치된 경우) Database 서버 위치 'FQDN or IP' 입력 및 인증 방법 선택



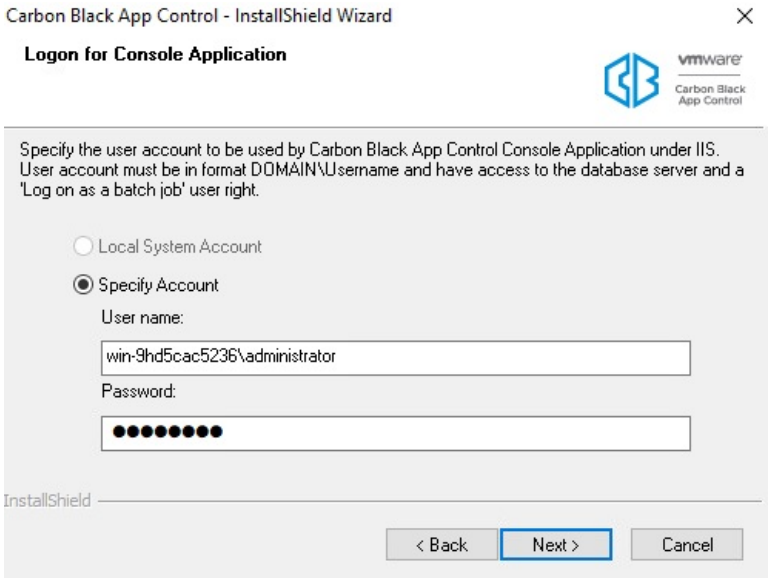
- 신규 설치의 경우, Create a new database 선택하여 신규 생성
* 기존 데이터베이스 사용의 경우, Use a exiting database 선택



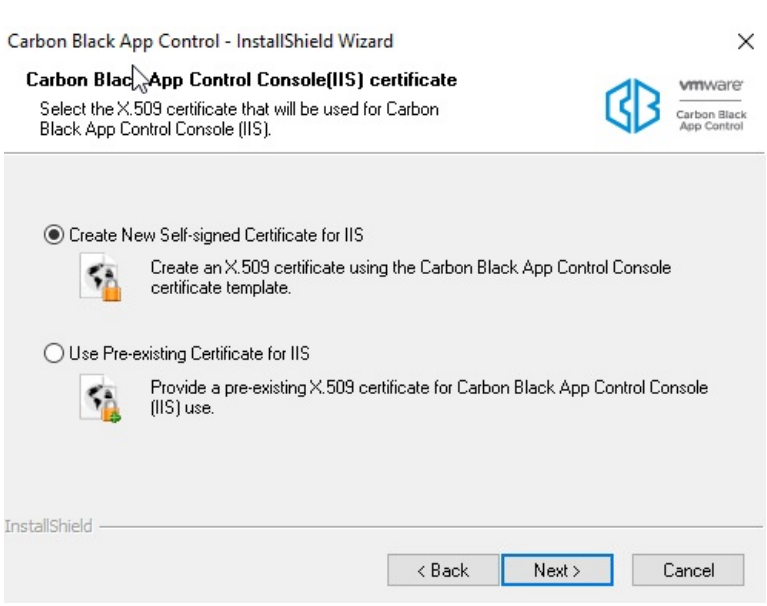
- App Control Server와 SQL Server 에 엑세스 가능한 Windows 사용자 계정 지정



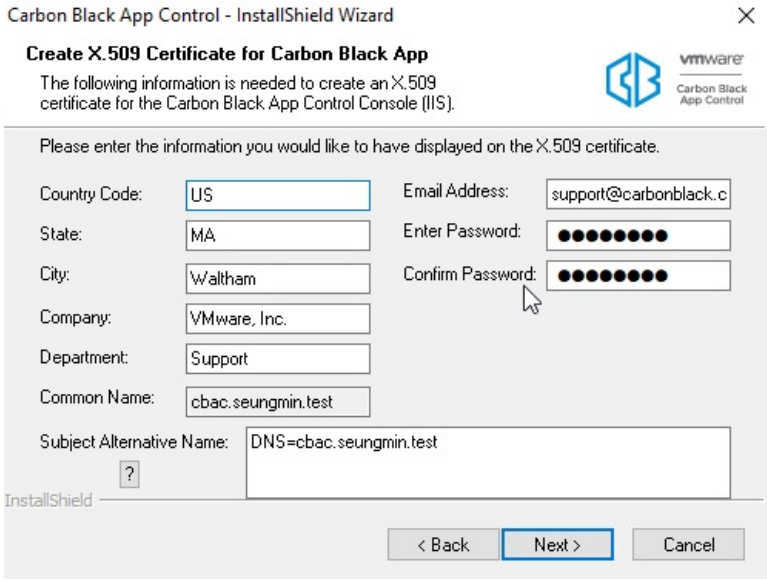
- App Control 웹 콘솔 접속에 사용할 IP or FQDN 정보 입력



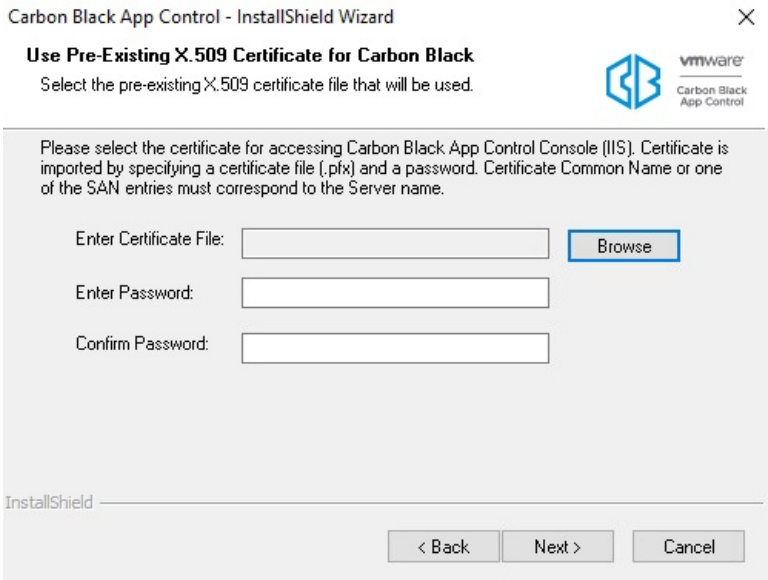
- App Control 웹 콘솔 IIS 서비스에 사용할 Windows 사용자 계정 지정 (App Control Server 및 SQL Server 엑세스 가능 계정)



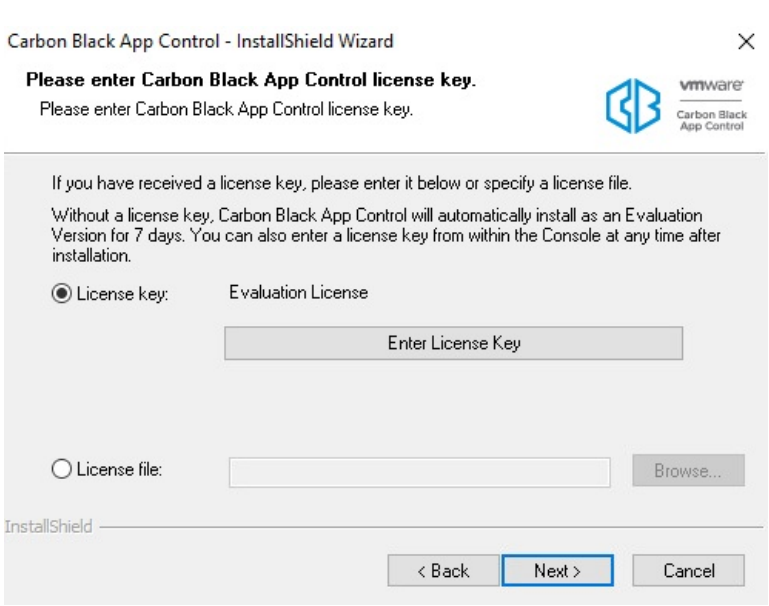
- App Control 웹 콘솔 인증서 선택



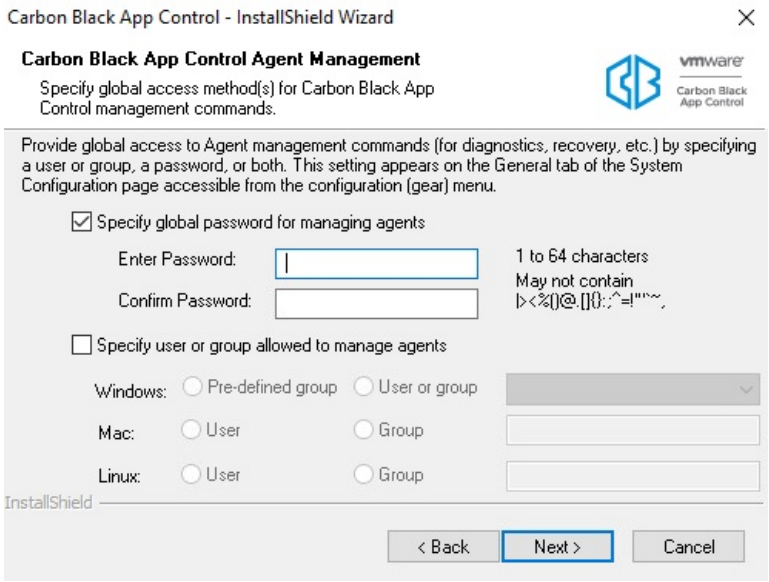
-- (Create New Self-signed Certificate for IIS 옵션 선택) 자체 인증서가 없는 경우 Carbon Black 인증서 신규 생성



-- (Use Pre-existing Certificate for IIS 옵션 선택) 자체 인증서가 있는 경우 인증서 업로드 사용

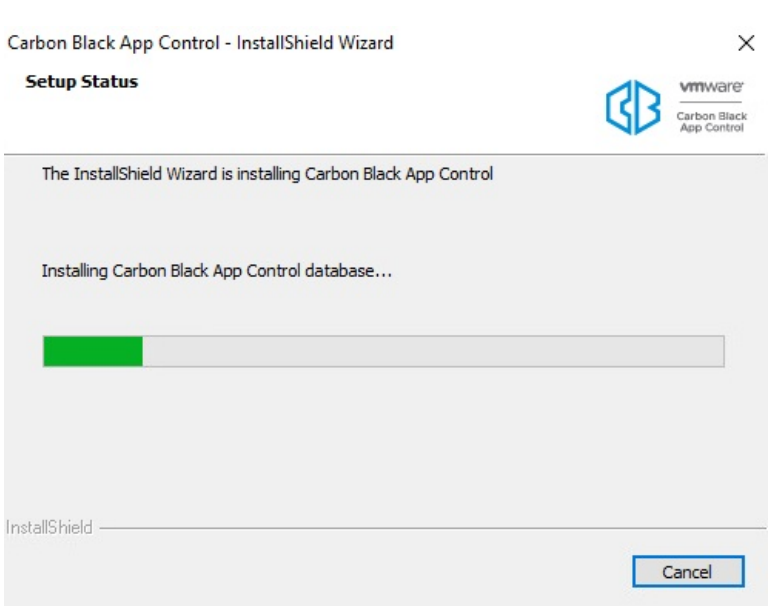


- App Control 라이선스 입력 (7일간의 평가판 라이선스 제공)

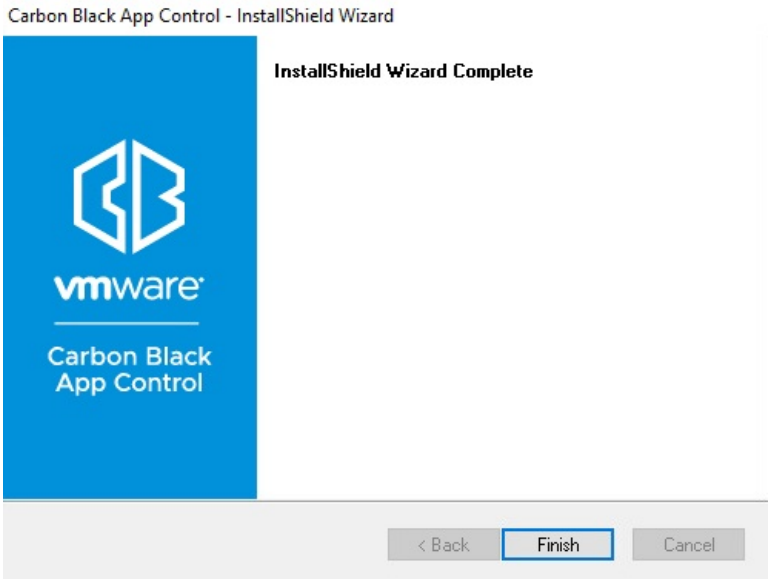


- 관리 시에 사용될 엔드포인트 에이전트에 대한 패스워드 입력 (생략 가능)

- App Control 웹 콘솔 admin 패스워드 입력



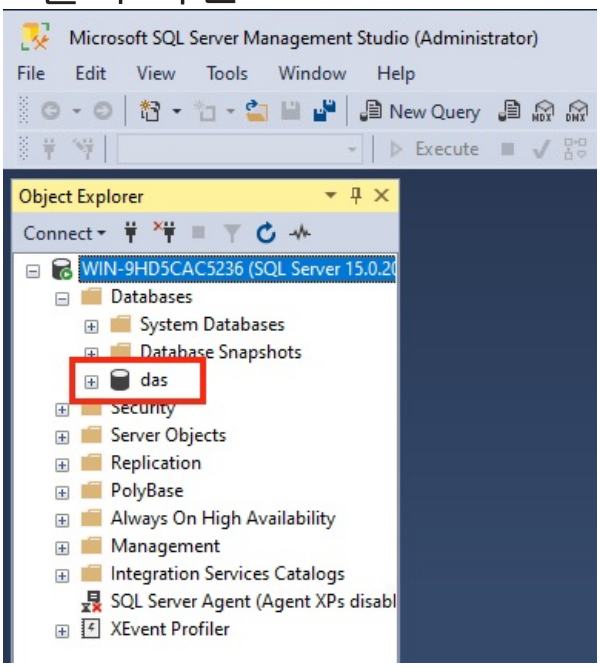
- 설치 진행



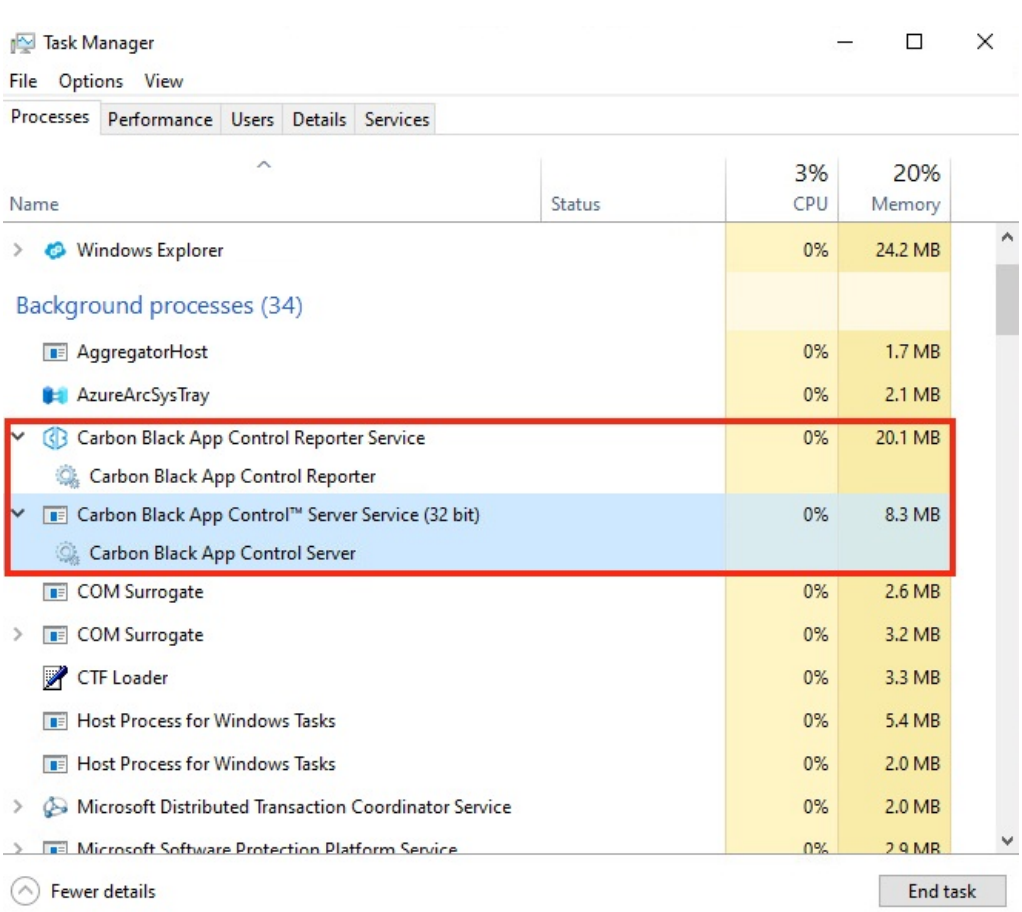
- 설치 완료

* 오프라인 서버 설치 시 : Certificate Install 필요

3. App Control 설치 확인



- App Control 서버에서 생성한 'das' DB 생성 확인

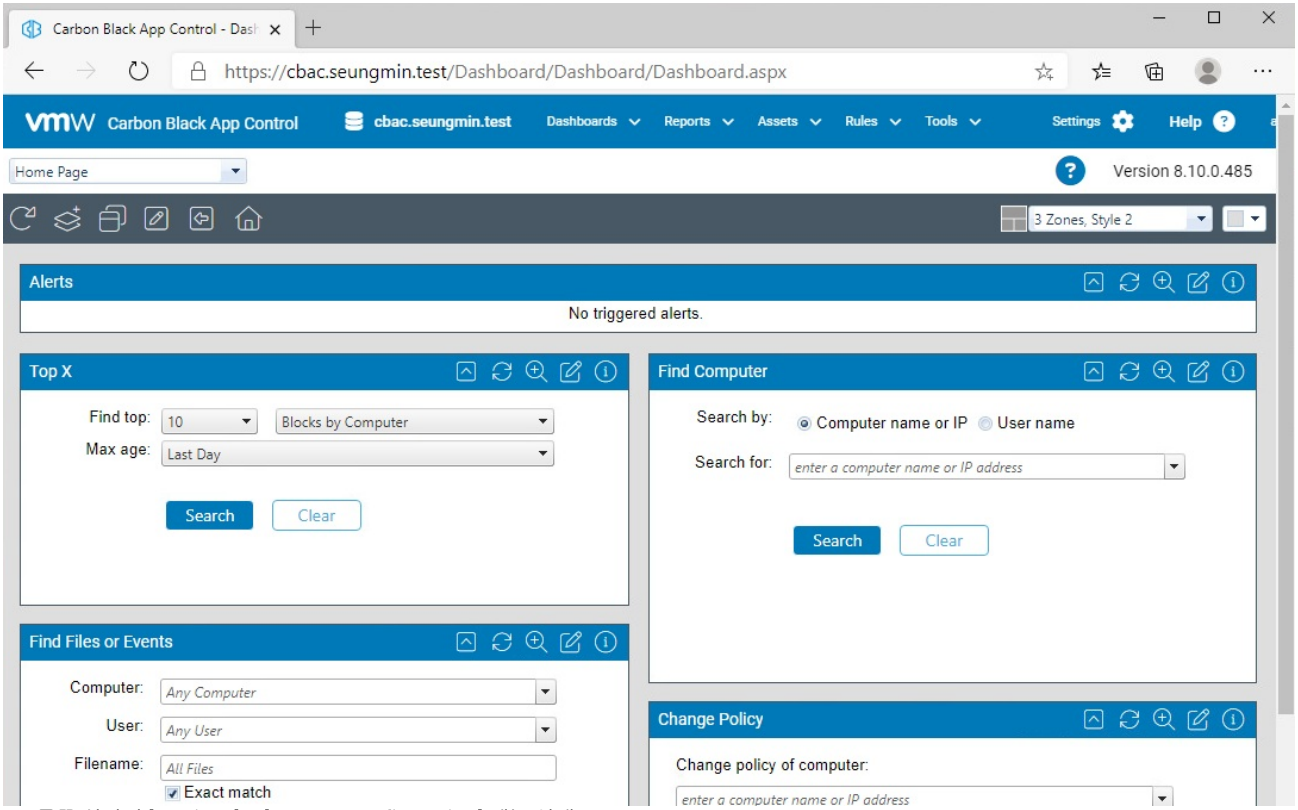


- 로컬 '작업 관리자' 의 프로세스 동작 확인

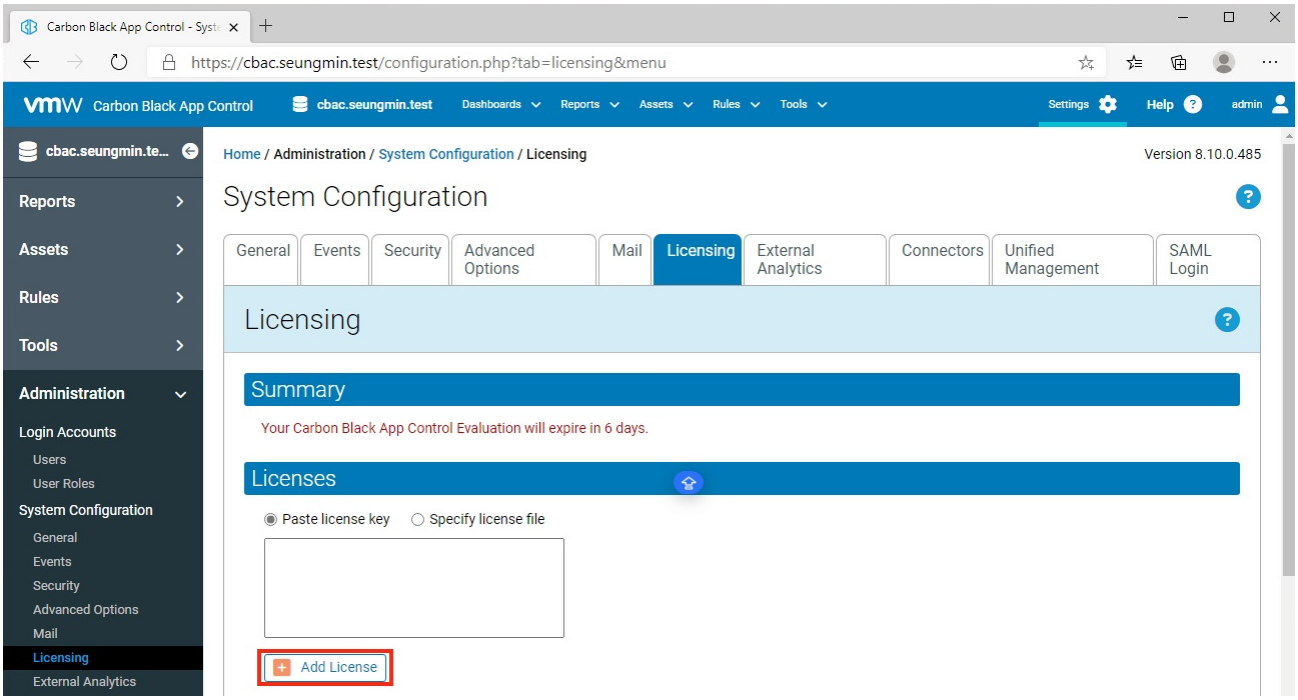
- Carbon Black App Control Reporter Service 프로세스
- Carbon Black App Control Server Service 프로세스

4. App Control 초기 설정

4.1 라이선스 적용

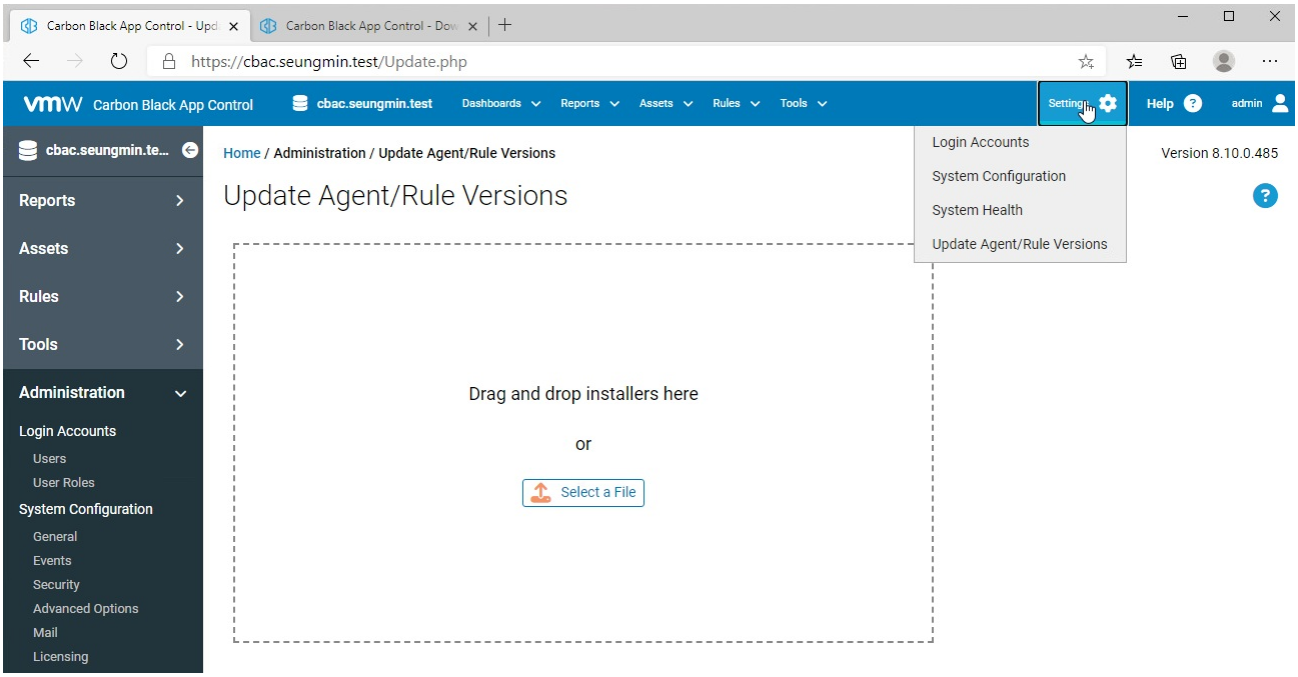


- 오른쪽 상단의 [Settings] > [System Configuration] 메뉴 선택

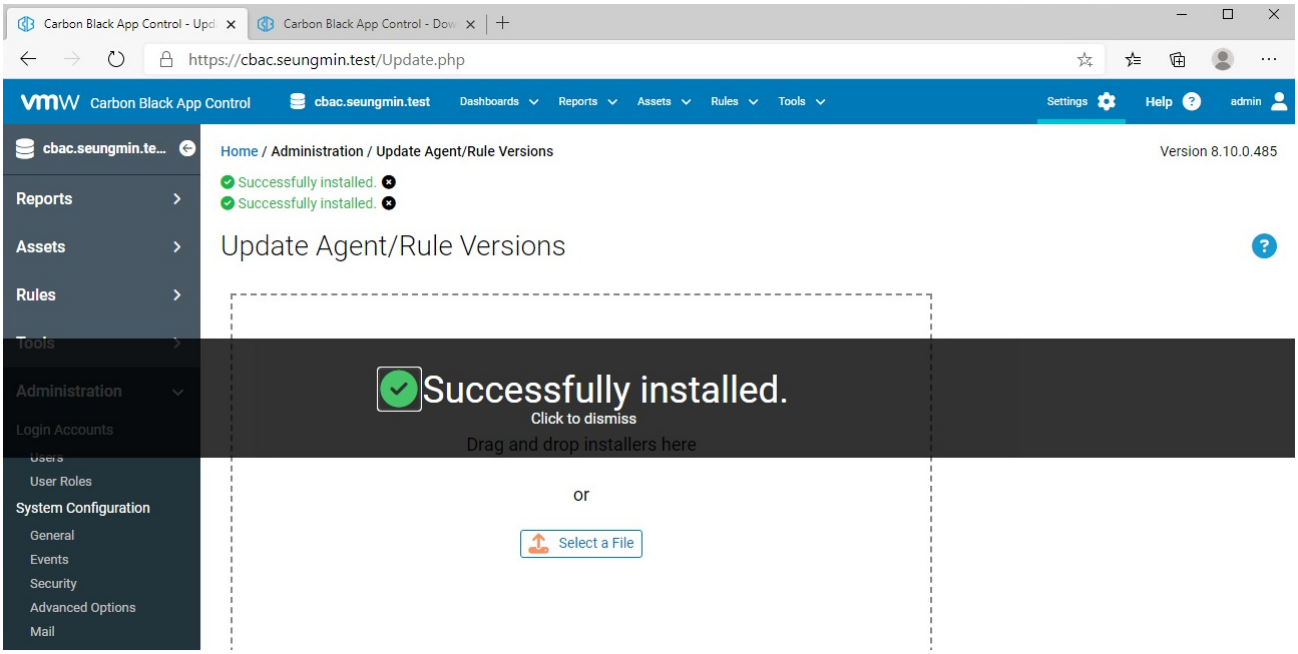


- [Licensing] 탭 이동 > '라이선스 파일 선택' 후 [Add License] 버튼 클릭하여 라이선스 적용

4.2 에이전트 및 룰 업로드

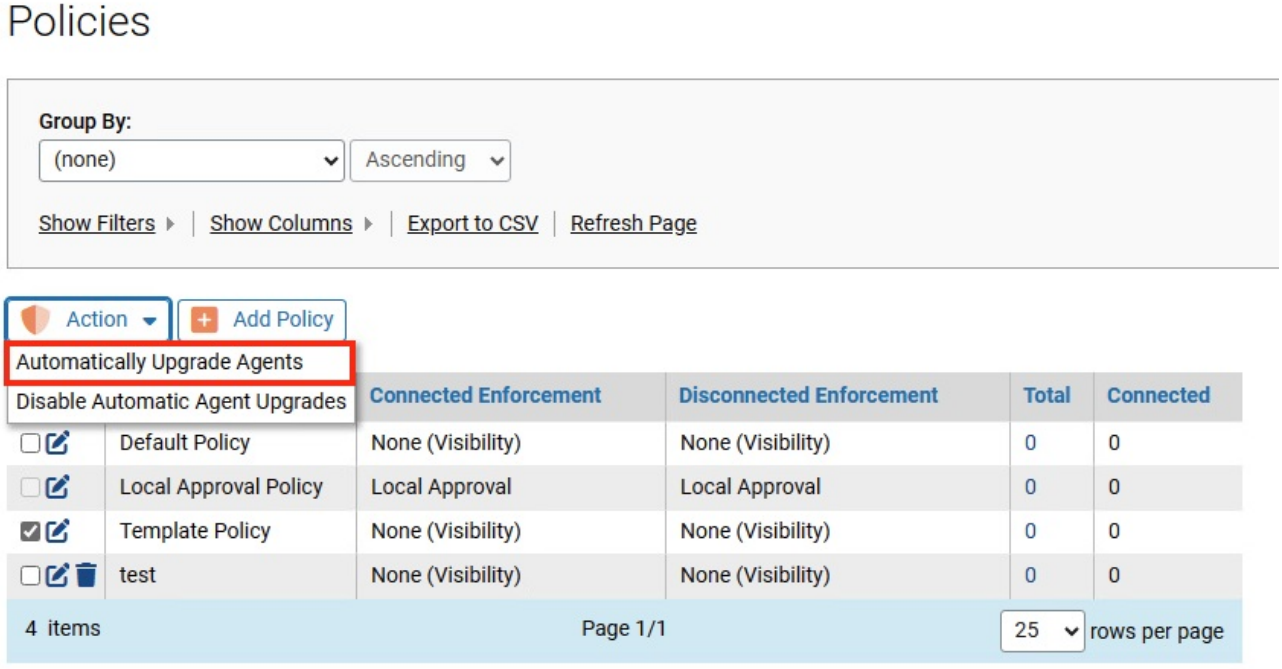


- 오른쪽 상단의 [Settings] > [Update Agent/Rule Version] 메뉴 이동



- 'Select a File' 또는 '드래그 앤 드롭' 방식으로 룰 및 OS 별 에이전트 업로드

- LinuxHostPackageInstaller.exe
- WindowsHostPackageInstaller.exe
- MacHostPackageInstaller.exe
- RulesInstaller.exe



- [Rules] > [Polices] 메뉴 이동하여 룰 생성 및 에이전트 룰 적용

Download Carbon Black App Control Agent Install Packages

Carbon Black App Control protects your computer and the network from viruses, spyware, and other malicious applications.

Installing the Carbon Black App Control Agent software is simple:

1. Click the installation setup file for the policy assigned to you by your network administrator.
2. Download the installation setup file to a convenient location on your hard-drive.
3. For executable files, double-click the newly downloaded file to install the Carbon Black App Control Agent. For archive files, see the User Guide for installation instructions.

Carbon Black App Control Agent Installation Setup Files

Refresh Page

Policy Name	Install Package		Description	Date Created	Date Modified
test	Windows (test.msi)	sha256: a4532d760353a240336802c979f9e0f6c62874788e201d879000739b8d15ebf6		Jan 15 2024 10:51:04 PM	Jan 15 2024 10:56:37
	Windows (test.zip)	sha256: faacf5433f13e8a551e06db57393793cd06767994a5ef5164e3f5a11331624f3			
	Mac (test-mac.dmg)	sha256: 0356494daddc8ff94bdb407ba06e60dd67fa99d2473fb45f620cd2249026310c			
	Red Hat (test-redhat.tgz)	sha256: 6b983aa9bb6cc9090ce68619beeada21405fba7f649c2cb8f77ab9ef9f8c5293			

1 item Page 1/1

- 에이전트 다운로드 페이지로 이동하여 에이전트 업로드 확인

> 에이전트 다운로드 페이지 : https://IP or FQDN/hostpkg/

설치: 에이전트

개요

OS 별 App Control 에이전트 설치 방법에 대한 문서입니다.

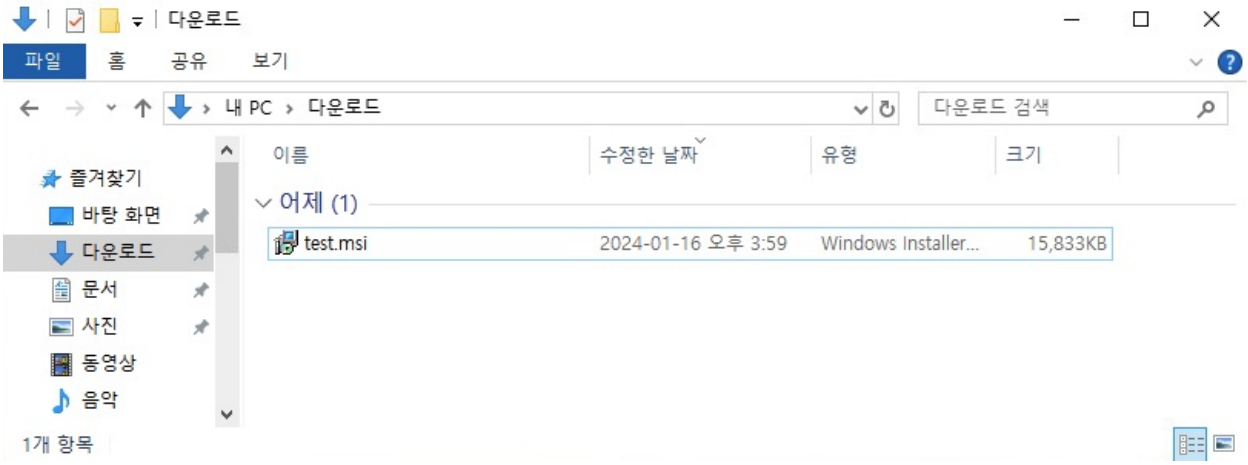
진행 방법

> 에이전트 다운로드 : https://IP or FQDN/hostpkg

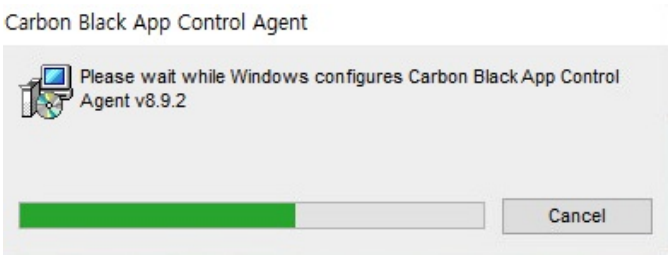
1. Windows 에이전트 설치

> 에이전트 호환성 : https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-appc-oer-winagent-desktop/GUID-A22FCC4B-CA35-4DDF-AA52-A101581E34F4.html

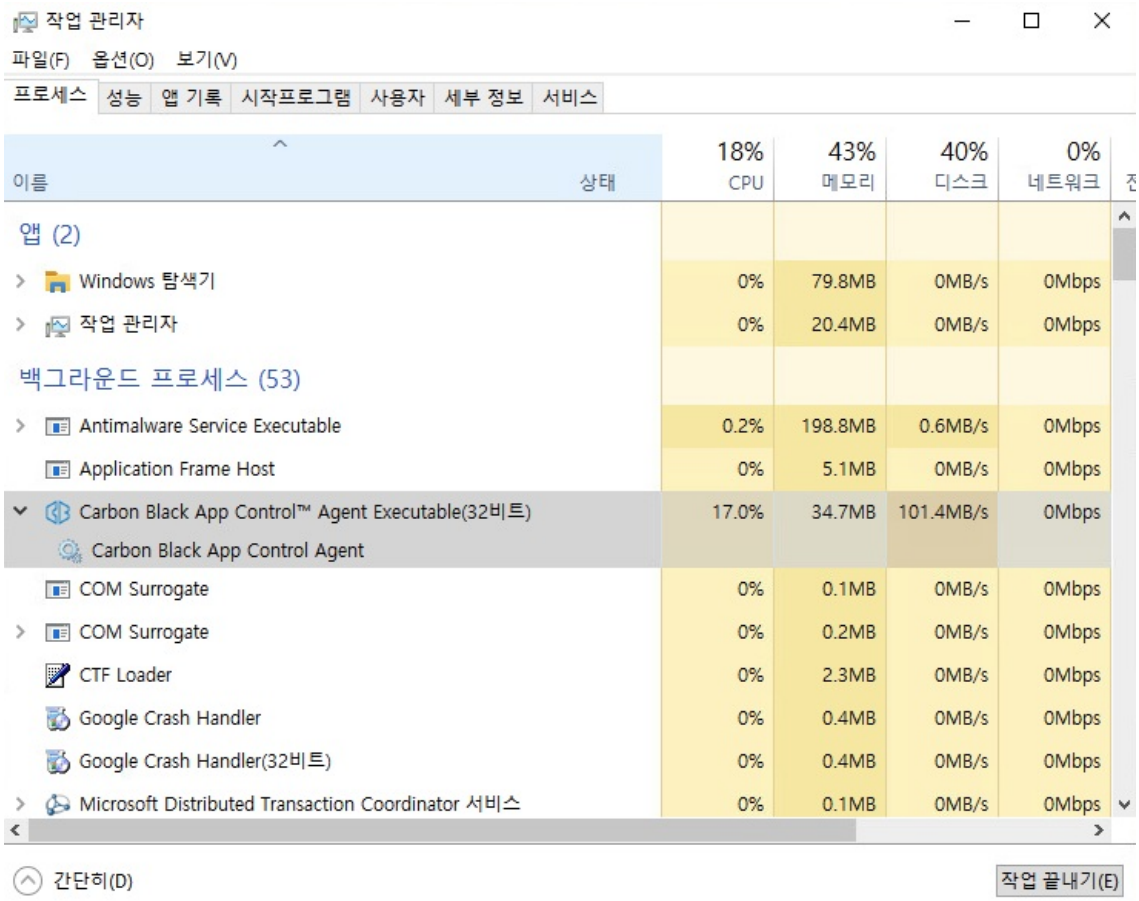
1.1 GUI 설치



- 사용자 PC에서 다운로드 받은 'App Control 에이전트 (정책명.msi)' 실행



- 설치 진행



- '작업 관리자' 또는 '서비스' 확인하여 에이전트 설치 확인

1.2 CLI 설치

> 클라이언트 등록 코드 확인 방법 (기본 값 : 비활성화)
> : [App Contro] 웹 콘솔 접속 > [Settings] - [System Configuration] - [Security] 메뉴 이동 > 'Client Registration Code' 확인

1.2.1 클라이언트 등록 코드 비활성화

```
# 설치 프로그램 경로 지정 후 설치
msiexec.exe /i "C:\Path\To\PolicyInstaller.msi" /qn /norestart /L*v "C:\Temp\AgentInstall.log"

# 설치 프로그램 다운로드 URL 지정 후 설치
msiexec /i "https://IP or FQDN/hostpkg/pkg.php?pkg=PolicyInstallerLink.msi" /qn /norestart /L*v
"C:\Temp\AgentInstall.log"
```

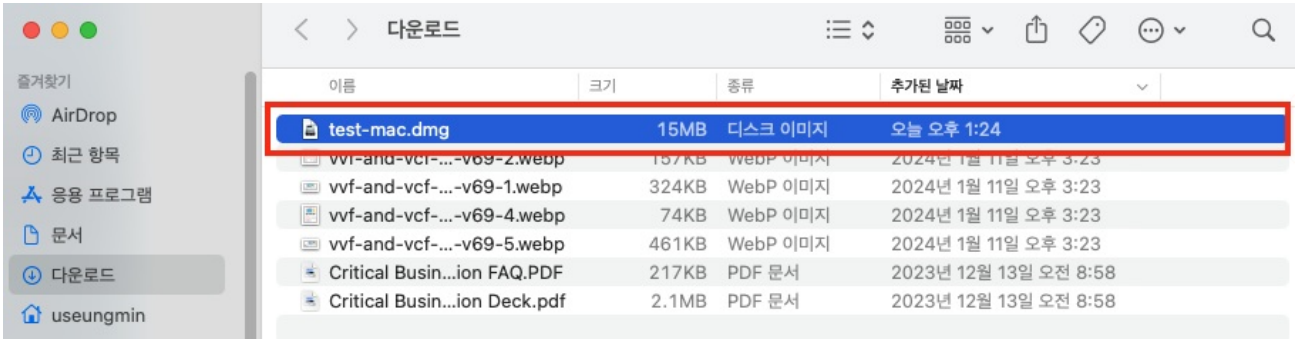
1.2.2 클라이언트 등록 코드 활성화

```
# 설치 프로그램 경로 지정 후 설치
msiexec.exe /i "PolicyInstaller.msi" B9_REGISTRATION_CODE=등록 코드goeshere /qn /norestart /L*v
"C:\Temp\AgentInstall.log"

# 설치 프로그램 다운로드 URL 지정 후 설치
msiexec /i "https://YourServer/hostpkg/pkg.php?pkg=PolicyInstallerLink.msi" B9_REGISTRATION_CODE=등록 코드 /qn
/norestart /L*v "C:\Temp\AgentInstall.log"
```

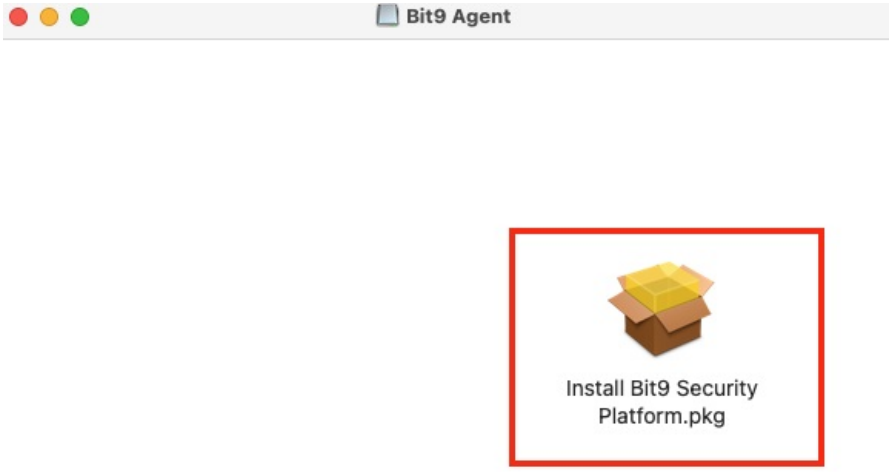
2. MAC 에이전트 설치

에이전트 호환성 : https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-appc-oer-macosagent/GUID-A0DFB81D-AA7B-4DD6-A3F7-FD6E7E2BDFDB.html

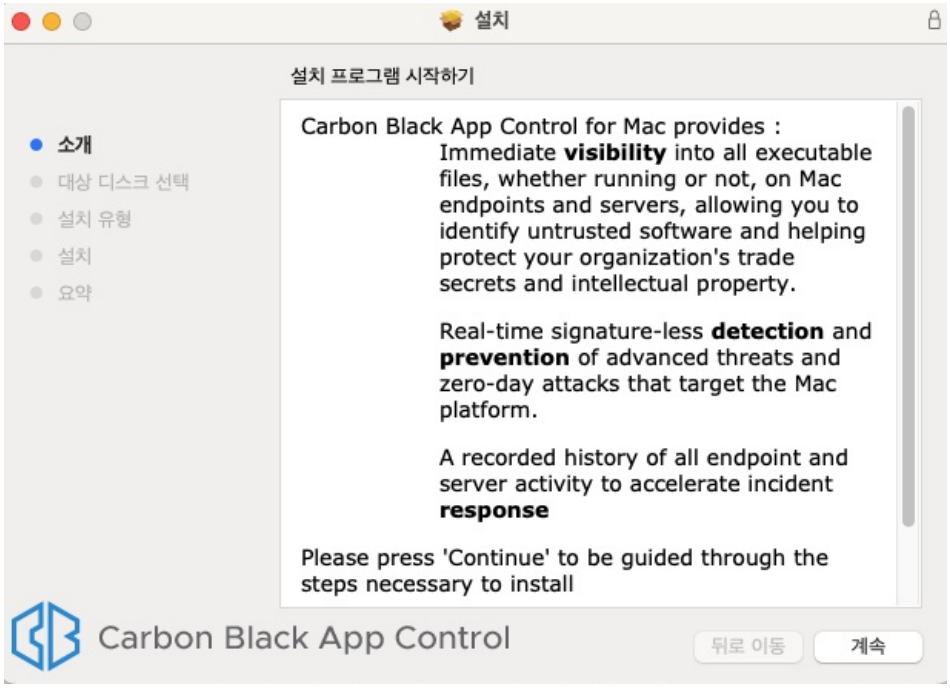
2.1 GUI 설치



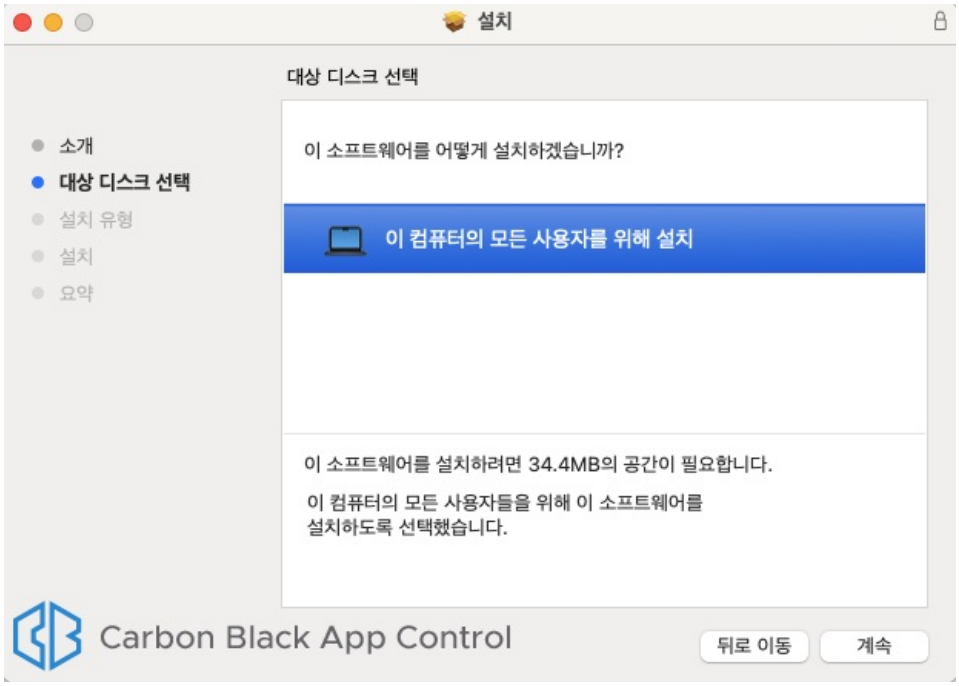
- 사용자 PC에서 다운로드 받은 'App Control 에이전트 (정책명.dmg)' 실행



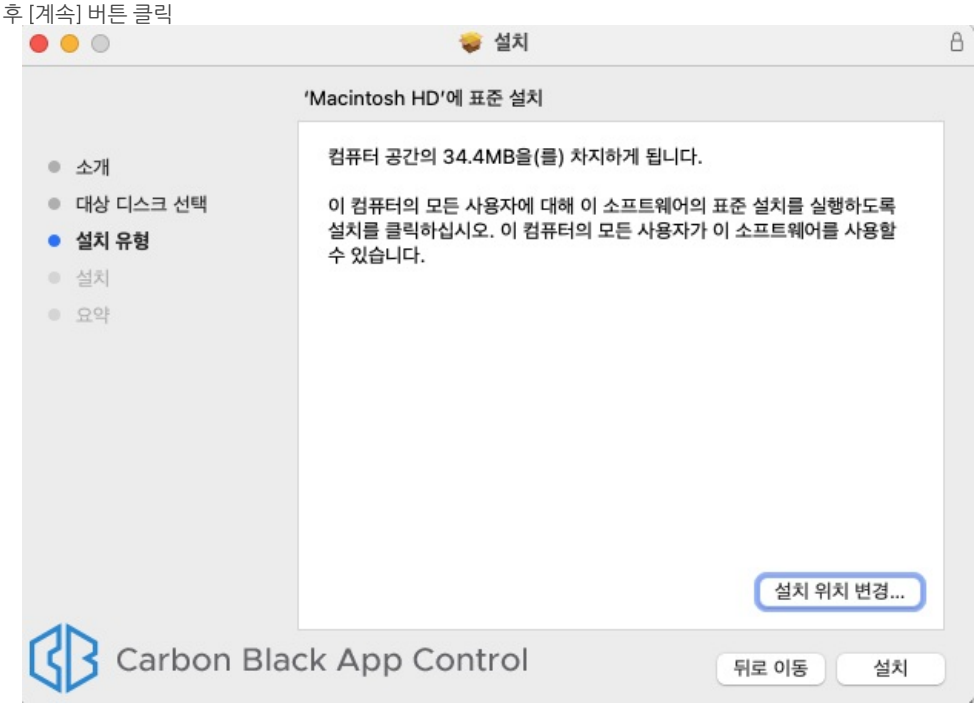
- 'Install Bit9 Security Platform.pkg' 파일 더블클릭하여 실행



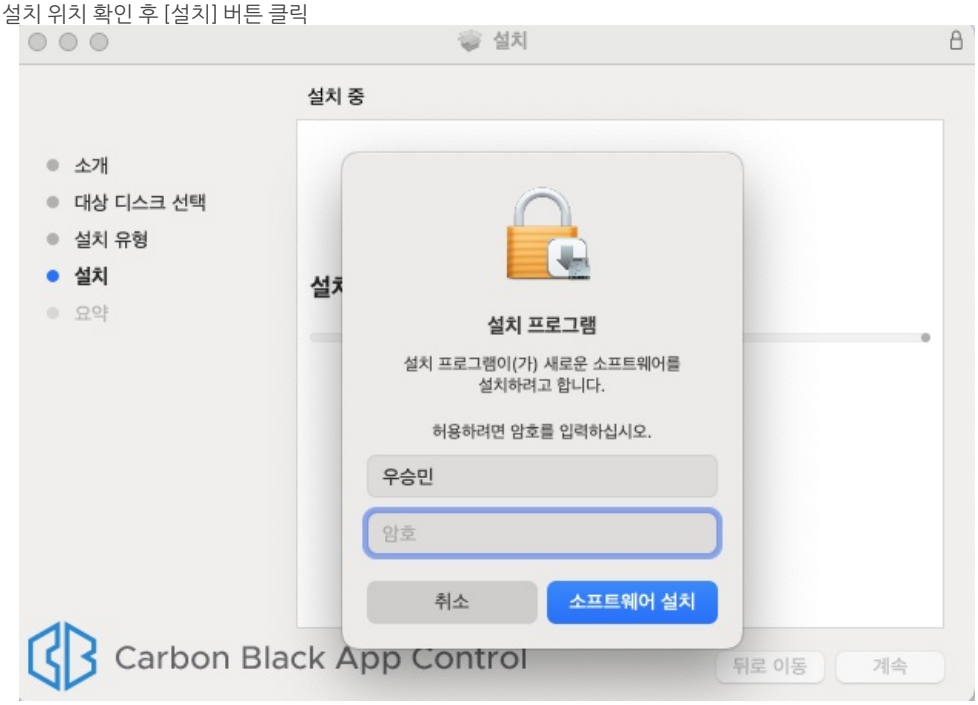
- [계속] 버튼을 클릭하여 설치 프로그램 시작



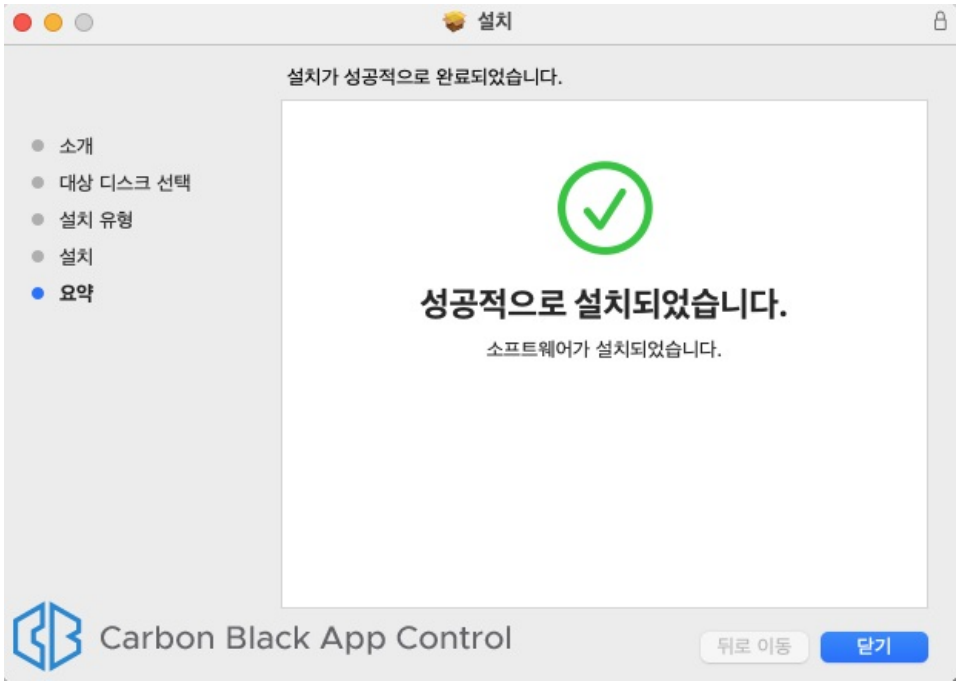
- 설치 유형 확인 후 [계속] 버튼 클릭



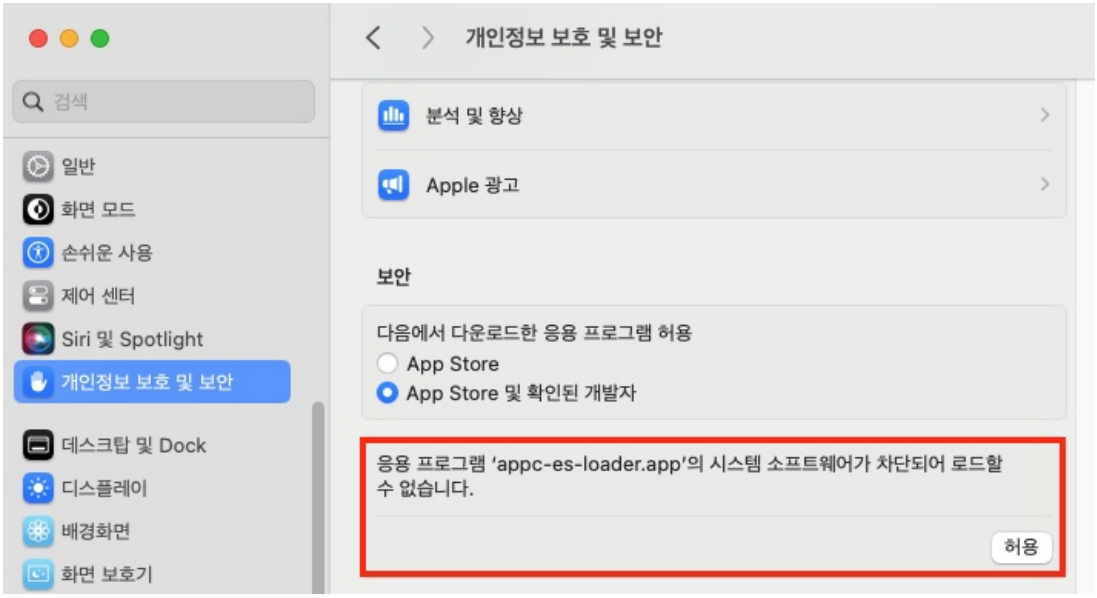
- 설치 사이즈 및 설치 위치 확인 후 [설치] 버튼 클릭



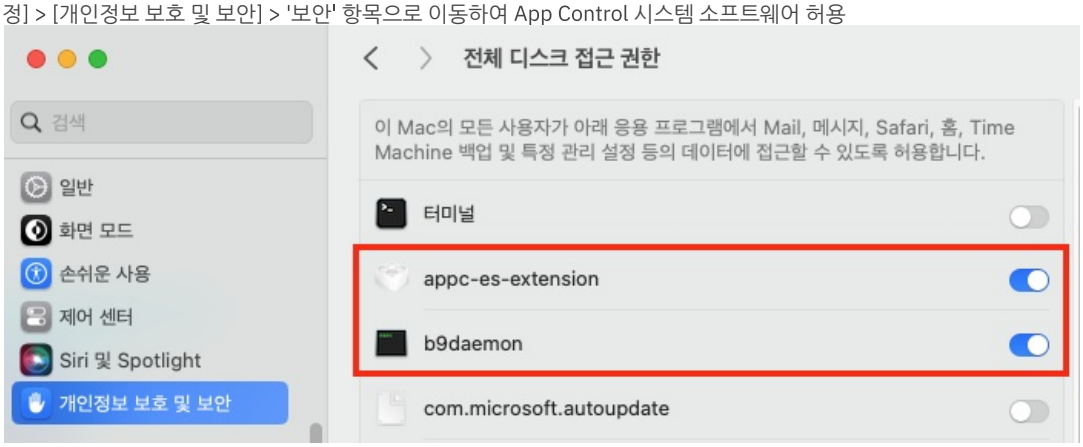
- 사용자 암호 입력 후 [소프트웨어 설치] 버튼 클릭



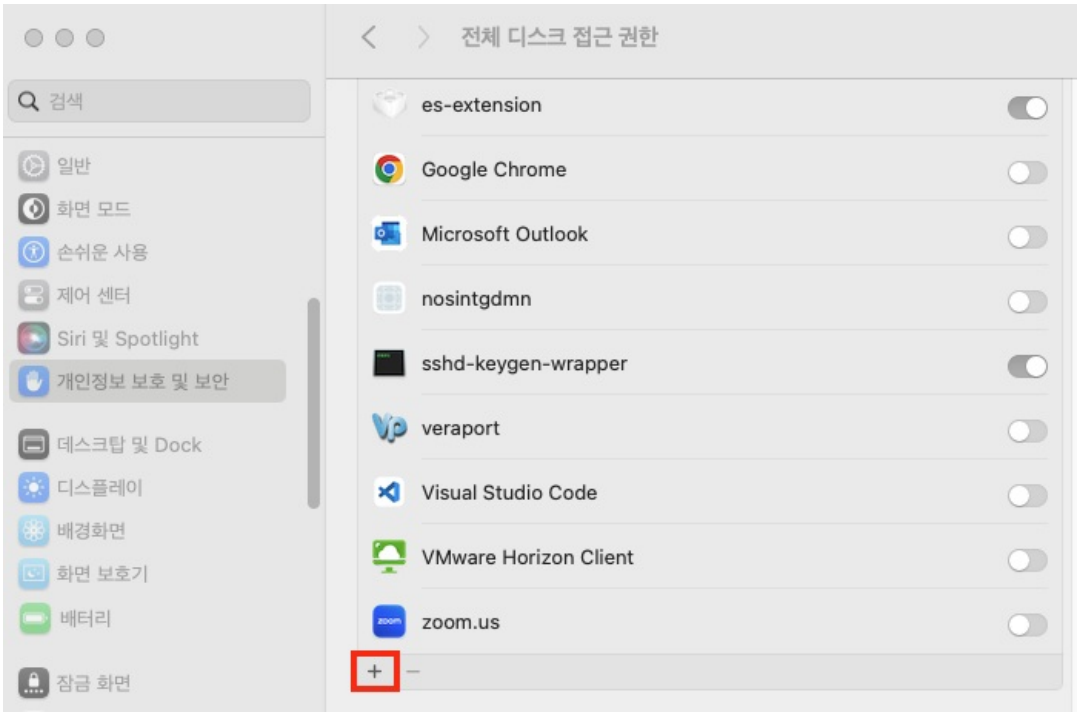
- 설치 완료 확인 후 [닫기] 버튼 클릭하여 설치 프로세스 종료



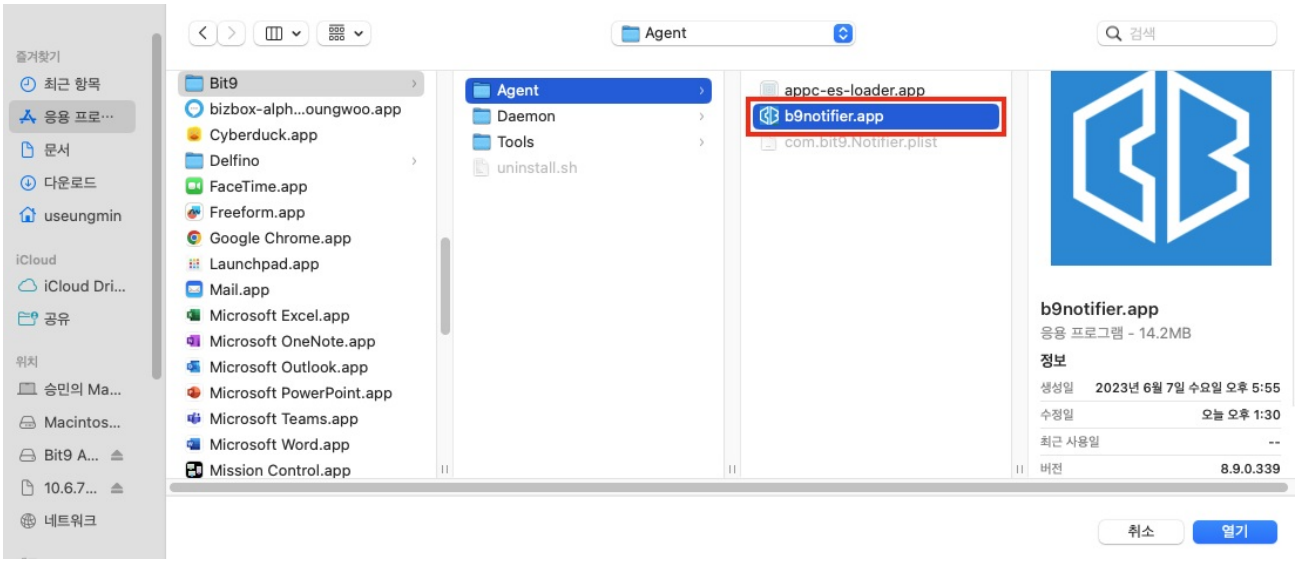
- [시스템 설정] > [개인정보 보호 및 보안] > '보안' 항목으로 이동하여 App Control 시스템 소프트웨어 허용



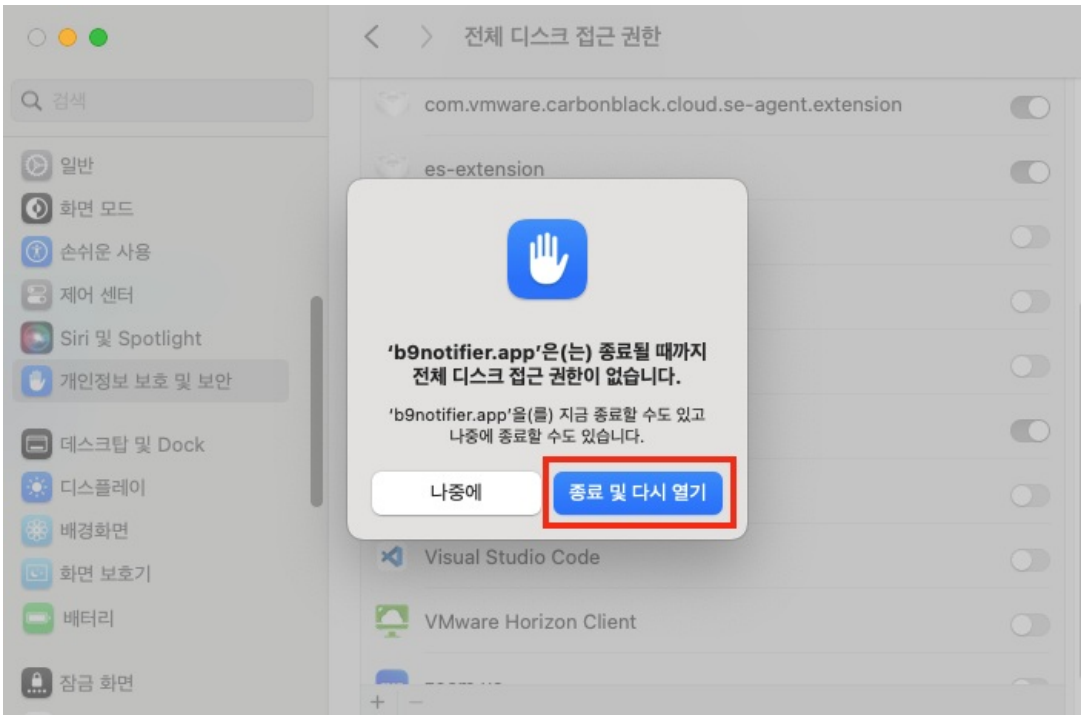
- [시스템 설정] > [개인정보 보호 및 보안] > [전체 디스크 접근 권한] 메뉴로 이동하여 App Control 프로그램 권한 허용



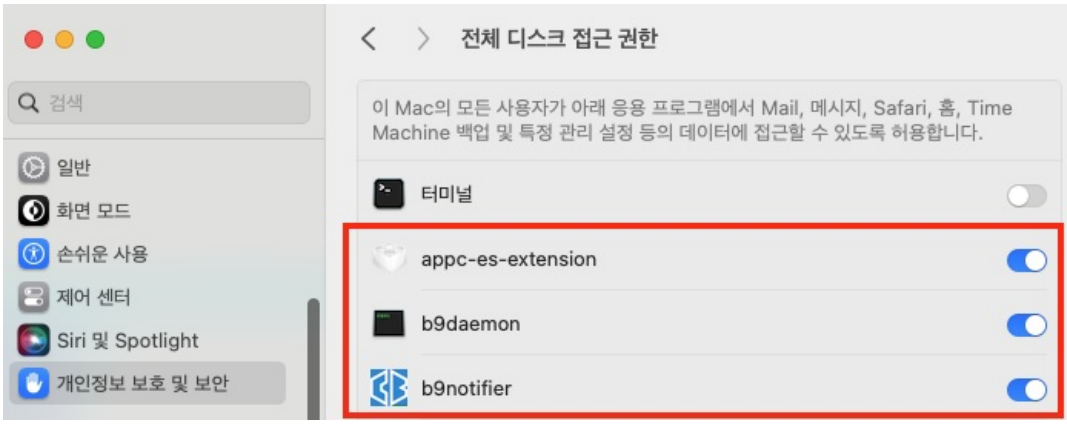
- [시스템 설정] > [개인정보 보호 및 보안] > [전체 디스크 접근 권한] > [+(추가)] 버튼 클릭



- [팝업창] > [응용 프로그램] > [Bit9] > [Agent] > [b9notifier.app] 선택 및 [열기] 버튼 클릭



- b9notifier.app 프로그램의 전체 디스크 접근 권한을 허용하기 위해 [종료 및 다시 열기] 버튼 클릭



- b9notifier.app 프로그램의 전체 디스크 접근 권한 확인

3. Linux 에이전트 설치

> 에이전트 호환성 : https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-appc-oer-linuxagent/GUID-CEDA5E05-2D84-4D58-BCD8-0F0FFA517AD2.html

3.1 CLI 설치

useungmin — root@rpm-minion:/tmp/agent — ssh root@10.6.71.11 — 93×16

```
[root@rpm-minion agent]# wget http://cbac.seungmin.test/hostpkg/pkg.php?php=test-redhat.tgz
--2024-01-17 03:18:23--  http://cbac.seungmin.test/hostpkg/pkg.php?php=test-redhat.tgz
Resolving cbac.seungmin.test (cbac.seungmin.test)... 10.6.71.17
Connecting to cbac.seungmin.test (cbac.seungmin.test)|10.6.71.17|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1525 (1.5K) [text/html]
Saving to: 'pkg.php?php=test-redhat.tgz'

100%[==================>] 1,525       --.-K/s   in 0s

2024-01-17 03:18:23 (230 MB/s) - 'pkg.php?php=test-redhat.tgz' saved [1525/1525]
```

- Liunx 에 App Control 설치 프로그램 업로드 (SSH 또는 Wget 이용)

useungmin — root@rpm-minion:/tmp/agent — ssh root@10.6.71.11 — 76×22

```
[root@rpm-minion agent]# tar -xvzf test-redhat.tgz
test-redhat/server.conf
test-redhat/configlist.xml
test-redhat/configlist_v2.xml
test-redhat/b9install.sh
test-redhat/b9install.asc
test-redhat/bit9cs.asc
test-redhat/bit9cs_sha2.asc
test-redhat/b9agentRedhat6.rpm
test-redhat/b9agentRedhat7.rpm
test-redhat/b9agentRedhat8.rpm
test-redhat/b9agentRedhat9.rpm
test-redhat/b9notifierRedhat6.rpm
test-redhat/b9notifierRedhat7.rpm
test-redhat/b9notifierRedhat8.rpm
test-redhat/b9notifierRedhat9.rpm
[root@rpm-minion agent]#
```

- 설치 프로그램 압축 해제

```
useungmin — root@localhost:/home/test-redhat — ssh root@10.6.71.112 — 96×24
[root@localhost test-redhat]# gpg --dearmor bit9cs_sha2.asc
[root@localhost test-redhat]# gpg --no-default-keyring --homedir . --keyring bit9cs_sha2.asc.gpg
 --verify b9install.asc b9install.sh
gpg: WARNING: unsafe permissions on homedir '/home/test-redhat'
gpg: Signature made Mon Nov 27 21:41:04 2023 KST
gpg:                using RSA key E7892ECDFDC509C6
gpg: /home/test-redhat/trustdb.gpg: trustdb created
gpg: Good signature from "build (carbonblack) <contact@carbonblack.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 3567 6AEE 452F 91A6 0D2F  4A43 E789 2ECD FDC5 09C6
```

- gpg 키 인증 통한 설치 스트립트 유효성 검사
- "Good signature from "build (carbonblack)"" 메세지 확인

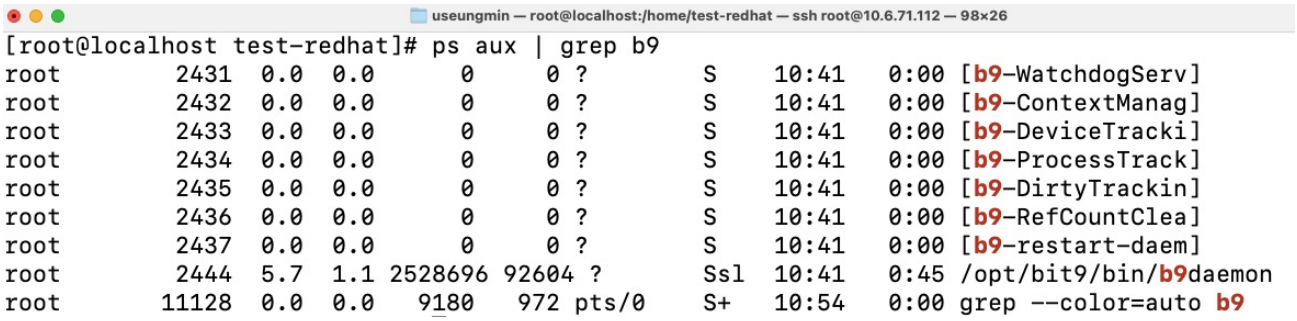
> 버전 별 Public Key 다운로드 : https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-ac-announcements/GUID-123F59D1-E2C4-431F-8CEE-5D924CF83F13.html

```
useungmin — root@localhost:/home/test-redhat — ssh root@10.6.71.112 — 98×26
[root@localhost test-redhat]# sh ./b9install.sh -n
Installing App Control agent package

Starting the App Control Daemon
Completed agent install on Thu, 18 Jan 2024 10:41:34 +0900

  Running scriptlet: nss-3.90.0-4.el8.x86_64                                9/9
  Running scriptlet: b9agent-8.7.20-1.el8.x86_64                            9/9
  Verifying        : nspr-4.35.0-1.el8.x86_64                               1/9
  Verifying        : nss-3.90.0-4.el8.x86_64                                2/9
  Verifying        : nss-softokn-3.90.0-4.el8.x86_64                        3/9
  Verifying        : nss-softokn-freebl-3.90.0-4.el8.x86_64                 4/9
  Verifying        : nss-sysinit-3.90.0-4.el8.x86_64                        5/9
  Verifying        : nss-util-3.90.0-4.el8.x86_64                           6/9
  Verifying        : libicu-60.3-2.el8_1.x86_64                             7/9
  Verifying        : unzip-6.0-46.el8.x86_64                                8/9
  Verifying        : b9agent-8.7.20-1.el8.x86_64                            9/9

Installed:
  b9agent-8.7.20-1.el8.x86_64                libicu-60.3-2.el8_1.x86_64
  nspr-4.35.0-1.el8.x86_64                   nss-3.90.0-4.el8.x86_64
  nss-softokn-3.90.0-4.el8.x86_64            nss-softokn-freebl-3.90.0-4.el8.x86_64
  nss-sysinit-3.90.0-4.el8.x86_64            nss-util-3.90.0-4.el8.x86_64
  unzip-6.0-46.el8.x86_64

Complete!
```

- 설치 진행 및 설치 완료

```
useungmin — root@localhost:/home/test-redhat — ssh root@10.6.71.112 — 98×26
[root@localhost test-redhat]# systemctl status b9daemon.service
● b9daemon.service - AppC b9daemon service
   Loaded: loaded (/usr/lib/systemd/system/b9daemon.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2024-01-18 10:41:34 KST; 4min 3s ago
 Main PID: 2444 (b9daemon)
    Tasks: 36 (limit: 49612)
   Memory: 1.0G
   CGroup: /system.slice/b9daemon.service
           └─2444 /opt/bit9/bin/b9daemon

Jan 18 10:41:30 localhost.localdomain systemd[1]: Starting AppC b9daemon service...
Jan 18 10:41:30 localhost.localdomain b9daemon[2370]: b9daemon called by start
Jan 18 10:41:30 localhost.localdomain b9daemon[2370]: Checking b9k_87201 Driver
Jan 18 10:41:30 localhost.localdomain b9daemon[2370]: Looking if modules directory is updated
Jan 18 10:41:34 localhost.localdomain b9daemon[2370]: insmod /lib/modules/4.18.0-193.el8.x86_64>
Jan 18 10:41:34 localhost.localdomain b9daemon[2370]: insmod /lib/modules/4.18.0-193.el8.x86_64>
Jan 18 10:41:34 localhost.localdomain b9daemon[2370]: Starting b9daemon: [  OK  ]
Jan 18 10:41:34 localhost.localdomain systemd[1]: Started AppC b9daemon service.
```

- 센서 동작 확인



- 에이전트 프로세스 동작 확인

정책 : 소프트웨어 정책

개요

Carbon Black App Control Software Rules 메뉴에 대한 상세 설명입니다.

정책 소개

> 소프트웨어 정책 메뉴 : [App Control] 웹 콘솔 접속 > [Rules] 메뉴 - 'Software Rule' 클릭 후 이동

정책 등록 시에 활용되는 파일,소프트웨어 등 바이너리는 엔드포인트 센서 스캔을 통해 등록됩니다.
처음으로 에이전트를 배포한 엔드포인트에서 전체 바이너리에 대해서 첫 등록 절차를 밟게 되니, 조직 내에서 첫 배포하는 운영체제 유형 등에 대해 영향을 받을 수 있으므로 클린 OS에 먼저 설치하여 기준 정책을 정의하여 사용함을 권장합니다.

1. Updaters

1.1.정책 설명

Select 35	Name	Platforms	Enabled	Date Created	Created By	Date Modified	Last Modified By
Enabled: Yes		**10 item(s)**					
	Allow Printer Installations	Windows	Yes	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System
	Apple System Performance	Mac	Yes	Feb 18 2024 04:46:27 PM	System	Feb 18 2024 04:46:27 PM	System
	Detection of Linux Shutdown sequence	Linux	Yes	Feb 18 2024 04:46:19 PM	System	Feb 18 2024 04:46:19 PM	System
	Linux Self Protection	Linux	Yes	Feb 18 2024 04:46:28 PM	System	Feb 18 2024 04:46:28 PM	System
	Linux System Performance	Linux	Yes	Feb 18 2024 04:46:19 PM	System	Feb 18 2024 04:46:19 PM	System
	Mac App Store Downloads	Mac	Yes	Feb 18 2024 04:46:18 PM	System	Feb 18 2024 04:46:18 PM	System
	Mac System Updates	Mac	Yes	Feb 18 2024 04:46:19 PM	System	Feb 18 2024 04:46:19 PM	System
	Microsoft .NET Framework	Windows	Yes	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System
	Windows 8, 10 and Server 2012 Updates	Windows	Yes	Feb 18 2024 04:46:18 PM	System	Feb 18 2024 04:46:18 PM	System
	Windows Update Temporary Files - Do Not Report	Windows	Yes	Feb 18 2024 04:46:18 PM	System	Feb 18 2024 04:46:18 PM	System
Enabled: No		**54 item(s)**					
	Adobe Acrobat Reader 10.0	Windows	No	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System
	Adobe Acrobat Reader 9.0	Windows	No	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System
	Adobe Acrobat Reader DC	Windows	No	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System

Updaters 정책은 승인되지 않은 업데이트 프로그램을 통해 악성 프로그램이 유입되는 동작을 방지하기 위한 정책입니다.
Carbon Black App Control 에 정의된 업데이트 프로그램에 대한 허용 여부를 선택하여 사용합니다.
업데이트 프로그램을 허용한 경우 프로그램을 통한 소프트웨어 업데이트가 진행하며, 업데이트 프로그램을 허용하지 않은 경우 프로그램을 통한 소프트웨어 업데이트가 진행되지 않습니다.
Updaters 정책의 경우, Carbon Black File Reputation 연동을 통해 최신 버전으로 자동 업데이트 진행됩니다.
또한 Carbon Black 에서 직접 제공 및 관리하는 정책이므로, 사용자가 추가 또는 수정하여 사용할 수 없습니다.

2. Rapid Configs

2.1.정책 설명

Select 3	Name	Description	Enabled	Configured	Platform	Modified By	Policy
	Browser Protection	Reports or prevents potentially malicious behavior related to browsers. This includes execution of files downloaded by browsers, modification of the hosts file, and modification of browser related registry entries. Minimum Carbon Black App Control agent version to use this Rapid Config is 8.0.0.	No	No	Windows	System	All Current and Future Policies
	Carbon Black App Control Server Tamper Protection	Provides protection against tampering with the Carbon Black App Control Server. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.	No	Yes	Windows	System	All Current and Future Policies
	Carbon Black EDR Tamper Protection	Prevents tampering with Carbon Black EDR. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.	No	Yes	Windows	System	All Current and Future Policies
	Cryptomining Protection	Reports or prevents potentially malicious behavior related to file based cryptomining attacks. Minimum Carbon Black App Control agent version to use this Rapid Config is 8.0.0.	No	No	Windows	System	All Current and Future Policies
	Delivery Optimization	Approve files written by the Delivery Optimization Service (DoSvc). This Rapid Config is not needed for agents running version 8.1 and later because files written by the Delivery Optimization Service will automatically be approved in those versions. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.	No	Yes	Windows	System	All Current and Future Policies
	Domain Controller Logon Scripts	Allows and optionally promotes all files under the Sysvol and NetLogon directories of the specified domain controllers if an agent is a member of the specified domain. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.	No	No	Windows	System	All Current and Future Policies
		Protect against the exploit known as Doppelganging on windows systems. Reference: https://communitv.carbonblack.com/docs/DOC-					

Rapid Configs 정책은 파일에 대한 허용 및 차단 등의 초기 정책 구성이 필요한 App Control의 제품의 특성을 고려하여, 사용자들이 보다 빠르게 안전한 엔드포인트 환경을 구성할 수 있는 정책입니다.
자주 사용되는 공격 기법을 방지하여 보안을 강화하거나 자주 사용되는 소프트웨어에 대한 승인 또는 변조 방지 정책을 미리 지정되어 있어 관리자가 보다 빠른 보안 환경 구성을 도와줍니다.
Updater 정책과 동일하게 Carbon Black 에서 직접 제공 및 관리하는 정책이므로, Carbon Black File Reputation 연동을 통해 활성화하며 최신

버전으로 자동 업데이트 진행됩니다. 따라서 사용자가 추가 또는 수정하여 사용할 수 없습니다.

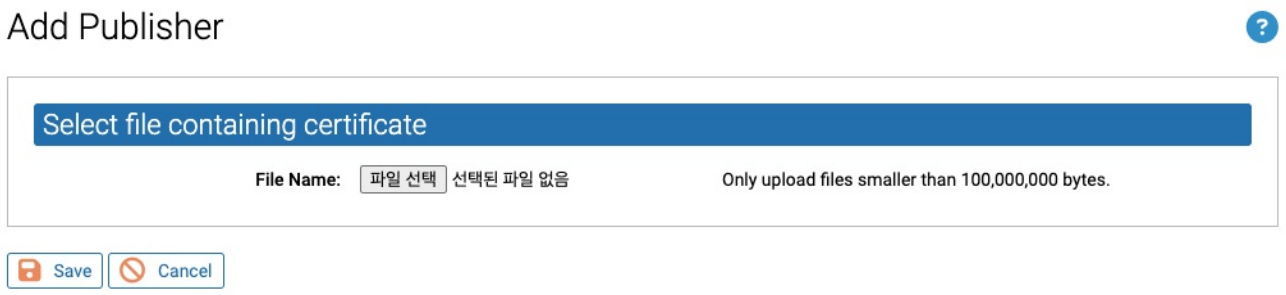
3. Publishers

3.1.정책 설명

Select 28	Name	State	Date Approved or Banned	Approved or Banned By	First Seen Date	Trust	Acknowledged	First Seen Com
	Windows Community Toolkit (.NET Foundation)	Unapproved			Feb 18 2024 05:03:15 PM	Not trusted (Unknown)	No	ETVS\SEUNGM
	Newtek Inc	Unapproved			Feb 18 2024 05:05:48 PM	Not trusted (Unknown)	No	ETVS\SEUNGM
	Microsoft Dynamic Code Publisher	Unapproved			Feb 18 2024 05:09:23 PM	Not trusted (Unknown)	No	ETVS\SEUNGM
	Microsoft Corp Enclave Signer	Unapproved			Feb 18 2024 05:10:09 PM	Not trusted (Unknown)	No	ETVS\SEUNGM
	Microsoft Windows Early Launch Anti-malware Publisher	Unapproved			Feb 18 2024 05:10:47 PM	Not trusted (Unknown)	No	ETVS\SEUNGM
	SecureTeam Software	Unapproved			Feb 18 2024 05:11:21 PM	Not trusted (Unknown)	No	ETVS\SEUNGM
	Nicholas Anderson	Unapproved			Feb 18 2024 05:13:11 PM	Not trusted (Unknown)	No	ETVS\SEUNGM
	Flexera Software LLC	Unapproved			Feb 18 2024 05:14:40 PM	Not trusted (Unknown)	No	ETVS\SEUNGM
	Microsoft 3rd Party Application Component	Unapproved			Feb 18 2024 05:23:56 PM	Not trusted (Unknown)	No	ETVS\SEUNGM
	Intel Corporation - Client Components Group	Unapproved			Feb 18 2024 05:24:34 PM	Medium	No	ETVS\SEUNGM
State: Approved		3 item(s)						
	Bit9, Inc.	Approved	Feb 15 2024 11:01:13 PM	System	Feb 15 2024 11:01:12 PM	High	No	
	Bit9, Inc	Approved	Feb 15 2024 11:01:13 PM	System	Feb 15 2024 11:01:13 PM	High	No	
	Carbon Black, Inc.	Approved	Feb 15 2024 11:01:13 PM	System	Feb 15 2024 11:01:13 PM	High	No	

Publishers 정책은 소프트웨어 인증서의 신뢰 여부를 판단하여 악성 소프트웨어 동작을 방지하기 위한 정책입니다.
엔드포인트 스캔을 통해 등록된 소프트웨어 인증서 또는 직접 등록한 소프트웨어 인증서의 승인 여부를 선택하여 소프트웨어 동작을 제어합니다.
Carbon Black 에 대한 소프트웨어 인증서는 기본적으로 허용 규칙이 정의되어 있으나, 그 외 소프트웨어 인증서는 승인 여부 선택이 필요합니다.

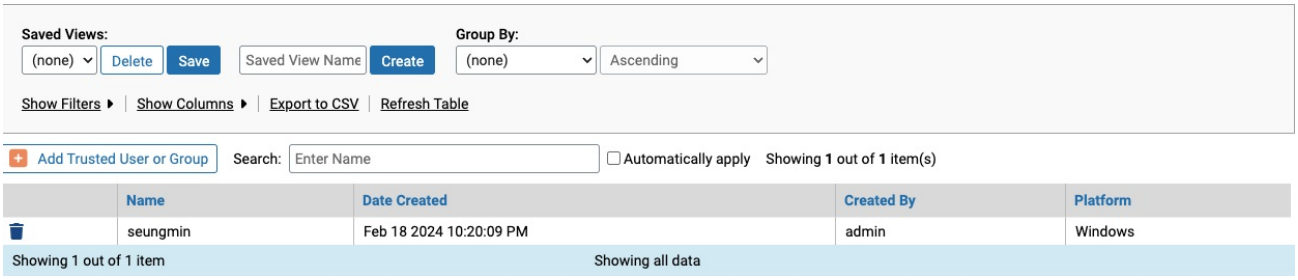
3.2.정책 생성



엔드포인트 센서 스캔을 통해 정의된 소프트웨어 인증서 외에 관리자가 추가하고자 하는 소프트웨어 인증서를 업로드하여 사용 가능합니다.
소프트웨어 인증서 파일의 크기는 100MB 미만으로 제한됩니다.

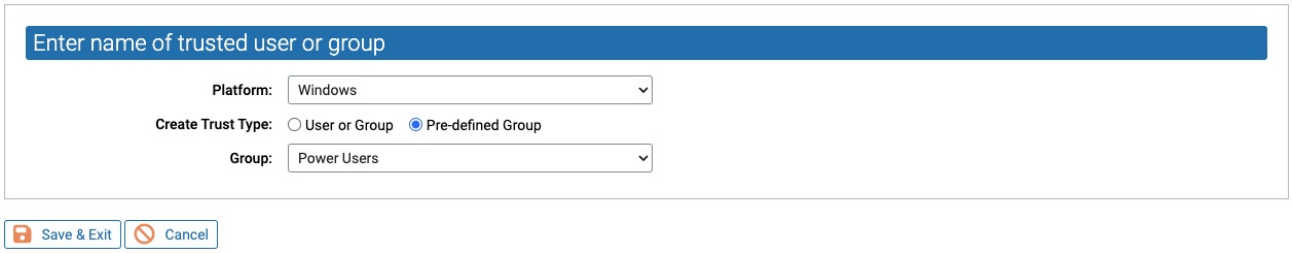
4. Users

4.1.정책 설명



Users 정책은 신뢰있는 사용자 또는 그룹을 정의하여 신뢰되는 사용자 또는 그룹을 통해 정책 상으로 동작하지 않던 엔드포인트의 파일 실행, 소프트웨어 실행 등의 행위를 허용하기 위한 정책입니다.
파일 및 소프트웨어 동작이 정의되어 제어하는 App Control 제품 특성 때문에, 소프트웨어 설치 및 파일 실행에 대해 일시적 허용이 필요한 경우 활용 가능합니다.
지속적인 적용이 필요한 경우 규칙을 분리하여 사용하여 관리도 가능하지만, 단발성 동작의 경우에는 신뢰하는 사용자 및 그룹을 설정하여 파일, 소프트웨어 실행에 대한 예외를 적용하여 편리성을 제공할 수 있습니다.
단, 파일 및 소프트웨어 실행에 대해 차단 정책이 적용된 경우는 사용이 불가합니다.

4.2.정책 생성

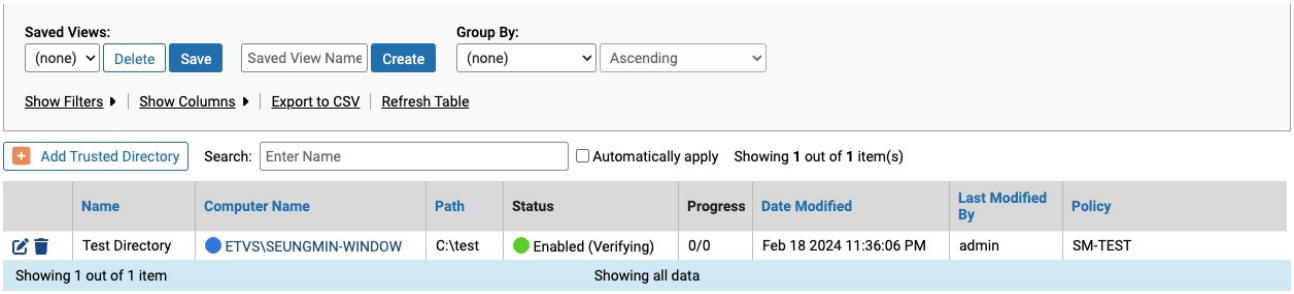


OS 플랫폼 별로 사용자 및 그룹을 입력하여 설정 가능합니다.

- Platform : 사용자 및 그룹의 OS 선택
  - Windows
  - Linux
  - Mac
- Create Trust Type : 신뢰 유형 지정
  - User : 사용자 계정 지정
  - Group : 사용자 그룹 지정
  - Pre-defined Group (Windows 만 지원) : 미리 정의된 사용자 그룹 선택

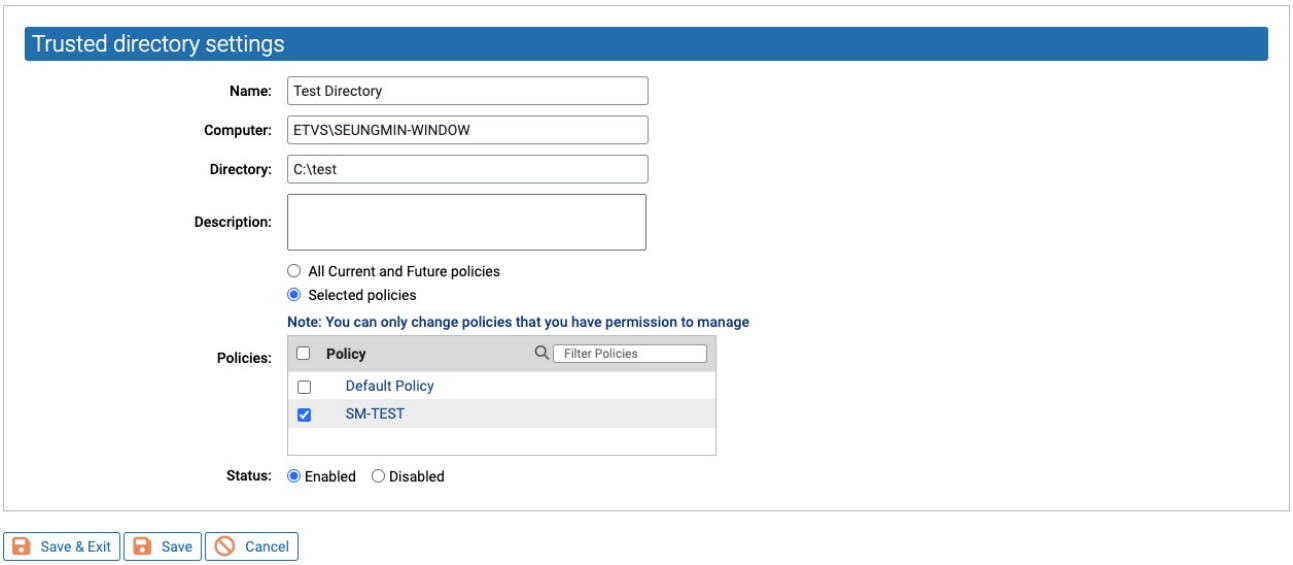
5. Directories

5.1.정책 설명



Directories 정책은 컴퓨터 내의 신뢰할 수 있는 폴더 경로를 지정하여, 해당 폴더 내의 파일 및 프로세스 행위를 허용하기 위한 정책입니다.
Windows OS의 경우 신뢰하는 폴더 내의 파일 및 프로세스 행위에 대한 제한은 없습니다. 그러나 커널 등의 권한 상승이 필요한 Linux 및 Mac OS의 경우 신뢰하는 폴더 내에 파일에 대하여 분석하거나 (테스트 필수..!)

5.2.정책 생성



신뢰하는 폴더 경로를 생성합니다.

- Name : 정책 이름
- Computer : 정책을 지정할 엔드포인트의 컴퓨터 이름 (ex : Windows - 도메인 이름\컴퓨터 이름, Other - 컴퓨터 이름\도메인)
- Diretory : 신뢰할 폴더 경로 지정
- Description : 정책 설명
- Policies : 정책 적용 범위
  - All Current and Future Policies : 모든 정책에 적용
  - Selected Policies : 선택한 정책에만 적용
- Status : 정책 활성화 여부
  - Enabled : 활성화
  - Disabled : 비활성화

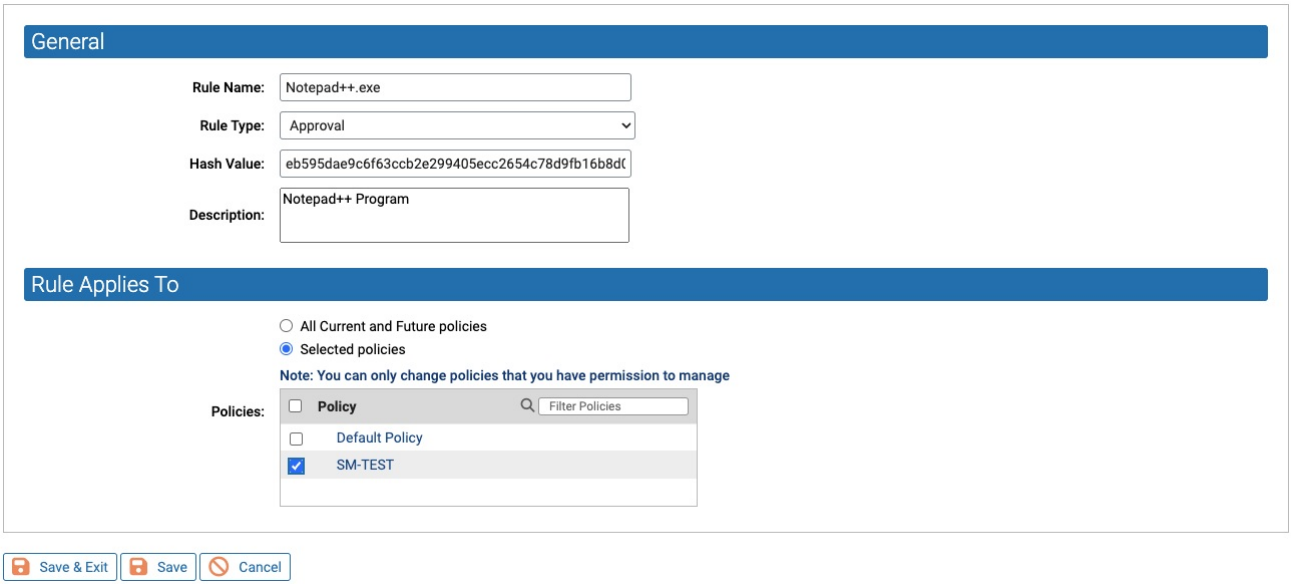
6. Files

6.1.정책 설명

Select 100	Type	Name	File Hash	Source	Is Global
Type: Approval			**240 item(s)**		
	Approval	B9CustomAction.dll	d7103f91ecf520fdfcf600c6bc24b1139d663be69f4a8a3376369b19ab374bce	Trusted Directory	Yes
	Approval	ParityAgentDB.dll	ec337f688a2045bf7210183493618c39662b20d38777547487d5e8bfe26325b3	Trusted Directory	Yes
	Approval	cb7zip.dll	96b0ddd51e2027b56ea499a4cd178246d9f3859bd252afd2dd04206702aa69b0	Trusted Directory	Yes
	Approval	Crawler.exe	cc85f2e65b0d1add8ebafa31558e62bcaa37745addc68a6e8f7b9f31753ec601	Trusted Directory	Yes
	Approval	DasCLI.exe	6581d9cc447c4dfe954e9b2cd674db89003d0f6914db0d3de7a5e5ebd5a52a86	Trusted Directory	Yes
	Approval	dbghelp.dll	1e3770a286d59b0a300535ff0c47696353c6549ea668aba1d81ee798e0ebd373	Trusted Directory	Yes
	Approval	ipworks8.dll	3d66133777b880f7ef677c414627482b99de340987402507cd27d308890eca0b	Trusted Directory	Yes
	Approval	ipworkssl8.dll	2242e0440836426c2d8cb8ee2a39a7392aaa24d8b8256637e649a1cedb9fa0e2	Trusted Directory	Yes
	Approval	Notifier.exe	04f29147aae5cb95fbeae1bdf26b59549d9d513c3fc62f32f00ff712326f36c7	Trusted Directory	Yes
	Approval	NotifierMessages.dll	bba0a01a7809e1637e099749880f8ccaf8c6aa2055fb6c529a9be068196b6fdb	Trusted Directory	Yes
	Approval	Parity.exe	d6f884090619a9bca3c49264e031247f2aece394cdfb8761a145db8133ebf8e0	Trusted Directory	Yes
	Approval	TimedOverride.exe	bd97271776eb667c3961c9978c601abcc73af7b66de9f3ecf9bae1ac50285355	Trusted Directory	Yes

Files 정책은 엔드포인트 내에서 신뢰되지 않은 프로그램이 실행되어 악성 행위를 진행하는 것을 방지하는 정책입니다.
파일의 해시값을 수집하고 이를 대상으로 실행 가능 여부를 판단하고 정의하여 사용이 가능합니다.
파일의 동작을 차단하는 기능인 만큼 오탐으로 인한 문제 상황이 발생되지 않도록, 모니터링 기능도 제공하여 관리자가 충분한 검토 후에 정책 적용이 진행됩니다.
또한 관리자가 파일의 신뢰 여부를 판단할 수 있도록 각 파일에 대한 세부 정보도 확인할 수 있습니다.
파일은 센서를 통해 수집되며, 수집되는 파일의 대상은 실행이 가능한 파일과 확장자가 일치하는 스트립트 파일입니다.

6.2.정책 생성



실행파일 및 스크립트 파일에 대한 정책을 생성합니다.

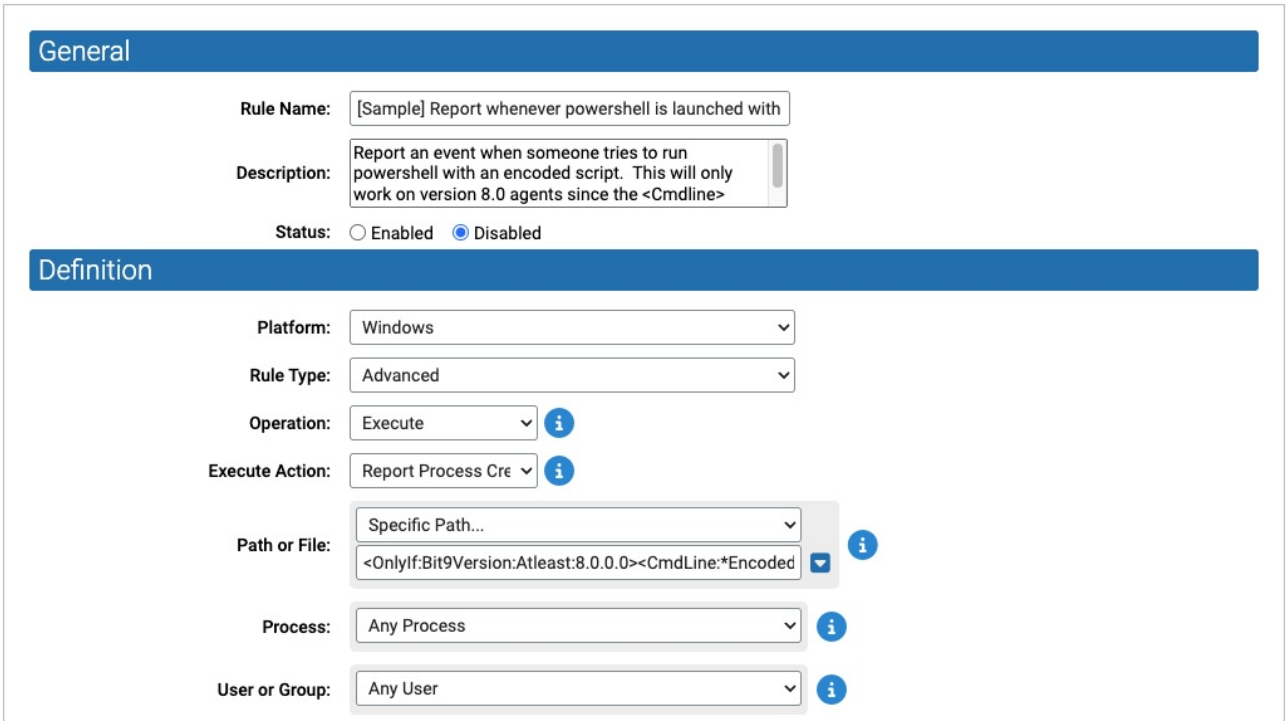
- Rule Name : 파일 규칙 이름
- Rule Type : 파일 실행 승인 여부
  - Approval : 승인
  - Ban : 차단
  - Ban (Report Only) : 모니터링
- Hash Value : 파일 해시값
- Description : 파일 규칙 설명
- Policies : 정책 적용 범위 지정
  - All Current and Future Policies : 전체 정책 적용
  - Selected Policies : 선택 정책 적용

7. Custom

7.1.정책 설명

Rule Type	Name	Action	Operation	Path
Advanced	Mac User Cache App Files	Track	Write, Write Delayed, Delete, Renam...	/Users/*/Library/Caches/*app/Conte
Performance Optimization	Mac User Data Files	Ignore	Write, Write Delayed, Delete, Renam...	/Users/*/Library/Application Support
Performance Optimization	Time Machine	Ignore	Write, Write Delayed, Delete, Renam...	*
Performance Optimization	Ignore Linux Log Files	Ignore	Write, Write Delayed, Delete, Renam...	/var/log/*
Advanced	Track system profile	Track	Write, Write Delayed, Delete, Renam...	<System>\Config\systemprofile*
Advanced	[Sample] Microsoft App-V Interoperability	Exec [Allow, Finish Rule Group] Wri...	Exec [Execute, Script Execute] Writ...	\device\sftvol*
Performance Optimization	[Sample] Visual Studio - Ignore Intermediate Files	Ignore	Write, Write Delayed, Delete, Renam...	*.obj (multiple)
Execution Control	[Sample] Visual Studio - Approve Builds	Finish Rule Group, Promote Target P...	Script Execute, Process Create	<Reg:HKLM-SoftwareX86\Classes\CI
Performance Optimization	[Sample] VMware Workstation	Ignore	Write, Write Delayed, Delete, Renam...	*
Performance Optimization	[Sample] TortoiseSVN	Ignore	Write, Write Delayed, Delete, Renam...	*
Execution Control	Allow .NET dll executions	Allow, Finish Rule Group	Execute, Script Execute	*.dll
Performance Optimization	Ignore Recycle Bin	Ignore	Write, Write Delayed, Delete, Renam...	<RecycleBin>

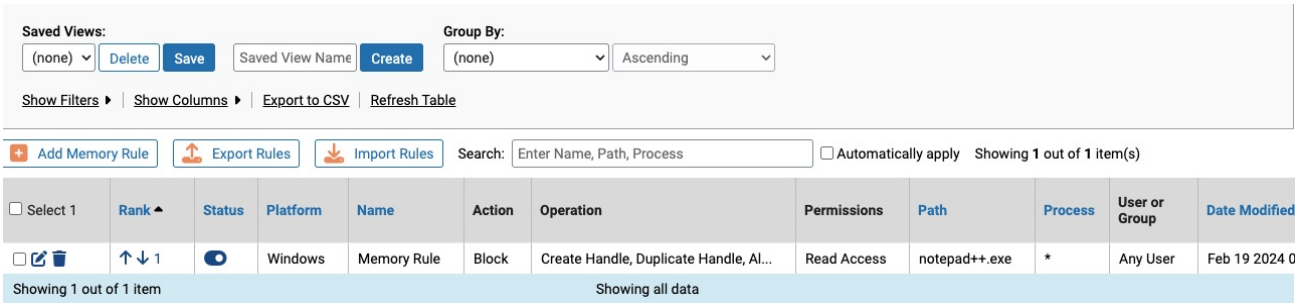
7.2. 정책 생성



테스트 필요함

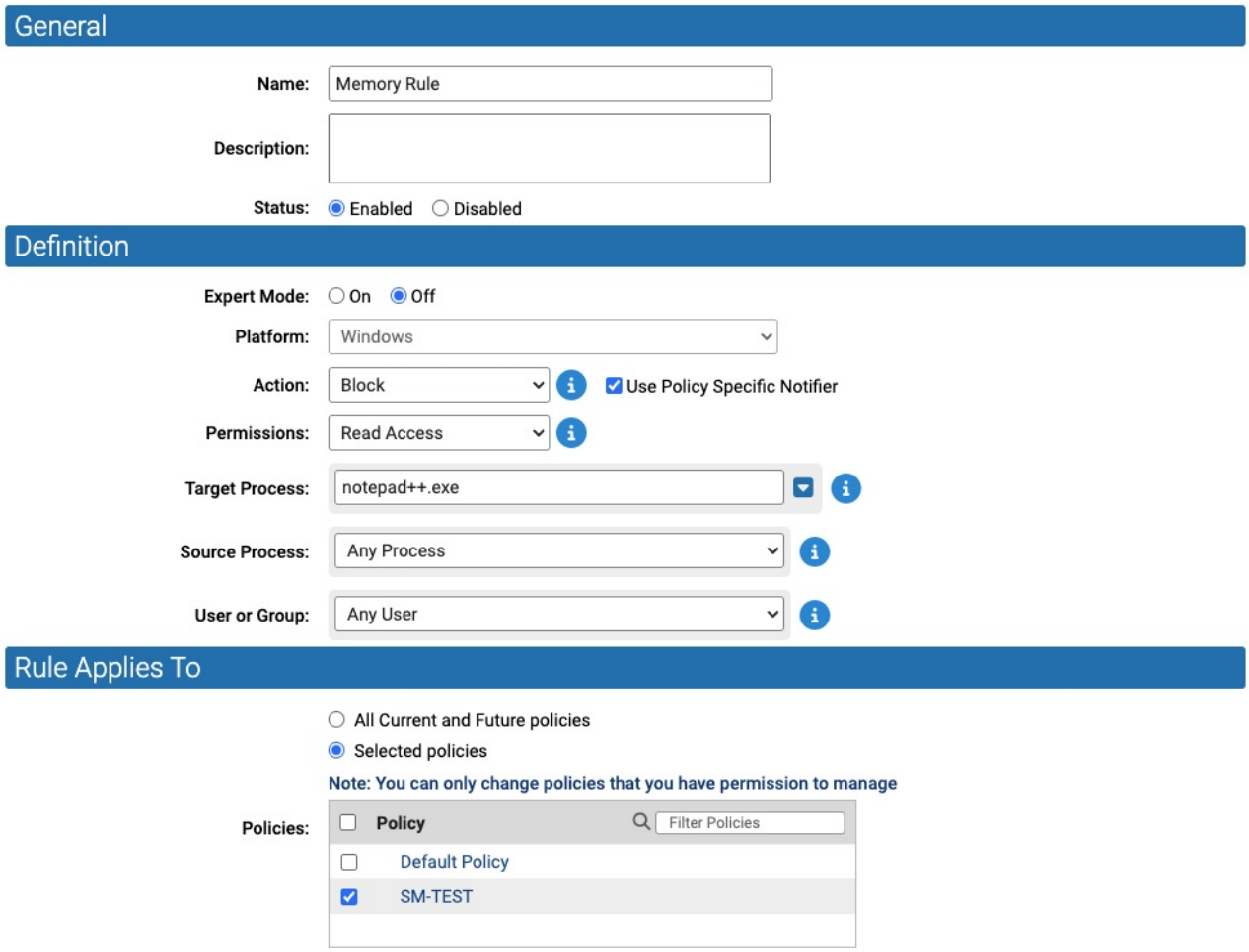
8. Memory

8.1. 정책 설명



Memory 정책은 인-메모리 공격, 파일리스 공격 등으로부터 메모리를 통한 공격 기법을 방지하기 위한 정책입니다.
지정된 실행 파일 내에 다른 실행파일 또는 사용자(그룹)가 메모리에 접근하거나 수정하지 못하도록 정의하여 사용이 가능합니다.
이는 메모리 공격을 시도하거나, 메모리 공격 발생했을 때에, 발생한 공격이 환경 내로 더 이상 확산되지 않도록 실행파일 내 메모리 접근 및 수정 등의 행위를 차단하여 환경을 보호합니다.

8.2. 정책 생성



살행 파일에 대한 메모리 정책을 생성합니다.

- Name : 정책 이름
- Description : 정책 설명
- Status : 정책 사용 여부
- Expert Mode : 전문가 모드 사용 여부
- Platform : Windows OS만 선택 가능
- Action : 메모리 접근 및 수정 행위 발생 시에 동작 방식 선택
  - Block : 차단
  - Prompt : 센서 알림 메세지를 통해 차단 및 허용 여부 선택
  - Report : 이벤트 발생
  - Allow : 허용
  - Block Silently : 센서 알림 메세지 및 이벤트 생성없이 차단
- Permissions : 대상 실행 파일에 허용 또는 차단할 권한 유형 선택
  - Control Process : 프로세스 제어 권한
  - Read Access : 읽기 엑세스 권한
  - Write Access : 쓰기 엑세스 권한
  - Write + Control : 읽기 및 제어 권한
  - Read + Write + Control : 읽기 및 쓰기 및 제어 권한
  - Dynamic Code Execution : 동적 코드 실행 권한
  - Kernel Memory Access : 사용자 프로세스의 커널 메모리 엑세스 권한 (Windows XP 만 지원)
  - Advanced : 세부 제어 설정
- Target Process : 메모리 제어 대상 프로세스
- Source Process : 권한 제어 대상 프로세스
- User or Group : 권한 제어 대상 사용자 또는 그룹
- Policies : 정책 적용 범위

9. Registry

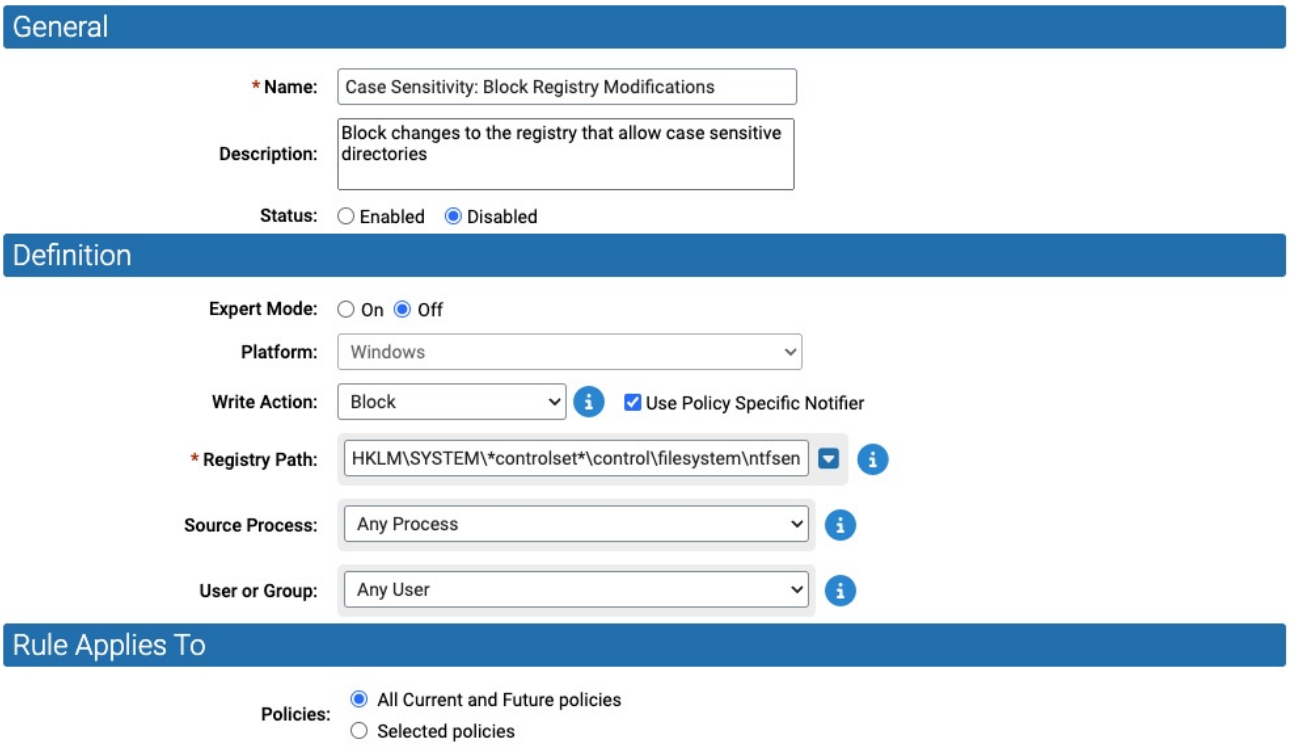
9.1. 정책 설명

Select 7	Rank	Status	Platform	Name	Action	Operation	Path
	1		Windows	Case Sensitivity: Block Registry Modifications	Block, Finis	Create Key, Rename Key, Delete Key,...	HKLM\SYSTEM*controlset*\control\filesystem
	2		Windows	[Sample] Block Suspicious System Changes	Block, Finis	Create Key, Rename Key, Delete Key,...	HKLM\software\microsoft\windows nt\current
	3		Windows	[Sample] Prompt on Suspicious changes to Start	Prompt, Fir	Create Key, Rename Key, Delete Key,...	*\software\microsoft\windows\currentversion\
	4		Windows	[Sample] Report Typical Changes to Startup Files	Report	Create Key, Rename Key, Delete Key,...	*\software\microsoft\windows\currentversion\
	5		Windows	[Sample] Report Changes to Trusted Zones	Report	Create Key, Rename Key, Delete Key,...	*\software\microsoft\windows\currentversion\
	6		Windows	[Sample] Report Changes to Home Page or Searc	Report	Create Key, Rename Key, Delete Key,...	*\software\microsoft\internet explorer\main\D
	7		Windows	Autostart Rules	Report	Create Key, Rename Key, Delete Key,...	<AutostartRules>

Registry 정책은 코드 삽입, 파일리스 공격 등으로부터 실행 프로그램에 대한 레지스트리 값이 악의적으로 변경되는 것을 방지하기 위한 정책입니

다. 다른 실행 프로그램 또는 사용자(그룹)이 지정된 레지스트리 경로 값을 수정하지 못하도록 정의하여 사용이 가능합니다.

9.2. 정책 생성



레지스트리에 대한 레지스트리 정책을 생성합니다.

- Name : 정책 이름
- Description : 정책 설명
- Status : 정책 사용 여부
- Expert Mode : 전문가 모드 사용 여부
- Platform : Windows OS만 선택 가능
- Write Action : 쓰기 행위 발생 시에 동작 방식 선택
  - Block : 차단
  - Prompt : 센서 알림 메세지를 통해 차단 및 허용 여부 선택
    Report : 이벤트 발생
    Allow : 허용
- Registry Path : 제어 대상 레지스트리
- Source Process : 권한 제어 대상 프로세스
- User or Group : 권한 제어 대상 사용자 또는 그룹
- Policies : 정책 적용 범위

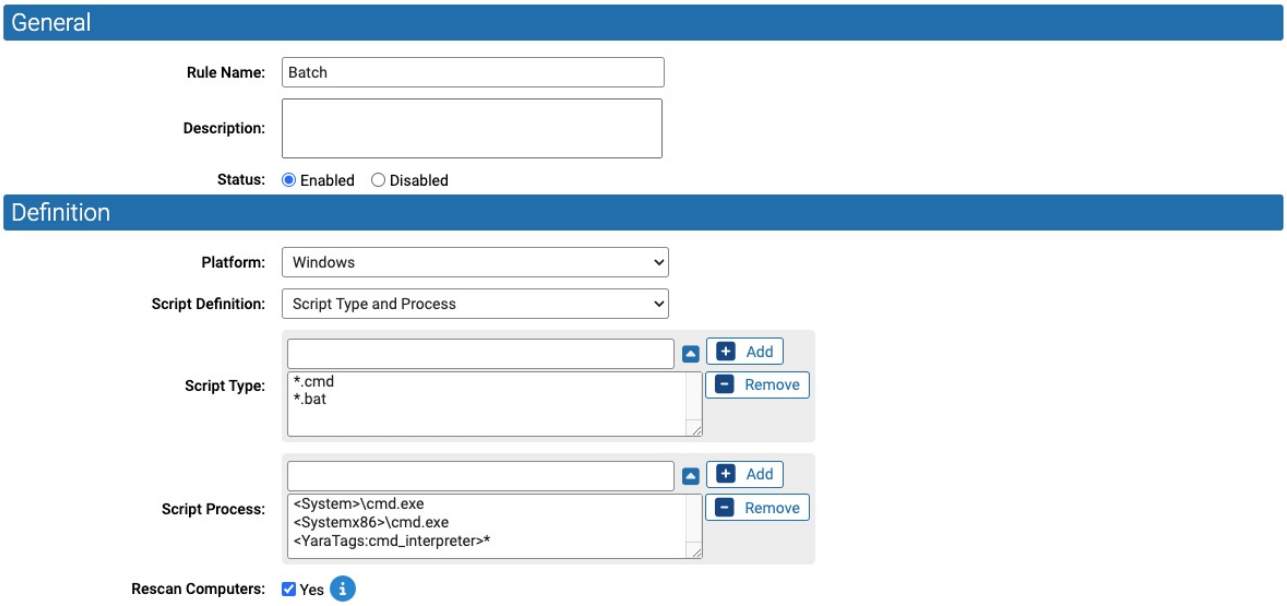
10. Scripts

10.1. 정책 설명

	Name	Type	Process	Enabled	Date Modified	Last Modified By
	Batch	*.cmd, *.bat	<System>\cmd.exe, <Systemx86	Yes	Feb 18 2024 04:45:53 PM	System
	Registry	*.reg	<System>\reg.exe, <Systemx86>	Yes	Feb 18 2024 04:45:53 PM	System
	Visual Basic	*.vb, *.vbe, *.vbs, *.wsh, *.wsf	<System>\cscript.exe, <Systemx	Yes	Feb 18 2024 04:45:53 PM	System
	Java	*.class, *.jar	*\java.exe, *\javaw.exe, <YaraTa	Yes	Feb 18 2024 04:45:53 PM	System
	Perl	*.pl, *.pm	*\perl.exe, <YaraTags:perl_interp	No	Feb 18 2024 04:45:53 PM	System
	Python	*.py, *.pyc, *.pyo, *.pyw	*\python.exe, *\pythonw.exe, <Ya	No	Feb 18 2024 04:45:53 PM	System
	PowerShell	*.ps1, *.psm1	*\powershell.exe, <YaraTags:pov	Yes	Feb 18 2024 04:45:53 PM	System
	TCL	*.tcl	*\wish.exe, *\tclsh.exe	No	Feb 18 2024 04:45:53 PM	System
	Ruby	*.rb	*\ruby.exe, *\rubyw.exe, <YaraTa	No	Feb 18 2024 04:45:53 PM	System

Scripts 정책은 확장자 및 프로세스 등의 규칙을 입력하여, App Control 센서에서 스크립트로 인식할 수 있는 파일을 정의하는 정책입니다.
Carbon Black App Control 의 수집 대상은 실행이 가능한 파일과 스트립트 파일입니다. App Control 에서 스트립트 파일을 인식하는 기준은 스크립트 정책으로 구별하여 정의합니다.
Carbon Black에서 사전에 정의한 표준 스크립트 규칙을 제공하고 있으나, 관리자가 별도로 추가하여 사용 가능합니다.

10.2. 정책 생성



스크립트 규칙을 지정하기 위한 스크립트 정책을 생성합니다.

- Rule Name : 정책 이름
- Discription : 정책 설명
- Status : 정책 사용 여부
- Platform : 정책 적용 OS
- Script Definition : 스크립트 유형 정의
  - File Association (Windows OS만 지원) : 응용 프로그램이 연결된 파일
  - Script Type and Process : 스크립트 및 프로세스 파일
- Script Type : 스크립트 파일 이름 및 확장자 지정
- Script Process : 스크립트 파일을 실행할 프로세스 지정
- Rescan Computer : 정책과 일치하는 컴퓨터 재확인

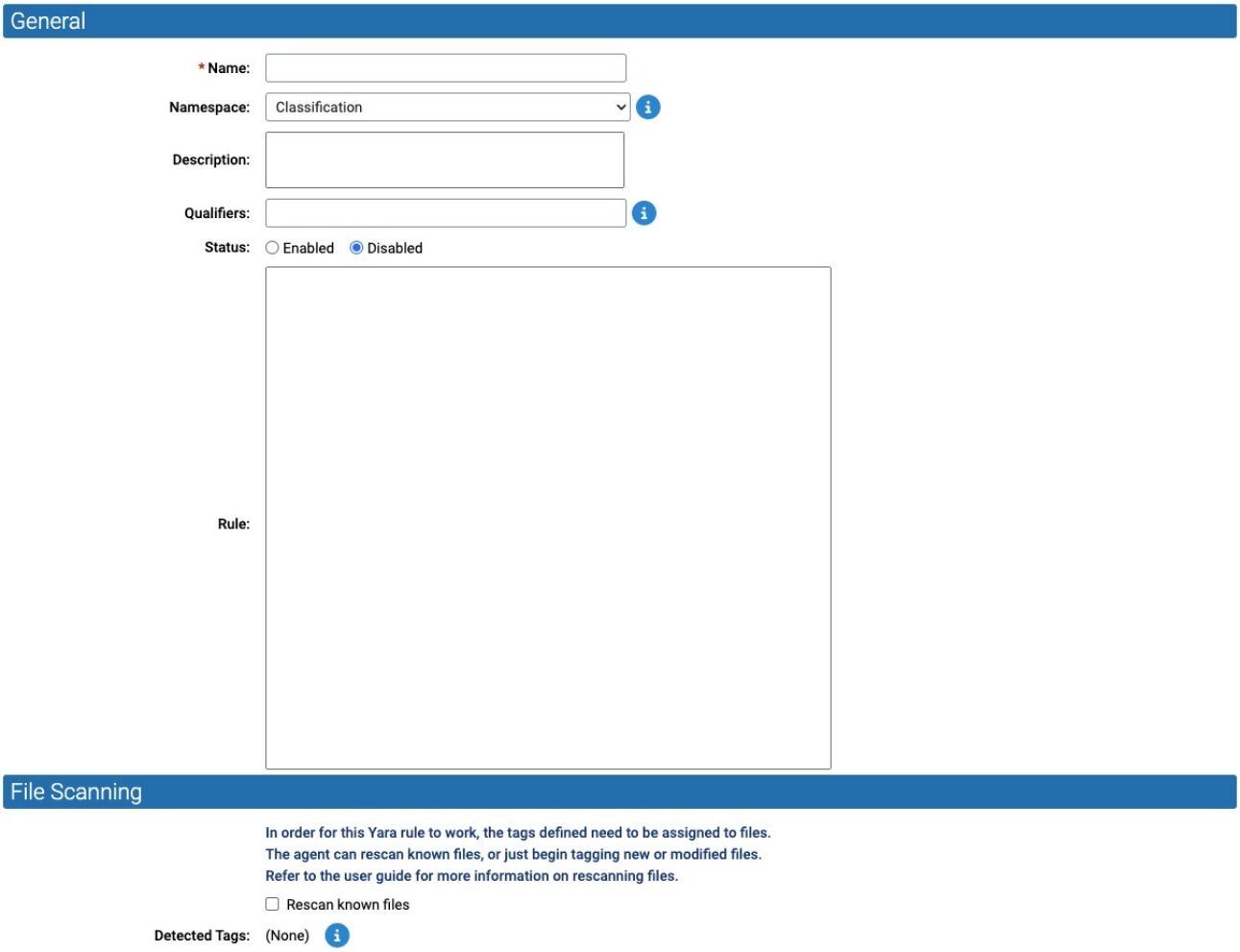
11. Yara

11.1. 정책 설명

	Yara Rule Name	Namespace	Status	Description	Qualifiers
	Python Script Interpreter	Classification	Enabled	Identifies Interpreters for python scripts	<OnlyIf:Bit9Version:Atleast:8.0.0.2454>
	Microsoft HTML Application Interpreter	Classification	Enabled	Identifies Interpreters for HTML applications	
	Ruby Script Interpreter	Classification	Enabled	Identifies interpreters for Ruby scripts	
	Chrome Extension Interpreter	Classification	Enabled	Identifies interpreters for Chrome extensions	
	Mozilla Extension Interpreter	Classification	Enabled	Identifies interpreters for Mozilla extensions (Firefox browser)	
	UPX Packing detector	Classification	Enabled	Identifies UPX packed exes	
	Msiexec detector	Classification	Enabled	Identifies msiexec	
	FileHeader	IsInteresting	Enabled	File header for the IsInteresting rule set. Includes any import	
	Portable Executable	IsInteresting	Enabled	Identifies win32 portable executables and dlls	
	Windows Installers	IsInteresting	Enabled	Identifies windows installers (MSI and MSP)	
	Systems Management Server Installers	IsInteresting	Enabled	Identifies Microsoft SMS installers	

Yara 정책은 Yara 규칙을 통해 악성코드를 식별하여, 파일 및 스크립트 내용의 악성 여부를 인식하여 보호하는 정책입니다.
App Control에서 사전 정의된 Yara 오픈소스 툴을 사용하여 컨텐츠 보호가 가능하며, 그 외 관리자가 Yara 규칙을 새롭게 생성하여 사용 가능합니다. Yara 정책의 경우, 악성코드 시그니처 식별하고 있어 환경에 대한 랜섬웨어 공격을 방지하는 데에 유용하게 사용합니다.

11.2. 정책 생성

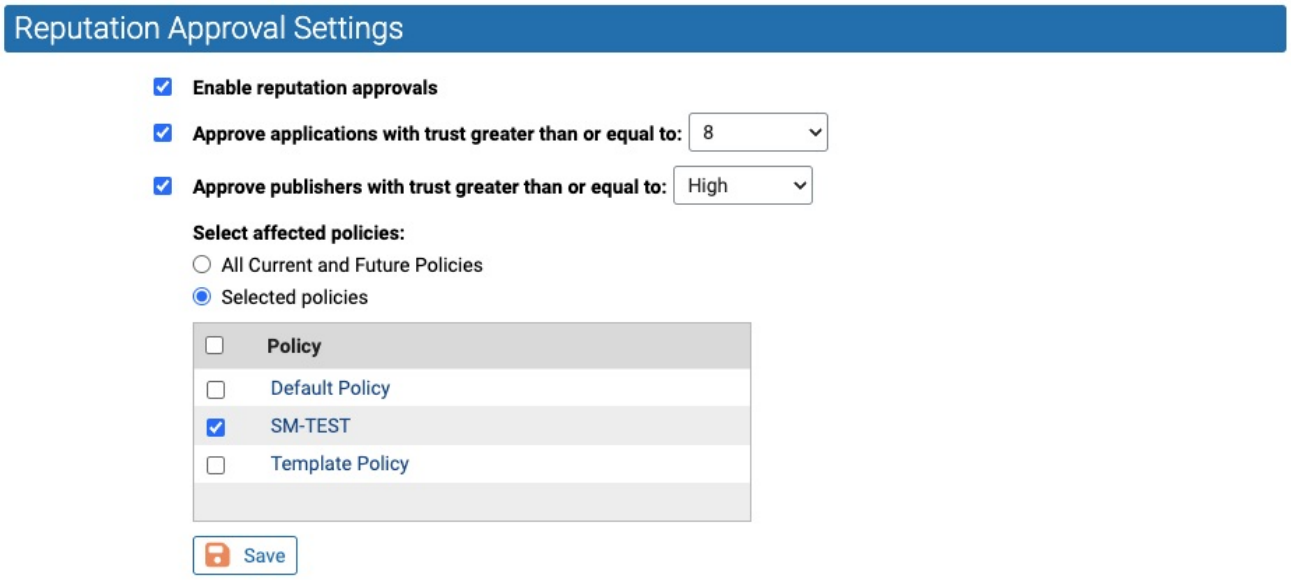


악성코드 식별을 위한 Yara 정책을 생성합니다.

- Name : 정책 이름
- Namespace : 정책 구분
  - Classification : 태그를 기반으로 Custom 정책을 사용하여 작업 수행하는 경우
  - IsInteresting : 자동으로 작업 수행하는 경우
- Description : 정책 설명
- Qualifiers : 정책을 적용할 센서 대상 정의 (작성한 조건에 맞는 센서를 대상으로 정책이 동작)
- Status : 정책 사용 여부
- Rule : 악성코드 식별에 사용할 Yara 규칙 입력
- Rescan known files (Classification 선택 시 사용) : 적용한 규칙에 해당되는 파일이 있는지, 센서가 아는 파일을 기준으로 재검사
- Full scan for new files (IsInteresting 선택 시 사용) : 적용한 규칙에 해당되는 파일이 있는지, 센서가 전체 시스템 기준으로 재검사
- Detected Tags : Carbon Black 에서 제공한 태그를 사용하여 정책 구분

12. Reputation

12.1. 정책 설명



Reputation 정책은 Carbon Black App Control에서 제공되는 파일 평판을 기반하여 파일 사용을 자동으로 승인하는 정책입니다.

Reputation 정책은 Carbon Black File Reputation 를 통해 제공되는 파일의 평판 신뢰도를 기준하여 승인되므로 Carbon Black File Reputation 기능 활성화가 필요한 정책입니다.
인증서와 응용 프로그램이 정책 적용 대상이 되며, 신뢰도의 기준을 단계별로 구분하여 선택 후 사용됩니다.

정책 : 정책 생성

개요

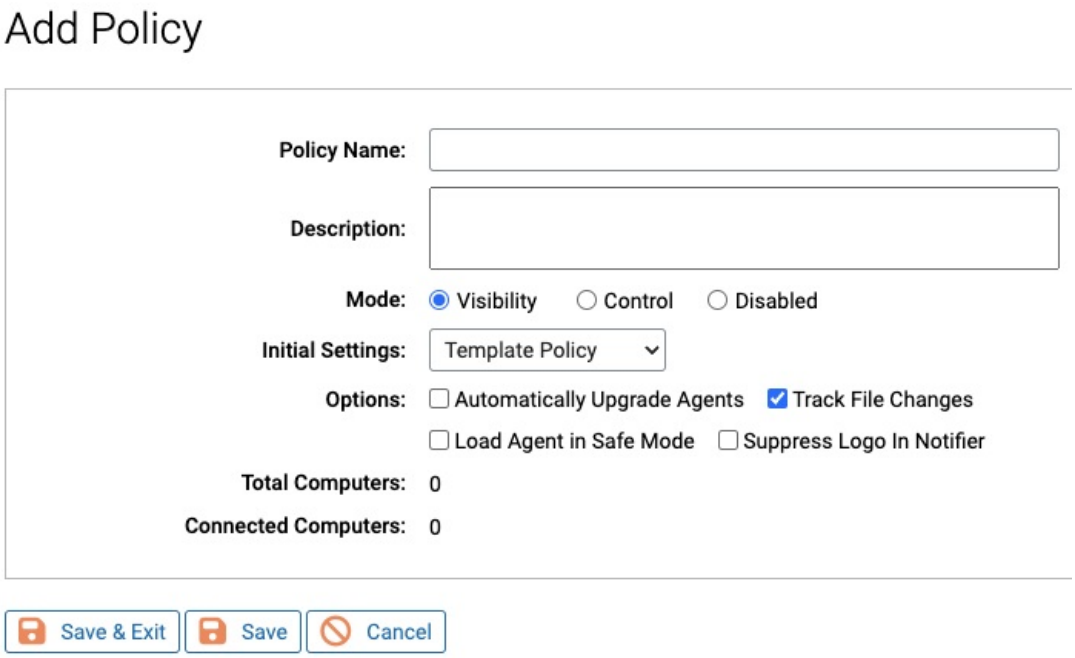
Carbon Black App Control 정책 생성에 대한 가이드 문서 입니다.

기능 소개

1. Policies

1.1 정책 생성

- [App Control] 웹 콘솔 접속 > [Policies] 메뉴 선택 > [Add Policy] 버튼 클릭하여 정책 생성



- 조직별 정책 및 목적별 정책을 생성하여 사용

- Policy Name : 정책 이름
- Description : 정책 설명
- Mode : 서버와 컴퓨터가 통신하는 상태 혹은 통신하지 않는 상태에 대해 동작할 모드 설정
  - Visibility : 파일 활동 및 이벤트 추적하기 위한 모드 (파일 실행/쓰기/금지 영향 없음) - 보안 기능을 인한 동작 방해 없음
  - Control : 파일 실행에 대한 제어 및 단계 설정
    - High (Block Unapproved) : 승인되지 않은 파일 실행 차단 및 이벤트 추적
    - Medium (Prompt Unapproved) : 승인되지 않은 파일 실행 차단 및 사용자가 파일 실행 여부 선택 가능
    - Low (Monitor Unapproved) : 승인되지 않은 파일 실행 허용 및 이벤트 추적
  - Disabled : 파일 활동에 대한 추적 중단 - 에이전트 제거 시 사용
- Initial Settings : 템플릿으로 사용할 정책 선택
- Options
  - Automatically Upgrade Agents : 에이전트에 대한 자동 업그레이드
  - Track File Changes : 파일 추가/삭제/변경 추적
  - Load Agent in Safe Mode (기본값) : 안전 모드에서 에이전트 로드
  - Suppress Logo in Notifier : 에이전트 알림이 발생할 경우 로고를 표시하지 않음
- Total Computer : 정책에 연결된 총 컴퓨터 갯수
- Connected Computer : 정책에 연결된 컴퓨터 중, 서버와 연결된 컴퓨터 개수

1.2 정책 구성

> 정책 별 상세 가이드 : https://bs.etevers.tech/books/carbon-black-app-control-handbook/page/3def1

- [App Control] 웹 콘솔 접속 > [Policies] 메뉴 선택 > '정책' 의 (View Details) 버튼 클릭

Advanced | File Rules | Custom Rules | Memory Rules | Registry Rules | Publisher Rules | Rapid Configs | Computers | Device Control Settings

Name	Status	Notifiers	
Block unanalyzed scripts and executables	Active	<default>: Block unanalyzed scripts and executables	Add Edit
Block unapproved scripts	Active	<default>: Block unapproved scripts	Add Edit
Block unapproved executables	Active	<default>: Block unapproved executables	Add Edit
Block banned file names	Active	<default>: Block banned file names	Add Edit
Block banned file hashes	Active	<default>: Block banned file hashes	Add Edit
Block executables run from a network drive	Off	<default>: Block executables run from a network drive	Add Edit
Block files with banned publishers or certificates	Active	<default>: Block files with banned publishers or certificates	Add Edit
Enforce memory rules	Active	<default>: Enforce memory rules	Add Edit
Enforce registry rules	Active	<default>: Enforce registry rules	Add Edit
Enforce custom (file and path) rules	Active	<default>: Enforce custom (file and path) rules	Add Edit
Enforce tamper protection	Active	<default>: Enforce tamper protection	Add Edit
Terminate processes with banned images	Report Only	<default>: Terminate processes with banned images	Add Edit

☑ Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High

- Advanced : 개별적으로 등록되는 타 정책과 달리 전체 범위에서의 특정 동작에 대한 파일/스크립트 허용 및 차단
  - Active : 활성화
  - Off : 비활성화
  - Report Only : 정책 테스트 - 파일 차단에 대한 로그 기록

Advanced | File Rules | Custom Rules | Memory Rules | Registry Rules | Publisher Rules | Rapid Configs | Computers | Device Control Settings

Show Filters | Show Columns | Export to CSV | Refresh Table

☑ Show Rules That Apply To All Policies

Search: Enter File Hash, Name ☐ Automatically apply Showing **25** out of **240** item(s) Showing **1** out of **1** group(s)

	Type	Name	File Hash	Source Name	Date Modified	Is Global
Type: Approval			**240 item(s)**			
	Approval	B9CustomAction.dll	d7103f91ecf520fdfcf600c6bc24b1139d663be69f4a8a3376369b19ab374bce	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	ParityAgentDB.dll	ec337f688a2045bf7210183493618c39662b20d38777547487d5e8bfe26325b3	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	cb7zip.dll	96b0ddd51e2027b56ea499a4cd178246d9f3859bd252afd2dd04206702aa69b0	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	Crawler.exe	cc85f2e65b0d1add8ebafa31558e62bcaa37745addc68a6e8f7b9f31753ec601	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	DasCLI.exe	6581d9cc447c4dfe954e9b2cd674db89003d0f6914db0d3de7a5e5ebd5a52a86	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	dbghelp.dll	1e3770a286d59b0a300535ff0c47696353c6549ea668aba1d81ee798e0ebd373	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	ipworks8.dll	3d66133777b880f7ef677c414627482b99de340987402507cd27d308890eca0b	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes

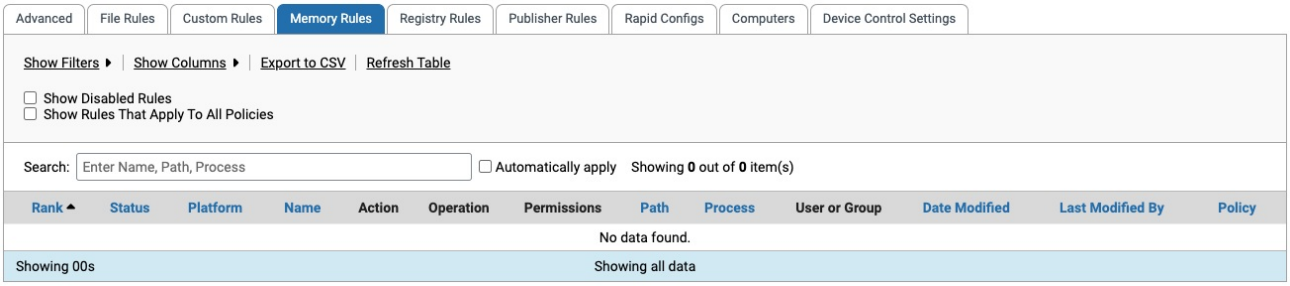
- File Rules : 엔드포인트 설치 시 검출된 파일 또는 사용자가 등록한 개별 파일 해시 값을 통한 파일 승인 및 차단
  - Approval : 파일 실행 허용
  - Ban : 파일 실행 차단
  - Ban (Monitor) : 파일 실행에 대한 이벤트 발생

Advanced | File Rules | Custom Rules | Memory Rules | Registry Rules | Publisher Rules | Rapid Configs | Computers | Device Control Settings

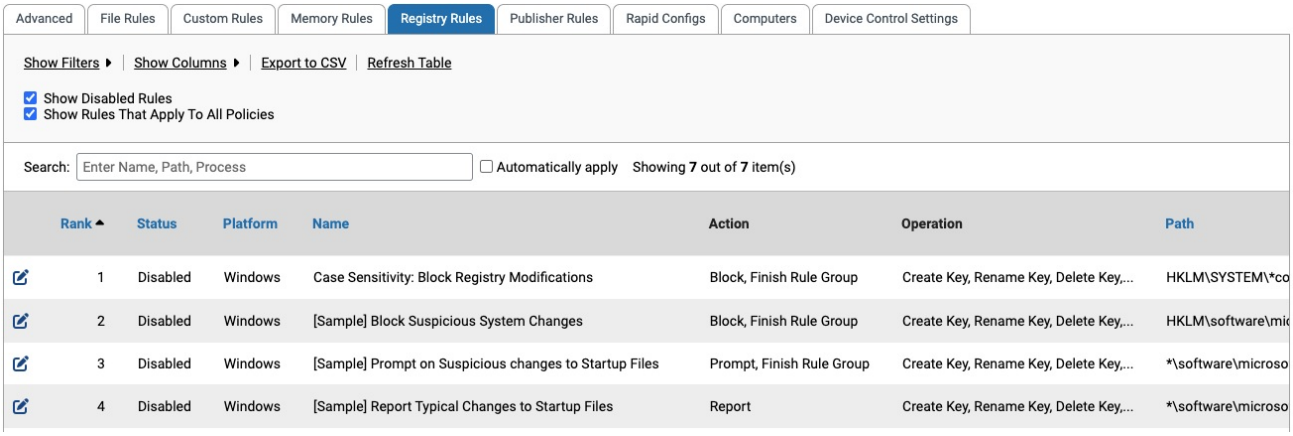
rch: Enter Name, Path, Process ☐ Automatically apply Showing **43** out of **43** item(s)

Rank	Status	Platform	Rule Type	Name	Action
1	Enabled	Windows	Expert	Tag process as msiexec identified by yara	Tag Target
2	Enabled	Windows	Performance Optimization	Ignore system log files	Ignore
5	Enabled	Windows	Expert	Examine powershell script contents	Tag Target
6	Enabled	Windows	Expert	Block powershell scripts that execute memory	Block, Finish Rule Group
8	Enabled	Windows	Expert	Do not treat these processes as .NET applications	Remove Process Tags
9	Enabled	Windows	Expert	Report read-only memory map operations on unapproved executables by .NET applications	Report, Query Reputation
12	Enabled	Windows	Expert	Deny read-only memory map operations on banned executables by .NET applications	Block

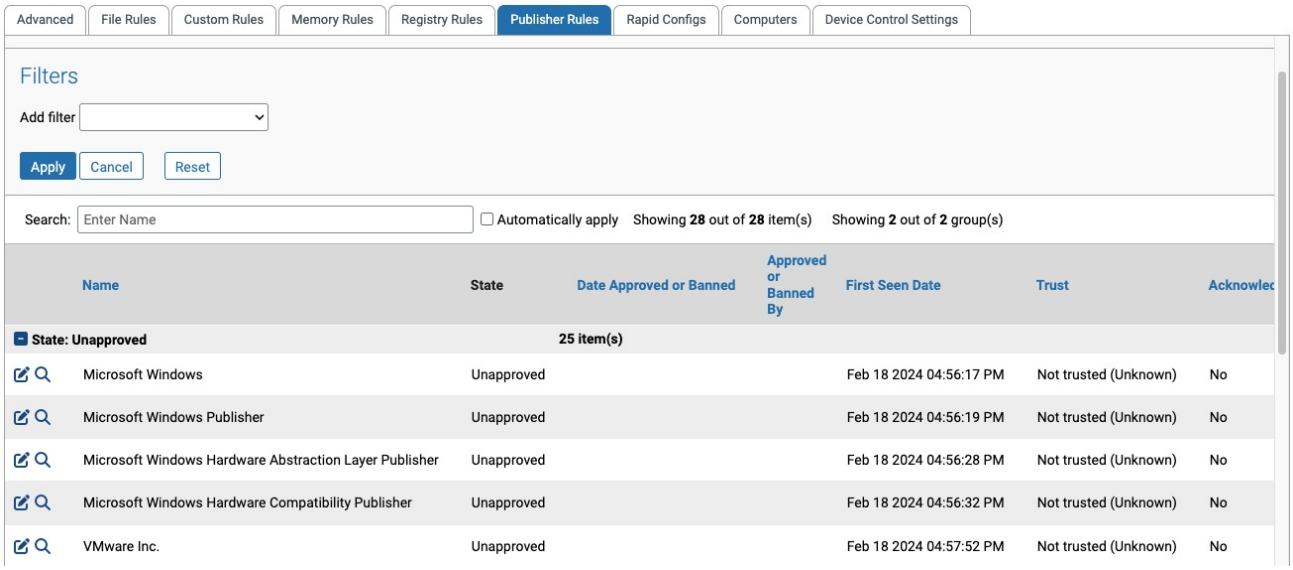
- Custom Rules : 사용자가 소프트웨어 프로세스 행위에 대한 작업 규칙



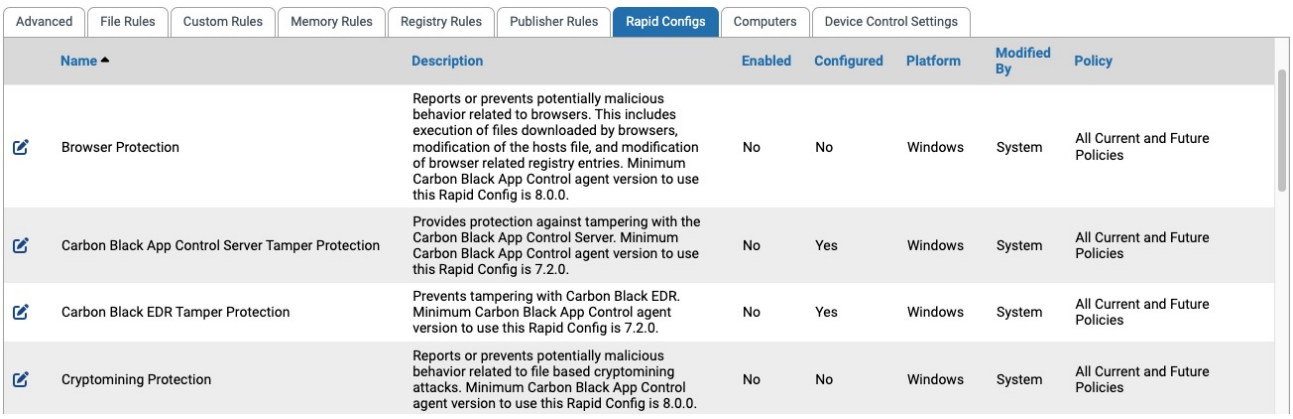
- Memory Rules : 사용자나 프로세스가 특정 프로세스의 메모리에 접근하거나 변경하는 등의 행위 허용 및 차단



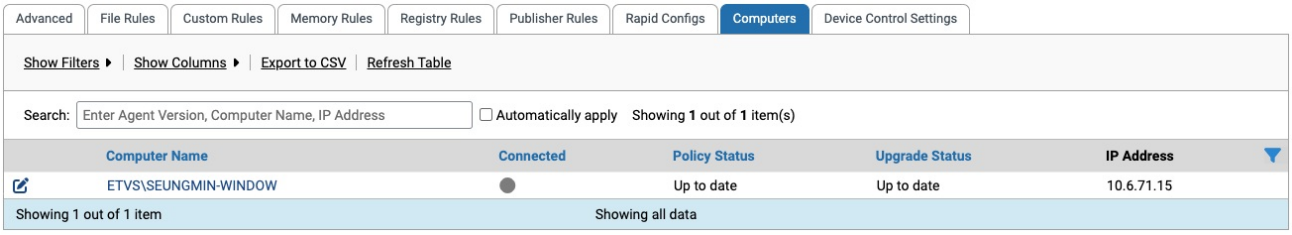
- Registry Rules : Windows OS에서 특정 레지스트리를 변경하는 행위 허용 및 차단



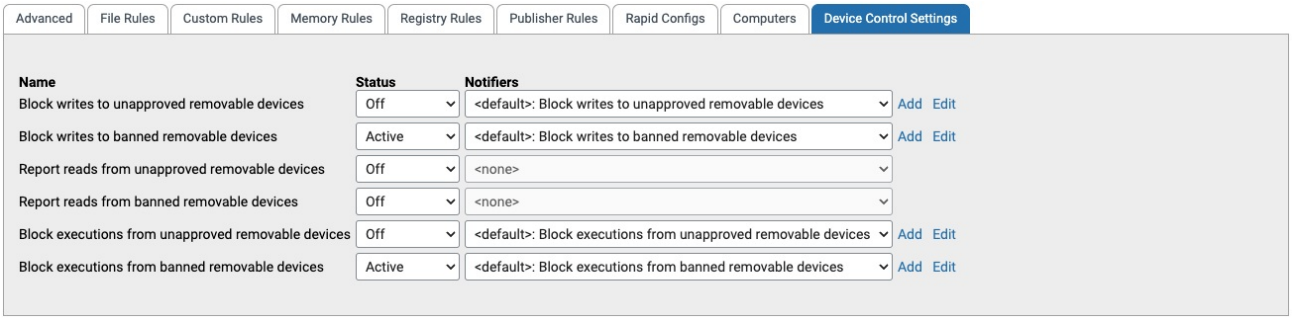
- Publisher Rules : Windows 및 MAC 에서 사용되는 소프트웨어 인증서에 대한 승인 및 미승인 규칙 정의하여 파일 허용 및 차단



- Rapid Configs : 세부적인 정책을 적용하기 전, 신속하게 엔드포인트 보호 환경을 정의하기 위한 정책 적용



- Computers : 정책이 적용된 엔드포인트 목록 확인



- Device Control Settings : 금지 및 미승인된 이동식 장치에 대한 실행 및 쓰기 행위에 대한 허용 및 차단