

구성: 환경 마이그레이션

개요

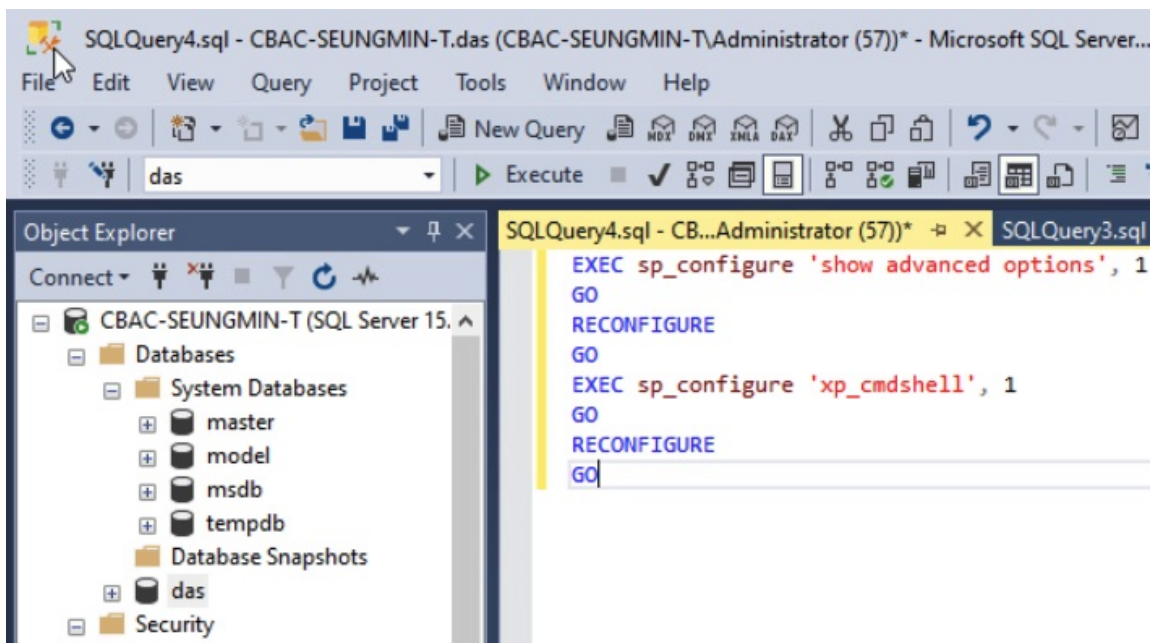
기존 App Control 서버를 신규 App Control 서버 환경으로 마이그레이션 하는 방법을 작성하였습니다.

진행 방법

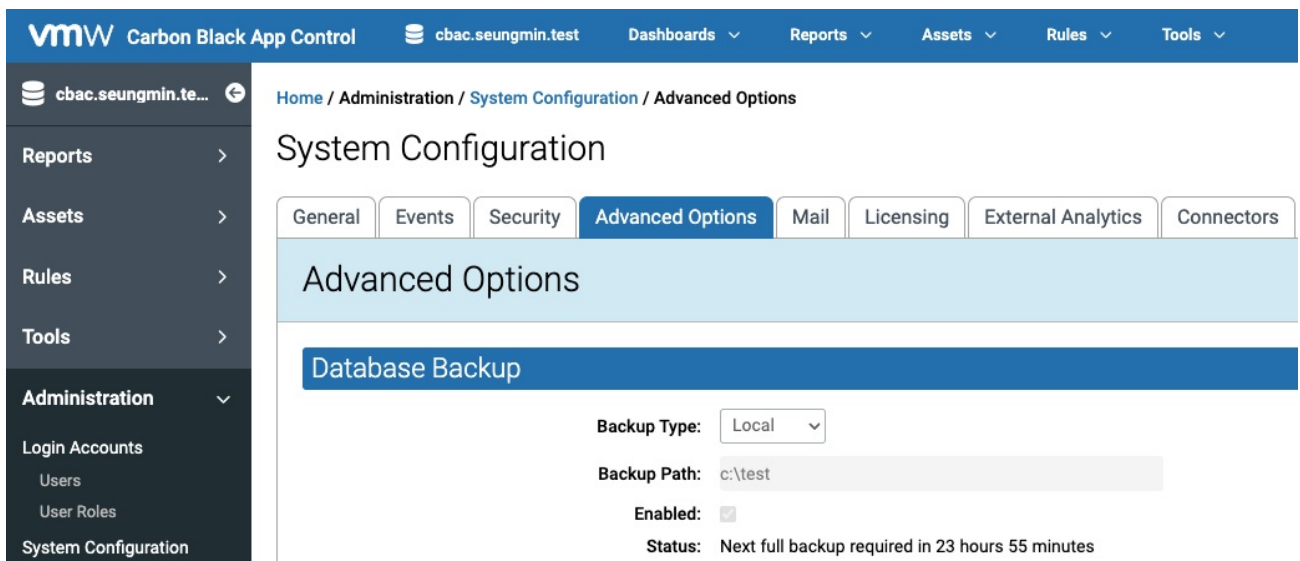
참고 문서 : <https://community.carbonblack.com/t5/Knowledge-Base/App-Control-How-to-Migrate-a-Server-Installation-Single-Tier/ta-p/43038>

1. 기존 서버 데이터 백업

1.1 데이터 백업



- SSMS 프로그램을 접속 후 'das' 데이터베이스에 쿼리문을 통해, 비활성화된 'xp_cmdshell' 기능 활성화



- [App Control] 웹 콘솔 > [Settings] - [System Configuration] 메뉴 접속 > 'Advanced Options' 탭으로 이동

System Configuration

General Events Security **Advanced Options** Mail Licensing External Analytics Connectors

Advanced Options

Database Backup

Backup Type: Local

Backup Path: c:\test

Enabled: ☒

Status: Next full backup required in 23 hours 55 minutes

- 데이터베이스 백업 설정 진행

- Backup Type : 로컬 폴더 저장 또는 네트워크 폴더에 저장 선택
- Backup Path : 로컬 경로 입력 또는 네트워크 경로 입력
- Enabled : 체크박스 선택하여 백업 활성화 진행
- Status : 백업의 현재 상태 확인

vmw Carbon Black App Control cbac-seungmin-test Dashboards Reports Assets Rules Tools Alerts 3 Settings

cbac-seungmin-t...

Reports Events Cached Events Dashboards Baseline Drift Reports Snapshots External Notifications Assets Rules Tools Administration

Saved Views: (The Current View Has Unsaved Changes - Discard) (none) Saved View Name Create Group By: (none) Ascending Subgroup By: (none)

Max Age: 2 days

Hide Filters Show Columns Export to CSV Access Event Archives Refresh Table

Filters Add filter Subtype is

Apply Cancel Reset

Action Search: Enter File Hash, IP Address, Platform, Source, Subtype Automatically apply Showing 425 out of 674 item(s)

Severity	Type	Subtype	Source	Description
Info	Server Management	Server backup started	System	Database backup has been enabled, starting backup service.
Notice	Server Management	Server backup stopped	System	Backup has been disabled, stopping backup service.

- [App Control] 웹 콘솔 > [Reports] - [Events] 메뉴 접속하여 백업 상태 이벤트 이력 확인

test

File Home Share View

This PC > Local Disk (C:) > test

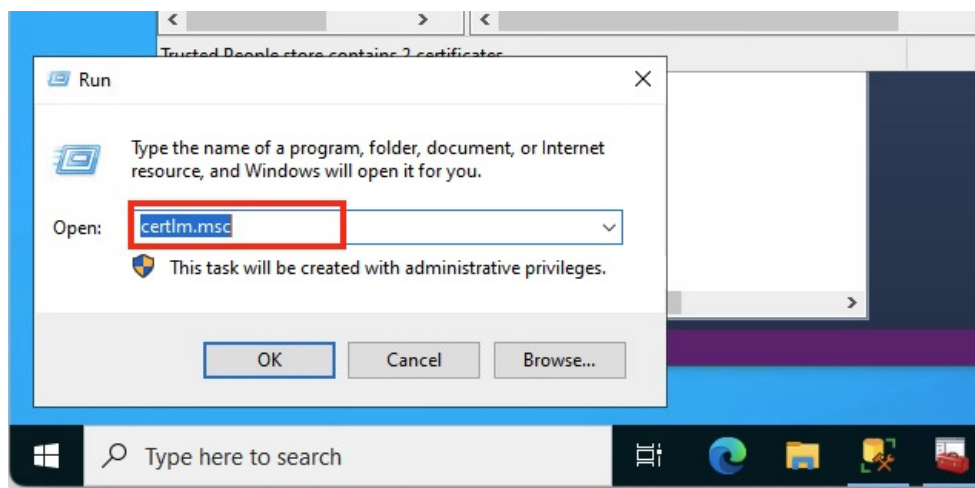
Quick access Desktop Downloads Documents

Name	Date modified	Type	Size
backup	2/5/2024 11:47 PM	Configuration sett...	1 KB
Full_backup.bak	2/5/2024 11:47 PM	BAK File	78,953 KB

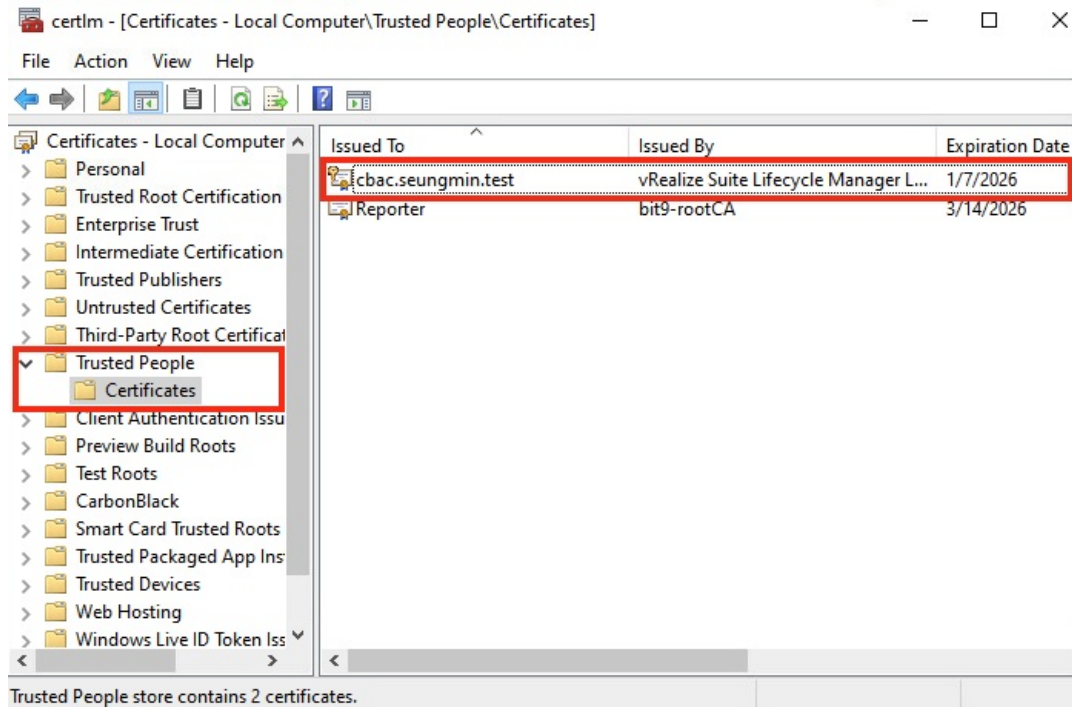
- 백업 경로에 생성된 backup.ini 및 Full_backup.bak 파일 확인

1.2 서버-에이전트 간 통신 인증서 백업 (선택사항)

참고 문서 : <https://community.carbonblack.com/t5/Knowledge-Base/App-Control-How-To-Export-the-App-Control-Agent-Communication/ta-p/51850>

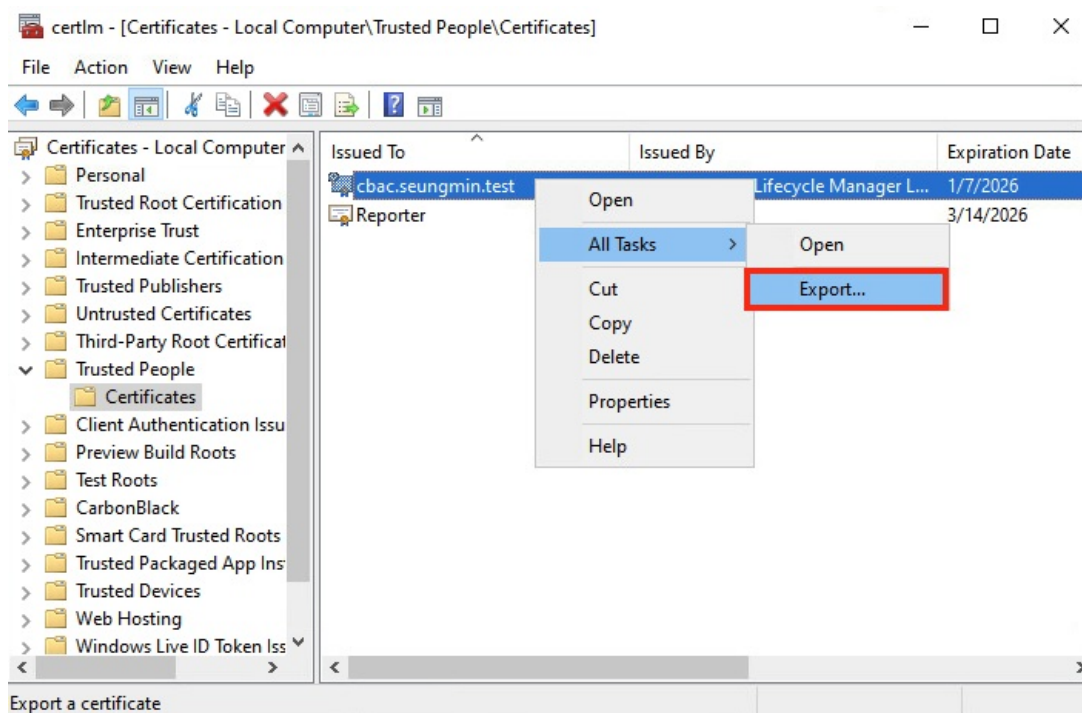


- App Control 서버 접속하여 'certlm.msc' 실행



- [Trusted People] - [Certificates] 선택하여 'App Control' 인증서 확인

① 사용 중인 인증서 확인 메뉴 : [App Control] 웹 콘솔 접속 > [Settings] - [System Configurations] 메뉴 선택 > [Security] 탭 선택



- 인증서 목록 우클릭하여 [Export] 진행



← Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

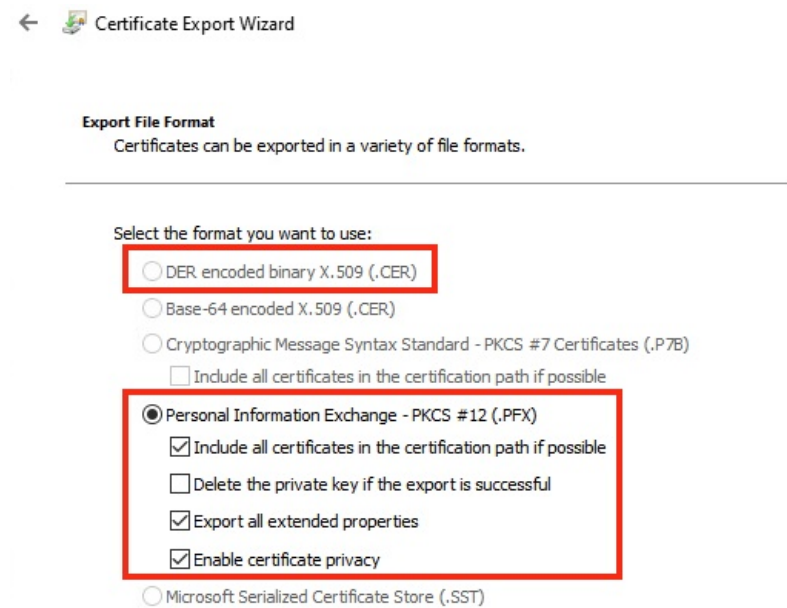
Do you want to export the private key with the certificate?

☐ Yes, export the private key

☒ No, do not export the private key

- 내보내기 옵션 선택

- 콘솔 백업 및 IIS 구성을 위한 인증서
 - Yes, export the private key 선택
- 엔드포인트 및 신뢰되는 통신을 위한 인증서
 - No, do not export the private key 선택



← Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

☐ DER encoded binary X.509 (.CER)

☐ Base-64 encoded X.509 (.CER)

☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☐ Include all certificates in the certification path if possible

☒ Personal Information Exchange - PKCS #12 (.PFX)

☒ Include all certificates in the certification path if possible

☐ Delete the private key if the export is successful

☒ Export all extended properties

☒ Enable certificate privacy

☐ Microsoft Serialized Certificate Store (.SST)

- 인증서 유형에 맞는 옵션 선택

- 콘솔 백업 및 IIS 구성을 위한 인증서
 - Include all certificates in the certification path if possible 체크
 - Export all extended properties 체크
 - Enable certificate privacy 체크
- 엔드포인트 및 신뢰되는 통신을 위한 인증서
 - DER encoded binary X.509 (.CER) 체크

Security

To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

Add

Remove

☒ Password:

.....

 Confirm password:

.....

Encryption: TripleDES-SHA1

- 콘솔 백업 및 IIS 구성을 위한 인증서의 경우 'Password' 체크 및 입력

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\A
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal In

Certificate Export Wizard

×

 The export was successful.

OK

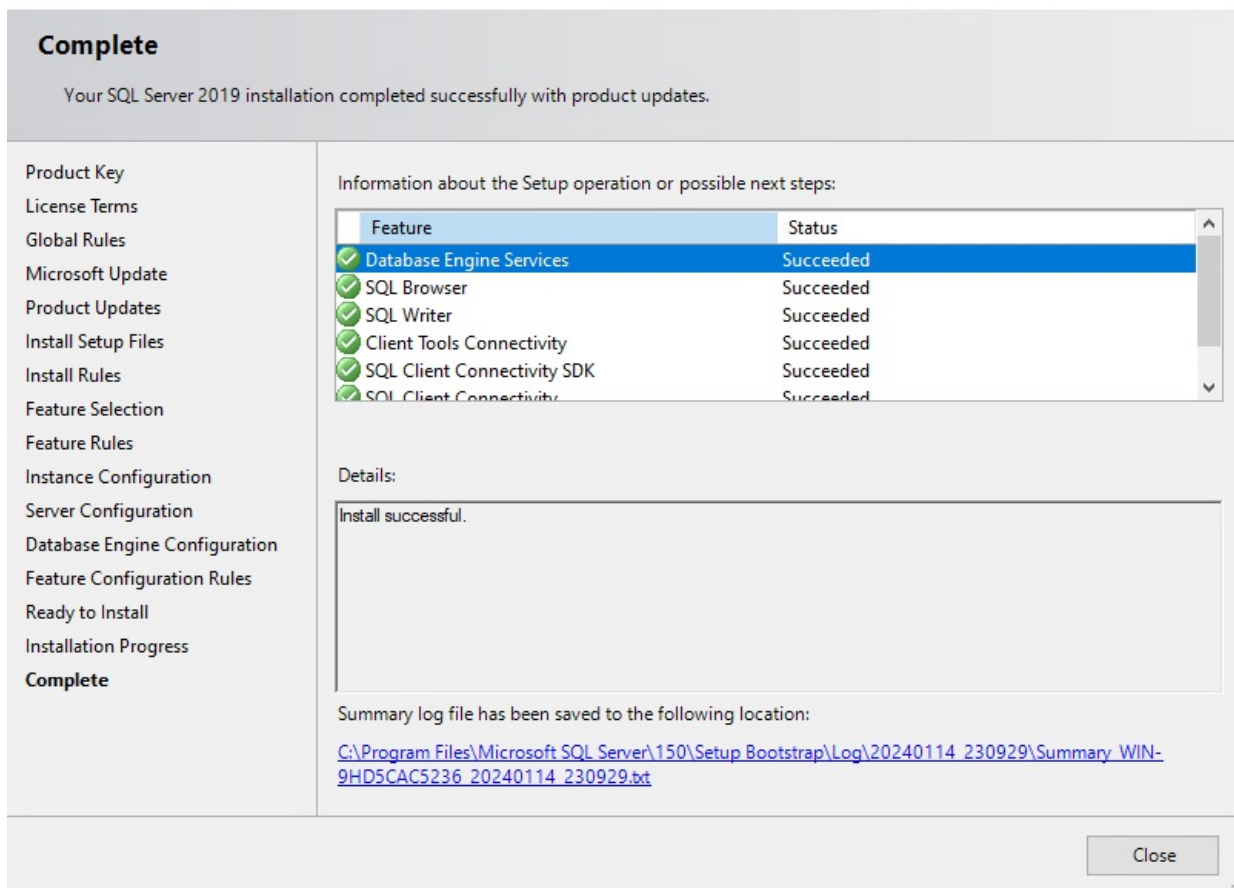
- 파일명 및 위치 지정하여 인증서 내보내기 완료

2. 신규 App Control 환경 구성

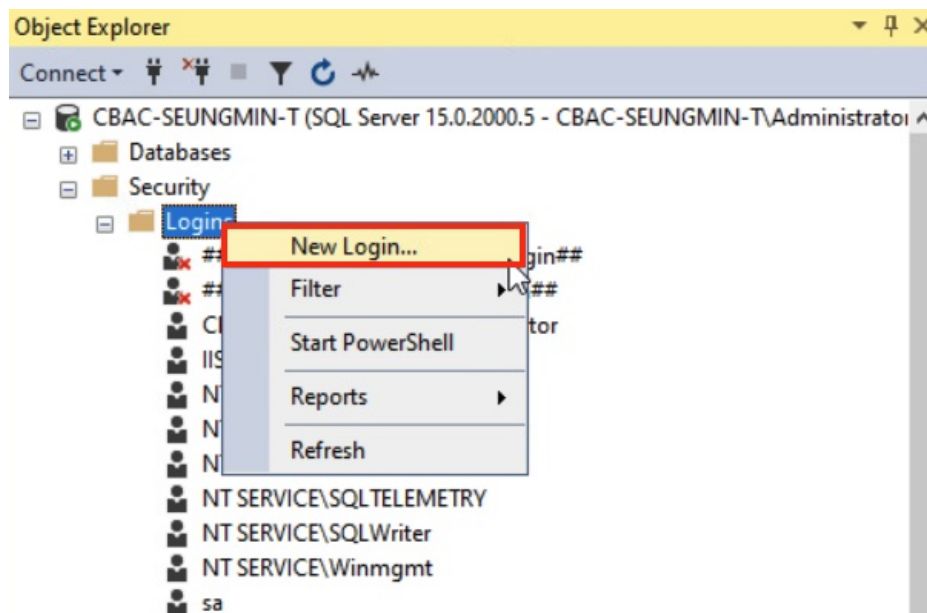
- 참조 문서 : <https://bs.etervers.tech/books/carbon-black-app-control-handbook/page/42e7a>

2.1 SQL Server 설치

① 기존 환경과 동일한 구성이 필요합니다.



- SQL Server 설치 (SQL Server 설치 가이드 참조)



- [SSMS] 접속 > [Security] > [Logins] 확장 및 접속 > 'New Login' 선택

Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Script Help

Login name: IIS APPPOOL\DefaultAppPool Search...

☒ Windows authentication
☐ SQL Server authentication

Password:
 Confirm password:
☐ Specify old password
 Old password:

☒ Enforce password policy
☒ Enforce password expiration
☒ User must change password at next login

☐ Mapped to certificate
☐ Mapped to asymmetric key
☐ Map to Credential Add

Mapped Credentials

Credential

 Remove

Default database: master
 Default language: <default>

Connection
 Server: CBAC-SEUNGMIN-T
 Connection: CBAC-SEUNGMIN-T\Administrator
[View connection properties](#)

Progress
 Ready

- 'IIS APPPOOL\DefaultAppPool' 계정 추가


2.2 App Control 설치

- 참조 문서 : <https://bs.etevers.tech/books/carbon-black-app-control-handbook/page/cd006>

Carbon Black App Control - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.



VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY

☒ I accept the terms of the license agreement
☐ I do not accept the terms of the license agreement

Print

InstallShield

< Back Next > Cancel

- ParityServerSetup.exe 프로그램 실행 및 라이선스 동의

Select Features

Select the features setup will install.



Select the features you want to install, and deselect the features you do not want to install.

<input checked="" type="checkbox"/> Carbon Black App Control Server	12 MB
<input checked="" type="checkbox"/> Carbon Black App Control Console	258 MB
<input checked="" type="checkbox"/> Carbon Black App Control Reporter	9 MB

Destination Folder
C:\Program Files (x86)\Bit9 Browse...

Space Required on C: 300 MB
Space Available on C: 77358 MB Disk Space...

InstallShield

< Back Next > Cancel

- 설치 진행할 기능 및 설치 위치, 용량 확인

Carbon Black App Control - InstallShield Wizard

Database Server

Select database server and authentication method.



Select the database server from the list below or click Browse to see a list of all database servers. You can also specify the way to authenticate your login using your current credentials or a SQL Login ID and Password.

Database Server:
(local) Browse...

Initially connect using:

☒ Windows authentication

☐ SQL Server authentication using the Login ID and password below

Login ID:

Password:

InstallShield

< Back Next > Cancel

- Database 서버 위치 '(local)' 선택 및 인증 방법 선택

Carbon Black App Control Database Configuration

Configure database to be used by Carbon Black App Control Server



Please select one of the following database configuration options:

☐ Create a new database

Create a new Carbon Black App Control Database

☐ Use an existing database

Use an existing Carbon Black App Control Database.

☒ Restore from a database backup

Restore from a Carbon Black App Control Database backup. Upgrade if necessary.

InstallShield

< Back

Next >

Cancel

- 기존 환경에서 백업한 데이터베이스 사용을 위해 'Restore from a database backup' 옵션 선택

Carbon Black App Control Backup Restoration

Please enter the location of the Carbon Black App Control Server backup.

Question

C:\V



The Carbon Black App Control Database contains a backup of previously used Console and Server certificates. Do you want to reuse them?

Yes

No

InstallShield

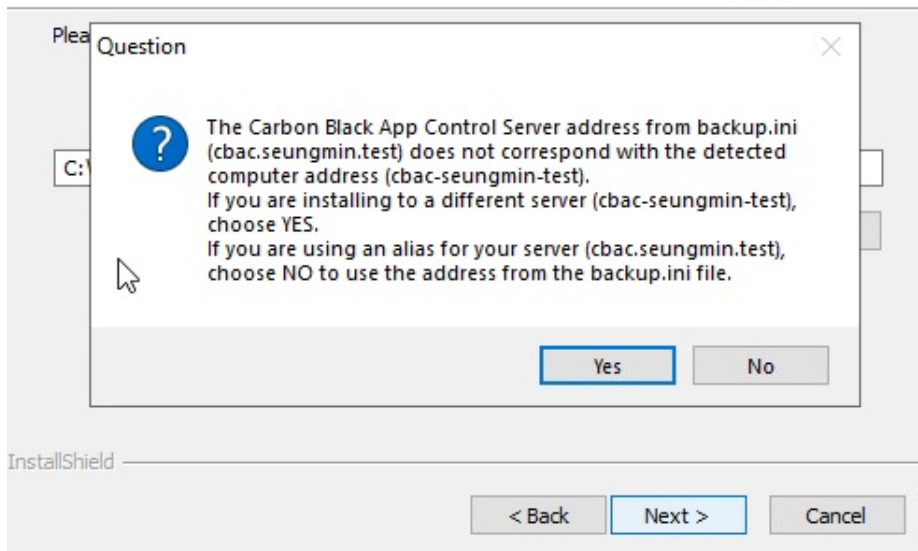
< Back

Next >

Cancel

- 콘솔 및 서버 인증서 재사용 여부 확인

Carbon Black App Control Backup Restoration

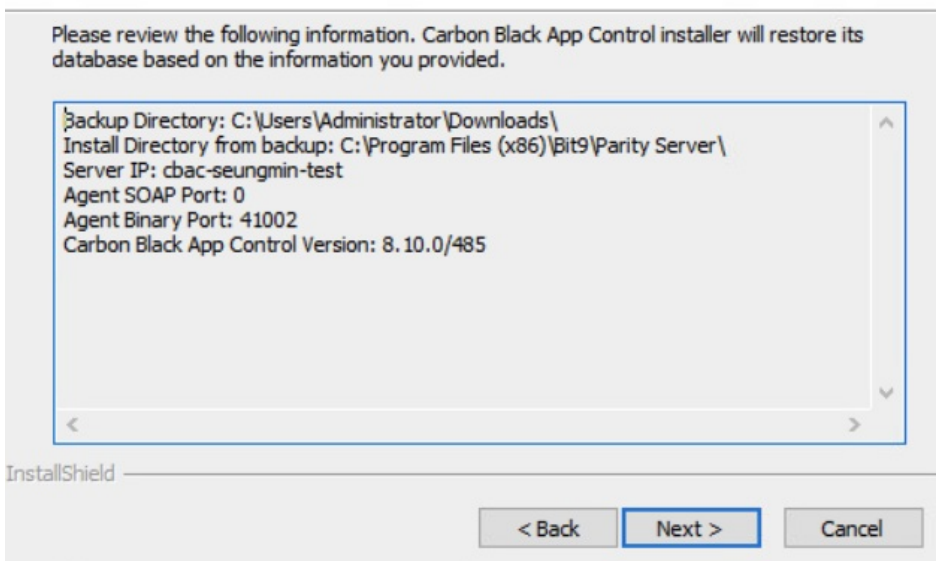


- 기존 서버와 다른 서버에 재설치 진행한다면 'Yes' 버튼 클릭, backup.ini 파일의 설정 값을 사용하여 재설치 진행한다면 'No' 버튼 클릭

Carbon Black App Control - InstallShield Wizard



Carbon Black App Control Backup Information



- Backup.ini 파일에 작성된 서버 설정 값이 정상적으로 입력되었는지 확인

Log On Carbon Black App Control Server As



Specify the user account to be used by Carbon Black App Control Server. The user account must be in the format "DOMAIN\Username" and must have access to the SQL database server.

☐ Local System Account

☒ Specify Account

User name:

cbac-seungmin-t\administrator

Password:

●●●●●●●●

InstallShield

< Back

Next >

Cancel

- App Control Server 및 SQL Server 에 액세스 가능한 Windows 사용자 계정 지정

Carbon Black App Control - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.



Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

InstallShield

< Back

Install

Cancel

- [Install] 버튼을 클릭하여 설치 진행

Restore Pre-Existing X.509 Certificate for Carbon

A password is required to re-use existing X.509 certificate file.



Specify password for Server certificate. Default value is the same like specified for Console (IIS) certificate.

Enter Password:

●●●●●●●●

Confirm Password:

●●●●●●●●

InstallShield

< Back

Next >

Cancel

- 기존 IIS 인증서에 대한 암호 입력

Carbon Black App Control - InstallShield Wizard

www.vmware.com

InstallShield Wizard Complete

vmware

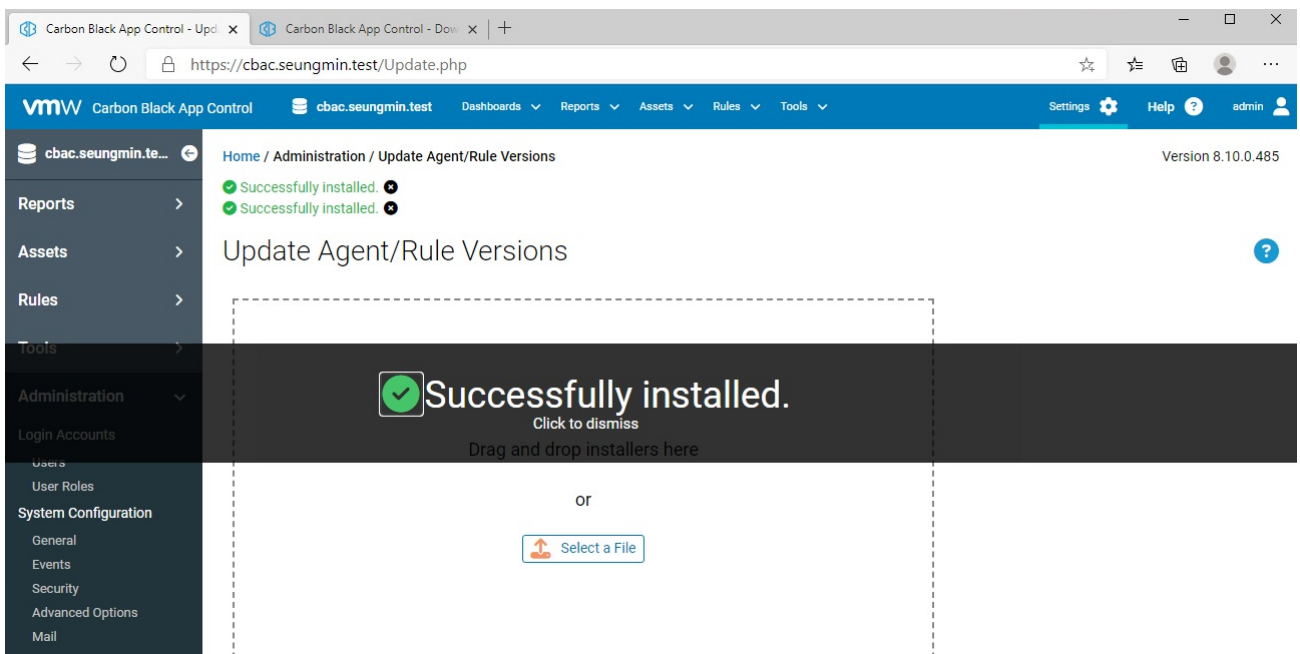
Carbon Black
App Control

< Back

Finish

Cancel

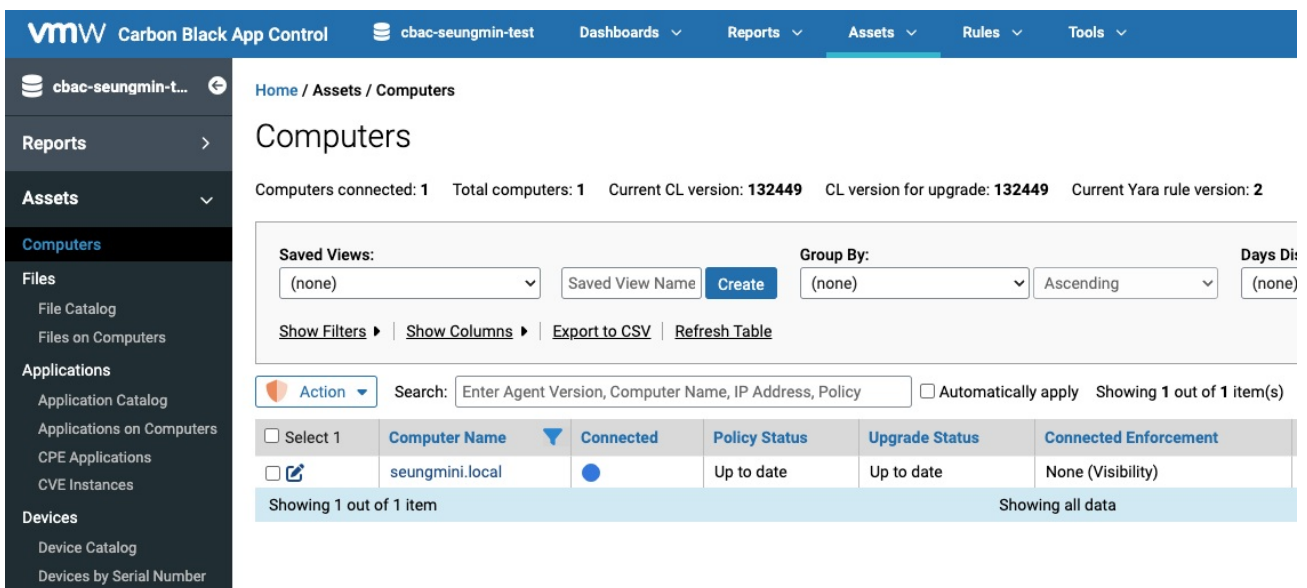
- 서버 설치 완료



- [App Control] 웹 콘솔 접속 > [Settings] > [Update Agent/Rule Version] 메뉴 이동 후 'Select a File' 또는 '드래그 앤 드롭' 방식으로 롤 및 OS 별 에이전트 업로드

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

3. 데이터 확인



- 에이전트 통신 확인

vmwCarbon Black App Control

cbac-seungmin-testDashboards▼Reports▼Assets▼Rules▼Tools▼

cbac-seungmin-t...⏪

Reports▼

Events

Cached Events

Dashboards

Baseline Drift

Reports

Snapshots

External Notifications

Assets>

Rules>

Tools>

Administration>

Saved Views: (The Current View Has Unsaved Changes - Discard)

(none)Saved View NameCreate

Group By: (none)Ascending

Max Age: 2 days

Show Filters>Show ColumnsExport to CSVAccess Event ArchivesRefresh Table

ActionSearch: Enter File Hash, IP Address, Platform, Source, SubtypeAutomatically applyShowing 674 out of 674 item

<input type="checkbox"/> Select 126	Timestamp	Severity	Type	Subtype	Source
<input type="checkbox"/>	Feb 5 2024 10:03:25 PM	Info	Policy Management	File approval created	System
<input type="checkbox"/>	Feb 5 2024 10:03:25 PM	Info	Policy Management	File approval created	System
<input type="checkbox"/>	Feb 5 2024 10:03:25 PM	Info	Policy Management	File approval created	System
<input type="checkbox"/>	Feb 5 2024 10:03:25 PM	Info	Policy Management	File approval created	System
<input type="checkbox"/>	Feb 5 2024 10:03:25 PM	Info	Policy Management	File approval created	System
<input type="checkbox"/>	Feb 5 2024 10:03:25 PM	Info	Policy Management	File approval created	System
<input type="checkbox"/>	Feb 5 2024 10:03:22 PM	Warning	Server Management	Server shutdown	System
<input type="checkbox"/>	Feb 5 2024 10:02:47 PM	Info	Server Management	Agent trust cert file created	System
<input checked="" type="checkbox"/>	Feb 5 2024 10:02:45 PM	Info	Server Management	Install succeeded	System
<input type="checkbox"/>	Feb 5 2024 10:02:42 PM	Info	Policy Management	AD rules loaded	System
<input type="checkbox"/>	Feb 5 2024 10:02:42 PM	Notice	Server Management	Server restart	System
<input type="checkbox"/>	Feb 5 2024 10:02:27 PM	Info	Policy Management	File approval created	System
<input type="checkbox"/>	Feb 5 2024 10:02:27 PM	Info	Policy Management	File approval created	System
<input type="checkbox"/>	Feb 5 2024 10:02:27 PM	Info	Policy Management	File approval created	System

- 로그/정책/설정 등 정보 확인

🔄버전 #17

★생성 5 2월 2024 11:00:49

✍수정 18 4월 2025 17:06:16