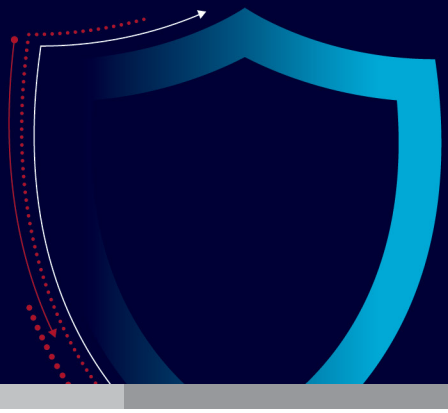
WHITE PAPER

Carbon Black® App Control

Carbon Black. by Broadcom



Getting Started Guide

TABLE OF CONTENTS

Overview

This guide will help set up a Carbon Black® App Control server, create policies, and deploy the App Control Agent to machines in an environment. For complete instructions, refer to: docs.vmware.com/en/VMware-Carbon-Black-App-Control/index.html.

Prepare the Environment

Before installing the App Control software, you must build the App Control server machine and install Microsoft SQL Server. For complete instructions, refer to: docs.vmware.com/en/VMware-Carbon-Black-App-Control/index.html.

- The Operating Environment Requirements document (OER) gives details on the hardware requirements for the App Control server. It is important that your machine conforms to these requirements. If you are installing this into a virtual environment, the virtual environment will need to meet those same specifications.
- The Carbon Black App Control Server Installation Guide provides detailed instructions on installing and configuring the server OS, Microsoft IIS, Microsoft SQL Server, and the App Control software.

NOTE: The installation sequence is important. .NET must be installed before IIS. It is highly recommended that you use a clean OS installation.

INSTALL ON A CLEAN OPERATING SYSTEM WITH THE LATEST VERSION, PATCH, AND SERVICE PACK

System Requirements

Operating System / DB	Architecture	Service Pack	Comments
Windows Server 2012 R2 or Above	x64	SP1 or latest	—
SQL Server 2012 R2 or Above OR	x86, x64	SP2 or latest	—
SQL Server Express 2012 R2 or Above	x86, x64	SP2 or latest	Max Ram utilized: 1 Gb Max DB size: 10 Gb

Parameter	Description
Central Processing Unit (CPU)	2 to 4 cores
Processor	Xeon/i7 processor/multi-core with at least 3 GHz
Random Access Memory (RAM)	4 to 16 Gb
Hard Disk Drive (HDD)	100 to 200 Gb

Additional Server Requirements

- Install on a clean operating system with the latest version, patch, and service pack.
- If you would like to test Active Directory integration, join the server to your Active Directory domain. The FQDN of the server must be resolvable by the endpoints where the App Control agents are installed. Refer to the Carbon Black App Control Server Installation Guide for additional information.
- Install .NET 3.5 SP1 and .NET 4.5 frameworks with the default settings. This must be installed before installing IIS.
- Install IIS and configure IIS as follows:

  NOTE: There is a PowerShell script included in the Utilities folder. Run PowerShell as Administrator.

  - Common HTTP Features:
    - » Static Content
    - » Default Document
    - » HTTP Errors
    - » HTTP Redirection
  - Application Development:
    - » ASP.NET (version 4.5)
    - » NET Extensibility (version 4.5)
    - » 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

PATCH EVERYTHING (THE OS, SQL, .NET 4.5, ISS, ETC.) TO THE LATEST PATCH LEVELS

- Install Microsoft SQL Server. For additional information, refer to the Carbon Black App Control Operating Environment Requirements (OER) document for Supported SQL Server Versions. If you need to obtain the MS SQL software, download SQL [recommended version for your OS] with Tools from the Microsoft website.

  NOTE: The SQL Server instance must be a dedicated SQL server.
- Patch everything (the OS, SQL, .NET 4.5, ISS, etc.) to the latest patch levels.
- Obtain the App Control server software along with the Rules Installer and OS Agent Installers. Your SE will provide you with information on how to obtain this software.

App Control Server Communications Requirements

Requirement	Description	Notes
Access to services.bit9.com	Outbound SSL from App Control Managemet console to CB Threat Intelligence	Allow connection to services.bit9.com (proxy connections are supported)
Port 443 Access	Inbound HTTPS from App Control console users and agents	—
Ethernet Connection	1 Gb/s connection required on both App Control server and SQL server	—
Static IP Address Only	(no DHCP) with an assigned FQDN or alias; IPv4 and/or IPv6 supported	—

Install the App Control Server Software

Download the App Control server software using the link sent in the evaluation provisioning email.

IN A PRODUCTION ENVIRONMENT IT IS NOT RECOMMENDED TO USE AN IP ADDRESS.

HOWEVER, FOR POC PURPOSES, IT IS ACCEPTABLE FOR TESTING PURPOSES.

Determine which user on the server the App Control software should be the *service user*—that is the user ID under which the App Control server software will run. This can be Local System (the easiest option), or it can be a user that you create. Ensure that the user has System Administrator permission in your installation of Microsoft SQL Server. Make sure that you are logged in as the service user (or as administrator if you have chosen to use Local System) before you install the App Control software. Leave this as a generic SQL install. The server installation program will set up the proper user accounts and database structure.

Follow the steps in the Carbon Black App Control Installation Guide to install the server software on the server. Pay attention to the following items:

1. Accept the defaults for everything.
2. When asked to *Specify Account*, use the default ID/password you are currently logged into the server with, or the ID/password you want to use to manage the database from this point forward.
3. The Server Address is the fully qualified domain name (FQDN) of the server, such as appcontrol.carbonblack.com or an IP address. This is how the agents communicate back to the server. If you use a FQDN, ensure that the address is resolvable.

   NOTE: In a production environment, it is not recommended to use an IP address. However, for POC purposes, it is acceptable for testing purposes.
4. You will be asked if you want to create a self-signed certificate or use a preexisting certificate. For POC purposes, it's usually easiest to use a self-signed certificate. This can be changed later.

5. When asked for a license, enter the key you were provided by your SE. If you were not provided a key, leave this field blank for now.
6. In the App Control Agent Management screen, it is highly recommended that you enable and specify a global password for managing agents. The recommended password for an evaluation is *control*.
7. Create a password for the App Control console. You will use this along with the ID *admin* to log in to the console for the first time. You will set up more user IDs during the POC for individual users.

Install the Rules Engine

Install the Rules Engine after you complete the App Control Server (Parity Server) installation. This provides Rapid Configs and Updaters.

1. Extract the Rules Installer file.
2. Open an Administrative command prompt and navigate to the Rules Installer file.
3. Execute the Rules Installer file.
4. A black window opens. When the window closes, the Rules have been installed.
5. Validate that the Rules have been installed after you log in to your console by navigating to Rules > Policies and using the *Click here to view available Carbon Black App Control Agent/Rules versions* link.

CARBON BLACK FILE REPUTATION RESIDES IN THE CARBON BLACK PRIVATE CLOUD, SO IF YOUR APP CONTROL SERVER NEEDS TO GO THROUGH A PROXY IN ORDER TO COMMUNICATE WITH THE INTERNET, THEN YOU WILL ALSO NEED TO SET UP YOUR SERVER TO USE A PROXY.

Install the OS Agents

Once the Rules Installer has run, install the agents for the OSs. Follow this process for each agent:

1. Extract the file for the agent installer you wish to install.
2. Open an Administrative command prompt and navigate to the Rules Installer file.
3. Execute the Agent Installer file.
4. A black window opens. When the window closes, the Rules have been installed.
5. Follow Steps 1 to 4 for each agent you would like to deploy.
6. Validate that the Rules have been installed after you log in to your console by navigating to Rules > Policies and using the *Click here to view available Carbon Black App Control Agent/Rules versions* link.

Communicate with Carbon Black File Reputation

Confirm that the App Control server can communicate with services.bit9com.

Carbon Black File Reputation resides in the Carbon Black private cloud. If the App Control server needs to go through a proxy to communicate with the Internet, then you will also need to set up your server to use a proxy.

Log in to the App Control console using the *admin* user name and the chosen password. If needed, set up the server to use a proxy before attempting the next steps.

1. Navigate to Administration > System Configuration and select the Licensing tab.
2. Edit the File Reputation Proxy settings, enter the appropriate proxy

information, and save the settings.

Activate the Collective Defense Cloud license key:

1. Navigate to Administration > System Configuration and select the Licensing tab.
2. In the File Reputation Activation settings, add the key that your SE sent you when your evaluation was provisioned. It is an alphanumeric key in this format: XXXXX-XXXXXXXXXX.

   NOTE: A Cloud Activation key is different from a license, and they are entered in different areas of the page.
3. A web page opens, requiring you to acknowledge a licensing agreement.
4. Return to the Licensing page and use the Verify Activation button to verify that your subscription to File Reputation is activated.

FOR ENHANCED SECURITY, APP CONTROL SELF-PROTECTS ITS APPLICATION DIRECTORY

Create Antivirus Exclusions

If you run antivirus software, exclude the App Control Agent installation directory from antivirus scanning. For enhanced security, App Control self-protects its application directory. To avoid performance issues, configure the antivirus software so that the following files and directories are not scanned or blocked:

- Parity.exe – the agent process
- `Program Files\Bit9` is the default agent program directory on 32-bit systems; if you did not choose the default, use the directory you chose.
- `Program Files (x86)\Bit9` is the default agent program directory on 64-bit systems; if you did not choose the default, use the directory you chose.
- `ProgramData\Bit9\Parity Agent` is the default agent data directory on Vista, Windows 7, 8 and 10, and Windows Server 2008 through 2016 systems; if you did not choose the default, use the directory you chose.
- `\Documents and Settings\All Users\Application Data\Bit9\Parity Agent` is the default agent data directory for supported OSs not listed in the previous items.

For more detailed instructions, contact your SE.

Create Basic Policies

To create policies, navigate in the Console to Rules > Policies. Click the Add Policy button to create a new policy.

Create the basic policies as follows, using the Save button to save each one:

1. A policy named Agent Disabled with the following settings:
   - Mode: Disabled
   - Initial Settings: Template Policy
   - Automatic Policy Assignment: Checked
   - Options: Allow Upgrades
2. A policy named Low Enforcement with the following settings:
   - Mode: Control
   - Enforcement Level : Low, Low

- Initial Settings: Template Policy
- Automatic Policy Assignment: Checked
- Options: Allow Upgrades, Track File Changes

3. After you've saved the Low Enforcement Policy, complete the following tasks:
   - Navigate to Assets > Computers
   - Click the machine name link to navigate to the Computer Details page
   - Click to Disable Tamper Protection under Advanced Settings on the right.

ONCE INITIALIZATION HAS COMPLETED, YOUR APP CONTROL EVALUATION INSTALLATION IS COMPLETE. YOUR SE WILL MEET WITH YOU REGULARLY TO GUIDE YOU THROUGH THE NEXT STEPS IN THE EVALUATION PROCESS.

NOTE: This is for POC purposes only. Your SE can advise on best practices for your production deployment.

Deploy Your First Agents

The MSI installation packages can be obtained from the App Control server using the URL near the top of the Rules > Policies page (`https ://<server>/hostpkg`).

NOTE: There will be two links, Agent Disabled and Monitor Only. Use the link for the Agent Disabled policy for all endpoints you want to test.

After verifying under Assets > Computers that the agent is checking in with the server, select Action > Move Computers to policy: Low Enforcement.

When an agent is moved into Low Enforcement, it will begin initializing, which lasts an average of 40 minutes. Once initialization has completed, your App Control evaluation installation is complete. Your SE will meet with you regularly to guide you through the next steps in the evaluation process.

CB-AppControl-GettingStarted-WP100 December 18, 2024