VMware
Carbon Black App Control v8.8.2
Supplemental Administrative Guidance

Version: 1.0
February 27, 2022

VMware, Inc.

3401 Hillview Ave
Palo Alto, CA 94304

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Contents

Table of Tables

1 Introduction

VMware Carbon Black App Control (also referred to as the TOE or App Control) is an Enterprise Security Management (ESM) product that provides host-based access control meaning it controls client user access to objects including files, processes, and system configuration settings on an endpoint system based on an enterprise-level access control policy. The TOE includes a policy management component that is used to configure the access control policies and an agent component which will enforce its policy to allow or prevent client users from performing read, modify, delete, execute, and other operations on objects. This allows for organizations to deploy centralized applications within an enterprise environment while ensuring that the organization's client users are given appropriate and consistent access to these applications based on user attributes that are organizationally defined.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating App Control version 8.8.2. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation.

The reader is expected to be familiar with the Security Target for App Control version 8.8.2 and the general CC terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions for how to perform the security functions that are defined by these SFRs.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below. These terms are also described in the App Control Security Target.

CC: stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

SFR: stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: stands for Target of Evaluation. This refers to the aspects of App Control that contain the security functions that were tested as part of the CC evaluation process.

4 References

The following documents are part of the App Control version 8.8 guidance documentation. This is the standard documentation set that is provided with the product. Only the specific sections of these documents referenced within this Supplemental Administrative Guidance document are considered part of the Common Criteria evaluation. Product functionality discussed within these documents and not directly referenced by this Supplemental Administrative Guidance document was not evaluated as part of this evaluation.

[1] Server Installation Guide VMware Carbon Black App Control 8.8, dated 8 December 2021
[2] Operating Environment Requirements VMware Carbon Black App Control 8.8, dated 8 December 2021
[3] SQL Server Configuration Guide VMware Carbon Black App Control 8.8, dated 8 December 2021
[4] VMware Carbon Black App Control User Guide Product Version 8.8, Document Version 1.0, dated 6 December 2021

The following document was created in support of the App Control CC evaluation.

[5] VMware Carbon Black App Control v8.8.2 Security Target

The following documents are guidance provided by the underlying operating system vendors as part of their respective Common Criteria evaluations.

[6] Microsoft Windows 10 and Windows Server 2019 (version 1809) GP OS Operational and Administrative Guidance
[7] Microsoft Windows 10 and Windows Server (version 1903) GP OS Operational and Administrative Guidance
[8] Red Hat Enterprise Linux 7.6 CC Guidance Version 1.4, dated June 19, 2020

5 Evaluated Configuration of the TOE

This section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself, environmental components that support the security behavior of the TOE, or non-interfering environmental components that were present during testing but are not associated with any security claims:

5.1 TOE Components

Component	Definition
App Control Agent (Agent)	TOE software that is installed on Windows and/or Linux endpoint systems to enforce access control policies/rules that are defined by the App Control Console. The Agent includes an SQLite database instantiation. In terms of the PPs, the Server is the 'Access Control product'.
App Control Console (Console)	TOE's web-based GUI that is used administratively to configure access control policies/rules and to observe status and log activity for the various deployed Agents. Administrative users using the Console are considered TOE users. In terms of the PPs, the Console and Server are the 'Policy Management product'.
App Control Server (Server)	TOE software which is the centralized component of the product. This TOE component is the back-end of the Console which contains the logic for managing the TOE and defining the access control policies which are enforced on endpoint systems. This TOE component also generates Agent installers, creates and distributes CLs to Agents, and collects object information from Agents to provide

	the TOE's host-based access control functionality. In terms of the PPs, the Server and Console are the 'Policy Management product'.

Table 5-1: TOE Components

5.2 Supporting Environmental Components

Component	Definition
Active Directory (AD)	This is an enterprise authentication server. In the evaluated configuration, TOE administrative users can be authenticated against an AD user account. AD is also used for client user identity data on endpoint systems. For endpoint systems running Linux a LDAP client, which is part of the operational environment, is used to map local system account information to network accounts defined in AD (since it is not natively supported on the Linux platforms) o Examples of this include realmd or SSSD. The TOE's Agent has no awareness of how the user is authenticated by the environment, it just knows the user's claimed identity on the system (e.g., username, UID)
Endpoint System(s)	Any general-purpose computer that has the TOE Agent software installed and that supports TLS/HTTPS communications. Supported operating systems for the evaluation include Windows and Linux. These operating systems provide all cryptography for the TOE Agents to communicate with the TOE's App Control Server. Users of the endpoint systems are considered 'client users'. 'Client users' are users that are considered the subjects to which the access control policies are applied and are not considered TOE users. Refer to Table 5-3 for these machines' specifications.
Management Workstation	Any general-purpose computer that is used by an administrative user to remotely manage the TOE via the Console. The management workstation requires a web browser which supports HTTPS (Google Chrome 36 or higher supported, recommend latest version) to access the Console.
SQL Server Database	The TOE requires a pre-installed instance of Microsoft SQL Server (2012 or higher supported, recommend latest version) on the same machine where App Control Server is installed. Microsoft SQL Server must be configured to use AES-256 encryption method. All TOE configuration data, audit data, and local user data is stored in the database.
Windows Server	A Windows Server that has the TOE App Control Server and App Control Console software installed. The SQL Server Database is also installed on this machine. The Windows Server supports TLS/HTTPS communications. The Windows operating system installed on this machine provides all cryptography required by the TOE's App Control Server and App Control Console components. Refer to Table 5-3 for this machine's specifications.

Table 5-2: Supporting Environmental Components

5.3 Evaluated Configuration

This section describes the configuration of the TOE components and the supporting environmental components as they were assessed for the Common Criteria evaluation. The following table describes the machines on which the TOE components are installed. The figure then depicts the entire configuration with all TOE components and supporting environmental components depicted.

Definition	Operating System	CPU
App Control Server and Console System software version 8.8.2	Microsoft Windows Server 2019 Datacenter (1809)	Intel Xeon Gold 6230 (Cascade Lake)
App Control Agent software version 8.7.6 - Linux Endpoint System(s)	Red Hat Enterprise Linux 7.6	Intel E5-2620 v4 (Broadwell)
App Control Agent software version 8.7.2 - Windows Endpoint System(s)	Windows 10 Professional (1903)	Intel Core i5-8365U (Whiskey Lake)

Table 5-3: Evaluated Components System Configurations

NOTE: For more information on the operating environment requirements for the system configurations, refer to Reference [2].

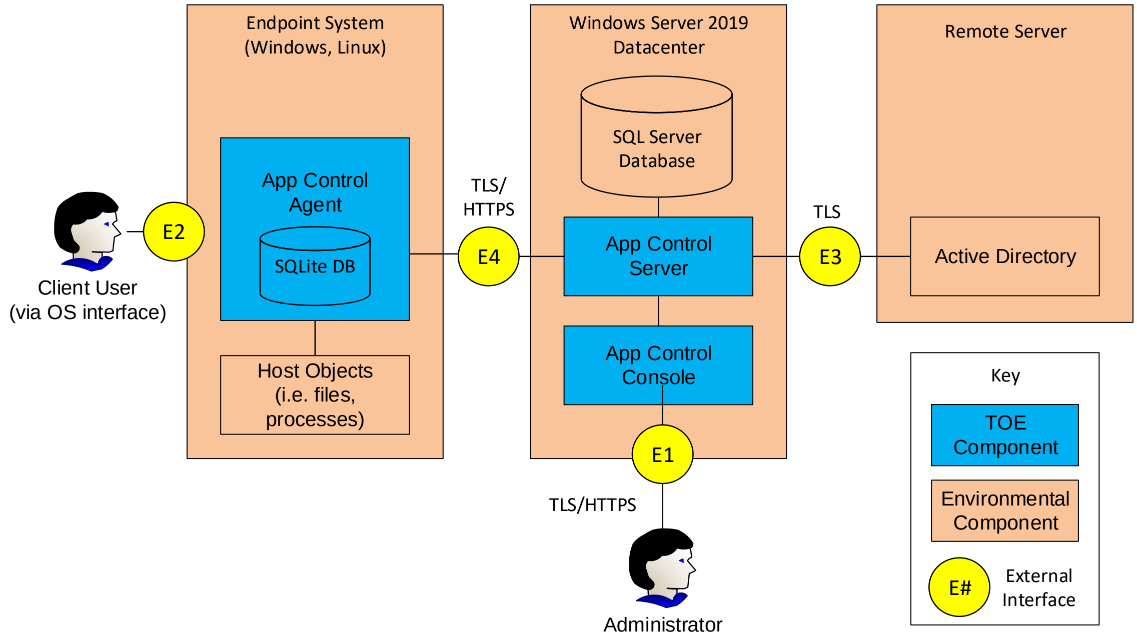


Figure 1 - Evaluated Configuration

5.4 Assumptions and Organizational Security Policies

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile:

- **Installation:** There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.
- **Management:** There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- **Enterprise Security Management:** The components of the TOE will be able to establish connectivity to each other in order to share security data.
- **System Time:** The TOE will receive reliable time data from the Operational Environment.

- **User Identifiers:** The TOE will receive identity data from the endpoint system's and Active Directory instances.
- **Cryptography:** The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- **Policy Data:** The TOE's Agents will be able to receive policy data from the TOE's Server.
- **Banner:** The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
- **Update Policy:** The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

6 Secure Installation and Configuration

6.1 Server

6.1.1 SQL Server Database Configuration

Prior to installing App Control Server on its machine, the SQL Server Database must be installed and configured. The SQL Server Database is an environmental component which is not provided by VMware. The following steps are general procedures for installing and configuring the SQL Server Database. The administrator installing the SQL Server Database needs to follow the installation steps provided by Microsoft, the SQL Server Database's vendor, with these steps in mind. The administrator should also review Reference [3] for information for additional management considerations regarding the SQL Server Database.

1. Join the App Control Server's machine to the appropriate Active Directory domain
2. Log in to the App Control Server's machine using an Active Directory administrator account
3. Install the SQL Server Database
    a. Download SQL Server Database
    b. Run the setup.exe in the ISO
    c. Switch to Installation in the left menu
    d. Click "New SQL Server stand-alone installation or add features to an existing installation"
    e. Select to accept the license terms, click Next
    f. Select to use Microsoft Update to check for updates, click Next
    g. Assuming all checks pass or are just a warning, click Next
    h. Feature Selection: Choose "Database Engine Services" and "Client Tools Connectivity". Default directories are OK if there is only one drive present, click Next
    i. Instance Configuration: Default settings are acceptable, click Next
    j. Server Configuration: Default settings are acceptable, click Next
    k. Database Engine Configuration:
        - Server Configuration: Select Mixed Mode, and enter a password twice. Under Specify SQL Server administrators, click "Add Current User"
        - TempDB: For data files, set Initial Size to 1024 MB, Autogrowth to 512 MB. For log file, set initial size to 2048 MB, Autogrowth to 1024 MB.

        - Click Next and acknowledge "Large log file size will increase setup time." message if it appears
    l. Click Install
    m. Once complete, click Close
4. Download and install SQL Server Management Studio. This will require a reboot
5. Configure SQL Server Database encryption
    a. Run SQL Server Configuration Manager
    b. Expand SQL Server Network Configuration
    c. Right-click on Protocols for MSSQLSERVER and select Properties
    d. Set Force Encryption to Yes
    e. Click OK, acknowledging the need to restart the service
    f. Run Services
    g. Select SQL Server (MSSQLSERVER) in the list
    h. Restart the service
6. Configure SQL Server Database
    a. Run SQL Server Management Studio
    b. Connect to the local server
    c. In the Object Explorer, right-click on the server and select Properties
    d. Select the Memory page on the left
    e. Enter the desired Maximum server memory (in MB) (e.g., 51200 on a system with 64 GB of RAM)
    f. Click OK

6.1.2 Machine Pre-Configuration

Prior to installing App Control Server on its machine, additional configuration is required of the underlying operating system and its components. The following steps are general procedures for installing and configuring these components. If additional information is needed, refer to Microsoft documentation for these components.

1. Install Microsoft Internet Information Services (IIS)
    a. Run the Server Manager
    b. Click Add roles and features
    c. If the "Before you begin" page displays, click Next
    d. Installation Type: Role-based or feature-based installation, click Next
    e. Server Selection: Should have current server selected by default, click Next
    f. Server Roles: Select "Web Server (IIS)". In the "Add Roles and Features Wizard" that pops up, click Add Features to select the default options and close the pop up. Click Next
    g. Features: Click Next
    h. Web Server Role (IIS): Click Next
    i. Role Services: Follow Microsoft's instructions on what to select. For example:
        - Deselect "Directory Browsing"
        - Select "HTTP Redirection"
        - Select "Logging Tools"
        - Select "Request Monitor"

        - Select “Tracing”
        - Deselect “Static Content Compression”
        - Select “IP and Domain Restrictions”
        - Select “URL Authorization”
        - Expand Application Development
        - Select “ASP.NET 4.8” and click Add Features on the pop up
        - Select “CGI”
        - Select “IIS Management Scripts and Tools”
        - Select “Management Service”
        - Click Next >
    j. Click Install
2. Configure Windows Defender Firewall Rule
    a. Control Panel -> Windows Defender Firewall -> Advanced Settings.
    b. In left tree pane, select “Inbound Rules”.
    c. Right click “Inbound Rules”, select “New Rule”.
    d. Rule Type: Program
       Program: “C:\Program Files (x86)\Bit9\Parity Server\parityServer.exe”
       Allow the connection
       Profile: All
       Name: Allow ParityServer
    e. Finish
3. The App Control Server’s underlying Microsoft Windows Server 2019 Datacenter (1809) operating system provides the TLS and HTTPS protocols necessary to secure the connections between the App Control Server and the Agents, the Active Directory Server, and remote users accessing the Console. The Microsoft Windows Server 2019 Datacenter (1809) must be configured in a manner consistent with its Common Criteria evaluation by referencing the configuration procedures described in [6].

NOTE: Use of cryptographic engines provided by other underlying operating systems were not evaluated nor tested during the Common Criteria evaluation of the TOE.

NOTE: The TOE is fully installed and configured after all steps defined in Section 6 of this document are completed. Once the TOE is fully installed and configured, if a connection between the App Control Server and either the Agents, the Active Directory Server, and/or remote users accessing the Console becomes unintentionally broken (e.g., physical disconnect, machine restart), the administrator does not need to perform any recovery actions through App Control or the underlying operating systems for the connections to be re-established securely after the connections are fixed. Once the broken connections are fixed, App Control will either automatically re-engage these connections or establish them based upon normal administrative use of the Console.

6.1.3 App Control Server Installation

VMware supplies the App Control Server installation program as an HTTPS download from their website. Once a customer initially purchases the App Control product, the administrator will be supplied with the installation program and license keys to be used during installation. Licenses are based on the number of agents running at each level.

Download the App Control installers from the User Exchange website:

1. Log in to https://community.carbonblack.com
2. Locate the latest version of Carbon Black App Control Server and download the installer
3. From that page, scroll down to find the link to the Rules Installer page (and download link)
4. Locate the latest version of Carbon Black App Control Linux Agent Host Package Installer and download it
5. Locate the latest version of Carbon Black App Control Windows Agent Host Package Installer and download it

Once the App Control Server installation program and license key are acquired, the administrator will need to perform the install per Chapter 3 Installing the App Control Server in Reference [1]. The admin will need to review the "Pre-installation Check" and "Installing the App Control Server Software" section for guidance. While performing the procedures defined under "Installing a New App Control Server", the administrator must follow the steps below for selection options.

1. Run the ParityServerSetup.exe installer
2. At Database Server selection, use the local server with Windows authentication
3. When specifying the account to run App Control under, enter the credentials for an Active Directory administrator account
4. These same credentials must be used (and entered by default) for App Control Console access

6.1.4 Machine Post-Configuration

After installing App Control Server on its machine, additional configuration is required of the underlying operating system and its components. The following steps are general procedures for installing and configuring these components. If additional information is needed, refer to Microsoft documentation for these components.

1. Configure Windows Defender Firewall
    a. Run Windows Defender Firewall with Advanced Security
    b. Select Inbound Rules
    c. Under the Actions panel on the right, click New Rule
    d. Select Program, click Next
    e. Select This program path, click Browse
    f. Navigate to C:\Program Files (x86)\Bit9\ParityServer and select ParityServer.exe, click Open
    g. Click Next
    h. Select Allow the connection, click Next
    i. Select Domain, Private, and Public, click Next
    j. Name: Parity Server, click Finish
2. Configure logging in Microsoft Internet Information Services (IIS)
    a. Run the Server Manager
    b. Expand the server entry under Connections in the left panel
    c. Expand Sites
    d. Select the Parity Console Web site
    e. Double click on Logging
    f. Click Select Fields…
    g. For each of the following settings, click Add Field and enter the necessary information:
        i. crypt-protocol / Server Variable / CRYPT_PROTOCOL

        ii. crypt-cipher / Server Variable / CRYPT_CIPHER_ALG_ID
        iii. crypt-hash / Server Variable / CRYPT_HASH_ALG_ID
        iv. crypt-keyexchange / Server Variable / CRYPT_KEYEXCHANGE_ALG_ID
        v. remote-port / Server Variable / REMOTE_PORT
    h. Click OK to close the dialog
    i. On the right Actions panel click Apply

3. Remove TCP binding in Microsoft Internet Information Services (IIS)
    a. Run the Server Manager
    b. Choose the “Parity Console Web” site from the left navigation tree.
    c. Click “Bindings…”
    d. Choose the http port 80 binding and click “Remove”.
    e. Confirm the removal.
    f. Click Close

6.1.5 App Control Server Configuration

After installing App Control Server on its machine, additional configuration is required of the App Control Server. This includes uploading the rules file and agent installer downloaded previously from the User Exchange website as well as configuring Active Directory integration, logging levels and other initial settings for the App Control Console.

1. Install rules file and agent installers
    a. Log in to the App Control Console
    b. Select the gear icon and click on Update Agent/Rule Versions
    c. Drop in the Rules Installer and wait for it to complete
    d. Drop in the Windows Agent Host Package Installer and wait for it to complete
    e. Drop in the Linux Agent Host Package Installer and wait for it to complete

    NOTE: Additional information can be found under “Uploading Agent Installers and Rules to the Server” of Chapter 4 Managing Computers in Reference [4]. Also note that MAC Agent was not included as part of the Common Criteria evaluation.

2. Add the license (if not done during installation)
    a. Select the gear icon and click Configuration
    b. Go to the licensing tab
    c. Select Specify license file
    d. Click Choose File
    e. Select the file and click OK
    f. Click Add License
3. Enable Active Directory / LDAP integration
    a. Select the gear icon and click Configuration
    b. Go to the General tab
    c. Scroll to the bottom and click the Edit button
    d. Under Active Directory / LDAP integration:
        i. Set AD-Based Logins to Enabled
        ii. Click Test to ensure it works
    e. Scroll to the bottom and click Update

   f. On the Confirmation page click Yes

4. Enable secure LDAP for the App Control Server to Active Directory connection
   a. Visit <server>/shepherd_config.php
   b. Defined Properties: AdTrySecure
   c. Property Value: true
   d. Click Change
5. Add Active Directory User Role Mappings
   a. Select the gear icon and click Login Accounts
   b. Go to the User Role Mappings tab
   c. Click Add Rule
   d. Under Relationship select “is member of group”
   e. Click the down arrow for Directory Object and select the domain account user group which will be mapped to the selected App Control role
   f. For User Role To Apply select App Control role
   g. Select Stop Evaluation
   h. Click Save
   i. Repeat the above steps for each domain account user group to App Control role mapping that will be defined for App Control Console users. For more information, refer to “Creating AD Mapping Rules” Section of Chapter 3 Managing Console Login Accounts in Reference [4].
6. Enable Server debug level 7
   a. Visit <server>/shepherd_config.php
   b. Defined Properties: DebugLevel
   c. Property Value: 7
   d. Click Change
7. Enable Script debug level 7
   a. Visit <server>/shepherd_config.php
   b. Defined Properties: ScriptDebugLevel
   c. Property Value: 7
   d. Click Change
8. Set ‘Multiple Failed Logins’ event after 1 failed login attempt
   a. Visit <server>/shepherd_config.php
   b. Defined Properties: NumFailedLoginsBeforeEvent
   c. Property Value: 1
   d. Click Change
9. Add the Rule Name column to the Events page
   a. Go to Reports / Events
   b. Click Show Columns
   c. In the Available list select Rule Name
   d. Click the right arrow to move Rule Name to the Selected list
   e. Click apply
10. Add the kernel debug agent flag
    a. Visit <server>/agent_config.php
    b. Click Add Agent Config

c. Property Name: Kernel debug flags
d. Host ID (0 For All): 0
e. Value: kernelFlagsEx=0x20000
f. Macros: <empty, do not enter anything>
g. Platform: All
h. Status: Enabled
i. Create For: All Current and Future Policies
j. Click Save

6.2 Agent

The App Control Server component is the Enterprise Security Management product (Policy Management product) that is able to define the Access Control Security Function Policy (SFP) implemented by the TOE by generating Agent installers and communicating with one or more Agents to provide them with updated policies and configuration lists (CLs). Conversely, the App Control Agent is the Enterprise Security Management product (Access Control product) that is able to enforce the Access Control Security Function Policy (SFP) implemented by the TOE.

6.2.1 Create an Initial Enforcement Policy for Agents

The App Control Console interface allows an administrative user to create policies, create rules, and associate rules with policies. Each endpoint system running an App Control Agent is assigned to a single App Control policy based upon the policy specific Agent installer. Policies allow administrative users to organize endpoint systems running the Agents into groups with common security requirements. The policy specifies an access control definition for the endpoint systems to which it has been assigned. The creation of a policy requires the administrative user to define policy settings, including its Connected Enforcement Level and Disconnected Enforcement Level.

In the evaluated configuration, Agents are assigned a policy using one of two methods:

- Agent Installer (all Agents initially) – Every policy an administrator creates generates a policy-specific App Control Agent installer for each supported platform, so when an administrator installs the Agent on an endpoint system, it is assigned a policy. When the Agent contacts the App Control Server after Agent installation, the endpoint system is added to table of computers in the Console.
- Manually – An administrator can move any Agent to a policy other than the one assigned by the installer.

The procedures below will define a basic medium enforcement policy called “Block and Ask” and then assigning endpoint systems to that policy once an Agent has been installed on the endpoint system. This is being done so that all components of the App Control product can be initially deployed before further host-based access control administration is performed. An administrator may want to define a more detailed policy and rule set prior to deploying an Agent. For further guidance in all the options for defining a policy, refer to Chapter 5 Creating and Configuring Policies in Reference [4].

1. Log in to the Console
2. Go to Rules / Policies
3. Click Add Policy

4. Policy Name: Block and Ask
5. Mode: Control
6. Enforcement Level: Medium / Medium
7. Options: Track File Changes
8. Click Save and Exit

6.2.2 Installing Agents

The Agents' underlying Windows 10 Professional (1903) and Red Hat Enterprise Linux 7.6 operating system provides the TLS and HTTPS protocols necessary to secure the connections between the Agents and the App Control Server. The underlying operating systems must be configured in a manner consistent with their Common Criteria evaluations by referencing the configuration procedures described in [7] and [8] respectively.

NOTE: Use of cryptographic engines provided by other underlying operating systems were not evaluated nor tested during the Common Criteria evaluation of the TOE.

App Control's use of the underlying operating systems' protocols prevents the consumption of malicious or otherwise unintended policies and configuration lists (CLs) that would constitute a replay attack. All legitimate policies and CLs in transit between the Server and Agent components of the TOE are secured using TLS, so it is not possible for an attacker to spoof or replay the transfer of legitimate policies or CL data using an existing connection between the Server and the Agent. If illegitimate traffic is received by the Agent's endpoint system, the endpoint system's operating system which provides the TLS will discard the traffic.

While logged in to the Console, the administrator will download the installer for a Windows Agent and Linux Agent following the procedures under "Downloading Agent Installers" of Chapter 4 Managing Computers in Reference [4] for the "Block and Ask" policy.

Once the Agent installers are downloaded, a system administrator for the endpoint system will need to install the Agent software manually on each endpoint system. The admin will need to review the "Installing App Control Agents" section of Chapter 4 Managing Computers in Reference [4] for guidance. While performing the procedures defined under "Installing the Agent on a Windows Computer" and "Installing the Agent on a Linux Computer", the administrator must follow the steps below for selection options.

1. Deploy Windows Agents
    a. On each target endpoint system:
        i. Log in the endpoint system
        ii. Verify the endpoint system is part of the same domain as the App Control Server
        iii. Save the Windows Agent installer for the 'Block and Ask' policy to the endpoint system
        iv. Install the package
2. Deploy Linux Agents
    a. On each target endpoint system:
        i. Log in the endpoint system
        ii. Verify the endpoint system is part of the same domain as the App Control Server

iii. Save the Linux Agent installer for the ‘Block and Ask’ policy to the endpoint system

iv. Navigate to the save directory in terminal and run: tar -xvzf <policy-redhat>.tgz

v. Install the package in terminal by navigating to the expanded <policy-redhat> directory and run: sudo bash b9install.sh

vi. Start the notifier, in terminal run: /opt/bit9/bin/b9notifier &

Once an Agent has been installed per the procedure above, it will automatically begin enforcing its policy and CL of rules as well as establish communications with the Server.

6.2.3 Agent to Server Communication Establishment

During the process of creating a new policy, the Server will generate a policy specific Agent installer which includes a random string which will be used to generate a key on the Agent. After a TLS connection is established between the Agent’s and Server’s underlying operating systems, the key will be used to verify the new Agent to the Server during this initial establishment as well as for the Agent to verify any updated policy or configuration list (CL) received from the Server. During the initial establishment, the Server will record the endpoint system’s hostname, IP address, and MAC address for its records and subsequent communications with the Agent. When the Server has policy or CL changes after initial establishment, each applicable Agent will be informed about the updated information upon that Agent’s next poll of the Server and the Agent will then pull this information to its configuration. The Server will then wait for a receipt message from each of the applicable Agent(s).

During initial establishment with the Server and for every subsequent policy or CL change received, the Agent will send a receipt back to the Server with its current policy name, enforcement level, CL version, and Agent software version. A receipt is sent back to the Server after the received information is consumed by the Agent and its configuration is updated; which can take upwards of 90 seconds based upon amount of changes and system load. This receipt is sent ‘immediately’ after this processing as long as a connection to the Server can be established at that time. If a connection cannot be established to the Server, the Agent will continue to attempt to establish a connection every 30 second and will send the receipt as soon as a connection is established.

An administrative user on the Console can verify the information about the endpoint system and the current status of the Agent’s configuration. For each endpoint system, an administrative user can view its hostname, its IP address, its MAC address, policy name consumed by Agent, Connected Enforcement Level consumed by Agent, Disconnected Enforcement Level consumed by Agent, CL version consumed by Agent, the Agent’s software version, the current Policy Status (policy and enforcement level issues), and Upgrade Status (Agent software issues). Refer to the “Viewing the Table of Computers” and “Viewing Complete Details for One Computer” sections of Chapter 4 Managing Computers in Reference [4] for a full explanation of navigating the Console to review this information.

6.2.4 Configure Agent Logging

Once the Agents have been installed, the administrator will need to set the debugging level for Agent logging and set Linux audit log rollover settings by performing the following steps:

1. Log in to the Console
2. Go to Assets / Computers

3. For each endpoint system:
    a. Click the View Details button
    b. In the right menu, expand Set Debug Level
    c. Debug Level:
        i. Set Verbose for Windows Agent
        ii. Set Medium for Linux Agent
    d. Debug Duration: Permanent
    e. Click Go
    f. Click the Computers breadcrumb to return to the Computers list
4. Visit <server>/agent_config.php
5. Click Add Agent Config
    a. Property Name: Max Diagnostic File Size
    b. Host ID (0 For All): 0
    c. Value: max_diagnostic_file_size_bytes=52428800
    d. Macros: <empty, do not enter anything>
    e. Platform: Linux
    f. Status: Enabled
    g. Created For: All Current and Future Policies
    h. Click Save
6. Click Add Agent Config
    a. Property Name: Max Diagnostic Files To Keep
    b. Host ID (0 For All): 0
    c. Value: max_diagnostic_files_to_keep=1
    d. Macros: <empty, do not enter anything>
    e. Platform: Linux
    f. Status: Enabled
    g. Created For: All Current and Future Policies
    h. Click Save

7 Secure Management

7.1 User and Role Management

Upon the initial authentication to the TOE's Console interface, the administrative user's session is associated with their validated username from either the TOE's local user table or from Active Directory, if applicable their AD Group Name, and their assigned role. Administrative user accounts can be explicitly assigned a role based upon their username or the role can be derived from their AD group membership as determined by their assigned AD Group Name. Roles are associated with usernames and AD Group Names within the SQL Server Database which is accessed by the TOE's Server. An administrative user's assigned role will determine the permissions that are available to the administrative user.

Any changes to an administrative user's role assignment will take effect immediately (before next action). If the permissions assigned to a role are changed while an administrative user with that role is logged in, those changes will also take immediate effect (administrative users may need to log out and log back in in order for new permissions to be implemented, but removed permissions will be revoked immediately).

7.1.1 Authenticating to the Console

Before allowing any other TSF-mediated actions, an administrative user must first identify and authenticate to the TOE via its Console interface. If a user attempts to access a Console webpage and does not have a valid user session, the Console will redirect the user to the login page for authentication to the TOE. An administrative user identifies and authenticates to the TOE by entering their username and password credentials. In the evaluated configuration, the TOE is configured to verify credentials against an Active Directory instance as well as the TOE's local credential table stored in an SQL Server Database. The TOE will first verify the entered credentials against the Active Directory instance with an LDAP bind request. If the credentials match an Active Directory user, the administrative user will be logged into the Console and will receive the role assigned to the user account based upon their AD username or AD Group Name within the SQL Server Database. If the credentials do not match an Active Directory user but the account exists, the administrative user will fail authentication and not be allowed access to the Console. If the credentials do not match an Active Directory user account, the credentials will then be checked against the local username and password table within the SQL Server Database. If the credentials match a locally defined user account, the administrative user will be logged into the Console and will receive the role assigned to the user account based upon their TOE defined username within the SQL Server Database. If the credentials do not match a locally defined user account, the administrative user will fail authentication and not be allowed access to the Console.

1. After the TOE has been successfully installed, open Google Chrome web browser and enter the correct URL. The URL will be:

   https://<server_name.domain.extension>

2. The Console login page will appear. The administrative user will then enter their username and password. For first-time login, enter the default username (admin) and password set during the Server's installation.
3. Click the Log In button.
4. The Console's Home page will then appear, confirming user login.

7.1.2 User Session Logout

For all TOE users and on every page of the Console, a log out command is available on the username menu in the upper right area of the web page. Logging out ends the user's Console session. The steps to logout are:

1. In the username menu at the top right corner of console menu (with the default user, this menu will show as "Admin"), choose Log Out.
2. Respond "Yes" to the confirmation prompt.
3. The Console login page will appear, confirming user logout.

7.1.3 User Session Inactivity Timeout

The TOE will terminate an administrative user's remote session to the Console, if the session is inactive for a specific period of time as configured by an Admin. Modifications are made on the System Administration page under the Advanced Options tab. The default timeout setting is 120 minutes but can be set between 1 and 120 minutes in the evaluated configuration. The steps to set the timeout value are:

1. Log in to the App Control Console.
2. Navigate by clicking the Administration Gear > System Configuration > Advanced Options.
3. Click Edit button at the bottom.
4. Under ‘Carbon Black App Control Console’ change the value of "Log Users Out After" from any value between 1 to 120 minutes.
5. Click Update button at the bottom.

7.1.4 User Account Management

Each App Control Console user logs in to the TOE with a username and password. Login Accounts provide system-management professionals, security team members, and others who use the Console the ability to access and manage App Control features.

There is one built-in login account for the App Control Console, the ‘admin’ account. It provides a way to log in to the Console before other accounts are created, and it cannot be deleted. By default, this account has administrative privileges. It also has the ability to create new accounts, and to define their privileges.

To create additional App Control Console accounts, an administrator has two choices in the evaluated configuration:

- They can create accounts individually through the Console. These accounts are managed through the Console, and can be modified or deleted by users whose login accounts have the proper privileges.
- They can permit users to log in using Active Directory (AD) credentials and map different AD groups to different privileges. AD-based App Control Console logins appear as “External Accounts.”

The steps to creating user accounts through the Console are defined in the “Creating Login Accounts in the Console” section of Chapter 3 Managing Console Login Accounts in Reference [4]. This process includes defining the account’s username, specifying the account’s password, and assigning one or more roles to the account. Once created, user accounts can be managed through the “Changing Passwords and Other Account Details”, “Deleting Login Accounts”, and “Disabling Login Accounts” Sections of Chapter 3 Managing Console Login Accounts in Reference [4].

The steps for configuring the App Control Server to communicate with an Active Directory Server were performed as part of the initial installation and configuration of App Control in Section 6.1.5 of this document. This section also includes the process for mapping Active Directory user groups to App Control roles. These steps have been included below for continued management of Active Directory user role mappings after initial installation and configuration of App Control. Repeat the steps below for each domain account user group to App Control role mapping that will be defined for App Control Console users. For more information, refer to “Creating AD Mapping Rules” Section of Chapter 3 Managing Console Login Accounts in Reference [4].

1. Select the gear icon and click Login Accounts
2. Go to the User Role Mappings tab
3. Click Add Rule
4. Under Relationship select “is member of group”
5. Click the down arrow for Directory Object and select the domain account user group which will be mapped to the selected App Control role
6. For User Role To Apply select App Control role

7. Select Stop Evaluation
8. Click Save

7.1.5 Role Management

App Control associates administrative users accessing the Console with roles and supports the following roles: Read-Only, Power User, Admin (specified ‘Administrator’ within the TOE), and custom. The roles Read-Only, Power User, and Admin are built-in roles with predefined permissions that are available upon installation of App Control. Based upon the default permissions, the Read-Only role is only able to review information on the Console and is not able to manage the TOE’s functions. The default permissions of the Power User and Admin roles allow them to perform the Common Criteria relevant management activities defined in Table 7-1.

Management Activities	Administrative User Role	
	Admin	Power
Creation of policies	X	X
Transmission of policies	X	X
Managing file’s Approved Status (Definition of object attributes, Association of attributes with objects)	X	X
Creation of rules (Definition of subject attributes, Association of attributes with subjects)	X	X
Managing user accounts (Management of authentication data for interactive users)	X	
Managing user accounts (Management of authentication data for interactive users)	X	
Creation of rules (Configuration of auditable events)	X	X
Creation of rules (Configuration of auditable events for defined external entities)	X	X
Configuration of external audit storage location	X	
Managing user accounts (Definition of default subject security attributes, modification of subject security attributes)	X	
Creation of rules and policies (Configuration of the behavior of other ESM products)	X	X
Ranking of rules (Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected)	X	X
Management of the users that belong to a particular role	X	
Maintenance of the banner	X	

Table 7-1: Evaluated Components System Configurations

For consistency with the Common Criteria evaluation, the permissions defined for the default App Control roles should not be modified. App Control does allow for an administrator to create one or more custom roles and assign permissions to those roles. The management functionality which a custom role can perform depends on the permissions assigned to the custom role. Refer to “Managing Console User Roles” section of Chapter 3 Managing Console Login Accounts in Reference [4] for guidance on creating, modifying, disabling, and deleting roles as well as explaining permissions and assigning them to roles.

7.1.6 Non-User Accounts

The TOE components have a communication establishment process described in Section 6.2.3 of this document. This process is not considered authentication. Additionally, no operational environment components authenticate to the TOE.

The TOE has only a single role when the Server is managing one of its Agents called administrator. The Server assumes this role every time an Agent polls the Server.

7.2 Login Banner

The TOE displays a warning message on the Console's login page prior to the TOE's administrative users are able to perform authentication. The warning message text can be edited by an Admin via the Console through the following steps:

1. Log in to the App Control Console.
2. Navigate by clicking the Administration Gear > System Configuration > Advanced Options.
3. Click Edit button at the bottom.
4. Under 'Login Banner':
    a. Check the box next to "Display Login Banner" to display the banner.
    b. In the "Banner Text" field, enter the text that will be displayed in the banner on the login page.
    c. In the "Font Color", Background Color", and "Border Color" fields, enter the HTML color codes as desired.
5. Click Update button at the bottom.

7.3 Access Control Management

The App Control Console interface allows an administrative user to create policies, create rules, and associate rules with policies. Each endpoint system running an App Control Agent is assigned to a single App Control policy based upon the policy specific Agent installer. Policies allow administrative users to organize endpoint systems running the Agents into groups with common security requirements. The policy specifies an access control definition for the endpoint systems to which it has been assigned. Each policy has a unique name which is also associated internally by the TOE with a unique numeric identifier. The rules associated with a policy can be viewed within the policy, but rules are managed separately and are then assigned to policies. There are two categories of rules that can be managed by an administrative user through the Console: internal and administrative user generated. The internal rules come preloaded with the TOE and the administrative user generated rules are defined by the administrative users.

7.3.1 Policy Management

One of the most important settings for a policy is its Mode and in the evaluated configuration all policies will be run with Control selected for the Mode. The other Modes do not enforce access control as described by the SFRs. Control Mode also requires the Connected Enforcement Level and Disconnected Enforcement Level to be selected for the policy. Enforcement Levels define how access control decisions specified by the policy settings are controlled. The Connected Enforcement Level is used by Agents when their network connection to the Server is active based upon their last poll to the Server. The Disconnected Enforcement Level is used by Agents when their network connection to the Server is disconnected based upon their last poll to the Server.

The Enforcement Level choices are:

- High – Only operations on files with the Approved Status of Approved are permitted by the Agent. The Agent blocks all operations on files with the Approved Status of Unapproved or Banned.
- Medium – Operations on files with the Approved Status of Approved are permitted by the Agent. The Agent blocks all operations on files with the Approved Status of Banned. The Agent displays

a dialog box that provides client users the option to permit or block the operation on files with the Approved Status of Unapproved.

- Low – Operations on files with the Approved Status of Approved are permitted by the Agent. The Agent blocks all operations on files with the Approved Status of Banned. The Agent permits operations on files with the Approved Status of Unapproved but also records these access control events.

If the Connected Enforcement Level is set to Low, the Disconnected Enforcement Level will also be automatically set to Low. If the Connected Enforcement Level is set to High or Medium, the administrative user can choose a Disconnected Enforcement Level of High or Medium, and it may differ from the Connected Enforcement Level.

For the steps to manage policies, refer to "Policy and Enforcement Level Overview", "Creating Policies", "Policy Definitions", "Policy Settings", "Template Policy and Default Policy", "Editing a Policy", "Related Views in Policy Details", "Enforcement Levels", and "Deleting Policies" Sections of Chapter 5 Creating and Configuring Policies in [4]. As a reminder, when creating a policy Control Mode must be selected as well as select "Track File Changes" under Options.

When an administrative user creates a new policy via the Console interface, the TOE's Server will generate a custom installer for that policy. The administrative user will then download the installer file from the Server's Console and install the Agent manually on the endpoint systems that will be assigned that policy. Refer to Section 6.2.2 of this document for instructions on installing an Agent. After installation, the Agent will connect to the Server so that the Server can record that endpoint system as having an Agent installed and its associated policy.

After initial establishment of an Agent, the Server will verify that the Agent's policy version and CL version are current. From that point on, any time the policy version or the CL version are updated on the Server, the Server will immediately upon an Agent's next poll:

- Send the latest policy to the Agents that enforce that policy
- Send the latest CL of all rules to all Agents; except under the following two conditions:
    - a rule is only applicable to a specific platform (e.g., Linux agents will not receive registry rules)
    - the Agent is running an older version of the software and an updated rule is not compatible with the Agent

The Agent will then immediately begin processing these updates to its access control SFP and self-protection SFP. The Agent will apply all changes to its policy version. However, the Agent will only apply the rules within the CL version that apply to its policy.

An administrative user can view the policy assigned to an Agent by navigating Assets > Computers and locating the policy listed on the Agent's endpoint system row in the Computers table. The steps for an administrative user to change the policy assigned to an Agent post installation are described within "Moving Computers to Another Policy" Section of Chapter 4 Managing Computers in [4]. As soon as an administrative user has completed the steps described in this section, the administrative user has performed the management activity of transmission of policies for the Agent that had its policy changed. The steps to manage rules resulting in a new CL are described in Sections 7.3.3 and 7.3.4.

7.3.2 Managing Objects

The TOE maintains the security attribute of Name for the files, processes, and host configuration objects for use within the TOE's access control SFP and self-protection SFP. Recording these attributes begins with the process of file initialization which starts immediately after the Agent software is installed on a new endpoint system. Refer to Section 6.2.2 of this document for instructions on installing an Agent. File initialization involves the Agent performing an inventory of interesting files (includes non-executables, executables/scripts/processes, and host configuration) on the endpoint system within all fixed drives and creates a hash of each interesting file. When an Agent first connects to the Server, the Agent sends the Names of the interesting files and their associated hashes to the Server to update the Server's file inventory. It is the Name attribute which is ultimately used within rules to determine if the object applies to the rule.

The TOE maintains the security attribute of Approved Status for the files objects for use within the TOE's access control SFP and self-protection SFP. Each Agent will use the 'local' Approved Status attribute value for making access control decisions. Note that the Server can also have a 'global' Approved Status attribute for a file, but this attribute is used as part of the TOE's logic to define the 'local' Approved Status value used by Agents on endpoint systems with this file. The 'global' Approved Status attribute is not used to make access control decisions by the TOE because an Agent uses only its 'local' Approved Status value to make the access control decision and does not connect to the Server for any reason to make an access control decision. Starting with initialization, files are assigned their Approved Status attribute which can have the value of:

- Approved – allowed
- Banned – unallowed
- Unapproved – an allowed or unallowed decision has not yet been made

Approved Status can be assigned and changed through the TOE's internal logic automatically or specifically defined by an administrative user. An example of the TOE's internal logic is that all files present on an endpoint system during initialization receive the 'local' Approved Status value of Approved, unless the file's 'global' Approved Status has already been set to Banned. The steps for an administrative user to change the Approved Status assigned to an object on an endpoint system are described within "File-Specific Rules: Approvals and Bans" Section of Chapter 8 Approving and Banning Software in [4].

When creating a policy, an administrative user is able to select "Track File Changes" as an option under that policy. Being assigned a policy where this option is checked, will result in the Agent continuing to update the Server regarding its interesting file inventory (files added, deleted, or changed) post initialization during the Agent's polls of the Server. Any new unidentified interesting files that appear on the fixed, local drives of Agents' endpoint systems after initialization are classified as having the value of Unapproved, both for 'local' Approved Status and 'global' Approved Status. The file will keep its Unapproved value until it becomes Approved or Banned. Note that if the file has its 'local' Approved Status value changed to Approved or Banned, this will not impact the 'global' Approved Status value of Unapproved.

7.3.3 Administrative User Generated Rules

There are several types of administrative user generated rules depending on the type of object being managed. Rules define if an access control request will be permitted or blocked based upon the subject, object, operation, and attribute combination of that request.

Administrative user generated rules require different sets of data to be specified depending on the type of rule being managed. In addition to specifying any specific subject, object, operation, and attribute information required by the rule, the administrative user will also need to define other necessary information including: the rule's name, if the rule is enabled or disabled, the platform to which the rule applies, rank position of the rule, action (e.g., permit, block), and policies to which the rule applies. Rules can be assigned by the administrative user to all policies (including policies that have not yet been created) or to one or more policies individually.

7.3.3.1 Custom Software Rules

A majority of the administrative user generated rules claimed as part of the Common Criteria evaluation are based upon custom software rules. Table 7-2 contains a cell for all subject, object, operation, and attribute combinations included within the evaluation, except for authentication function which is described separately in this Section. Cells that are shaded black are handled using another type of administrative user generated rule described elsewhere in Section 7.3 of this document. The following steps must be followed for creating custom software rules for the applicable subject, object, operation, and attribute combinations. For more information on creating custom software rules refer to "Creating a Custom Rule", "Editing a Custom Rule", "Custom Rule Fields", "Specifying Paths and Processes", "Specifying Users or Groups", and "Deleting Custom Rules" Sections of Chapter 14 Custom Software Rules in [4].

NOTE: Other fields in custom software rules which are described in Chapter 14 Custom Software Rules in [4] were not explicitly tested in the Common Criteria evaluation.

1. Log in to the Console
2. Navigate to Rules > Software Rules
3. Click the Custom tab
4. Click the Add Custom Rule button
5. Enter the rule fields as follows:
    a. Rule Name: Define a rule name
    b. Status: Select 'Enabled' when ready to enforce
    c. Actions: Select 'Block', 'Permit', or 'Report'
    d. Rule Type: Refer to Table 7-2 to specify the Rule Type field and additional rule fields that are defined based upon the subject, object, operation, and attribute combinations defined through the Table's Columns and Rows
    e. Notifier: Check User Policy Specific Notifier
    f. Path or File: Specify the object on the Agent system for the rule to apply to
    g. Process:
        i. When defining a specific user or group as the subject, select 'Any Process'
        ii. When defining a process as the subject, select 'Any Process' or 'Specific Process' and define the process
    h. User or Group:

i. When defining a specific user or group as the subject, select ‘Any User’ or ‘Specific User or Group’ and define the user or group

ii. When defining a process as the subject, select ‘Any User’

i. Policies: Select all policies the rule will apply to

j. Enforcement Levels: Select Enforcement Levels to which the rule is applicable

6. Click the Save button

<table>
<thead>
<tr><th>Objects</th><th>Object Attributes</th><th>Operations</th><th>Windows User / Group</th><th>Windows Process</th><th>Linux User / Group</th><th>Linux Process</th></tr>
</thead>
<tbody>
<tr><td rowspan="5">Processes</td><td rowspan="5">Name</td><td>Execute</td><td colspan="4">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’ or ‘Windows’
Operations: Select ‘Execute’ and ‘Script Execute’</td></tr>
<tr><td>Delete</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Windows’
Operations: Select ‘Delete’</td><td colspan="2">Rule Type: Select ‘File Creation Control’
Platform: Select ‘Linux’</td></tr>
<tr><td>Terminate</td><td colspan="4" rowspan="2"></td></tr>
<tr><td>Change Permission</td></tr>
<tr style="display:none"><td></td></tr>
<tr><td rowspan="7">Files</td><td rowspan="5">Name</td><td>Create</td><td colspan="4">Rule Type: Select ‘File Creation Control’
Platform: Select ‘Linux’ or ‘Windows’</td></tr>
<tr><td>Read</td><td colspan="4">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’ or ‘Windows’
Operations: Select ‘Read’</td></tr>
<tr><td>Modify</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Windows’
Operations: Select ‘Write’</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’
Operations: Select ‘Write’
OR
Rule Type: Select ‘File Creation Control’
Platform: Select ‘Linux’</td></tr>
<tr><td>Delete</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Windows’
Operations: Select ‘Delete’</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’
Operations: Select ‘Delete’
OR
Rule Type: Select ‘File Creation Control’
Platform: Select ‘Linux’</td></tr>
<tr><td>Change Permission</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Windows’
Operations: Select ‘Permission Change’</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’
Operations: Select ‘Permission Change’
OR
Rule Type: Select ‘File Creation Control’
Platform: Select ‘Linux’</td></tr>
<tr><td rowspan="2">Approved Status</td><td>Read</td><td colspan="4">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’ or ‘Windows’
Operations: Select ‘Read’
File State: Select ‘Unapproved’, ‘Approved’, or ‘Banned’</td></tr>
<tr><td>Modify</td><td colspan="4">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’ or ‘Windows’
Operations: Select ‘Write’
File State: Select ‘Unapproved’, ‘Approved’, or ‘Banned’</td></tr>
</tbody>
</table>

<table>
<tr><td></td><td></td><td>Delete</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’ or ‘Windows’
Operations: Select ‘Delete’
File State: Select ‘Unapproved’, ‘Approved’, or ‘Banned’</td></tr>
<tr><td></td><td></td><td>Change Permission</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’ or ‘Windows’
Operations: Select ‘Permission Change’
File State: Select ‘Unapproved’, ‘Approved’, or ‘Banned’</td></tr>
<tr><td>Host Configuration</td><td>Name</td><td>Read</td><td colspan="2">Rule Type: Select ‘Expert’
Platform: Select ‘Linux’ or ‘Windows’
Operations: Select ‘Read’</td></tr>
<tr><td></td><td></td><td>Modify[1]</td><td colspan="2">Rule Type: Select ‘File Creation Control’
Platform: Select ‘Linux’ or ‘Windows’</td></tr>
<tr><td></td><td></td><td>Delete</td><td>■</td><td>Rule Type: Select ‘Expert’
Platform: Select ‘Linux’
Operations: Select ‘Delete’</td></tr>
</table>

Table 7-2: Custom Software Rules

7.3.3.2 Memory Rules

Some of the administrative user generated rules claimed as part of the Common Criteria evaluation are based upon memory rules. Table 7-3 contains a cell for all subject, object, operation, and attribute combinations which apply to memory rules. Cells that are shaded black are handled using another type of administrative user generated rule described elsewhere in Section 7.3 of this document. The following steps must be followed for creating memory rules for the applicable subject, object, operation, and attribute combinations. For more information on creating memory rules refer to “Creating Memory Rules”, “Editing a Memory Rule”, “Memory Rule Fields”, “Specifying the Rule Permissions”, “Specifying Target and Source Processes”, “Specifying Users or Groups”, and “Disabling or Deleting Memory Rules” Sections of Chapter 16 Memory Rules in [4].

NOTE: Other fields in memory rules which are described in Chapter 16 Memory Rules in [4] were not explicitly tested in the Common Criteria evaluation.

1. Log in to the Console
2. Navigate to Rules > Software Rules
3. Click the Memory tab
4. Click the Add Memory Rule button
5. Enter the rule fields as follows:
    a. Rule Name: Define a rule name
    b. Status: Select ‘Enabled’ when ready to enforce
    c. Expert Mode: Select ‘On’
    d. Operations: Refer to Table 7-3 to specify the Operations field that is defined based upon the subject, object, operation, and attribute combinations defined through the Table’s Columns and Rows
    e. Actions: Select ‘Block’, ‘Allow’, or ‘Report’
    f. Notifier: Check User Policy Specific Notifier

[1] This rule would only apply to Host Configuration files and not registry keys. Refer to Registry Rules for creating rules regarding registry keys.

g. Permissions: Refer to Table 7-3 to specify the Permissions field that is defined based upon the subject, object, operation, and attribute combinations defined through the Table's Columns and Rows
h. Target Process: Specify the object on the Agent system for the rule to apply to
i. Source Process:
    i. When defining a specific user or group as the subject, select 'Any Process'
    ii. When defining a process as the subject, select 'Any Process' or 'Specific Process' and define the process
j. User or Group:
    i. When defining a specific user or group as the subject, select 'Any User' or 'Specific User or Group' and define the user or group
    ii. When defining a process as the subject, select 'Any User'
k. Policies: Select all policies the rule will apply to
l. Enforcement Levels: Select Enforcement Levels to which the rule is applicable

6. Click the Save button

Objects	Object Attributes	Operations	Windows User / Group	Windows Process	Linux User / Group	Linux Process
Processes	Name	Execute				
		Delete				
		Terminate	Operations: Select 'Create Handle', 'Duplicate Handle', and 'Kill Process' Permissions: Select 'Control Process'			
		Change Permission	Operations: Select 'Create Handle' and 'Duplicate Handle' Permissions: Select 'Write Access'			

Table 7-3: Memory Rules

7.3.3.3 Registry Rules

Some of the administrative user generated rules claimed as part of the Common Criteria evaluation are based upon registry rules. Table 7-4 contains a cell for all subject, object, operation, and attribute combinations which apply to registry rules. Cells that are shaded black are handled using another type of administrative user generated rule described elsewhere in Section 7.3 of this document. The following steps must be followed for creating registry rules for the applicable subject, object, operation, and attribute combinations. For more information on creating registry rules refer to "Creating Registry Rules", "Editing a Registry Rule", "Registry Rule Fields", "Specifying a Write Action", "Specifying Registry Paths", "Specifying Processes in Registry Rules", "Specifying Users or Groups", and "Disabling or Deleting Registry Rules" Sections of Chapter 15 Registry Rules in [4].

NOTE: Other fields in registry rules which are described in Chapter 15 Registry Rules in [4] were not explicitly tested in the Common Criteria evaluation.

1. Log in to the Console

2. Navigate to Rules > Software Rules
3. Click the Registry tab
4. Click the Add Registry Rule button
5. Enter the rule fields as follows:
    a. Rule Name: Define a rule name
    b. Status: Select ‘Enabled’ when ready to enforce
    c. Expert Mode: Select ‘Off’
    d. Write Actions: Select ‘Block’, ‘Allow’, or ‘Report’
    e. Notifier: Check ‘User Policy Specific Notifier’
    f. Registry Path: Refer to Table 7-3 to specify the Registry Path field that is defined based upon the subject, object, operation, and attribute combinations defined through the Table’s Columns and Rows
    g. Source Process:
        i. When defining a specific user or group as the subject, select ‘Any Process’
        ii. When defining a process as the subject, select ‘Any Process’ or ‘Specific Process’ and define the process
    h. User or Group:
        i. When defining a specific user or group as the subject, select ‘Any User’ or ‘Specific User or Group’ and define the user or group
        ii. When defining a process as the subject, select ‘Any User’
    i. Policies: Select all policies the rule will apply to
    j. Enforcement Levels: Select Enforcement Levels to which the rule is applicable
6. Click the Save button

Objects	Object Attributes	Operations	Windows User / Group	Windows Process	Linux User / Group	Linux Process
Host Configuration	Name	Read				
		Modify	Registry Path: Specify the object on the Agent system for the rule to apply to			
		Delete	Registry Path: Specify the object on the Agent system for the rule to apply to			

Table 7-4: Registry Rules

7.3.3.4 Rapid Configs

Some of the administrative user generated rules claimed as part of the Common Criteria evaluation are based upon rapid configs rules. Table 7-5 contains a cell for all subject, object, operation, and attribute combinations which apply to rapid configs rules. Cells that are shaded black are handled using another type of administrative user generated rule described elsewhere in Section 7.3 of this document. Rapid config rules are generated by VMware and require contacting VMware Support to obtain, refer to Section 9 of this document for VMware Support contact information.

1. Log in to the Console
2. Visit <server>/support.php
3. Under Advanced Configuration, select Show Import Buttons
4. Click Update
5. Go to Rules > Software Rules
6. Select the Rapid Configs tab
7. Click Add Rapid Config

8. Choose <rapid config filename>.b9u
9. Enter the password: CommonCriteria
10. Click the Upload button

The following steps must be followed for creating rapid configs rules for the applicable subject, object, operation, and attribute combinations. The steps are specific for each type of rapid config.

For the LinuxUserSpecificMemoryProtection.b9u rapid config:

1. Click the View Details button next to the rapid config name
2. Status: Select ‘Enabled’ when ready to enforce
3. Report Or Block Linux Process Termination: ‘Block’ or ‘Report’
4. Linux Processes To Block Termination: Specify the object on the Agent system for the rule to apply to
5. Notifier: Select ‘Enforce memory rules’
6. Users Allowed To Block Termination: Identify the user as the subject to be blocked
7. Select all policies the rule will apply to
8. Click the Save button

For the LinuxGroupSpecificMemoryProtection.b9u rapid config:

1. Click the View Details button next to the rapid config name
2. Status: Select ‘Enabled’ when ready to enforce
3. Report Or Block Linux Process Termination: ‘Block’ or ‘Report’
4. Linux Processes To Block Termination: Specify the object on the Agent system for the rule to apply to
5. Notifier: Select ‘Enforce memory rules’
6. Groups Allowed To Block Termination: Identify the user group as the subject to be blocked
7. Select all policies the rule will apply to
8. Click the Save button

For the LinuxProcessSpecificMemoryProtection.b9u rapid config:

1. Click the View Details button next to the rapid config name
2. Status: Select ‘Enabled’ when ready to enforce
3. Report Or Block Linux Process Termination: ‘Block’ or ‘Report’
4. Linux Processes To Block Termination: Specify the object on the Agent system for the rule to apply to
5. Processes To Block Termination BY: Identify the process as the subject to be blocked
6. Notifier: Select ‘Enforce memory rules’
7. Select all policies the rule will apply to
8. Click the Save button

For the LinuxMachineSpecificMemoryProtection.b9u rapid config:

1. Click the View Details button next to the rapid config name
2. Status: Select ‘Enabled’ when ready to enforce
3. Report Or Block Linux Process Termination: ‘Block’ or ‘Report’
4. Linux Processes To Block Termination: Specify the object on the Agent system for the rule to apply to
5. Machines To Block Termination On: Identify the machines that this rule will apply to by hostname
6. Notifier: Select ‘Enforce memory rules’
7. Select all policies the rule will apply to

8. Click the Save button

The rapid config LinuxMachineSpecificMemoryProtection.b9u is not listed in Table 7-5 because it is not based upon a user, group, or process operating as the subject to determine if the rule is enforced but the hostname of the endpoint system (i.e., machine) to which it is being applied. Refer to Section 7.3.3.6 for applying hostname to administrative user generated rules that are not rapid config rules.

Objects	Object Attributes	Operations	Windows User / Group	Windows Process	Linux User / Group	Linux Process
Processes	Name	Execute				
		Delete				
		Terminate			LinuxUserSpecific MemoryProtection.b9u LinuxGroupSpecific MemoryProtection.b9u	LinuxProcessSpecific MemoryProtection.b9u
		Change Permission			LinuxUserSpecific MemoryProtection.b9u LinuxGroupSpecific MemoryProtection.b9u	LinuxProcessSpecific MemoryProtection.b9u

Table 7-5: Rapid Config Rules

7.3.3.5 Block Authentication Function

App Control is able to deny access to the authentication function of an endpoint system on which one of its Agents is installed. Session establishment can be prevented when a rule blocks a specific client user, as defined by their Username, from executing the logon process for the endpoint system, as defined by its hostname.

1. Log in to the Console
2. Manually enter the following URL with App Control Server’s domain name filled in https://<server_name.domain.extension>/agent_config.php
3. Click Add Agent Config button
    a. Property Name: Define a configuration name
    b. Host ID: Search for endpoint system by Host ID and select endpoint system
    c. Value: Add the following to the field (additional usernames can be added and separated with a comma): block_users_from_logon=<username>
    d. Platform: Select ‘Windows’ or ‘Linux’
    e. Status: Select ‘Enabled’ when ready to enforce
    f. Created for: All Current and Future Policies
4. Click the Save button

7.3.3.6 Hostname Restrictions

All administrative user generated rules, except rapid config rules, can be restricted to only apply to an endpoint system based upon its hostname matching the hostname(s) defined within the rule. This is accomplished by using the OnlyIf macros with the Hostname condition. The syntax of OnlyIf macros is: <**OnlyIf:Hostname:***value*>. This could be entered into the Path or File field of a custom software rule, the Target Process field of a memory rule, and the Source Process field of a registry rule. For rapid config rules which are endpoint system specific, refer to Section 7.3.3.4.

7.3.3.7 Enabling and Ranking Rules

As an administrative user makes changes on the Console that will impact the TOE's access control Security Function Policy (SFP) and/or the TOE's self-protection SFP, the TOE's Server will generate a new configuration list (CL) with a unique version. When a new CL is generated, it is transmitted to all Agents, upon each Agent's next poll to the Server, so that the latest access control SFP and self-protection SFP can be applied on the endpoint systems.

The management of rules described within Sections 7.3.3 and 7.3.4 of this document will result in the Server generating a new CL. Additionally, administrative users can enable or disable rules and rank rules to generate new CLs. In any rule table, if the toggle switch in the Status column indicates that the rule is enabled (green background), the administrative user can click the toggle switch. The button will move to the left, the background will become white, and the rule is disabled. The reverse is performed to enable a currently disabled rule

The TOE requires administrative users to hierarchically rank all rules, and this is regardless of what policies to which the rules have been assigned. As a byproduct of the rule processing algorithm, there will not be a case where inconsistent rules are detected. This is because no two rules can have the same rank and as soon as a rule is moved up or down the hierarchy, the remaining rules are shifted by the TOE automatically. Rules have a rank number that are enforced by an Agent from lowest number to highest number, beginning with the rule ranked '1'. If an object matches one rule that blocks an action and another rule that allows it, the highest-ranking rule (that is, the one with the lowest number), takes precedence and the lower-ranked (higher number) rule has no effect. Administrative users can change the ranking of rules if they decide that they want one of the rules to be considered before its current position. For steps on ranking rules refer to "Rule Ranking" Section of Chapter 14 Custom Software Rules in [4]. Although this is described under Chapter 14 Custom Software Rules, these steps work for all administrative rules.

7.3.4 Internal Rules

Internal rules apply to all platforms and all can be reviewed by administrative users, but only certain internal rules can be modified by administrative users. One method an internal rule can be modified by an administrative user includes configuring it as either Active (i.e., enabled), Off (i.e., disabled), or Report Only. Report Only will permit the action but will record what would have been blocked if the setting were active.

The Custom Rules table includes rules labeled Internal. These are the rules administrative users enable or disable in other parts of the Console, specifically in the "Device Control Settings" and "Advanced" tabs on the Edit Policy page. Refer to Section 7.3.1 of this document for information on managing policies.

An internal rule shows its status as Enabled in the rules table if it is enabled in any policy. An administrative user cannot enable, disable, modify, or move Internal Rules in the Custom Rules table, but the administrative user can move administrator user generated Custom Rules, relative to the Internal Rules to better control how and when different rules are enforced. Refer to Section 7.3.3.7 of this document for ranking rules.

7.4 Secure State

7.4.1 Failure of Agent to Server Communications

When connectivity is down between the Agent and the Server, the Agent will enforce the last received policy and CL, and request a connection to the Server every 30 seconds until communications are restored. Once connectivity is restored, the Agent will immediately query the Server for the most up-to-date policy and CL data. This is automatically configured in the evaluated configuration and thus, requires no action by an administrative user to configure.

The TOE's Agent will always enforce its latest configuration as defined by its policy and CL of rules regardless of if communication with the Server is currently active or not active based upon the Agent's last polling attempt of the Server. An Agent's policy defines two Enforcement Levels: one when the Agent is actively connected to the Server called the Connected Enforcement Level and another when the Agent cannot reach the Server called the Disconnected Enforcement Level. The configuration of these Enforcement Levels can be the same or one may be stricter than the other depending on the manner that the configuring administrative user wants access control enforced on the endpoint system when there is a communication outage between the Agent and Server. Refer to Section 7.3.1 of this document for more information on Enforcement Levels and defining them as part of managing policies.

7.4.2 Failure of an Agent

The TOE will preserve a secure state in the event of an unanticipated termination of an Agent by automatically restarting the Agent. This requires no action by an administrative user.

For an Agent installed on Windows endpoint system, Windows' Service Control Manager (SCM) will restart the service automatically in the event of a crash after 1000 milliseconds. This value is stored in the Windows registry and cannot be modified because of the TOE's default self-protection SFP.

For an Agent installed on Linux endpoint system, the crash handler is implemented by the Agent. The Agent's kernel driver will detect an unclean exit of the process and perform an automatic restart.

8 Auditing

The Agent generates its own audit data for its events. All audit data produced by the Agent is sent to the Server over a TLS connection provided by the TOE's underlying operating systems; except audit data related to failed connections to the Server which is written to the Agent's audit logs (TOE-internal storage) stored on the underlying operating system. Note each Agent relies on its underlying operating system to provide TLS, replay detection is built into this protocol, for the connection between the Agent and the Server. Thus, the underlying operating system would be responsible for auditing any rejected TLS traffic (i.e., detection of replay) which would occur without the Agent's knowledge.

The Agent sends its audit events to the Server in batches of every ten events or every 30 seconds (whichever occurs first). This requires the Agent to buffer these audit events before sending them to the Server as well as remove the events from its buffer once they are successfully sent to the Server.

If the connection to the Server is severed, the Agent will continue to operate. The Agent will still attempt to connect to the Server and these attempts will be audited to the Agent's audit logs (TOE-internal storage). The Agent will also buffer up to 5,000 audit events for sending to the Server. When this cap is exceeded, the Agent will begin deleting the oldest 10% of the audit events in its buffer, until the number of audit events is below the cap. Once the connection is re-established, the Agent will continue to send its buffered audit events to the Server. This includes any audit events that occurred during the communication outage between the Agent and the Server, up to the last audit event previously sent to the Server before the communication outage or the oldest audit event still buffered by the Agent. Therefore, if more than 5,000 audit events occurred during the communication outage, not all audit events that occurred during the communication outage will be audited by the TOE.

The Agent stores different types of audit records in its audit logs and those that it sends to the Server. Therefore, there is no scenario where audit reconciliation is possible between the audit logs (TOE-internal storage) and the Server.

The Server generates audit data for events that occur on the Server and Console. All audit data produced by the Server is stored in the SQL Server Database; except audit data related to receiving connections from Agents, connecting to the SQL Server Database, and connecting to the Active Directory which is written to the Server's audit logs (TOE-internal storage) stored on the underlying operating system. The Server will also store audit data received from the Agent in the SQL Server Database.

The Server stores different types of audit records in the SQL Server Database and its audit logs. Therefore, there is no scenario where audit reconciliation is possible between the audit logs (TOE-internal storage) and the SQL Server Database.

During the App Control Server's initialization, the Server will initiate and maintain a connection to the SQL Server Database which is required for the Server and its Console interface to perform any function. The connection from the Server to the SQL Server Database occurs within the local Windows machine on which both of these components are installed. Throughout the Server's operation, audit records and other TOE data is stored and retrieved from the SQL Server Database by the Server making SQL statements and queries. If the connection from the Server to the SQL Server Database is severed, no management functions can be performed on the Console as well as all Server functions that would result in audit data being stored in the SQL Server Database cannot be performed. The Server will still attempt to connect to the SQL Server Database and these attempts will be audited to the Server's audit logs. Once the connection is re-established Console management functionality, Server functionality, and all auditing resumes automatically.

8.1 Audit Record Examples

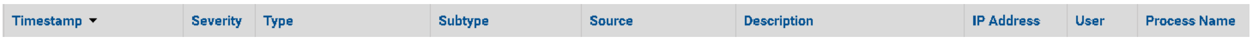
8.1.1 Events Audit Records

The Events audit records are stored in the SQL Server Database and can be access with the following steps:

1. Log in to the Console
2. Navigate to Reports > Events
3. The Events page will be displayed

The Events page allows administrative users to customize the view of the audit records by applying filters, searching, and changing the columns displayed. For more information on customizing the view of audit records, refer to “Pages, Tabs and Saved Views” Section of Chapter 2 Using the Console in Reference [4].

At least the following columns need to be displayed to properly review the Events audit records and the columns contain the following information in each field:

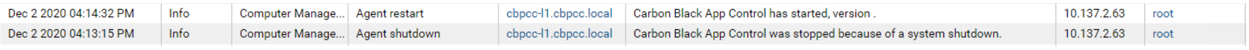


Timestamp ▾	Severity	Type	Subtype	Source	Description	IP Address	User	Process Name

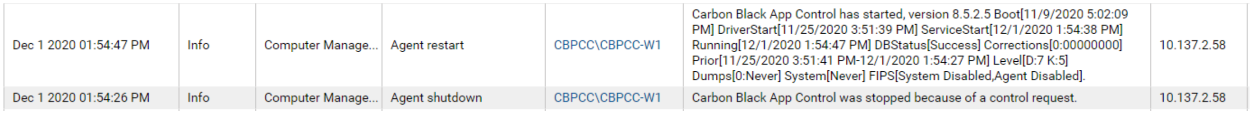
- Timestamp – Date and time of the event
- Severity – Categorization of severity of the event, based upon Syslog message guidelines
- Type – High-level categorization of the event
- Subtype – Type of event
- Source – TOE component which produced the event
- Description – Detailed information regarding the event, includes the outcome (success or failure) of the event
- IP Address – TOE component impacted by the event
- User – Subject identity (if applicable) of the event
- Process Name – Subject identity (if applicable) of the event

Below is an overview of the audit records which can be viewed on the Events page. The overview includes the name of the event (bold text), one or more examples of the event (picture), and an explanation of any additional information included within the event.

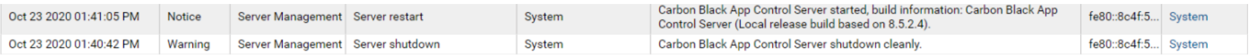
Start-up and shutdown of the audit functions



Dec 2 2020 04:14:32 PM	Info	Computer Manage...	Agent restart	cbpcc-l1.cbpcc.local	Carbon Black App Control has started, version .	10.137.2.63	root
Dec 2 2020 04:13:15 PM	Info	Computer Manage...	Agent shutdown	cbpcc-l1.cbpcc.local	Carbon Black App Control was stopped because of a system shutdown.	10.137.2.63	root



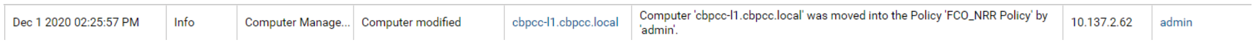
Dec 1 2020 01:54:47 PM	Info	Computer Manage...	Agent restart	CBPCC\CBPCC-W1	Carbon Black App Control has started, version 8.5.2.5 Boot[11/9/2020 5:02:09 PM] DriverStart[11/25/2020 3:51:39 PM] ServiceStart[12/1/2020 1:54:38 PM] Running[12/1/2020 1:54:47 PM] DBStatus[Success] Corrections[0:00000000] Prior[11/25/2020 3:51:41 PM-12/1/2020 1:54:27 PM] Level[D:7 K:5] Dumps[0:Never] System[Never] FIPS[System Disabled,Agent Disabled].	10.137.2.58
Dec 1 2020 01:54:26 PM	Info	Computer Manage...	Agent shutdown	CBPCC\CBPCC-W1	Carbon Black App Control was stopped because of a control request.	10.137.2.58



Oct 23 2020 01:41:05 PM	Notice	Server Management	Server restart	System	Carbon Black App Control Server started, build information: Carbon Black App Control Server (Local release build based on 8.5.2.4).	fe80::8c4f:5...	System
Oct 23 2020 01:40:42 PM	Warning	Server Management	Server shutdown	System	Carbon Black App Control Server shutdown cleanly.	fe80::8c4f:5...	System

The above three pairs of audit record examples depict the shutdown and then start-up of the audit functions for an Agent installed on a Linux endpoint, an Agent installed on a Windows endpoint, and the App Control Server.

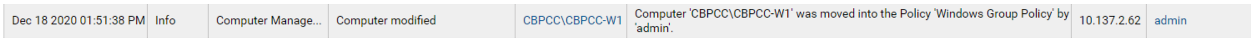
The invocation of the non-repudiation service



Dec 1 2020 02:25:57 PM	Info	Computer Manage...	Computer modified	cbpcc-l1.cbpcc.local	Computer 'cbpcc-l1.cbpcc.local' was moved into the Policy 'FCO_NRR Policy' by 'admin'.	10.137.2.62	admin

The Description field also includes the policy name (i.e., identification of the information), the endpoint which received the policy (i.e., the destination) and as a whole it covers the evidence back to the App Control Server (i.e., copy of the evidence provided).

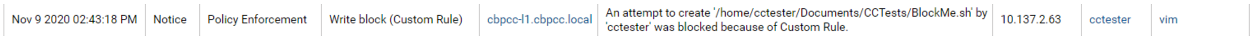
Any changes to the enforced policy or policies



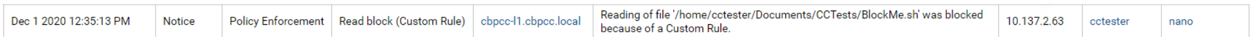
Dec 18 2020 01:51:38 PM	Info	Computer Manage...	Computer modified	CBPCC\CBPCC-W1	Computer 'CBPCC\CBPCC-W1' was moved into the Policy 'Windows Group Policy' by 'admin'.	10.137.2.62	admin

The IP address provides identification of Policy Management product making the change.

All requests to perform an operation on an object covered by the SFP



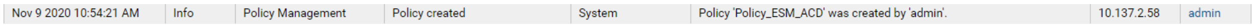
Nov 9 2020 02:43:18 PM	Notice	Policy Enforcement	Write block (Custom Rule)	cbpcc-l1.cbpcc.local	An attempt to create '/home/cctester/Documents/CCTests/BlockMe.sh' by 'cctester' was blocked because of Custom Rule.	10.137.2.63	cctester	vim



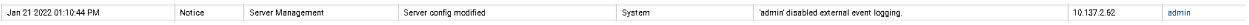
Dec 1 2020 12:35:13 PM	Notice	Policy Enforcement	Read block (Custom Rule)	cbpcc-l1.cbpcc.local	Reading of file '/home/cctester/Documents/CCTests/BlockMe.sh' was blocked because of a Custom Rule.	10.137.2.63	cctester	nano

The Description field includes the path and/or name of the object (i.e., object identity) and the requested operation (e.g., reading, create).

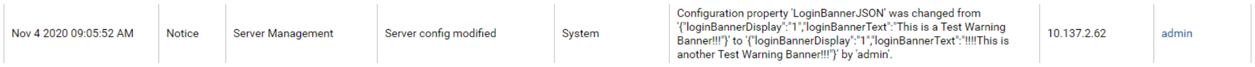
All modifications to TSF behavior



Nov 9 2020 10:54:21 AM	Info	Policy Management	Policy created	System	Policy 'Policy_ESM_ACD' was created by 'admin'.	10.137.2.58	admin



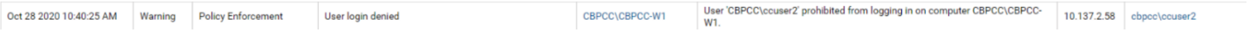
Jan 21 2022 01:10:44 PM	Notice	Server Management	Server config modified	System	'admin' disabled external event logging.	10.137.2.62	admin



Nov 4 2020 09:05:52 AM	Notice	Server Management	Server config modified	System	Configuration property 'LoginBannerJSON' was changed from '{"loginBannerDisplay":"1","loginBannerText":"This is a Test Warning Banner!!!"}' to '{"loginBannerDisplay":"1","loginBannerText":"!!!!This is another Test Warning Banner!!!"}' by 'admin'.	10.137.2.62	admin

The above audit record examples are for the creation of a policy, modifying the audit storage location, and modifying the banner. Additional Event page audit records examples within Section 8.1 also provide examples of audit records for modifying the TSF behavior. The Description field also includes the management function performed during the event.

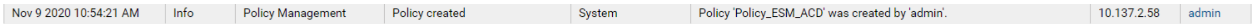
Denial of session establishment



Oct 28 2020 10:40:25 AM	Warning	Policy Enforcement	User login denied	CBPCC\CBPCC-W1	User 'CBPCC\ccuser2' prohibited from logging in on computer CBPCC\CBPCC-W1.	10.137.2.58	cbpcc\ccuser2

The above audit record is depicting a policy blocking a client user's authentication to an endpoint system. Refer to the "All use of the authentication mechanism" audit record for administrative user's authentication actions via the Console.

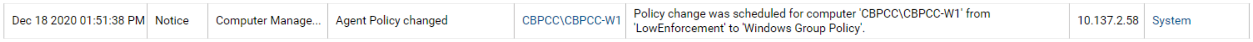
Creation or modification of policy



Nov 9 2020 10:54:21 AM	Info	Policy Management	Policy created	System	Policy 'Policy_ESM_ACD' was created by 'admin'.	10.137.2.58	admin

The Description field includes the policy's name (i.e., unique policy identifier).

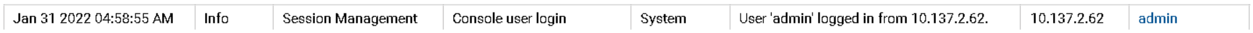
Transmission of policy to Access Control products



Dec 18 2020 01:51:38 PM	Notice	Computer Manage...	Agent Policy changed	CBPCC\CBPCC-W1	Policy change was scheduled for computer 'CBPCC\CBPCC-W1' from 'LowEnforcement' to 'Windows Group Policy'.	10.137.2.58	System

The Description field identifies the Agent which is receiving the policy (i.e., destination of policy).

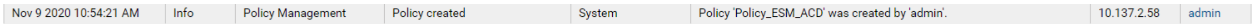
All use of the authentication mechanism



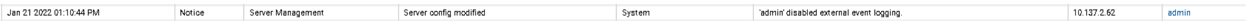
Jan 31 2022 04:58:55 AM	Info	Session Management	Console user login	System	User 'admin' logged in from 10.137.2.62.	10.137.2.62	admin

The above audit record is depicting an administrative user's authentication actions via the Console. Refer to the "Denial of session establishment" audit record for policy blocking a client user's authentication to an endpoint system.

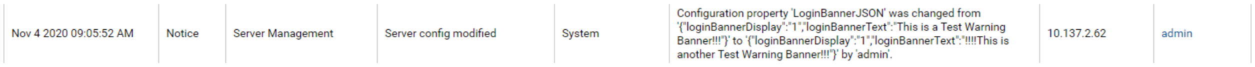
Use of the management functions



Nov 9 2020 10:54:21 AM	Info	Policy Management	Policy created	System	Policy 'Policy_ESM_ACD' was created by 'admin'.	10.137.2.58	admin



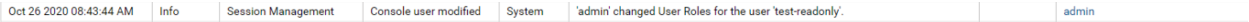
Jan 21 2022 01:10:44 PM	Notice	Server Management	Server config modified	System	'admin' disabled external event logging.	10.137.2.62	admin



Nov 4 2020 09:05:52 AM	Notice	Server Management	Server config modified	System	Configuration property 'LoginBannerJSON' was changed from '{"loginBannerDisplay":"1","loginBannerText":"This is a Test Warning Banner!!!"}' to '{"loginBannerDisplay":"1","loginBannerText":"!!!!This is another Test Warning Banner!!!"}' by 'admin'.	10.137.2.62	admin

The above audit record examples are for the creation of a policy, modifying the audit storage location, and modifying the banner. Additional Event page audit records examples also provide examples of audit records for modifying the TSF behavior. The Description field also includes the management function performed during the event.

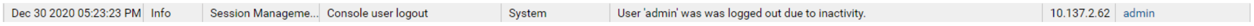
Modifications to the members of the management roles



Oct 26 2020 08:43:44 AM	Info	Session Management	Console user modified	System	'admin' changed User Roles for the user 'test-readonly'.		admin

The above audit record example is for changing an administrative user’s assigned role.

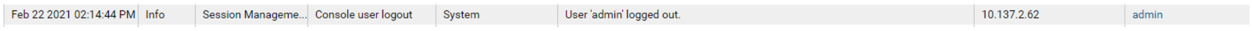
All session termination events



Dec 30 2020 05:23:23 PM	Info	Session Manageme...	Console user logout	System	User 'admin' was was logged out due to inactivity.	10.137.2.62	admin

The above audit record example is for an administrative user being automatically logged out of the Console due to inactivity.

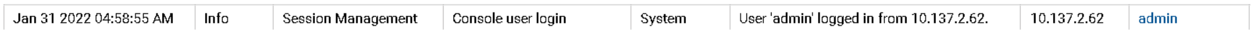
All session termination events



Feb 22 2021 02:14:44 PM	Info	Session Manageme...	Console user logout	System	User 'admin' logged out.	10.137.2.62	admin

The above audit record example is for an administrative user manually logging out of the Console.

All attempted uses of the trusted path functions



Jan 31 2022 04:58:55 AM	Info	Session Management	Console user login	System	User 'admin' logged in from 10.137.2.62.	10.137.2.62	admin

The User field provides identification of user associated with all trusted path functions.

8.1.2 Rules Audit Records

The Rules audit records are stored in the SQL Server Database and can be access with the following steps:

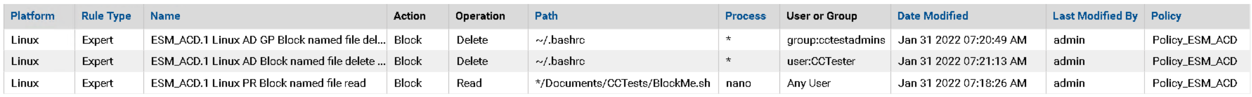
1. Log in to the Console
2. Navigate to Rules > Software Rules
3. The Software Rules page will be displayed

The Rules page allows administrative users to customize the view of the rules audit records by applying filters, searching, and changing the columns displayed. For more information on customizing the view of rules audit records, refer to “Pages, Tabs and Saved Views” Section of Chapter 2 Using the Console in Reference [4].

Each Rules audit record covers the following types of audit records:

- All modifications to audit configuration – The TOE’s selectable audit is based upon administrative users defining rules and specifying that events triggering the rules need to be audited
- Definition of subject attributes – As part of defining rules, an administrative users create subjects and by doing so assigns them attributes (i.e., Username, AD Group Name, Process Name)
- Association of attributes with subjects – As part of defining rules, an administrative users create subjects and by doing so assigns them attributes (i.e., Username, AD Group Name, Process Name)

At least the following columns need to be displayed to properly review the Rules audit records and the columns contain the following information in each field:



Platform	Rule Type	Name	Action	Operation	Path	Process	User or Group	Date Modified	Last Modified By	Policy
Linux	Expert	ESM_ACD.1 Linux AD GP Block named file del...	Block	Delete	~/.bashrc	*	group:cctestadmins	Jan 31 2022 07:20:49 AM	admin	Policy_ESM_ACD
Linux	Expert	ESM_ACD.1 Linux AD Block named file delete ...	Block	Delete	~/.bashrc	*	user:CCTester	Jan 31 2022 07:21:13 AM	admin	Policy_ESM_ACD
Linux	Expert	ESM_ACD.1 Linux PR Block named file read	Block	Read	*/Documents/CCTests/BlockMe.sh	nano	Any User	Jan 31 2022 07:18:26 AM	admin	Policy_ESM_ACD

- Platform – The platform to which the rule is applicable
- Rule Type – Type of event
- Name – The name given to the rule
- Action – The action the Agent will take if the rule is enforced
- Path – The path and/or name of the object attribute defined within the rule
- Process – Identification of the subject attribute defined within the rule, if a process has been defined
- User or Group – Identification of the subject attribute defined within the rule, if a user or group has been defined
- Date Modified – Date and time of the event
- Last Modified By – Subject identity (if applicable) of the event
- Policy – The names of the policy to which the rule is assigned

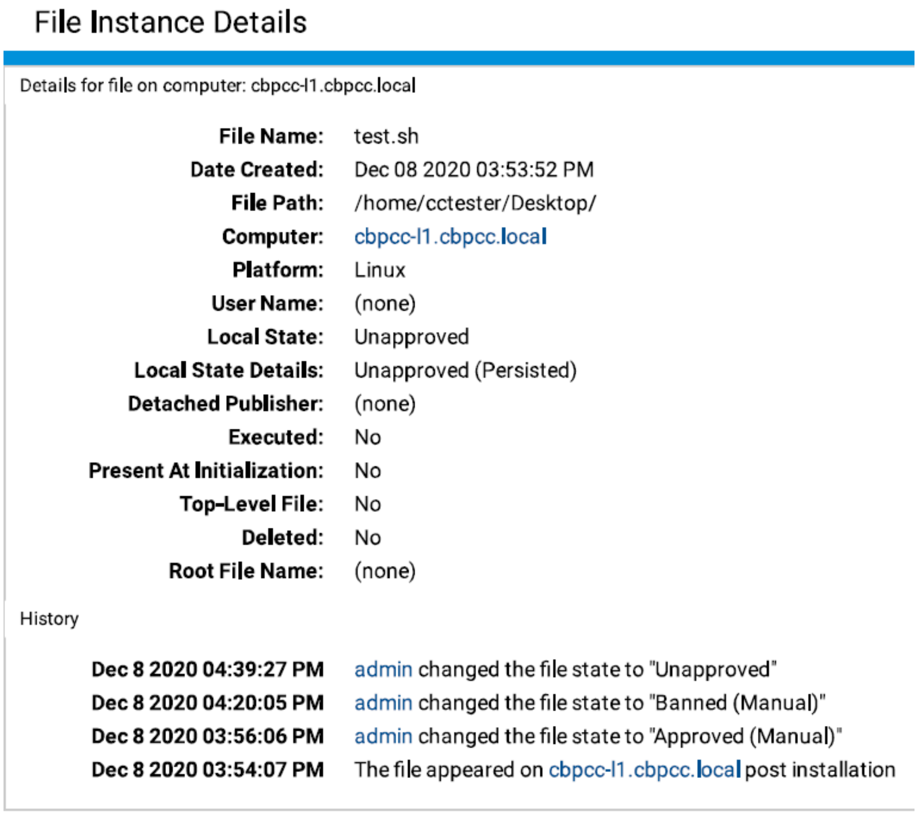
8.1.3 Files Audit Records

The Files audit records are stored in the SQL Server Database and can be access with the following steps:

1. Log in to the Console
2. Navigate to Assets > Computers
3. Select the Details button next to the endpoint system that has the file to be reviewed
4. On the right pane, select ‘Files on this Computer’
5. Search for the file with the audit records to be reviewed

Each Files audit record covers the following types of audit records:

- Definition of object attributes – specification of the attributes Name and Approved Status to the file object
- Association of attributes with objects – assigning of the attributes Name and Approved Status to the file object



File Instance Details

Details for file on computer: cbpcc-l1.cbpcc.local

File Name:	test.sh
Date Created:	Dec 08 2020 03:53:52 PM
File Path:	/home/cctester/Desktop/
Computer:	cbpcc-l1.cbpcc.local
Platform:	Linux
User Name:	(none)
Local State:	Unapproved
Local State Details:	Unapproved (Persisted)
Detached Publisher:	(none)
Executed:	No
Present At Initialization:	No
Top-Level File:	No
Deleted:	No
Root File Name:	(none)

History

Dec 8 2020 04:39:27 PM	admin changed the file state to "Unapproved"
Dec 8 2020 04:20:05 PM	admin changed the file state to "Banned (Manual)"
Dec 8 2020 03:56:06 PM	admin changed the file state to "Approved (Manual)"
Dec 8 2020 03:54:07 PM	The file appeared on cbpcc-l1.cbpcc.local post installation

NOTE: The File Instance Details page includes additional information between the 'Details for file on computer' and 'History' sections. This information is to help track files across a full deployment and not part of the Files audit records. The other information has been excluded in the picture above to depict only the fields related to the audit content.

- File Name – Together with the File Path and Computer fields, this provides the identification of the object and the attribute (Name)
- Date Created – Time this file was created on the endpoint system
- File Path – Together with the File Name and Computer fields, this provides the identification of the object and the attribute defined (i.e., Name attribute)
- Computer – Together with the File Name and File Path fields, this provides the identification of the object and the attribute defined (i.e., Name attribute)
- Platform – Platform (i.e., Windows, Linux) of the endpoint system on which the file exists
- User Name – Name of the client user logged in when this file was created.
- Local State – Identification of the attribute defined (Approved Status attribute)
- Local State Details – File-state metadata for use by VMware Support engineers
- Detached Publisher – If this file did not have its own certificate but was indirectly signed via a "detached certificate," this field appears and shows the name of the publisher.
- Executed – Indicates whether this file instance has been executed or not.
- Present At Initialization – Indicates whether this file instance was among the files present on the computer when the App Control Agent was installed (i.e., Yes), or whether it appeared after installation (i.e., No).

- Top-Level File – Indicates whether the file is a top-level file; that is, one that was not installed by or copied from another file.
- Deleted – Indicates whether this file instance has been deleted from the computer it was on.
- Root File Name – File that wrote the current file.
- History – Contains the following:
    - Date and time of the event (e.g., Dec 8 2020 04:39:27 PM)
    - Type of event (e.g., file appeared, changed the file state)
    - Subject identity (if applicable) (e.g., admin)
    - Outcome (success or failure) of the event (e.g., appeared, changed)

8.1.4 Server Log File Audit Records

The Server Log File is access through the Windows filesystem by the administrator navigating to the directory C:\Program Files (x86)\Bit9\Parity Server and opening the file ServerLog.bt9 with a text editor.

The format of the Server Log File audit records is:

[Record identifier] Date and timestamp (Server process) Details field

Below is an overview of the audit records which can be viewed in the Server Log File. The overview includes the name of the event (bold text), an example of the event, and an explanation of the information included within the event.

All use of trusted channel functions

[304907] 2022-02-01 13:03:02 (12876 Admin Thread 1)   2/1/2022 1:03:02 PM: DEBUG: 1: GetObjectTrySecureWithPassword: Initiating secure connection to LDAP:

The above audit record example is for a connection from the App Control Server to the Active Directory instance. The information within the audit record:

- Date and time of the event (i.e., 2022-02-01 13:03:02)
- Type of event (i.e., secure connection)
- Subject identity (if applicable) – App Control Server which is generating the event, identified by its process (i.e., 12876 Admin Thread 1)
- Outcome (success or failure) of the event (i.e., Initiating)
- Identity of the initiator of the trusted channel – App Control Server initiating the connection, identified by its process (i.e., 12876 Admin Thread 1)
- Identity of the target of the trusted channel – Active Directory server (i.e., LDAP:)

All use of trusted channel functions

[187291] 2020-12-03 10:32:48 (1636 Main)Accepted new connection from 10.137.2.58 on port 41002.

The above audit record example is for a connection from the Agent to the App Control Server. The information within the audit record:

- Date and time of the event (i.e., 2020-12-03 10:32:48)
- Type of event (i.e., new connection)

- Subject identity (if applicable) – App Control Server which is generating the event, identified by its process (i.e., 1636 Main)
- Outcome (success or failure) of the event (i.e., Accepted)
- Identity of the initiator of the trusted channel – Agent initiating the connection (i.e., 10.137.2.58)
- Identity of the target of the trusted channel – App Control Server accepting the connection, identified by its process (i.e., 1636 Main)

Establishment and disestablishment of communications with audit server

[96482] 2022-01-31 17:38:21 (11844 ProcessManifests)   Connection attempt failed: [Microsoft][SQL Server Native Client 11.0]Named Pipes Provider: Could not open a connection to SQL Server [2].

The above audit record example is for the disestablishment with the SQL Server Database (i.e., audit server). The information within the audit record:

- Date and time of the event (i.e., 2022-01-31 17:38:21)
- Type of event (i.e., Connection attempt)
- Subject identity (if applicable) – App Control Server which is generating the event, identified by its process (i.e., 11844 ProcessManifests)
- Outcome (success or failure) of the event (i.e., failed)
- Identification of audit server – SQL Server Database stored on the same machine as the App Control Server (i.e., SQL Server)

[96486] 2022-01-31 17:38:21 (11844 ProcessManifests)   Created new SQL Connection. Server: localhost

The above audit record example is for the establishment with the SQL Server Database (i.e., audit server). The information within the audit record:

- Date and time of the event (i.e., 2022-01-31 17:38:21)
- Type of event (i.e., new SQL Connection)
- Subject identity (if applicable) – App Control Server which is generating the event, identified by its process (i.e., 11844 ProcessManifests)
- Outcome (success or failure) of the event (i.e., failed)
- Identification of audit server – SQL Server Database stored on the same machine as the App Control Server (i.e., Server: localhost)

8.1.5 Agent Log File Audit Records

The Agent Log File is access through the Agent's filesystem by navigating to the directory:

- Windows filesystem – C:\ProgramData\Bit9\Parity Agent\Logs\ and opening the file Trace.bt9 with a text editor
- Linux filesystem – /srv/bit9/data/Logs and opening the file Trace.bt9 with a text editor

The format of the Agent Log File audit records is:

Date and timestamp, timestamp in MS, thread ID - Details field

Below are overviews of the audit records which can be viewed in the Agent Log File for each endpoint system operating system. The overview includes the name of the event (bold text), an example of the event, and an explanation of the information included within the event.

Failure of communication between the TOE and Policy Management product

```
2022-02-01 13:17:07 5309730000 25092 - HttpTransport:InitiateResolve: Connect Server[APPCONTROL.LAB.LOCAL] Port[41002]

2022-02-01 13:17:07 5309730000 25092 - HttpTransport:GetPendingRequest: No requests

2022-02-01 13:17:07 5309730000 25091 - HttpTransport:HandleResolve: Connect

2022-02-01 13:17:07 5309730000 25091 - HttpTransport:InitiateConnect: Connect

2022-02-01 13:17:07 5309730000 25091 - Persistence:Next: Stmt[SELECT value FROM Settings WHERE name=?] Results[0]

2022-02-01 13:17:07 5309730000 25091 - HttpTransport:filterProtocolOptions: HTTPS/SSL Windows protocol encodings 0x00000000, HTTPS/SSL optionsMask= 0x00000000

2022-02-01 13:17:07 5309730000 25091 - HttpTransport:filterProtocolOptions: HTTPS/SSL specific protocols disabled: <>

2022-02-01 13:17:07 5309730000 25091 - HttpTransport:filterProtocolOptions: HTTPS/SSL SSL_CTX_get_options(): 0x01020004

2022-02-01 13:17:10 5309730000 25091 - HttpTransport:HandleConnect: Connect

2022-02-01 13:17:10 5309730000 25091 - HttpTransport:HandleConnect: Error[No route to host]

2022-02-01 13:17:10 5309730000 25091 - HttpTransport:HandleCompletion: Connect Transaction[0] Error[4-ConnectError]
```

The above audit record example is for the failure of communications between an Agent on a Linux endpoint and the App Control Server. The information within the audit record specifies:

- Date and time of the event (i.e., 2022-02-01 13:17:07)
- Type of event (i.e., Connect Server)
- Subject identity (if applicable) – Not Applicable
- outcome (success or failure) of the event (i.e., Error)
- Identity of the Policy Management product – Domain name of the App Control Server (i.e., APPCONTROL.LAB.LOCAL)
- Reason for the failure (i.e., No route to host)

Failure of communication between the TOE and Policy Management product

```
2022-01-14T12:55:47-05:00 181928783 (0C94) - B9WinHttpContext::SetRequest Begin: OldRequest[1FF5A8F0] NewRequest[00000000]

2022-01-14T12:55:47-05:00 181928783 (0C94) - B9WinHttpContext::SetRequest: Async callback disabled Handle[1FF5A8F0]
```

```
2022-01-14T12:55:47-05:00 181928783 (0C94) - B9WinHttpContext::SetRequest End:
OldRequest[00000000] NewRequest[00000000]

2022-01-14T12:55:47-05:00 181928783 (0C94) - SignalConnectionActivity isError[true]

2022-01-14T12:55:47-05:00 181928783 (0C94) - SignalConnectionActivity setting connection inactive
due to timeout

2022-01-14T12:55:47-05:00 181928783 (0C94) - ********* We are transitioning to OFFLINE while out
of session

2022-01-14T12:55:47-05:00 181928783 (0C94) - Post message to the kernel: Type[ChangeConfigProp]
Size[136]

2022-01-14T12:55:47-05:00 181928784 (0C94) - Post message to the kernel: Type[ChangeConfigProp]
Size[136]

2022-01-14T12:55:47-05:00 181928784 (0C94) - ********* We are transitioning to OUTOFSESSION
while OFFLINE

2022-01-14T12:55:47-05:00 181928784 (0C94) - Server communication Error[0]

2022-01-14T12:55:47-05:00 181928784 (0C94) - Poll Ret[0] AB[0] EVT[2] Mask[00000000|<None>]
Param1[40] Param2[40] Interval[30000]

2022-01-14T12:55:47-05:00 181928784 (0C94) - Poll: Failure Desc[Waiting] Error[0]
```

The above audit record example is for the failure of communications between an Agent on a Windows endpoint and the App Control Server. The information within the audit record specifies:

- Date and time of the event (i.e., 2022-01-14T12:55:47-05:00)
- Type of event (i.e., communication)
- Subject identity (if applicable) – Not Applicable
- outcome (success or failure) of the event (i.e., Error)
- Identity of the Policy Management product – App Control Server (i.e., Server)
- Reason for the failure (i.e., inactive due to timeout)

8.2 Audit Selection

The TOE performs selectable audit based upon administrative users defining rules and specifying that events triggering the rules need to be audited. Therefore, if a rule requiring auditing is triggered by an access request on an endpoint system protected by an Agent, the Agent will send the audited event to the Server. On the other hand, if a rule not requiring auditing is triggered by an access request on an endpoint system protected by an Agent, the Agent will not send an audited event to the Server. The following list describes the attributes and how they are specified in different rules as well as selecting certain rules:

- Object identity will be used to determine if an access request will generate an audit based upon the rule using the object’s Name or Approved Status attributes.
  - Refer to rules defined in Section 7.3.3.1 and their use of the "Path or File" field and when applicable the "File State" field
  - Refer to rules defined in Section 7.3.3.2 and their use of the "Target Process" field

    - Refer to rules defined in Section 7.3.3.3 and their use of the "Registry Path" field
    - Refer to rules defined in Section 7.3.3.4 and their use of the "Linux Processes To Block Termination" field
- User identity will be used to determine if an access request will generate an audit based upon the rule using the client user identity’s Username or AD Group Name attributes.
    - Refer to rules defined in Sections 7.3.3.1, 7.3.3.2, and 7.3.3.3, and their use of the "User or Group" field
    - Refer to rules defined in Section 7.3.3.4 and their use of the "Users Allowed To Block Termination" field and the “Groups Allowed To Block Termination” field
- Subject identity will be used to determine if an access request will generate an audit based upon the rule using the subject identity’s Process Name attribute.
    - Refer to rules defined in Section 7.3.3.1 and their use of the "Process" field
    - Refer to rules defined in Sections 7.3.3.2 and 7.3.3.3, and their use of the "Source Process" field
    - Refer to rules defined in Section 7.3.3.4 and their use of the "Processes To Block Termination BY" field
- Host identity will be used to determine if an access request will generate an audit based upon the rule using the endpoint system host identity’s hostname attribute.
    - Refer to the user of hostname defined in Section 7.3.3.4 for rapid config rules
    - Refer to the use of hostname defined in Section 7.3.3.6 for all rules but rapid config rules
- Event type will be used to determine if an access request will generate an audit based upon the rule defining the type of operation the subject is performing on the object.
    - Refer to rules defined in Section 7.3.3.1 and their use of the "Operations" field
    - Refer to rules defined in Section 7.3.3.2 and their use of the "Permissions" field
    - Refer to rules defined in Section 7.3.3.3 which cover the modify and delete operations
    - Refer to rules defined in Section 7.3.3.4 and their use of the terminate and change permission operations

8.3 Configuring Additional Audit Storage

The App Control Server can be configured to have audit records stored in an additional SQL database instance. It is important to note that this additional SQL database instance was not configured and used as part of the Common Criteria evaluation. However, this would allow for audit records to be potentially backed up and/or stored remotely. The steps below provide an overview for configuring the additional SQL database. Refer to “Logging Events to a Supplemental SQL Server” Section of Chapter 26 System Configuration in [4]

1. Log in to the Console
2. Navigate to System Configuration > Events
3. Enable “Use External Database”
4. Configure the domain string with the information for the second SQL Server
5. Click the Update button

9 Obtaining Technical Assistance

For your convenience, VMware Carbon Black Technical Support offers several channels for resolving support questions:

- Carbon Black User Exchange: https://community.carbonblack.com
- Email: cb-support@vmware.com
- Phone: 877.248.9098