Assurance Activities Report
for a Target of Evaluation

VMware
Carbon Black App Control v8.8.2

Assurance Activities Report (AAR)
Version 1.0

February 27, 2022

For Security Target Version 1.0

Evaluated by:

Booz | Allen | Hamilton

delivering results that endure

Cyber Assurance Testing Laboratory
NIAP Lab #200423-0
1100 West Street
Laurel, MD 20707

Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
VMware
3401 Hillview Ave
Palo Alto, CA 94304

The Author of the Security Target:
Booz Allen Hamilton,
1100 West Street,
Laurel, 20707 USA

The TOE Evaluation was sponsored by:
Booz Allen Hamilton

Evaluation Personnel:
Herbert Markle
Christopher Rakaczky

Applicable Common Criteria Version

Common Criteria for Information Technology Security Evaluation, September 2012 Version 3.1 Revision 4

Common Evaluation Methodology Version

Common Criteria for Information Technology Security Evaluation, Evaluation Methodology, September 2012 Version 3.1 Revision 4

Table of Contents

1 Purpose

The purpose of this document is to serve as a non-proprietary attestation that this evaluation has satisfied all of the TSS, AGD, and ATE Assurance Activities required by the Protection Profiles/Extended Packages to which the TOE claims exact conformance. This will give system integrators valuable information about product configuration and testing, help to align Common Criteria evaluations with DISA Security Requirements Guides and Security Test Implementation Guides (SRGs/STIGs), and thereby streamline the process for U.S. Government procurement of validated products.

2 TOE Summary Specification Assurance Activities

The evaluation team completed the testing of the Security Target (ST) VMware Carbon Black App Control v8.8.2 Security Target v1.0' and confirmed that the TOE Summary Specification (TSS) contains all Assurance Activities as specified by the *Protection Profile for Enterprise Security Management Access Control version 2.1* [ESM_AC_PP] and *Protection Profile for Enterprise Security Management Policy Management version 2.1* [ESM_PM_PP]. The evaluators were able to individually examine each SFR's TSS statements and determine that they comprised sufficient information to address each SFR claimed by the TOE as well as meet the expectations of the ESM_AC_PP and ESM_PM_PP Assurance Activities.

Through the evaluation of ASE_TSS.1-1, described in the ETR, the evaluators were able to determine that each SFR was described in enough detail to demonstrate that the TSF addresses the SFR. However, in some cases the Assurance Activities that are specified in the claimed source material instruct the evaluator to examine the TSS for a description of specific behavior to ensure that each SFR is described to an appropriate level of detail.

The following is a list of each SFR, the TSS Assurance Activities specified for the SFR, and how the TSS meets the Assurance Activities. Additionally, each SFR is accompanied by the source material ESM_AC_PP and ESM_PM_PP that defines where the most up-to-date TSS Assurance Activity was defined. Because the ST claims conformance to two Protection Profiles, the SFRs are preceded with [AC], [PM], or [AC+PM] to indicate whether each SFR comes from the ESM_AC_PP, ESM_PM_PP, or both.

[PM] ESM_ACD.1 – *"The evaluator shall do the following:*

- *Verify that the TSS identifies one or more compatible Access Control products*

Section 8.1.1 of the ST identifies the compatible agent as the App Control Agent. Based on the shorthand nomenclature in the overview section this is identified as the VMware Carbon Black App Control Agent.

- *Verify that the TSS describes the scope and granularity of the entities that define policies (subjects, objects, operations, attributes)*

Section 8.1.1 of the ST describes there are several types (e.g. file, custom, registry) 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. The subject, object, operation, and attribute combinations which the TOE manages are defined in Tables 6-2 and Tables 6-3 of the ST. Additionally, the attribute hostname can be used to restrict a rule to only apply to an endpoint system based upon its hostname matching the hostname(s) defined within the rule.

Table 6-2 and 6-3 of the ST identifies the subjects, subject attributes, objects, object attributes, and Operations into an clear understandable and granular method to understand the policies that can be created and the scope of what the policies can enforce.

- *Review STs for the compatible Access Control products and verify that there is correspondence between the policies the TOE is capable of creating and the policies the Access Control products are capable of consuming*

Section 8.1.1 of the ST states that 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 compatible Access Control product has been identified earlier as the VMware Carbon Black App Control Agent.

- *Verify that the TSS indicates how policies are identified"*

Section 8.1.1 of the ST describes that each policy has a unique name which is associated internally by the TOE with a unique numeric identifier.

All required information has been found in Section 8.1.1 of the ST and the evaluation team considers this activity satisfied.

[PM] ESM_ACT.1 – *"The evaluator shall check the TSS and ensure that it summarizes when and how policy data will be transmitted to Access Control products. This includes the ability to specify the product(s) that the policy data will be sent to."*

Section 8.1.2 of the ST states that after the initial manual installation has occurred, all updates will happen upon the Agent's next poll.

"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"

All required information has been found in Section 8.1.2 of the ST and the evaluation team considers this activity satisfied.

[PM] ESM_ATD.1 – *"The evaluator shall check the TSS to ensure that it describes the object attributes that are defined by the TOE and the purpose for their definition."*

Section 8.1.3 of the ST states that:

- 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.
- 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.

This is consistent with Table 6-2 and Table 6-3 of the ST. All required information has been found in Section 8.1.3 of the ST and the evaluation team considers this activity satisfied.

[PM] ESM_ATD.2 – *"The evaluator shall check the TSS to ensure that it describes the subject attributes that are defined by the TOE and the purpose for their definition."*

Section 8.1.3 of the ST states that:

- The TOE maintains the security attribute of Username and AD Group Name for the Active Directory Users Subjects for use within the TOE's access control SFP and self-protection SFP.

- The TOE maintains the security attribute of Process Name for the Processes Subjects for use within the TOE's access control SFP and self-protection SFP.

This is consistent with Table 6-2 and Table 6-3 of the ST. All required information has been found in Section 8.1.4 of the ST and the evaluation team considers this activity satisfied.

[PM] ESM_EAU.2 – *"The evaluator shall check the TSS in order to determine that it describes the TSF as requiring authentication to use and that it describes, for each type of user or IT entity that authenticates to the TOE, the identification and authentication mechanism that is used.*

The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each authentication mechanism that is used by the TSF."

Section 8.1.5 of the ST states that before allowing any other TSF-mediated actions, an administrative user must first identify and authenticate to the TOE via its Console interface. An administrative user identifies and authenticates to the TOE by entering their username and password credentials.

The TOE in the evaluated configuration is authenticated against an Active Directory instance as well as a local credential store. The description also defines that the Active Directory is used first to authenticate the administrative user. If no account exists on the Active Directory, then the TOE will check the local store.

In either case, if an account exists and the supplied password is incorrect the user is denied access.
Based on the second application note there is no need for an iteration because these are not two distinct sets of subjects being authenticated by two different mechanisms. The TSF is validating one subject first via Active Directory and then if need by the local store.

All required information has been found in Section 8.1.5 of the ST and the evaluation team considers this activity satisfied.

[AC] ESM_EID.2 – *"The evaluator shall check the TSS and ensure that it describes where the subject identity data that the TOE uses to make access control decisions comes from.*

The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each identification mechanism that is used by the TSF."

Section 8.1.6 of the ST states that the Agent relies on the endpoint system to provide a verified identity of a client user before they perform any TSF-mediated actions on the endpoint system.

The operating system will verify the entered credentials against the Active Directory instance with an LDAP bind request. If the credentials match an Active Directory user, the operating system will receive AD Group Names that the user account is associated with from Active Directory. The operating system will then provide the Agent with the verified username and AD Group Names associated with that client user's account. The Agent will then use this information to make access control decisions based upon its policy and rules

There is only one mechanism so there is no iteration. All required information has been found in Section 8.1.6 of the ST and the evaluation team considers this activity satisfied.

[PM] ESM_EID.2 – *This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.* This SFR does not contain any additional ESM_PM_PP TSS Assurance Activities.

[AC+PM] FAU_GEN.1 – *"The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records."*
Section 8.2.1 of the ST states that the audit records contain the date and time of the event, type of event type, subject identity (if applicable), and success or failure of the event are audited. Additionally, specific

audit events will include other data in the event's audit record based upon the 'Additional Information' columns in Table 6-4 and Table 6-5. Table 6-4 and 6-5 also define what audit records are generated specified by SFR and whether generated by the server [PM] or the Agent [AC].

All required information has been found in Section 8.2.1 of the ST and the evaluation team considers this activity satisfied.

[AC] FAU_SEL.1 – *"The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to have selective auditing and that it summarizes the mechanism(s) by which auditable events are selected for auditing."*

Section 8.2.2 of the ST states for the Agent: 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.

All required information has been found in Section 8.2.2 of the ST and the evaluation team considers this activity satisfied.

[PM] FAU_SEL_EXT.1 – *"The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to configure selective auditing for an Access Control product and that it summarizes the mechanism(s) by which auditable events are selected for auditing."*

Section 8.2.2 of the ST states for that 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 audit rules are based on the same attributes defined for subjects, objects and operations in ESM_ACD.1.

All required information has been found in Section 8.2.2 of the ST and the evaluation team considers this activity satisfied.

[AC] FAU_STG.1 – *"The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally, what happens when the local audit data store is full, and how these records are protected against unauthorized access."*

Section 8.2.3 of the ST states Administrative users do not have the ability to delete, modify, or manipulate the audit data that resides in the Agent's audit logs (TOE-internal storage) because the TOE does not provide an interface or mechanism to complete such actions. Additionally, the Agent will protect the TOE-internal storage from unauthorized deletion and unauthorized modification based upon the Agent enforcing the TOE's self-protection SFP
The Agent maintains two local audit logs with a maximum size of 50MB each. One audit log is actively being written to by the Agent and the other audit log is dormant, containing the events which occurred prior to the last rotate. When the active audit log reaches its maximum size, the Agent will rotate the audit logs by overwriting the dormant audit log with the previously active audit log and creating a new active log.

All required information has been found in Section 8.2.3 of the ST and the evaluation team considers this activity satisfied.

[AC+PM] FAU_STG_EXT.1 – TD0066 – *"The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit."*
If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM

product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.). Lastly, the described loss minimization mechanisms must be tested to ensure that they behave as documented.

Section 8.2.4 of the ST specifies the storage location as:

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 AD which is written to the Server's audit logs (TOE-internal storage) stored on the underlying operating system. The SQL Server Database is an Operational Environment component which is installed locally on the same system where the Server is installed. The Server will also store audit data received from the Agent in the SQL Server Database.

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. 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. Thus, audit records are not stored in two locations.

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.

All required information has been found in Section 8.2.4 of the ST and the evaluation team considers this activity satisfied.

[AC] FCO_NRR.2 – *"The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s).*

The evaluator shall also check the TSS to see that it discusses how the TOE identifies itself to the Policy Management product and how it provides evidence of the policy's consumption to the Policy Management product."

Section 8.3.1 of the ST identifies the Agent's attributes as hostname, IP address, and MAC address. Additionally, this section identifies the Policy's attributes as the current policy name, enforcement level, CL version, and Agent software version. The assigned attributes for both the Agent and Policy are consistent with the application notes provided in the PP.

Section 8.3.1 of the ST states that 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 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.

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.

All required information has been found in Section 8.3.1 of the ST and the evaluation team considers this activity satisfied.

[AC] FDP_ACF.1(1) – *"The evaluator shall check the TSS in order to verify that the TOE is capable of mediating the activities that are defined in Table 6 [within the ESM_AC_PP] and that the access control policy enforcement mechanism is described.*

The evaluator shall also check the TSS to determine that the method by which access control rules are applied is sufficiently detailed to allow for the creation of scenarios that allow for thorough positive and negative testing of the policy enforcement mechanism based on the types of policy rules and their contents."

Section 8.4.1 of the ST states that the TOE's Agents will enforce its access control SFP against all operations between subjects and objects based upon their attributes defined within Table 6-2 and Table 6-3 of the ST as well as the hostname attribute which identifies specific endpoint systems.

The enforcement of the policy is handled at the Agent. When a subject attempts to perform an operation on an object, the Agent will review the rules (i.e., Custom Software Rules, Memory Rules, Registry Rules, and Rapid Configs) assigned to its policy starting with the lowest numbered rule first to determine if the rule is applicable to the operation being performed by the subject on the object. When a rule is found that is applicable, the Agent will enforce the first applicable rule's access control decision (i.e., block, permit/allow, report/report only) on the attempted operation and will stop reviewing any additional rules. The access control decision will ultimately either permit or deny the requested access when the request matches a rule.

All required information has been found in Section 8.4.1 of the ST and the evaluation team considers this activity satisfied.

[AC] FDP_ACC.1(1) – *"If the TSF enforces multiple distinct types of access control policies, the evaluator shall also ensure that the SFRs for each policy are properly iterated in the ST and that all of the assurance activities for each individual iteration are satisfied."*

The TOE only enforces a single distinct type of access control, host based access control, as defined by the ESM_AC_PP. There are no specific assurance activities associated with this SFR.

[AC] FDP_ACF.1(2) – *"The evaluator shall check the TSS in order to verify that it identifies the objects that reside in the Operational Environment that impact the TOE's behavior such as registry values, executable processes, and/or configuration files."*

Section 8.4.2 of the ST states The TOE's Agents will enforce the TOE's self-protection SFP on all Agent objects on their endpoint system. This includes all operations between subjects and an Agent's own objects based upon their attributes. The subjects are Active Directory Users based upon Username and Processes based upon Process Name.

The Agent's protected objects are identified by their Name attribute and their associated operations include:

- Read, Modify, Delete, or Change Permissions on the Agent binaries (host configuration)
    - Windows Endpoint System: C:\ProgramFiles\Bit9\ParityAgent
    - Linux Endpoint System: /opt/bit9
- Create, Read, Modify, Delete, or Change Permissions on the data that controls the Agent's behavior (including audit records) (files)
    - Windows Endpoint System: C:\ProgramData\Bit9\ParityAgent

    - Linux Endpoint System: /srv/bit9/data
- Modify or Delete the Agent's registry keys (host configuration - Windows only)
    - \HKLM\System\ControlSet*\Services\Parity
    - \HKLM\System\ControlSet*\Services\ParityDriver
    - \HKLM\Software\Wow6432Node\Bit9
- Terminate the Agent's process or service (programs)
- Execute uninstall of the Agent's software (programs)
- Execute remove of Agent's kernel module (programs – Linux only)

All required information has been found in Section 8.4.2 of the ST and the evaluation team considers this activity satisfied.

[AC] FDP_ACC.1(2) – *"If the TSF enforces multiple distinct types of access control policies, the evaluator shall also ensure that the SFRs for each policy are properly iterated in the ST and that all of the assurance activities for each individual iteration are satisfied."*

The TOE only enforces a single distinct type of access control, host based access control, as defined by the ESM_AC_PP. There are no specific assurance activities associated with this SFR.

[PM] FIA_USB.1 – *"The evaluator shall check the TSS in order to determine that it describes the security attributes that are assigned to administrators and the means by which the administrator is associated with these attributes, both during initial assignment and when any changes are made to them."*

Section 8.5.1 of the ST states:

"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."

This section goes on to describe that changes to a administrator's role assignment will take effect immediately. If permissions that are assigned to a role are changed will also take immediate effect: "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)."

All required information has been found in Section 8.5.1 of the ST and the evaluation team considers this activity satisfied.

[PM] FMT_MOF.1 – *"The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s).*

The evaluator shall also check the TSS to see that it describes the ability of the TSF to perform the required management functions and the authorizations that are required to do this."

Section 8.6.1 of the ST states that the management functions that are available to administrative users include determine the behavior of, disable, enable, and modify the behavior of the Access Control SFP, administrative users, audit events, and the TOE's own security functions. Table 6-6 of the ST provides a list of management functions and the role an administrative user must have to be able to perform them. Table 6-6 is part of the FMT_SMF.1 SFR definition ensuring that the stated functionality is correctly

mapped and satisfies the application note for the first assignment. This table describes the function and the role required which satisfies application note for the second assignment.

FMT_SMF describes the functions available to be the management functions that are available to administrative users include managing: the Access Control SFP, administrative users, audit events, and the TOE's own security functions. Table 6-6 of the ST provides a list of management functions and the role an administrative user must have to be able to perform them.

All required information has been found in Section 8.6.1 of the ST and because there is consistency between the FMT_MOF.1 and FMT_SMF.1 descriptions of available functions and roles required to exercise the functions this requirement is considered satisfied.

[AC] FMT_MOF.1(1) – *"The evaluator shall check the TSS in order to determine that it summarizes how the management functions described in the SFR are performed (or, if their behavior is fixed, why this is the case) and how the TSF determines that the management request is authorized."*

Section 8.6.3 of the ST states that the Agent is configured by a single Server which assumes the role of administrator when these components are communicating. administrative users manage the TOE (Agent) by changing an Agent's policy and/or the CL, the Server will communicate with the Agent to perform these management functions.

All required information has been found in Section 8.6.3 of the ST and the evaluation team considers this activity satisfied.

[AC] FMT_MOF.1(2) – *"The evaluator shall check the TSS in order to determine that it indicates the ESM products (or distributed TOE components if multiple ESM PPs are claimed) that are authorized to query the TOE and that this includes, at minimum, a Policy Management component."*

Section 8.6.4 of the ST states that the TOE's Server component is the Enterprise Security Management product (Policy Management product) that is able to define the Access Control SFP implemented by the TOE by generating Agent installers and communicating with one or more TOE Agents to provide them with updated policies and CLs.

All required information has been found in Section 8.6.4 of the ST and the evaluation team considers this activity satisfied.

[PM] FMT_MOF_EXT.1 – *"The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s).*

The evaluator shall also check the TSS to see that it summarizes the Access Control product functions that the TOE is able to manage and the authorizations that are required in order to manage these functions."

Section 8.6.2 of the ST states that the Server has the ability query the behavior of and modify the functions of one or more Agents:

- audited events – defined within each rule
- repository for audit storage – this is fixed to ensure the TOE has access to the necessary audit events and allow for them to be reviewed by administrative users
- Access Control SFP – this is defined by the Agent's policy and CL
- policy version being implemented – this is defined by the Agent's policy and CL
- Access Control SFP behavior to enforce in the event of communications outage – this is defined by the Disconnected Enforcement Level which is part of an Agent's policy

This is consistent with the SFR definition. The first assignment does not claim any additional functions.

The second assignment refers the reader back to Table 6-6 in the ST for a list of management functions and the role an administrative user must have to be able to perform them. The reference to Table 6-6 is consistently used for FMT_MOF.1, FMT_MOF_EXT.1, and FMT_SMF.1 supports the consistency of the

defined management functionality available and the roles required. This satisfied that the assignments were appropriately done based on the application notes.

There is consistency between the FMT_MOF.1, FMT_MOF_EXT.1, and FMT_SMF.1 descriptions of available functions and roles required to exercise the functions; therefore, this requirement is considered satisfied.

[AC] FMT_MSA.1 – *"The evaluator shall review the TSS and the operational guidance to confirm that the indicated attributes are maintained by the TOE."*

Section 8.6.5 of the ST states the TOE has the ability to change the default, query, modify, and/or delete the security attributes access control policies, access control policy attributes, and implementation status of access control policies of its access control. The TOE's Agent is configured by a single Server which assumes the role of administrator when these components are communicating.

All required information has been found in Section 8.6.5 of the ST and the evaluation team considers this activity satisfied.

[AC] FMT_MSA.3 – *"The evaluator shall review the TSS in order to determine how the TSF puts restrictive default values into place (for example, access control policies should operate in deny-by-default mode so that the absence of an access control rule doesn't fail to restrict an operation) and what authorizations are required in order to override these defaults."*

Section 8.6.6 of the ST states that a new file has the default Approved Status of Unapproved and the Agent will deny access when the Enforcement Level is high. If an administrative user wanted a less restrictive default state, the Enforcement Level of medium will require the user to choose whether they are granted or denied access and the Enforcement Level of low will permit access.
All required information has been found in Section 8.6.6 of the ST and the evaluation team considers this activity satisfied.

[PM] FMT_MSA_EXT.5 – *"The evaluator shall review the TSS and in order to determine that it explains what potential contradictions in policy data may exist. For example, a policy could potentially contain two rules that permit and forbid the same subject from accessing the same object.*

Alternatively, the TOE may define an unambiguous hierarchy that makes it impossible for contradictions to occur.

If the TOE does not allow contradictory policy to exist, the evaluator shall verify that this assertion has been made in the TSS and that justification is provided to support the assertion."

Section 8.6.7 of the ST states that 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. Additionally, the Agent processes the rules assigned to their policy in a hierarchical manner, ensuring the lowest numbered rule (i.e. highest ranked hierarchically) is always enforced. This ensures that the definition and application of the TOE's policies and CL are always unambiguous.

All required information has been found in Section 8.6.7 of the ST and the evaluation team considers this activity satisfied.

[PM] FMT_SMF.1 – *"The evaluator shall check the TSS in order to determine that it summarizes the management functions that are available."*

Section 8.6.8 of the ST describes the management functions available to administrative users include managing: the Access Control SFP, administrative users, audit events, and the TOE's own security functions. Refer to Table 6-6 of the ST for a list of management functions and the role an administrative user must have to be able to perform them.
The table defines the functions with enough information that the reader can understand what the function is for and what role is required to operate that function.
There is consistency between the FMT_MOF.1, FMT_MOF_EXT.1, and FMT_SMF.1 descriptions of available functions and roles required to exercise the functions; therefore, this requirement is considered satisfied.

[AC] FMT_SMF.1 – *"The evaluator shall check the TSS in order to determine what Policy Management and Secure Configuration Management product(s) (if applicable) are compatible with the TOE."*

Section 8.6.8 states Administrative users configure the TOE starting with an Admin installing the TOE and then post-installation the TOE is managed through the Console interface.
The Console interface equates to the interface on the TOE server which is the VMware Carbon Black App Control Server product. The App Control Server is the only product identified for managing the VMware Carbon Black App Control Agent product.

All required information has been found in Section 8.6.8 of the ST and the evaluation team considers this activity satisfied.

[PM] FMT_SMR.1 – *"The evaluator shall review the TSS to determine the roles that are defined for the TOE.*

The evaluator shall also review the TSS to verify that the roles defined by this SFR are consistently referenced when discussion how management authorizations are determined."

Section 8.6.9 of the ST states that the TOE Server associates administrative users accessing the TOE via the Console with roles. The TOE Server supports the following roles: Read-Only, Power User, Admin (specified 'Administrator' within the TOE Server), and custom. The Read-Only role is only able to review information on the Console and is not able to manage the TOE's functions. The Power User role is able to manage the TOE's access control functions but is not able to manage some of the TOE Server's own security functions; such as: create new administrative user accounts, create and/or change roles, and manage the banner. The Admin role is able to perform all management functions on the TOE Server and one of the administrative users with the Admin role is expected to install the TOE Server. The TOE Server also allows for custom roles to be created and assigned permissions. The management functionality which a custom role can perform depends on the permissions assigned to the custom role.

Based on the definitions of the roles it is expected that table 6-6 should only have power and admin roles defined. Upon analyzing table 6-6 it is clear that only the power and admin roles have been declared. The admin role, as expected, can exercise all functionality whereas the power role had more limited functionality.

[AC] FMT_SMR.1 – *"The evaluator shall examine the TSS to verify that it describes how management authority is delegated via one or more roles and how an authorized Policy Management product is associated with those roles."*

Section 8.6.9 of the ST states that the TOE Agent has a single role called administrator. The TOE Server assumes this role every time an Agent polls the Server. This is consistent with the SFR assignment and the Server connecting to the Agent . All required information has been found in Section 8.6.9 of the ST and the evaluation team considers this activity satisfied.

[AC+PM] FPT_APW_EXT.1 – *"The evaluator shall examine the TSS to determine that it details all authentication data, other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential*

data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts).

The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS."

Section 8.7.1 of the ST states that the user accounts, which are used to verify the administrative users' usernames and passwords for authenticating to the Console, are stored in either the SQL Server Database or Active Directory. Both the SQL Server Database and Active Directory repositories are considered part of the operational Environment. Local user account passwords are stored as SHA-256 hashes in the encrypted SQL Server Database. Active Directory account passwords are also stored as hashes in Active Directory's database (ntds.dit) and this database is also encrypted. There is no interface to read administrative users' credential data in plaintext.

The client users' passwords are hashed and encrypted in Active Directory's database in the same manner as the administrative user accounts. There is no interface to read client users' credential data in plaintext.

All required information has been found in Section 8.7.1 of the ST and the evaluation team considers this activity satisfied.

[AC] FPT_FLS.1 – *"The evaluator shall check the TSS in order to determine that it describes the failure states the TOE may encounter and the actions that are taken by the TSF to resolve these states. The evaluator shall use this information to confirm that the TSF resolves the failure states in a manner that preserves a secure state as defined by the application note."*

Section 8.7.2 of the ST states that to preserve a secure state the TOE Agent, whether on Windows or Linux, will restart automatically upon detection of an unclean exit or crash.
All required information has been found in Section 8.7.2 of the ST and the evaluation team considers this activity satisfied.

[AC] FPT_FLS_EXT.1 – *"The evaluator shall check the TSS in order to determine that it describes how the SFP(s) defined in FDP_ACC.1 are enforced when the TOE cannot communicate with the Policy Management product that provided the enforced policy.*

If communications are not expected to be severed (for example, if the TOE and Policy Management product run on the same system), the evaluator shall check the TSS in order to determine that this assertion has been made.

If the assignment is chosen to define an alternate failure state behavior, the evaluator shall verify that the failure state behavior is documented in sufficient detail to be unambiguously verifiable."

Section 8.7.3 of the ST states that 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. All required information has been found in Section 8.7.3 of the ST and the evaluation team considers this activity satisfied.

[AC] FPT_RPL.1 – *"The evaluator shall check the TSS in order to determine that it describes the method by which the TSF detects replayed data. For example, it may provide a certificate or other value that can be validated by the TSF to verify that the policy is consistent with some anticipated schema. Alternatively, the TOE may use a protocol such as SSL for transmitting data that immunizes it from replay threats."*

Section 8.7.4 of the ST states that 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. All required information has been found in Section 8.7.4 of the ST and the evaluation team considers this activity satisfied.

[AC+PM] FPT_SKP_EXT.1 – *"The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured."*

Section 8.7.5 of the ST states that the symmetric key for encrypting/decrypting the SQL Server Database which is accessed by the TOE's Server is protected by Windows. The symmetric key for encrypting/decrypting the Windows Agent's SQLite database is randomly generated upon installation by the Windows Agent calling the Windows platform to generate the key. Once generated, the symmetric key is encrypted by Windows and protected by the TOE's self-protection SFP.

The symmetric key for encrypting/decrypting the SQLite database which is part of the TOE's Linux Agent is stored and obfuscated within the Linux Agent's binary and protected by the TOE's self-protection SFP. There is no direct interface that is intended to be used to extract any of these symmetric keys.

All required information has been found in Section 8.7.5 of the ST and the evaluation team considers this activity satisfied.

[AC] FRU_FLT.1 – *"The evaluator shall check the TSS in order to determine that describes how the TSF ensures that it is enforcing the most up-to-date policy. If a malicious user was able to disconnect their system and the TOE misses a policy update from Policy Management during this outage, it is expected that the updated policy will be received once communications are resumed."*

Section 8.8.1 of the ST states 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. All required information has been found in Section 8.8.1 of the ST and the evaluation team considers this activity satisfied.

[PM] FTA_TAB.1 – "*The evaluator shall check the TSS in order to determine that it discusses the ability of the TSF to display a configurable banner prior to administrator authentication."*

Section 8.9.1 of the ST states 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. All required information has been found in Section 8.9.1 of the ST and the evaluation team considers this activity satisfied.

[PM] FTA_SSL.3 – *"The evaluator shall check the TSS in order to determine that it discusses how inactivity is handled for remote administrative sessions."*

Section 8.9.3 of the ST states the TOE terminates 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 9999 minutes. All required information has been found in Section 8.9.3 of the ST and the evaluation team considers this activity satisfied.

[PM] FTA_SSL.4 – *"The evaluator shall check the TSS in order to determine that it discusses the ability of an administrator to terminate their own session."*

Section 8.9.3 of the ST states that any administrative user can initiate termination from their own interactive Console session by using the Username dropdown and selecting 'Log Out'. All required

information has been found in Section 8.9.3 of the ST and the evaluation team considers this activity satisfied.

[AC] FTA_TSE.1 – *"The evaluator shall examine the TSS to determine that all of the attributes on which a session can be denied are specifically defined."*

Section 8.9.2 of the ST states that 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. All required information has been found in Section 8.9.2 of the ST and the evaluation team considers this activity satisfied.

[AC+PM] FTP_ITC.1 – TD0576 – *"The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST."*

Section 8.10.1 of the ST states the following connections and protocols:

- The Agent to Server trusted channel is secured with TLS/HTTPS for the transfer of policy data (i.e. updated policy or CL) to the Agent, the transfer of software updates to the Agent, and audit data to the Server. All connections between Agent and Server are initiated by the Agent.

- The Server to Active Directory trusted channel is secured with TLS, is always initiated by the Server, and is used for remote administrative user authentication.

The TLS and HTTPS protocols are implemented by the underlying TOE components' operating systems: Windows OS and Linux OS for the Agent, and Windows OS for the Server. These protocols are used to protect the data traversing the trusted channels from disclosure and/or modification. The operating systems' implementation of these protocols will also validate the identification of the endpoint being contacted by the TOE component. All required information has been found in Section 8.10.1 of the ST and the evaluation team considers this activity satisfied.

[PM] FTP_TRP.1 – TD0576 – *"The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST."*

The evaluator shall also check the TSS to ensure that the ST author specifies whether remote administration is applicable to the TOE and if applicable, specifies all the methods of remote administration, along with how those communications are protected."

Section 8.10.3 of the ST states that by initiating the trusted path via a web browser to the Console, administrative users can perform authentication and management activities remotely. The Console path is protected by the underlying Windows OS implementation of HTTPS, which is used to protect the data traversing the path from disclosure and/or modification. The Console is the only remote administrative mechanism identified, therefore, all required information has been found in Section 8.10.2 of the ST and the evaluation team considers this activity satisfied.

3 Operational Guidance Assurance Activities

The evaluation team completed the testing of the Operational Guidance, which includes the review of the *VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0* (AGD) document and confirmed that the Operational Guidance contains all Assurance Activities as specified by the *Enterprise Security Management Access Control Protection Profile version 2.1* [ESM_AC_PP] and *Enterprise Security Management Policy Management Protection Profile version 2.1* [ESM_PM_PP]. The evaluators reviewed these PPs to identify the security functionality that must be discussed for the operational guidance. This is prescribed by the Assurance Activities for each SFR and the AGD SARs. The evaluators have listed below each of the SFRs defined in both the ESM_AC_PP and ESM_PM_PP that have been claimed by the TOE (some SFRs are conditional or optional) as well as the AGD SAR, along with a discussion of where in the operational guidance the associated Assurance Activities material can be found. The AGD includes references to other guidance documents that must be used to properly install, configure, and operate the TOE in its evaluated configuration. The AGD and its references to other VMware Carbon Black App Control guidance documents were reviewed to assess the Operational Guidance Assurance Activities. The AGD contains references to these documents in Chapter 4 and these references can also be found below:

> [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

[PM] ESM_ACD.1 – *"The evaluator shall review the operational guidance to ensure that that it indicates the compatible Access Control product(s) as well as the allowable contents and means of identification of the access control policies that can be defined by the TOE."*

Section 5.1 of the AGD describes the Agent component of the TOE being the compatible Access Control Product to the Server and Console's Policy Management product. Section 7.3 and its subsections of the AGD describe the management of policies, objects, rules to include their operations and subjects, as well as their respective attributes which together cover the access control policies that can be defined by the TOE. All required information has been found and the evaluation team considers this activity satisfied.

[PM] ESM_ACT.1 – *"The evaluator shall review the operational guidance to determine how to create and update policies, and the circumstances under which new or updated policies are transmitted to consuming ESM products (and how those circumstances are managed, if applicable)."*

Section 7.3 and its subsections of the AGD describe the management of policies, objects, rules to include their operations and subjects, as well as their respective attributes which together cover the access control policies that can be defined by the TOE. Section 7.3.1 of the AGD specifically states the following regarding new or updated policies being sent to Agents after initial establishment between an Agent and Server, "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"

Section 7.3.3.7 of the AGD states that any management of the rules will result in a new CL as well as enabling/disabling rules and ranking rules. All required information has been found and the evaluation team considers this activity satisfied.

[PM] ESM_ATD.1 – *"The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure the object attributes."*

Section 7.3.2 of the AGD states that object's name attribute is defined based upon the file initialization process that the TOE does when an Agent is installed on the endpoint system. Additionally, files have an Approved Status attribute that is initially assigned based upon the file initialization process but can also be modified by administrative users through the "File-Specific Rules: Approvals and Bans" Section of Chapter 8 Approving and Banning Software in the VMware Carbon Black App Control User Guide. All required information has been found and the evaluation team considers this activity satisfied.

[PM] ESM_ATD.2 – *"The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure these attributes."*

Section 7.3.3 of the AGD describes several types of rules and in each of the rules the administrative user can define the subject by their attributes. This can be accomplished by defining the username or Active Directory group name for a user subject or define the process name for a process subject. All required information has been found and the evaluation team considers this activity satisfied.

[PM] ESM_EAU.2 – *"The evaluator shall check the operational guidance in order to determine how the TOE determines whether an interactive user requesting access to it has been authenticated and how the TOE validates authentication credentials or identity assertions that it receives. If any IT entities authenticate to the TOE, the evaluator shall also check the operational guidance to verify that it identifies how these entities are authenticated and what configuration steps must be performed in order to set up the authentication."*

Section 7.1 and 7.1.1 of the AGD describe that the TOE's Console uses user session management to recognize if a user has been authenticated or not. If the user has not been authenticated, the user will need to authenticate to the TOE by having the user entered username and password be checked against either a Active Directory domain user account or a user account managed by the TOE and stored in the SQL Server Database. Section 7.1.6 of the AGD states that TOE components and operational environment components do not authenticate to the TOE. All required information has been found and the evaluation team considers this activity satisfied.

[AC+PM] ESM_EID.2 – This SFR does not contain any ESM_AC_PP and ESM_PM_PP AGD Assurance Activities.

[AC+PM] FAU_GEN.1 – *"The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record.*

Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3 [within both the ESM_AC_PP and ESM_PM_PP]."

Section 8.1 and its subsections in the AGD covers all audit events listed within the Security Target which has been determined to be conformant to the Protection Profiles through the evaluation team's assessment of the Security Target. For each audit event, Section 8.1 and its subsection in the AGD provide directions on how an administrative user would access the audit record, reviews the audit record's format which includes a description of each field, one or more examples of the audit record, and as necessary further information to explain the audit record examples' content.

[AC] *"The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event."*

The methodology used was to review the AGD and Security Target for information regarding TOE interfaces used to configure the SFR mechanisms when the TOE is in the evaluated configuration. The evaluation team determined that only interface for managing the TOE's SFR functionality in the evaluated configuration is the TOE's Console. This interface is depicted in the ST Figure 1 and its use is described throughout the ST, AGD, and the other guidance documentation sections specifically referenced from the AGD. The configuration of the SFR mechanisms has been described in the AGD and its references to the other guidance documentation. The evaluation team has determined that this information is complete through the completion of the assessment of the operational guidance assurance activities within Section 3 of the AAR. The evaluation team has also determined that the full set of audit events listed in the Security Target, and thus those required by the Protection Profiles, have been documented in Section 8.1 and its subsections of the AGD based upon our analysis of the first half of the FAU_GEN.1 assurance activity. As this set of all required audit records includes the management audit records and the Console is the only interfaces used, then all management related audit records produced by the TOE have been covered.

All required information has been found and the evaluation team considers this activity satisfied.

[AC] FAU_SEL.1 – *"The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target."*

Section 8.2 of the AGD describes that the audit selection process depends on the access control rules that are generated and enforced. Section 8.2 also overviews each attribute defined in the Security Target and then references the Sections in the AGD which describes the creation of the rules and if applicable the field(s) in each rule which associate with that attribute getting defined. The evaluation team has determined that all selections identified in the Security Target have been covered in the AGD. All required information has been found and the evaluation team considers this activity satisfied.

[PM] FAU_SEL_EXT.1 – *"The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target."*

Section 8.2 of the AGD describes that the audit selection process depends on the access control rules that are generated and enforced. Section 8.2 also overviews each attribute defined in the Security Target and then references the Sections in the AGD which describes the creation of the rules and if applicable the field(s) in each rule which associate with that attribute getting defined. The evaluation team has determined that all selections identified in the Security Target have been covered in the AGD. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FAU_STG.1 – *"The evaluator shall examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and 'cleared' periodically by sending the data to the audit server."*

Section 8 of the AGD information matches that of the Security Target and describes that each Agent and the App Control Server have an audit log file (TOE-internal storage) but a majority of the audit logs these TOE components produce are sent to remote storage which is the SQL Database Server which is connected

to the App Control Server. This Section makes it clear the types of audit logs stored in a component's audit log file have no relation to the audit logs which a component sends to be stored in the SQL Database Server. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FAU_STG_EXT.1 – TD0066 – *"The evaluator shall check the operational guidance in order to determine that it lists any configuration steps required to set up audit storage. If audit data is stored in a remote repository, the evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established."*

Section 6.1.1 of the AGD describes configuration of the SQL Server Database which is the remote audit storage repository and Section 6.1.3 of the AGD describes identifying the SQL Server Database as the Database Server during the App Control Server's installation. Section 6.2.4 of the AGD includes procedures to configure Agent logging including the log rollover function for the audit log file (TOE-internal storage) of an Agent on a Linux endpoint. The last paragraph in Section 8 describes the communication between the App Control Server and the SQL Server Database as the external repository. This description includes that the connection is established when the App Control Server is initialized, the App Control Server makes SQL statements and queries to the SQL Server Database that occur within the underlying Windows operating system, and that the connection to the SQL Server Database is necessary for the App Control Server's operation which will stop working when the connection is lost and start again when re-established.

ESM PPs - TD0066: "*If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.). Lastly, the described loss minimization mechanisms must be tested to ensure that they behave as documented."*

Section 8 of the AGD explicitly states that the TOE does not perform audit reconciliation as the situation does not apply to the TOE as the same audit records are not recorded in more than one location. The audit log files (i.e., local audit storage) and the SQL Server Database (i.e., the external repository and ultimate destination for all other audit records) do not store the same type of audit records produced by the Agents and App Control Server. Additionally, when the Agent buffers audit events before sending them to the Server, the Agent will remove events from its buffer once they are successfully sent to the Server. Thus, events are not stored in two locations simultaneously.

All required information has been found and the evaluation team considers this activity satisfied.

[PM] FAU_STG_EXT.1 – TD0066 – *"The evaluator shall check the operational and preparatory guidance in order to determine that they describe how to configure and use an external repository for audit storage. The evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established."*

Section 6.1.1 of the AGD describes configuration of the SQL Server Database which is the remote audit storage repository and Section 6.1.3 of the AGD describes identifying the SQL Server Database as the Database Server during the App Control Server's installation. Section 6.2.4 of the AGD includes procedures to configure Agent logging including the log rollover function for the audit log file (TOE-internal storage) of an Agent on a Linux endpoint. The last paragraph in Section 8 describes the communication between the App Control Server and the SQL Server Database as the external repository. This description includes that the connection is established when the App Control Server is initialized, the App Control Server makes SQL statements and queries to the SQL Server Database that occur within the underlying Windows operating system, and that the connection to the SQL Server Database is necessary for

the App Control Server's operation which will stop working when the connection is lost and start again when re-established.

ESM PPs - TD0066: "*If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.). Lastly, the described loss minimization mechanisms must be tested to ensure that they behave as documented."*

Section 8 of the AGD explicitly states that the TOE does not perform audit reconciliation as the situation does not apply to the TOE as the same audit records are not recorded in more than one location. The audit log files (i.e., local audit storage) and the SQL Server Database (i.e., the external repository and ultimate destination for all other audit records) do not store the same type of audit records produced by the Agents and App Control Server.

All required information has been found and the evaluation team considers this activity satisfied.

[AC] FCO_NRR.2 – *"The evaluator shall check the operational guidance in order to determine how the TOE confirms evidence of received policy data back to the Policy Management product that originally sent it that policy data. This should include the contents and formatting of the receipt such that the data that it contains is verifiable."*

Section 6.2.3 explains that the Agent will send a receipt back to the Server with its current policy name, enforcement level, CL version, and Agent software version. This Section also refers to the "Viewing the Table of Computers" and "Viewing Complete Details for One Computer" sections of Chapter 4 Managing Computers in the VMware Carbon Black App Control User Guide Product Version 8.8 Document Version 1.0. The information in this document provides an overview of how this information is displayed in the Console for review and verification by an administrator. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FDP_ACF.1(1) – *"The evaluator shall check the operational guidance in order to verify that it provides instructions on how it receives access control policy data. For example, if the TOE receives policy rules in some defined language, the operational guidance shall indicate the statements in this language that correspond with the activities that are defined in Table 15 [within the ESM_AC_PP].*

The evaluator shall also check the operational guidance to verify that it provides information about how the TOE's rule processing engine. This allows administrators to design access control policies with appropriate expectations for how they will be enforced."

The evaluation team found the required information in the following sections:

- Section 7.3 of the AGD as a whole describes how policies are defined
- The AGD uses the objects defined in Table 6-2 (Host-based operations for Active Directory Users) of the ST to create the mapping in Table 7-2 which itemizes the operations down to the particular Windows/Linux Agent that is applicable. Table 7-2 of the AGD describes the Processes, Files, and Host Configuration objects. The Authentication Function object is addressed on its own in Section 7.3.3.5
- The AGD further maps specifics for objects defined in the ST Table 6-3 to itemize the Memory Rules (Table 7-3), Registry Rules (7-4), Rapid Configs (7-5) in the same manner.
- Section 7.3.3.6 describes the ability for configuring the hostname attribute used for Hostname Restriction
- Section 7.3.3.7 describes the enabling and ranking of the rules
- The tables in the AGD create a clear mapping for all objects, object attributes, and operations defined in the ST

All required information has been found and the evaluation team considers this activity satisfied.

[AC] FDP_ACF.1(2) – This SFR does not contain any ESM_AC_PP AGD Assurance Activities.

[PM] FIA_USB.1 – *"The evaluator shall check the operational guidance in order to verify that it describes the mechanism by which external data sources are invoked and mapped to user data that is controlled by the TSF."*

Section 7.1 of the AGD describes the process by which the TOE invokes Active Directory and maps Active Directory user's Group Names TOE roles. Additionally, Section 7.1.4 of the AGD refers to "Creating AD Mapping Rules" Section in Chapter 3 Managing Console Login Accounts of the VMware Carbon Black App Control User Guide for the steps to perform the role mapping. All required information has been found and the evaluation team considers this activity satisfied.

[PM] FMT_MOF.1 – *"The evaluator shall review the operational guidance in order to determine what restrictions are in place on management of these attributes and how the TSF enforces them. For example, if management authority is role-based, then the operational guidance shall indicate this."*

Section 7.1.5 of the AGD explains the TOE's roles and contains Table 7-1 which matches the ST's Table 6-6 regarding the role attribute and what TOE relevant management functions each role provides. Section 7.1.5 also refers to the "Managing Console User Roles" section of Chapter 3 Managing Console Login Accounts in the VMware Carbon Black App Control User Guide for guidance on creating, modifying, disabling, and deleting roles as well as explaining permissions and assigning them to roles. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FMT_MOF.1(1) – *"The evaluator shall check the operational guidance in order to determine that it describes the process by which the TOE can be associated with a Policy Management product and how that product is subsequently used to manage the TOE."*

Sections 6.2.1 and 6.2.2 of the AGD explains that each endpoint system running an App Control Agent is assigned to a single policy and this initially occurs based upon the policy specific Agent installer. The policy and Agent installer are created by the App Control Server by an administrative user through the Console. A system administrator then installs the Agent on an endpoint system. Section 6.2.3 of the AGD then describes how the initial establishment occurs between an Agent and the App Control Server that created the Agent installer. Section 6.2.3 of the AGD also references several sections in Chapter 4 Managing Computers in VMware Carbon Black App Control User Guide which describe that when the Agent contacts the App Control Server after Agent installation, the Agent's endpoint system is added to the table of endpoint systems (i.e., computers) associated with the App Control Server and can be managed through the Console. Section 2 of the AGD states the purpose of the AGD is to manage the TOE per the Common Criteria evaluation and throughout the AGD the use of the Console is described to manage the TOE. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FMT_MOF.1(2) – *"The evaluator shall check the operational guidance in order to determine that it describes the process by which the TOE can be associated with other ESM products and why these other products are used to interface with the TSF."*

Section 6.2.1, 6.2.2, and 6.2.3 of the AGD describes the process of associating the ESM products together by creating an Agent installable through the Server, installing the Agent, and the Agent will then be fully associated with the Server by communicating back to the Server. Section 6.2 provides an overview of why these products are used together to provide TOE functions. All required information has been found and the evaluation team considers this activity satisfied.

[PM] FMT_MOF_EXT.1 – *"The evaluator shall check the operational guidance in order to determine that it provides instructions for how to connect to an Access Control product and what privileges are required to perform management functions on it once the connection has been established."*

Section 6.2.1 of the AGD describes that from the Console an administrative user creates an initial policy which then creates a policy specific Agent installer. Section 6.2.2 states that a system administrator for the endpoint system must install the Agent manually on each endpoint system and once installed the Agent will automatically establish communications with the Server. Section 7.1.5 of the AGD describes the default roles an administrative user needs to be assigned to perform management functions on the TOE which includes managing the Agent (i.e. Access Control product). Section 7.1.5 of the AGD also describes custom roles and assigning permissions to perform TOE management functions by referring to "Managing Console User Roles" section of Chapter 3 Managing Console Login Accounts in VMware Carbon Black App Control User Guide. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FMT_MSA.1 – *"The evaluator shall review the TSS and the operational guidance to confirm that the indicated attributes are maintained by the TOE.*

The evaluator shall also confirm that the operational guidance defines how authorizations to manage the defined security attributes are derived so that an administrator will know how to configure separation of duties."

Section 7.3 and its subsections of the AGD describe the management of policies, objects, rules to include their operations and subjects, as well as their respective attributes which together cover the access control policies that can be defined by the TOE. Section 7.3.1 of the AGD specifically states the following regarding new or updated policies being sent to Agents after initial establishment between an Agent and Server, "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"

Section 7.3.3.7 of the AGD states that any management of the rules will result in a new CL as well as enabling/disabling rules and ranking rules. Section 7.1.5 of the AGD describes the default roles and the TOE management activities, to include the security attributes related to the access control Security Functional Policy, available to each default role. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FMT_MSA.3 – *"The evaluator shall review the operational guidance in order to ensure that it warns the reader of the restrictive nature of default values and provides instructions on how to override them."*

Section 7.3.2 of the AGD describes the default value of the Approved Status attribute for objects and the process for administrative users to modify this attribute by following the steps in "File-Specific Rules: Approvals and Bans" Section of Chapter 8 Approving and Banning Software in the VMware Carbon Black App Control User Guide. Section 7.3.1 of the AGD describes the creation of policies which includes defining the initial value for enforcement levels and the process to modify these attributes by referring to the "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 the VMware Carbon Black App Control User Guide. Additionally, Section 7.3.1 of the AGD describes how the enforcement levels of a policy and the Approved Status attribute of an object together will be enforced by the TOE, thus warning the reader of the restrictive nature of the default values. All required information has been found and the evaluation team considers this activity satisfied.

[PM] FMT_MSA_EXT.5 – *"If the TOE requires manual intervention in order to resolve contradictory policy data, the evaluator shall review the operational guidance in order to verify that it provides a*

summary of contradictory policy situations and the steps that must be taken in order to resolve them. If the TOE's policy engine prevents such contradictions, the evaluator shall review the operational guidance in order to verify that it describes how the TSF reconciles any contradictory policy data (such as different rules simultaneously allowing and denying a certain behavior)."

Section 7.3.3.7 of the AGD describes that all rules regardless of policy are globally ranked numerically and that no two rules can have the same ranking value. Additionally, the Section states that the Agent process rules from lowest rank to highest, thus rules can never be in conflict because the lowest ranked rules is always processed. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FMT_SMF.1 – *"The evaluator shall check the operational guidance in order to ensure that it describes how to configure the TOE to interface with the compatible products discussed in the TSS. The evaluator shall also check the operational guidance to verify that it provides instructions for performing each of the defined management functions."*

Section 6.2.1 of the AGD explains that each endpoint system running an App Control Agent is assigned to a single App Control policy based upon the policy specific Agent installer. Initially, Agents are assigned a policy via the Agent Installer. 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.

Section 6.2.3 of the AGD explains that during the process of creating a new policy, the Server includes a random string which will be used to generate a key on the Agent as part of the installation package. 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.

AC Management Function	Location in AGD
Configuration of audited events	Section 8.2: Rules define what agents audit based upon a rule existing – a rule is defined based upon attributes
Configuration of repository for trusted audit storage	Section 8.3
Configuration of Access Control SFP	All of Section 7.3 and subsections
querying of policy being implemented by the TSF	Section 7.3.1 last paragraph
management of Access Control SFP behavior to enforce in the event of communications outage	Section 7.3.1 disconnected enforcement level

All required information has been found and the evaluation team considers this activity satisfied.

[PM] FMT_SMF.1 – *"The evaluator shall check the operational guidance in order to determine that it defines all of the management functions that can be performed against the TSF, how to perform them, and what they accomplish."*

Sections 7 and 8 of the AGD focus on the security management of the TOE. The evaluator used the Table 6-6 in the ST to ensure all management activities are described.

Management Activities	Administrative User Role		Section in AGD
	Admin	Power	
Creation of policies	X	X	7.3.1

Transmission of policies	X	X	7.3.1 (last paragraph)
Definition of object attributes Association of attributes with objects	X	X	7.3.2
Definition of subject attributes Association of attributes with subjects	X	X	7.3.3.1 – 7.3.3.6 Note: Each rule has a "User or Group" or username or similar field where the username or group name are defined.
Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	X		7.1.4 N/A
Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	X		7.1.4 N/A
Configuration of auditable events	X	X	8.2 Note: Rules define what Agents audit based upon a rule existing and each rule is defined based upon attributes specified for selective audit.
Configuration of auditable events for defined external entities	X	X	8.2 Note: Rules define what Agents audit based upon a rule existing and each rule is defined based upon attributes specified for selective audit.
Configuration of external audit storage location	X		8.3
Definition of default subject security attributes, modification of subject security attributes	X		7.1.4
Configuration of the behavior of other ESM products	X	X	7.3.1
Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)	X	X	7.3.3.7 Note: The ranking of rules prevents inconsistencies from occurring.
Management of the users that belong to a particular role	X		7.1.4
Maintenance of the banner	X		7.2

All required information has been found and the evaluation team considers this activity satisfied.

[AC] FMT_SMR.1 – *"The evaluator shall review the operational guidance in order to verify that it discusses the various administrative role(s) that are used to manage the TSF and any applicable steps that are required for an administrator to assume such a role."*

Section 7.1.6 of the AGD states that the TOE has only a single role when the App Control Server is managing one of its Agents called administrator and assumes this role when the Agent polls the Server. All required information has been found and the evaluation team considers this activity satisfied.

[PM] FMT_SMR.1 – *"The evaluator shall review the operational guidance in order to verify that it provides instructions on how to assign users to roles. If the TSF provides only a single role that is automatically assigned to all users, then the evaluator shall review the operational guidance to verify that this fact is asserted."*

Section 7.1.5 of the AGD describes the various administrative role(s) and refers to "Managing Console User Roles" section of Chapter 3 Managing Console Login Accounts in the VMware Carbon Black App Control User Guide for managing custom roles. Section 7.1.4 of the AGD describes assigning roles to user accounts as either part of the management of a user's account or mapping roles to Active Directory groups. For the management of a user's account, Section 7.1.4 also refers to "Creating Login Accounts in the Console", "Changing Passwords and Other Account Details", "Deleting Login Accounts", and "Disabling Login Accounts" sections of Chapter 3 Managing Console Login Accounts in the VMware Carbon Black App Control User Guide. For mapping roles to Active Directory groups, Section 7.1.4 also refers to "Creating AD Mapping Rules" Section in Chapter 3 Managing Console Login Accounts in the VMware Carbon Black App Control User Guide. Section 7.1 of the AGD also states that sessions are created after successful authentication which identify a user's assigned role. All required information has been found and the evaluation team considers this activity satisfied.

[AC+PM] FMT_APW_EXT.1 – This SFR does not contain any ESM_AC_PP and ESM_PM_PP AGD Assurance Activities.

[AC] FPT_FLS.1 – *"The evaluator shall check the operational guidance to verify that it documents all failure states of the TSF, what actions are performed by the TOE in response, and what actions, if any, must be performed by the administrator in order to clear the failure state. The evaluator shall confirm that this information is sufficient to ensure that a secure state is preserved."*

Section 7.4.2 of the AGD describes failure of an Agent due to its unanticipated termination. The Section states that no actions are required by an administrative user to fix the failure state because a Windows Agent will be automatically restarted by the Windows' Service Control Manager (SCM) and the Linux Agent will be automatically restarted by the Agent's kernel driver. The evaluation team has determined that this information is sufficient to ensure a secure state as it describes addressing a failure of an Agent on each type of endpoint operating system. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FPT_FLS_EXT.1 – *"The evaluator shall check the operational guidance (and developmental evidence, if available) in order to determine that it discusses how the TOE is deployed in relation to other ESM products. This is done so that the evaluator can determine the expected behavior if the TOE is unable to interact with its accompanying Policy Management product."*

Section 5.1 of the AGD describes the Agent component of the TOE being the compatible Access Control Product to the Server and Console's Policy Management product. Section 5.3 of the AGD provides a graphical depiction of the evaluated configuration. Section 6 of the AGD describes the installation and configuration of the TOE components to set up the TOE and specifically Section 6.2.3 discuss the initial establishment of communications between the Agent and the Server. Section 7.4.1 of the AGD describes that during a communication outage between the Agent and Server that the Agent will continually attempt every 30 seconds to restore the connection and that policies will enforce their Disconnected Enforcement Level during the outage. Section 7.3.1 of the AGD further describes the Disconnected Enforcement Level and how to manage this setting as part of a policy. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FPT_RPL.1 – *"If the method of replay detection is configurable, the evaluator shall check the operational guidance in order to determine that it provides instructions for setting up and configuring the*

replay detection mechanism. This may be simple (e.g. setting up and enabling a TLS channel with shared secret) or complex (e.g. defining specific policy attributes that are positively associated with unauthorized changes), depending on how specifically replay detection is implemented by the TSF."

Sections 6.1.2 and 6.2.2 of the AGD describes that the TOE's underlying operating systems need to be configured per the instructions of the Common Criteria guidance used during the operating systems' evaluations. The AGD provides references to the operating system guidance documentation for all three operating systems the TOE components (App Control Server and Console, Windows Agent, and Linux Agent) are installed upon. These configurations together will result in the secure TLS and HTTPS connections between the App Control Server and the Agents. Section 6.2.2 of the AGD provides an overview of the replay detection provided by the Agents' operating systems implementation of TLS. All required information has been found and the evaluation team considers this activity satisfied.

[AC+PM] FPT_SKP_EXT.1 – This SFR does not contain any ESM_AC_PP and ESM_PM_PP AGD Assurance Activities.

[AC] FRU_FLT.1 – *"The evaluator shall check the operational guidance in order to verify that it discusses how the TSF receives the latest policy from the Policy Management product once a communications failure has been resolved, including any options that an administrator has in configuring this capability."*

Section 7.4.1 of the AGD describes the failure of a connection between the Agent and the Server, that the Agent will continue to attempt a connection every 30 seconds, and once the connection is restored will query the Server for the most up-to-date policy and CL data for the Agent. This Section also states that this is automatically configured and requires no action by the administrative users. All required information has been found and the evaluation team considers this activity satisfied.

[PM] FTA_TAB.1 – *"The evaluator shall review the operational guidance to determine how the TOE banner is displayed and configured."*

Section 7.2 of the AGD describes configuring the banner and that it is displayed on the Console's login page. All required information has been found and the evaluation team considers this activity satisfied.

[PM] FTA_SSL.3 – *"The evaluator shall also check the operational guidance in order to verify that it describes how to set the idle time threshold."*

Section 7.1.3 of the AGD describes how an admin can configure the "Log Users Out After" value (i.e. idle time threshold) between a value of 1 to 120 minutes through the Console. All required information has been found and the evaluation team considers this activity satisfied.

[PM] FTA_SSL.4 – *"The evaluator shall check the operational guidance in order to verify that it describes how an administrator can terminate their own administrative session for each administrative interface that is supported by the TOE."*

Section 7.1.2 of the AGD describes how any administrative user can terminate their Console session. The Console is the only administrative interface for the TOE. All required information has been found and the evaluation team considers this activity satisfied.

[AC] FTA_TSE.1 – *"The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS."*

Section 7.3.3.5 of the AGD describes the ability of an administrative user to block the ability of a client user to authenticate to an endpoint system. This is accomplished by defining the attributes username and hostname as part of an Agent configuration. All required information has been found and the evaluation team considers this activity satisfied.

[AC+PM] FTP_ITC.1 – TD0576 – *"The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken."*

Sections 6.1.2 and 6.2.2 of the AGD describes that the TOE's underlying operating systems need to be configured per the instructions of the Common Criteria guidance used during the operating systems' evaluations. The AGD provides references to the operating system guidance documentation for all three operating systems the TOE components (App Control Server and Console, Windows Agent, and Linux Agent) are installed upon. The only configuration required through the TOE is in Section 6.1.5 of the AGD which specifies the use of secure LDAP for connecting to Active Directory. These configurations together will result in the secure TLS and HTTPS connections between the App Control Server and the Agents, the Active Directory Server, and remote users accessing the Console. Section 6.1.2 of the AGD indicates in a NOTE "that once the TOE is fully installed and configured, there are no recovery actions that need to be performed." All required information has been found and the evaluation team considers this activity satisfied.

[PM] FTP_TRP.1 – TD0576 – *"The evaluator shall confirm that the guidance documentation contains instructions for how users will interact with the TOE such as a web application via HTTPS. The evaluator shall also ensure that the guidance documentation discusses the mechanism by which a trusted path to the TOE is established and which environmental components (if any) the TSF relies on to assist in this establishment.*

If remote administration is applicable to the TOE per the TSS, the evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method."

Section 5.2 of the AGD describes a management workstation with a web browser providing HTTPS (i.e., Google Chrome) being used by administrative users to interact with the Console. Section 5.1 of the AGD describes the Console as a web-based GUI and is the only administrative interface described in the AGD. Section 7.1.1 of the AGD describes how administrative users connect to the Console and authenticate to the TOE. The remaining portions of Section 7 and 8 of the AGD further describe operations that administrative users are able to perform on the Console. Section 6.1.2 of the AGD describes that the App Control Server and Console's underlying operating system needs to be configured per the instructions of the Common Criteria guidance used during the operating system's evaluation. The AGD provides a reference to the operating system guidance documentation for the App Control Server and Console machine. Together the App Control Server and Console's underlying operating system and the web browser are providing the HTTPS for the user connections to the Console. All required information has been found and the evaluation team considers this activity satisfied.

4 Test Assurance Activities (Test Report)

The following sections demonstrate that all ATE Assurance Activities for the TOE have been met. This evidence has been presented in a manner that is consistent with the "Reporting for Evaluations Against NIAP-Approved Protection Profiles" guidance that has been provided by NIAP. Specific test steps and associated detailed results are not included in this report in order for it to remain non-proprietary. The test report is a summarized version of the test activities that were performed as part of creating the Evaluation Technical Report (ETR).

4.1 Platforms Tested and Composition

Evaluator-conducted manual testing was completed in February 2022. The evaluation team set up a test environment for the independent functional testing that allowed them to perform all test assurance activities against the VMware Carbon Black App Control over the SFR relevant interfaces. There was no sampling of testing, as all required test assurance activities were preformed against the TOE for the VMware Carbon Black App Control that was claimed in the Security Target.

The evaluation team performed testing of the TSF functionality against the VMware Carbon Black App Control as well as the only available management interface, App Control Console. The full set of tests were developed to stimulate the applicable TSF relevant interface; which would fully test all combinations of VMware Carbon Black App Control and their TSF relevant interfaces. The testing is consistent with the use of the interfaces defined within the ST. Thus, the testing of the interfaces was based upon testing SFR functionality related to user actions over each interface.

4.1.1 Test Configuration

The evaluation team conducted testing at the Booz Allen CCTL facility, Laurel MD, on an isolated network. The evaluation team configured the TOE for testing according to the *VMware Carbon Black App Control Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces.

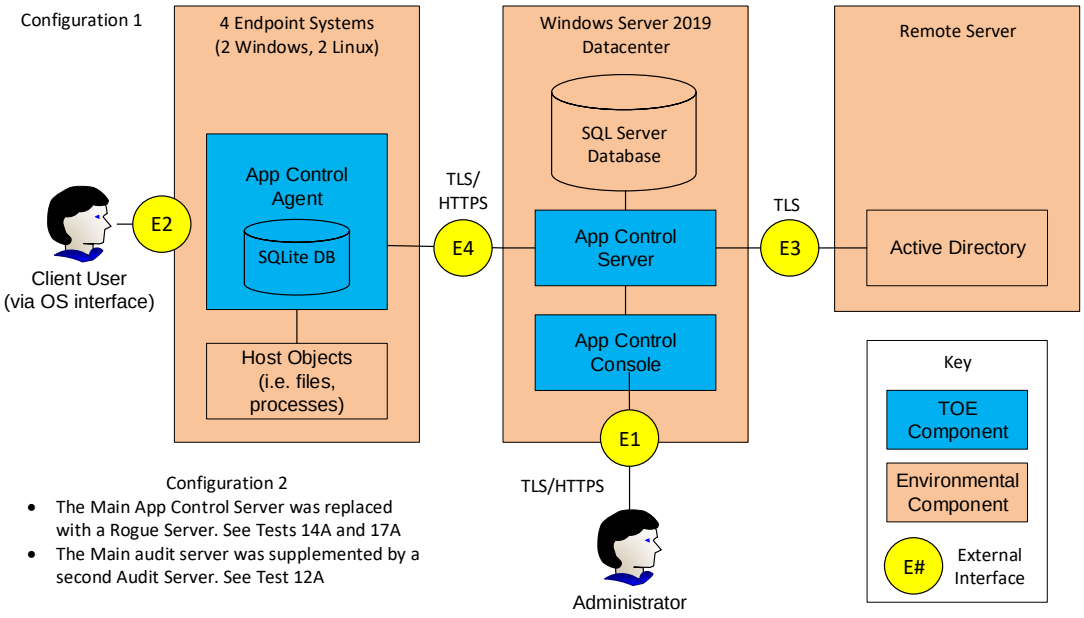

Figure 1 – Logical Boundary Diagram

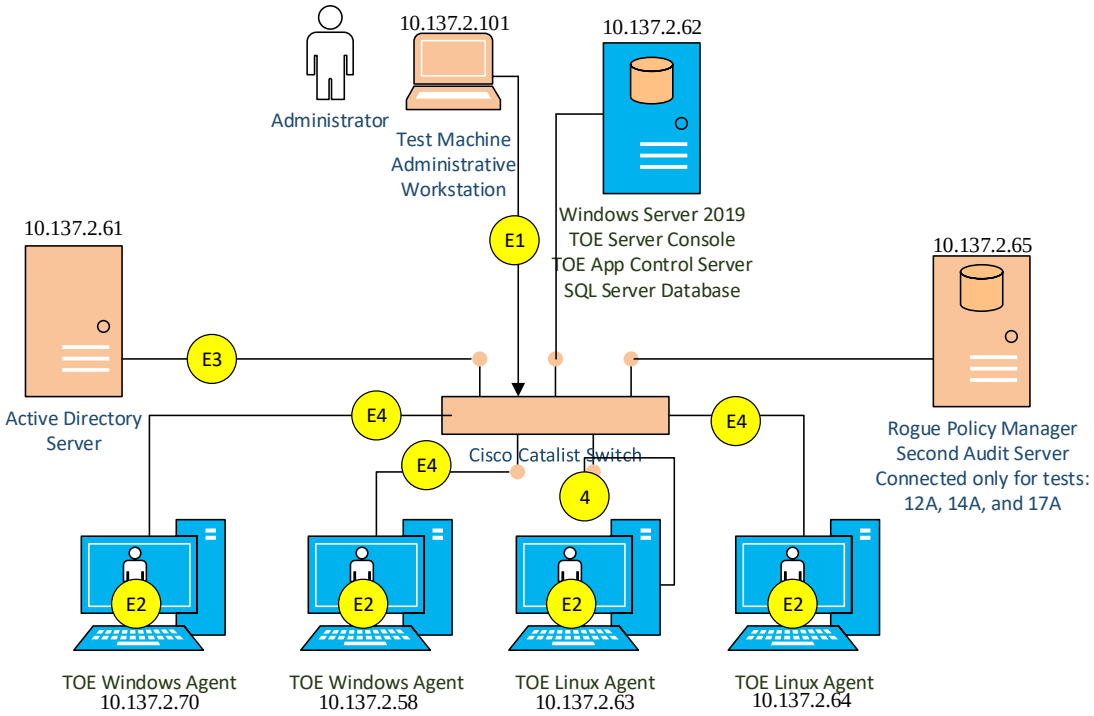

Figure 2 – Network Diagram

Network infrastructure was provided by:

- Function: Switch (all machines connected to one switch to provide isolated network)
  - Platform: Cisco Catalyst WS-C Switch, WS-C3560X-24P-L
  - OS: Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 12.2(55)SE3
  - IP: N/A
  - Netmask: N/A
  - MAC: 30:E4:DB:DF:CC:80
  - Domain name: N/A
  - Test Credentials: N/A

The TOE software components were configured as follows:

- Function: App Control Server (TOE), App Control Console (TOE), SQL Database (OE)
  - Platform: Windows Server 2019 (Version 1809)
  - IPv4 - 10.137.2.62/25
  - MAC - 3C:EC:EF:46:7A:BE
  - Domain name – CBPCC-S1.CBPCC.LOCAL
  - Timing: Internal, Manual set per evaluator mobile phone
  - Tools: Wireshark 3.6.1

- Function: App Control Linux Agent (TOE),
  - Platform: Red Hat Enterprise Linux Server release 7.6 (Maipo) with openldap-client installed
  - IPv4 - 10.137.2.63/25
  - MAC - 3C:EC:EF:4B:10:80
  - Domain name – cbpcc-l1.cbpcc.local
  - Timing: Internal, Manual set per evaluator mobile phone
  - Tools: Wireshark 3.6.1

- Function: App Control Linux Agent (TOE),
    - Platform: Red Hat Enterprise Linux Server release 7.6 (Maipo) with openldap-client installed
    - IPv4 - 10.137.2.64/25
    - MAC - 3C:EC:EF:4B:10:82
    - Domain name – cbpcc-l2.cbpcc.local
    - Timing: Internal, Manual set per evaluator mobile phone

- Function: App Control Windows Agent (TOE),
    - Platform: Windows 10 (Version 1903)
    - IPv4 - 10.137.2.58/25
    - MAC - 10:82:86:06:96:6F
    - Domain name – CBPCC-W1.CBPCC.LOCAL
    - Timing: Internal, Manual set per evaluator mobile phone
    - Tools: Wireshark 3.6.1

- Function: App Control Windows Agent (TOE),
    - Platform: Windows 10 (Version 1903)
    - IPv4 - 10.137.2.70/25
    - MAC - 00:E0:4C:30:0E:A7
    - Domain name – CBPCC-W2.CBPCC.LOCAL
    - Timing: Internal, Manual set per evaluator mobile phone
    - Tools: Wireshark 3.6.1

The TOE was configured to communicate with the following environment component:

- Active Directory Server
    - Function: Active Directory server
    - Platform: Windows Server 2019 (Version 1809)
    - IPv4 - 10.137.2.61/25
    - MAC - 3C:EC:EF:6A:35:64
    - Domain name – CBPCC-AD.CBPCC.LOCAL
    - Timing: Internal, Manual set per evaluator mobile phone
    - Tools: Wireshark 3.6.1

The following test workstation and server were used for testing purposes and are considered part of the OE:

- Function: Test Machine, Management Workstation
    - Platform: Windows 10 (Version 2004)
    - IPv4 - 10.137.2.101/25
    - MAC - 34:E6:D7:60:B3:B9
    - Domain name – DESKTOP-CMMA9LO
    - Timing: Internal, Manual set per evaluator mobile phone
    - Tools: Wireshark 3.6.1, Nmap 7.60

- Function: 2nd instance of App Control Server (TOE), App Control Console (TOE), SQL Database (OE)
    - Only used in Configuration 2 for the following tests and functions:
        - Test 14A FMT_MSA.1 rogue Policy Manager
        - Test 17A FMT_SMR.1 rogue Policy Manager,
        - Test 12A FMT_MOF.1(1) second audit server
    - Platform: Windows Server 2019 (Version 1809)
    - IPv4 - 10.137.2.65/25
    - MAC - 3C:EC:EF:46:79:C4
    - Domain name – CBPCC-S2
    - Timing: Internal, Manual set per evaluator mobile phone
    - Tools: Wireshark 3.6.1

4.2 Omission Justification

There were no testing omissions because there was no sampling of testing, as all required test assurance activities were performed against the TOE that was claimed in the Security Target.

4.3 Test Cases

The evaluation team completed the functional testing activities within the Booz Allen laboratory environment. The evaluation team conducted a set of testing that includes all ATE Assurance Activities as specified by the *Protection Profile for Enterprise Security Management Access Control version 2.1* [ESM_AC_PP] and *Protection Profile for Enterprise Security Management Policy Management version 2.1* [ESM_PM_PP]. The evaluators reviewed these PPs to identify the security functionality that must be verified through functional testing. This is prescribed by the Assurance Activities for each SFR.

If an SFR is not listed, one of the following conditions applies:

- The Assurance Activity for the SFR specifically indicates that it is simultaneously satisfied by completing a test Assurance Activity for a different SFR.
- The Assurance Activity for the SFR does not specify any actions related to ATE activities.

Note that some SFRs do not have Assurance Activities associated with them at the element. In such cases, testing for the SFR is considered to be satisfied by completion of all Assurance Activities at the component level.

The TOE claims conformance to both the Enterprise Security Management Access Control and Policy Management Protection Profiles but it is a self-contained product in its evaluated configuration. This means that all references to 'one or more Access Control products', 'one or more Policy Management products', or similar in the test objectives can be interpreted as all referring to the same TOE. Additionally, any cases where the evaluator is instructed to repeat a test multiple times if the TOE claims to be compatible with multiple products have been omitted from the test objectives because the TOE is only used to manage the behavior of itself in the evaluated configuration; no separate 'compatible' ESM Access Control or Policy Management products are included as part of the TOE's Operational Environment.

The following lists for each ATE Assurance Activity, the test objective, test instructions, test steps, and test results for the claimed PPs. Several SFRs are defined in both claimed PPs. Unless specified otherwise, the assurance activities for each duplicate instance of the SFR are identical to one another save for their scope and can be performed alongside one another. For example, both the ESM_AC_PP and ESM_PM_PP define FAU_GEN.1. The generation of audit data and expected contents of the audit records are the same for both PPs. The only difference between the two are the auditable events that each instance of the SFR requires. Therefore, in testing the audit data generation for the entire TSF, auditing for both the access control and the policy management capabilities is tested. Note that unless otherwise specified, the test configuration is to be in the evaluated configuration as defined by the AGD. This includes having each Agent's policy configured with "Control" selected for the Mode and "Track File Changes" selected under Options. Note that some tests require the TOE to be brought out of the evaluated configuration. For example, to temporarily disable cryptography to prove that the context of transmitted data is accurate. As part of the cleanup for each test, the TOE is returned to the evaluated configuration.

4.3.1 ESM_AC_PP Security Functional Requirements

4.3.1.1 Enterprise Security Management

Test Case Number	001A
SFR	ESM_EID.2
Test Objective	This SFR is not separately tested; appropriate behavior of the access control SFP is sufficient to assert that accurate subject identity data is received by the TOE.

Test Instructions	N/A
Test Steps and Rationale	N/A
Test Results	Pass
Execution Method	Manual

4.3.1.2 Security Audit

Test Case Number	002A
SFR	FAU_GEN.1
Test Objective	The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST. This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly identify the policy that was defined.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	**Startup and Shutdown of Audit Functions:** The evaluator accessed the operating system the App Control Server is installed on, stopped the App Control Server service, and then started the App Control Service. The evaluator accessed the Console and confirmed an audit record was generated for the shutdown of audit functions and startup of audit functions which occurred when the App Control Server stopped and started. In the Console, the evaluator disabled Tamper Protection. The evaluator then accessed a Windows endpoint system and Linux Endpoint system protected by an Agent, stopped each Agent's services, and started each Agent's services. The evaluator accessed the Console and confirmed an audit record was generated for the shutdown of audit functions and startup of audit functions which occurred when each Agent stopped and started. **Use of the management functions – Rule Ranking:** The evaluator accessed the Console, selected a rule not ranked 1 by its rank number, and moved the rule 'before' rank 1. The rule was then ranked 1 and an audit record was generated for the management event. **Remaining Audit Events:** The remaining audit events required by this test are satisfied with the testing of other test cases within this test plan. A mapping of each audit event has been provided in the two audit event tables below this Test Case. This mapping provides the defined audit event listed in the Security Target and the test case that the audit record for the event was generated. Each function performed to produce the audit record was performed in the prescribed manner as instructed in the AGD. The mapping is not an exhaustive list of all instances were these audit records were generated throughout the testing but a single instance of the audit record being generated. The evaluator has determined that based upon the testing performed directly under

	this Test Case as well as all other SFR assurance activities claimed, that the events that require audit records per the Security Target claimed are generated by the TOE. Additionally, these audit records were written to their specified repository based upon the manner in which they were reviewed by the evaluator. The evaluator confirmed the audit records were the correct audit events and the audit records contain the attributes as defined by the Security Target based upon comparing the audit records generated during testing to the examples provided in Section 8.1.1 of the AGD.
Test Results	Pass
Execution Method	Manual

ESM_AC_PP SFR	Audit Event	Test Case Were Generated
FAU_SEL.1	All modifications to audit configuration	003A
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	009P
FCO_NRR.2	The invocation of the non-repudiation service	007A
FDP_ACC.1(1)	Any changes to the enforced policy or policies	002P
FDP_ACC.1(2)	Any changes to the enforced policy or policies	002P
FDP_ACF.1(1)	All requests to perform an operation on an object covered by the SFP	001P
FDP_ACF.1(2)	All requests to perform an operation on an object covered by the SFP	009A
FMT_MOF.1	All modifications to TSF behavior	Audited Events: 003A Repository for trusted audit storage: 012A Access Control SFP: 001P Policy being implemented by the TSF: 001P Access Control SFP behavior to implement in the event of communications outage: 001P
FPT_FLS_EXT.1	Failure of communication between the TOE and Policy Management product	020A
FPT_RPL.1	Detection of replay	021A
FTA_TSE.1	Denial of session establishment	024A
FTP_ITC.1	All use of trusted channel functions	025A

ESM_PM_PP SFR	Audit Event	Test Case Were Generated
ESM_ACD.1	Creation or modification of policy	001P
ESM_ACT.1	Transmission of policy to Access Control products	002P
ESM_ATD.1	Definition of object attributes	001P 009A

ESM_ATD.1	Association of attributes with objects	001P 009A
ESM_ATD.2	Definition of subject attributes	003A
ESM_ATD.2	Association of attributes with subjects	003A
ESM_EAU.2	All use of the authentication mechanism	005P
FAU_SEL_EXT.1	All modifications to audit configuration	003A
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	009P
FMT_SMF.1	Use of the management functions	Creation of policies: 001P Transmission of policies: 002P Definition of object attributes, Association of attributes with objects: 001P Definition of subject attributes, Association of attributes with subjects: 003A Management of authentication data for interactive users: 011P Management of authentication data for authorized IT entities (if managed by the TSF): N/A Configuration of auditable events: 003A Configuration of auditable events for defined external entities: 003A Configuration of external audit storage location: 012A Definition of default subject security attributes, modification of subject security attributes: 011P Configuration of the behavior of other ESM products: 001P Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable): 002A Management of the users that belong to a particular role: 016A Maintenance of the banner: 022A
FMT_SMR.1	Modifications to the members of the management roles	016P
FTA_SSL.3	All session termination events	019P
FTA_SSL.4	All session termination events	021P
FTP_ITC.1	All use of trusted channel functions	023P
FTP_TRP.1	All attempted uses of the trusted path functions	027P

Test Case Number	003A
SFR	FAU_SEL.1

Test Objective	The evaluator shall test this capability by using a compatible ESM Policy Management or ESM Secure Configuration Management product to configure the TOE in the following manners: - All selectable auditable events enabled - All selectable auditable events disabled - Some selectable auditable events enabled For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the management of Agents (i.e., Access Control products) by the App Control Server and Console (i.e., together being the Policy Management product) for all of the tests performed. The TOE performs selectable audit based upon administrative users defining rules and specifying that events triggering the rules need to be audited. **All selectable auditable events enabled:** Through the course of the evaluator testing ESM_ACD.1, FDP_ACC.1(1), and FDP_ACF.1(1) by performing Test Case 001P, all administrative user generated rules for all subject, object, operation, and attribute combinations that were claimed by the evaluation through Security Target Tables 6-2 and 6-3 have been tested. These rules resulted in an audit record being generated when the rule was enforced, and the audit record was confirmed by the evaluator. The evaluator also confirmed that it was due to the rule that the audit record was generated because when the subject, object, operation, and attribute combination did not exactly match the rule, the rule was not enforced, and no audit record was generated. Therefore, the evaluator has completed the testing for all selectable auditable events enabled. **All selectable auditable events disabled:** On the Console, the evaluator ensured all administrative user generated rules were disabled or disabled the rule so that only rules that are prepackaged with the TOE are enabled. Next the evaluator created the 'No Selectable Audit' policy, assigned it to all Agents, and waited for the Agents to consume the new policy. The evaluator then accessed a Windows and a Linux endpoint system protected by an Agent and attempted to kill the Agent's process on each endpoint system. The evaluator then logged into the Console and verified that audit records were created for the Agents policy change and attempting to kill the Agent's process on each endpoint system. The evaluator determined that when all selectable auditable events are disabled, based upon the administrative user generated rules being disabled, that the TOE still performs auditing of events that are not selectable. **Some selectable auditable events enabled:** For an Agent on a Windows and Linux endpoint system, the evaluator conducted the following 'some selectable audit events enabled' test. The evaluator created four rules: all rules were created disabled, each rule identified a different object, two of the rules were applicable to all subjects, one of the rules was specific to a client user by their username, and one of the rules was specific to a process by their process name. The evaluator then moved the Agent to a new policy. On the endpoint system protected by the Agent, in a shared directory between multiple users, create five files with different names, four of the files' names should match the object names defined in the four rules. The evaluator then performed an action which would have trigged one of the rules

	applicable to all subjects, if it were enabled, and confirmed that an audit record was not generated. The evaluator then enabled that rule and waited for the Agent to consume the updated configuration list. The evaluator then performed the same action on the endpoint and this time the rule was enforced by the Agent and an audit record was created. The evaluator then performed an action which would have trigged the rule applicable to a specific user subject, if it were enabled, and confirmed that an audit record was not generated. The evaluator then enabled that rule and waited for the Agent to consume the updated configuration list. The evaluator then performed the same action on the endpoint with the client user whose username was within the rule and with a client user with a different username. This time the rule was enforced by the Agent for the user whose username matched the rule and an audit record was created for the enforcement but there was no enforcement nor audit record for the user whose username did not match the rule. The evaluator then performed an action which would have trigged the other rule that is applicable to all subjects, if it were enabled, and confirmed that an audit record was not generated. The evaluator then enabled that rule and waited for the Agent to consume the updated configuration list. The evaluator then performed the same action on the endpoint and this time the rule was enforced by the Agent and an audit record was created. The evaluator then performed an action which would have trigged the rule applicable to a specific process subject, if it were enabled, and confirmed that an audit record was not generated. The evaluator then enabled that rule and waited for the Agent to consume the updated configuration list. The evaluator then performed the same action on the endpoint with the process whose process name was within the rule and with a process with a different process name. This time the rule was enforced by the Agent for the process whose process name matched the rule and an audit record was created for the enforcement but there was no enforcement nor audit record for the process whose process name did not match the rule. The evaluator determined based upon performing the 'some selectable audit events enabled' test that the selectable audit worked as described because audit records would only be generated for enabled rules and when the rule is enforced because the subject, object, operation, attribute combination was a match to the rule.
Test Results	Pass
Execution Method	Manual

Test Case Number	004A
SFR	FAU_STG.1
Test Objective	The evaluator shall test this capability by attempting to access locally-stored audit data without authorization and observe that the attempts fail. They shall also observe that the space allocated for audit storage is consistent with the TSF's capabilities.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator attempted to access the local log file for the Agent on the Windows and Linux endpoints by attempting to delete, modify, move and rename the local log file with a client user on the endpoint system. In all instances, the TOE prevented the client user action. This demonstrated that audit data stored in the local log files are protected from unauthorized access. On the Windows endpoint, the evaluator then observed the current state and size of the active and dormant local log files. The evaluator ensured enough actions occurred resulting in a

	rollover event and verified once the active local log file reached 50MB it was rolled over to the dormant local log file. On the Linux endpoint, the evaluator then observed the current state and size of the active and dormant local log files. The evaluator ensured enough actions occurred that the active local log file was greater than 50MB and during the next roll over thread that the active local log file became the dormant local log file. The evaluator has determined that the audit storage space is consistent with the TSF capabilities for log rotation behavior.
Test Results	Pass
Execution Method	Manual

Test Case Number	005A
SFR	FAU_STG_EXT.1 – TD0066 & TQ1196
Test Objective	The evaluator shall test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit storage contain identical data. The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one. If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.). Lastly, the described loss minimization mechanisms must be tested to ensure that they behave as documented.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	Per the Section 8.2.4 of Security Target, Section 8 of the AGD, and the results of the testing, the evaluator knows that different types of audit records are stored in the local log files and the SQL Server Database. Therefore, there is no scenario where audit reconciliation is possible between the audit logs (TOE-internal storage) and the SQL Server Database. As the App Control Server and Console rely on the SQL Server Database to function as well as to write audit records to, the test could not be performed as described. The evaluator received guidance from NIAP through Technical Query #1196 and the following test was performed to verify that no audit data is lost when the connection to the SQL Server Database is unavailable because no audit data could be generated by the App Control Server and no audit data could be received from Agents. The evaluator observed the last audit record recorded to the SQL Server Database through the Console and then shutdown the SQL Server Database. The evaluator then attempted to perform actions in the Console and confirmed its functionality was disabled. The evaluator then restarted the SQL Server Database, authenticated to the Console, verified no audit records were recorded to the SQL Server Database while it was shut down, and that auditing to the SQL Server Database has resumed. The evaluator also verified through conducting test case 025A that audit data which is sent between remote IT entities (i.e., Agents to App

	Control Server) are protected within TLS/HTTPS.
Test Results	Pass
Execution Method	Manual

4.3.1.3 Communication

Test Case Number	007A
SFR	FCO_NRR.2
Test Objective	The evaluator shall test this capability by configuring an environment such that the TOE is allowed to accept a policy from a certain source, sending it a policy from that source, observing that the policy is subsequently consumed, and that an accurate receipt is transmitted back to the Policy Management product within the time interval specified in the ST. The evaluator confirms accuracy by using the Policy Management product to view the receipt and ensure that its contents are consistent with known data.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator set up a full instance of the TOE with an App Control Server sending the policy and Agents on Windows and Linux endpoints receiving the policy. The evaluator then created a new policy for the Agents which was then consumed by the Agents. Upon the new policy's consumption, each Agent sent a receipt back to the App Control Server. On the App Control Server, the evaluator observed the hostname, IP address, and MAC address for each Agent's endpoint system to which the policy was sent and that next to this information was the receipt contents of the policy to include the name identifier of the policy sent, enforcement levels for that policy, the latest CL version, and the current Agent software version. Lastly the evaluator confirmed that an audit record for the invocation of the non-repudiation service was generated. The evaluator demonstrated that the TOE Agent accepts a policy from the TOE Server and returns a receipt once the policy is consumed.
Test Results	Pass
Execution Method	Manual

4.3.1.4 User Data Protection

Test Case Number	008A
SFR	FDP_ACC.1(1) and FDP_ACF.1(1)
Test Objective	The evaluator shall test this capability by using an authorized and compatible Policy Management product to define policies that contain rules for mediating the activities defined in Table 15. For each subject/object/operation/attribute combination, the evaluator shall execute at least one positive and one negative test in order to show that the TSF is capable of appropriately mediating these activities. For example, the policy may define a rule that allows one user to execute a certain process and another that forbids a different user from executing the same process. Once this policy is implemented, the evaluator will access a system as each of these users and observe that the ability to execute the specified process is appropriately allowed or denied. Additionally, for each conditional attribute that is supported (such as time of day restrictions), the evaluator will devise a positive and negative test that proves that the conditional attribute affects whether or not the requested operation is allowed. This activity is then repeated for each other subject/object/operation/attribute tuple.

	If the TOE enforces any additional access control policy rules, the evaluator shall devise positive and negative tests that cause these to be invoked and observe that appropriate behavior is performed.
Test Instructions	Execute this test per the test steps. This assurance activity is tested in conjunction with [ESM_PM_PP] ESM_ACD.1 (Test Case 001P).
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the management of Agents (i.e., Access Control products) by the App Control Server and Console (i.e., together being the Policy Management product) for all of the tests performed. The ESM_AC_PP has Table 6 (incorrectly referenced as Table 15 in the assurance activity) defined which has been defined in the Security Target through Tables 6-2 and 6-3 which will be used as the basis for discussion of this testing assurance activity. Tables 6-2 and 6-3 expand on the original table's concept of a mapping between subjects, objects, and operations by introducing another type of subject (i.e., processes) in Table 6-3 and adding the subjects attributes and object attributes to both tables. Tables 6-2 and 6-3 now depict all subject, object, operation, and attribute rule combinations that require testing to address this assurance activity, with one addition and one note. Additionally, the attribute hostname can be used to restrict a rule to only apply to an endpoint system based upon its hostname matching the hostname(s) defined within the rule. Note that Active Directory Users, AD Group Name, Authentication Function, and Login are not a combination for creating access control policies because AD Group Name is not a credential for authentication to an endpoint system. The evaluator created a single policy and verified that an audit record was generated for the policy's creation. The evaluator created rules for all subject, object, operation, and attribute combinations defined in Tables 6-2 and 6-3 from the Security Target. The evaluator also created rules focused on the hostname attribute defined and it was processed in rules with subjects using the username attribute, all objects using the name and approved status attributes, and all operations. Through the process of creating each rule, the rule was assigned to the single policy. The evaluator then assigned the policy to all Agents and waited for the Agents to consume the policy. The evaluator then queried the Computers table to verify the policy is being implemented by each Agent which is confirmed with the policy's name (i.e., policy identifier) being listed on each Agent's row and under the Policy column. For each rule created, the evaluator performed the following general steps to positively and negatively test the rule: 1. Enabled the rule and waited for the Agents to consume their policy's updated configuration list with the enabled rule 2. Accessed an Agent protected endpoint system that would enforce the rule selected; note the rule may not apply to all Agents that consumed the policy to which the rule applies due to the different operating systems (i.e., Windows versus Linux) and the hostname attribute a. Authenticate as a subject who has their attribute defined in the rule OR start a process on the endpoint system which would be the subject defined in the rule based upon its attribute b. Either as the subject or by proxy having the process be the subject, perform the operation defined by the rule on the object

	defined in the rule based upon its attribute(s) 3. Verify that the rule was enforced and the operation on the object by the subject was blocked by the Agent 4. Repeat step 2 to perform an operation on the object by a subject on an Agent protected endpoint system but change an attribute for the subject, object, or hostname to make the event not match the rule (e.g., login to the endpoint system as a client user whose username does not match the rule) 5. Verify that the rule was not enforced and the operation on the object by the subject was allowed by the Agent
Test Results	Pass
Execution Method	Manual

The FDP_ACF.1(1) SFR's rule processing description states: "The Agent will review the rules assigned to its policy starting with the lowest numbered rule first to determine if the rule is applicable to the operation being performed by the subject on the object. When a rule is found that is applicable, the Agent will enforce the first applicable rule's access control decision on the attempted operation and will stop reviewing any additional rules." The first sentence has to do with the TOE analyzing the operation being performed by the subject on the object by using their attributes. This directly relates to subject, object, operation, and attribute combinations described in Tables 6-2 and 6-3 of the Security Target. The evaluation team has determined that once this analysis has been made, the second sentence from the SFR is processed which enforces the access control decision defined by the SFR. The access control decisions claimed by the evaluation are block, permit/allow, and report/report only. As all analysis which results in matching a rule will result in the defined access control decision being processed, it is not necessary to test every permutation of access control decision with every possible subject, object, operation, and attribute combination. However, verifying the TOE's ability to enforce the access control decision types is required. Throughout the course of testing the SFRs, the access control decisions of block, permit/allow, and report/report only were tested and confirmed by the evaluation team to perform the action as described in the Security Target.

Test Case Number	009A
SFR	FDP_ACC.1(2) and FDP_ACF.1(2)
Test Objective	**The evaluator shall test this capability by performing the following actions:** **- Attempting to terminate the process or processes that comprise the TOE** - Attempting to delete or make arbitrary modifications to the defined configuration files or registry values - Attempting to modify the system's startup sequence such that the TOE's associated process or processes is excluded from system startup. **Throughout this, the evaluator shall observe that the TOE never stops running, that the TOE appropriately prevents the relocation, alteration, and/or removal of the parts that comprise it,** and in the third case above, that the TOE is still started during system boot.
Test Instructions	Execute this test per the test steps. Note that this test case is covering the bolded portions of the Test Objective. Refer to Test Case 010A and 011A which covers the remaining portions of the Test Objective.
Test Steps and Rationale	On an Agent for a Windows endpoint system, the evaluator attempted to kill the Agent process by using Task Manager and the command 'taskkill'. The Agent blocked both attempts to kill the Agent process and the Agent never stopped

	running. On an Agent for a Linux endpoint system, the evaluator attempted to kill the Agent process by using System Monitor and the command 'kill'. The Agent blocked both attempts to kill the Agent process and the Agent never stopped running. The evaluator verified audit records were generated for the blocked events.
Test Results	Pass
Execution Method	Manual

Test Case Number	010A
SFR	FDP_ACC.1(2) and FDP_ACF.1(2)
Test Objective	**The evaluator shall test this capability by performing the following actions:** - Attempting to terminate the process or processes that comprise the TOE **- Attempting to delete or make arbitrary modifications to the defined configuration files or registry values** - Attempting to modify the system's startup sequence such that the TOE's associated process or processes is excluded from system startup. **Throughout this, the evaluator shall observe that the TOE never stops running, that the TOE appropriately prevents the relocation, alteration, and/or removal of the parts that comprise it,** and in the third case above, that the TOE is still started during system boot.
Test Instructions	Execute this test per the test steps. Note that this test case is covering the bolded portions of the Test Objective. Refer to Test Case 009A and 011A which covers the remaining portions of the Test Objective.
Test Steps and Rationale	On an Agent for a Linux endpoint system, the evaluator attempted to rename, move, and delete files within the /opt/bit9/bin/ and /srv/bit9/data directories, and attempted to remove the kernel module. The Agent blocked the attempts from being processed and the Agent never stopped running. The evaluator verified audit records were generated for the blocked events. Through the Console, the evaluator then created a rule to block read access to the files within the /opt/bit9/ and /srv/bit9/data paths on Linux endpoint systems, assigned the rule to all policies, and waited for the Agent to consume the updated configuration list with the rule. On an Agent for a Linux endpoint system, the evaluator attempted to read files within /opt/bit9/bin/ and /srv/bit9/data. The Agent blocked the attempts from being processed and the Agent never stopped running. Through the Console, the evaluator then disabled the rule that was previously created and waited for the Agent to consume the updated configuration list. On same Agent, the evaluator attempted to read the same files within /opt/bit9/bin/ and /srv/bit9/data and the Agent allowed these actions to be performed. The evaluator verified audit records were generated for the blocked events. On an Agent for a Windows endpoint system, the evaluator attempted to rename and delete files within the C:\Program Files (x86)\Bit9\Parity Agent directory, rename, move, and delete the driver 'parity.sys' in C:\Windows\System32\Drivers directory, and modify and delete the registry keys: HKLM\SYSTEM\CurrentControlSet\Services\Parity, HKLM\SYSTEM\CurrentControlSet\Services\ParityDriver, and HKLM\SOFTWARE\SOFTWARE\WOW6432Node\Bit9. The Agent blocked the attempts from being processed and the Agent never stopped running. The evaluator verified audit records were generated for the blocked events. Through the Console, the evaluator then created a rule to block read access to the

	files within the <ProgramFilesx86>\bit9\parity agent\ and C:\ProgramData\Bit9\Parity Agent\ paths on Windows endpoint systems, assigned the rule to all policies, and waited for the Agent to consume the updated configuration list with the rule. On an Agent for a Windows endpoint system, the evaluator attempted to read files within <ProgramFilesx86>\bit9\parity agent\ and C:\ProgramData\Bit9\Parity Agent\. The Agent blocked the attempts from being processed and the Agent never stopped running. Through the Console, the evaluator then disabled the rule that was previously created and waited for the Agent to consume the updated configuration list. On same Agent, the evaluator attempted to read the same files within <ProgramFilesx86>\bit9\parity agent\ and C:\ProgramData\Bit9\Parity Agent\ and the Agent allowed these actions to be performed. The evaluator verified audit records were generated for the blocked events.
Test Results	Pass
Execution Method	Manual

Test Case Number	011A
SFR	FDP_ACC.1(2) and FDP_ACF.1(2)
Test Objective	**The evaluator shall test this capability by performing the following actions:** - Attempting to terminate the process or processes that comprise the TOE - Attempting to delete or make arbitrary modifications to the defined configuration files or registry values **- Attempting to modify the system's startup sequence such that the TOE's associated process or processes is excluded from system startup.** **Throughout this, the evaluator shall observe that the TOE never stops running, that the TOE appropriately prevents the relocation, alteration, and/or removal of the parts that comprise it, and in the third case above, that the TOE is still started during system boot.**
Test Instructions	Execute this test per the test steps. Note that this test case is covering the bolded portions of the Test Objective. Refer to Test Case 009A and 010A which covers the remaining portions of the Test Objective.
Test Steps and Rationale	On an Agent for a Windows endpoint system, the evaluator attempted to modify the value and delete the registry keys: HKLM\SYSTEM\CurrentControlSet\Services\Parity and HKLM\SYSTEM\CurrentControlSet\Services\ParityDriver. The Agent blocked the attempts from being processed and the Agent never stopped running. The evaluator then rebooted the endpoint system and confirmed that the Agent was running post boot. The evaluator verified audit records were generated for the blocked events. On an Agent for a Linux endpoint system, the evaluator attempted to rename and move the b9daemon file within the /opt/bit9/bin/ directory. The Agent blocked the attempts from being processed and the Agent never stopped running. The evaluator then rebooted the endpoint system and confirmed that the Agent was running post boot. The evaluator verified audit records were generated for the blocked events.
Test Results	Pass
Execution Method	Manual

4.3.1.5 Security Management

Test Case Number	012A
SFR	FMT_MOF.1(1)
Test Objective	The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator shall verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification. The evaluator shall also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities: - Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior - Repository for trusted audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository - Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP. - Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP. - Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied. Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the management of Agents (i.e., Access Control products) by the App Control Server and Console (i.e., together being the Policy Management product) for all of the tests performed. Through the Console, the evaluator modified the behavior of the functions of the TOE, verified the function was modified and performed other actions which confirmed that the TOE operated per the manner it was configured. The evaluator performed testing to modify the

	items below. **A portion of this assurance activity is satisfied with other test cases. For those portions, below is a mapping of the test cases that satisfy that portion.** **Audited Events**: This portion of the assurance activity is satisfied by Test Case 003A. **Repository for trusted audit storage**: The evaluator placed the TOE into configuration two, which is strictly a test configuration, before conducting this test. This was accomplished by setting up a second SQL database and configuring the TOE to use it as a second audit repository. Once configured, the evaluator logged into the Console, confirmed that log in event was sent to the second SQL database. The evaluator then disabled the TOE's configuration to use the second SQL database. The evaluator logged into the Console again and verified that this audit event was not written to the disconnected second SQL database. This audit record was still written to the SQL Server Database. **Access Control SFP**: This portion of the assurance activity is satisfied by Test Case 002P. **Policy being implemented by the TSF**: This portion of the assurance activity is satisfied by Test Case 002P. **Access Control SFP behavior to implement in the event of communications outage**: This portion of the test case is satisfied by Test Case 020A. The last portion of the assurance activity was satisfied by performing the following test with an Agent on a Linux endpoint system and an Agent on a Windows endpoint system. The evaluator created a rule, assigned the rule to the Agent's policy, and waited for the Agent to consume the updated configuration list with the rule. On the Agent's endpoint system, the evaluator performed an operation on an object that matched the rule. This was blocked by the Agent and an audit record for the block was created. On the Agent, the evaluator used the dascli utility to disconnect the Agent which would stop the Agent from polling and being managed by the App Control Server. The evaluator confirmed that the Agent recognized its disconnected status and after a few minutes confirmed that the App Control Server also recognized that the Agent was now disconnected. The evaluator then deleted the rule created earlier. The evaluator verified that the App Control Server was not able to manage the Agent by providing the Agent the latest configuration list. The evaluator further verified the Agent was not being managed by performing the same operation on the same object that matched the rule and confirming the Agent still enforced the rule. The evaluator determined that the App Control Server could no longer manage the Agent.
Test Results	Pass
Execution Method	Manual

Test Case Number	013A
SFR	FMT_MOF.1(2)
Test Objective	The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it.

	The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to query the policy being implemented by the TOE. Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	This AA is satisfied by the testing of FMT_MOF.1(1). The first paragraph of this AA is covered by the first paragraph of the test explanation under FMT_MOF.1(1). The last paragraph of this AA is covered by the last paragraph of the test explanation under FMT_MOF.1(1).
Test Results	Pass
Execution Method	Manual

Test Case Number	014A
SFR	FMT_MSA.1
Test Objective	The evaluator shall test this capability by using the associated Policy Management product to confirm that each identified operation against the indicated attributes may be performed, and that the TOE interfaces do not provide the ability for any other roles to perform operations against the indicated attributes.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	Through the course of testing the assurance activities associated with the FDP_ACC.1(1), FDP_ACF.1(1), FDP_ACC.1(2), and FDP_ACF.1(2), the evaluator changed the default, queried, modified, and deleted the security attributes access control policies, access control policy attributes, and implementation status of access control policies of its access control. This was accomplished by the evaluator through the TOE's Console by creating rules for each subject, object, operation, and associated attributed defined for the access control Security Function Policy and assigning each of them to a policy which was consumed by Agents. The evaluator then verified that the rules were enforced by the Agent as expected, proving that the App Control Server provided this information to the Agent over their interface. This confirms that the App Control Server (i.e., Policy Management product) has the ability and role to make these changes to an Agent's configuration. The evaluator created two instances of the App Control Server which will be referred to as TOE Server and Rogue Server. The evaluator set up an Agent on a Windows and Linux endpoint to be managed by the TOE Server and confirmed the connections with the Agents. The evaluation team then disabled tamper protection on the Agents and shutdown the TOE Server. The evaluators then configured the Agents locally to connect to the Rogue Server, and confirmed that a connection could not be made between the Agents and Rogue Server. This confirmed that the Rogue Server did not have the ability to make any changes to the Agent's configuration.
Test Results	Pass
Execution Method	Manual

Test Case Number	015A
SFR	FMT_MSA.3
Test Objective	The evaluator shall test this capability by using the associated Policy Management

	product to confirm that for each identified security attribute and restrictive initial state, the TOE implements the correct restrictive value and that it can be overridden in the manner specified by the operational guidance.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator created a policy for each of the three Enforcement Levels (High, Medium and Low). The evaluator then connected to an Agent with the High Enforcement Level and created a new file that was unapproved. Then the evaluator attempted to run the file and verified that an unapproved file was not able to be run. The evaluator then changed the policy for that Agent to the Medium Enforcement Level and verified that the Agent prompted the client user to either "allow" or "block" the action requested. The evaluator attempted to run the file and selected "block" which blocked the file from running. The evaluator attempted to run the file and selected "allow" which allowed the file to be executed. The evaluator then changed the policy for that Agent to the Low Enforcement Level and verified that an approved file was able to be run. This demonstrates that the applied enforcement level can be overridden by defining a different Enforcement Level in a policy which is described in Section 7.3.1 of the AGD.
Test Results	Pass
Execution Method	Manual

Test Case Number	016A
SFR	FMT_SMF.1
Test Objective	The evaluator shall test this capability by configuring the TOE in a manner that is consistent with the evaluated configuration. For each management function that has been defined in the ST, the evaluator shall perform the function in a manner that is consistent with the operational guidance and verify that the observed behavior is consistent with the expectations of what the function should accomplish.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	This test is satisfied with the testing of other test cases within this test plan. A mapping of each function has been provided below. This mapping provides the defined management functions listed in the Security Target and the test case that the functions are performed. Each function was performed in the prescribed manner as instructed in the AGD. configuration of audited events – Test Case 003A configuration of repository for trusted audit storage – Test Case 012A configuration of Access Control SFP – Test Case 001P querying of policy being implemented by the TSF – Test Case 001P management of Access Control SFP behavior to enforce in the event of communications outage – Test Case 001P The mapping is not an exhaustive list of all instances were these management functions were performed throughout the testing but a single instance of the management function being performed to verify that each function exists, that it can be performed in the prescribed manner, and that it accomplishes the documented capability. The evaluator has determined that based upon testing all other SFR assurance activities claimed that the management functions accomplished their capability.

Test Results	Pass
Execution Method	Manual

Test Case Number	017A
SFR	FMT_SMR.1
Test Objective	The evaluator shall use the associated Policy Management product to connect to the TOE and confirm that it is operating in the assigned role. The evaluation shall also confirm that a user or other external entity that has not been authorized for the indicated role cannot assume the indicated role.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator created two instances of the App Control Server which will be referred to as TOE Server and Rogue Server. The evaluator set up an Agent on a Windows and Linux endpoint to be managed by the TOE Server and confirmed the connections with the Agents. The evaluation team then disabled tamper protection on the Agents and shutdown the TOE Server. The evaluators then configured the Agents locally to connect to the Rogue Server, and confirmed that a connection could not be made between the Agents and Rogue Server. This confirmed that the Rogue Server did not have the ability to make any changes to the Agent's configuration.
Test Results	Pass
Execution Method	Manual

4.3.1.6 Protection of the TSF

Test Case Number	018A
SFR	FPT_APW_EXT.1
Test Objective	The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator as an administrator of the underlying Windows operating system accessed the SQL Database Server with a database management utility and performed a query on the user table. The returned rows had a hash in the "password" column and a random value in the "salt" column for all users. The evaluator attempted to repeat these steps as a user that was not an administrator, and that user was not able to access the user information in the SQL Database Server. The evaluator as domain administrator accessed the Active Directory and extract the user information. The extracted information had a hash under each user's secrets. The evaluator attempted to repeat these steps as a user that was not the domain administrator, and that user was not able to access the user information in Active Directory.
Test Results	Pass
Execution Method	Manual

Test Case Number	019A
SFR	FPT_FLS.1
Test Objective	The evaluator shall test this capability by deliberately inducing the failure states

	described in the SFR and observing whether or not the TSF reacts in a manner that is consistent with the Security Target's description of its expected behavior.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator demonstrated that the TOE's Agent automatically restarts its processes if unexpectedly stopped. The evaluator disabled the Agent's tamper protection through the Console for an Agent on a Windows and Linux endpoint system. The evaluator then accessed each Agent's endpoint system, deliberately ended the Agent's process, and ensured that the Agent restarted without any administrative action. This is consistent with the description in the Security Target.
Test Results	Pass
Execution Method	Manual

Test Case Number	020A
SFR	FPT_FLS_EXT.1
Test Objective	The evaluator shall test this capability by terminating the Policy Management product (if the TOE resides on the same system) or by severing the network connection between the Policy Management product and the TOE (if the TOE resides on a different system). The evaluator shall then interact with the TOE while these communications are suspended in order to determine that the behavior it exhibits in this state is consistent with the expected behavior. If the assignment is chosen to define an alternate failure state behavior, the evaluator shall verify that the observed behavior corresponds to its description in the TSS.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator satisfied this assurance activity by creating a policy on the App Control Server (i.e., the Policy Management product) with the Connected and Disconnected Enforcement Levels being the same Low enforcement and assigned it a rule which blocked a file. Once the Agents on the Windows and Linux endpoints consumed the policy, the evaluator then verified on each Agent that when the Agent is connected to the App Control Server access to the file was blocked. Then the evaluator severed the connection between the Agents and the App Control Server, waited for the Agent to recognize it was disconnected, and again verified that access to the file was blocked. The evaluator determined that regardless of communication status between an Agent and App Control Server that the Agent will always enforce its latest configuration as defined by its policy and configuration list of rules which is consistent with the Security Target. The evaluator then fixed the connection between the Agents and the App Control Server, and on the App Control Server created a policy with the Connected Enforcement Level of Medium and the Disconnected Enforcement Level of High. Once the Agents on the Windows and Linux endpoints consumed the policy, the evaluator attempted to access an unapproved file, a dialog box was displayed to client user asking to approve or block the access to the file, and the evaluator selected block. Then the evaluator severed the connection between the Agents and the App Control Server, waited for the Agent to recognize it was disconnected, and attempted to access the file which was now automatically blocked by the Agent. The evaluator determined that depending on the communication status between an Agent and App Control Server the Agent will enforce access differently, when connected the Connected Enforcement Level is applied and when disconnected the Disconnected Enforcement Level is applied which is consistent with the Security Target.
Test Results	Pass
Execution Method	Manual

Test Case Number	021A
SFR	FPT_RPL.1 – TQ1195
Test Objective	The evaluator shall test this capability by configuring replay detection in a manner specified by the operational guidance (if applicable), running a packet sniffer application (such as Wireshark) on the local network with the TOE, sending a valid policy to it, and observing the packets that comprise this policy. The evaluator can then take these packets and re-transmit them to the TOE. Once this has been done, the evaluator shall execute an appropriate subset of User Data Protection testing with the expectation that the policy enforced will be the first policy transmitted. If the expected results are met, the TOE is sufficiently resilient to rudimentary policy forgery.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluation team conducted this test based upon feedback provided through Technical Query 1195. The following test was performed on both the Agent on the Windows Endpoint System and Agent on the Linux Endpoint System. The evaluation team captured the multi-directional TLS traffic sent between the Agent and Server when a new policy was transferred to the Agent. The evaluation team then filtered the packet capture to only include the unidirectional packets being sent from the Server to the Agent. The evaluation team then replayed the unidirectional packets by sending them to the Agent. The evaluation team observed that the TOE's underlying operating system network stack successfully rejected the replayed unidirectional packets from the prior policy transmission. The replayed packets were not processed by the TOE application as a result of the underlying operating system network stack's rejection as evidenced by RST packets. For this reason, no audit record would be produced by the TOE. The TOE is sufficiently resilient to rudimentary policy forgery due to its use of the underlying operating system network stack and implementation of TLS.
Test Results	Pass
Execution Method	Manual

Test Case Number	022A
SFR	FPT_SKP_EXT.1
Test Objective	There are no Test Assurance Activities for this requirement defined within ESM_AC_PP.
Test Instructions	N/A
Test Steps and Rationale	N/A
Test Results	Pass
Execution Method	Manual

4.3.1.7 Resource Utilization

Test Case Number	023A
SFR	FRU_FLT.1
Test Objective	The evaluator shall test this capability by severing the network connection between the TOE and the Policy Management product, defining an updated policy, and reestablishing the connection will determine if the TOE appropriately receives the new policy data within the time interval specified in FCO_NRR.2.3. The evaluator shall devise a scenario such that the old policy allows a specific action and that the new policy denies that same action. The evaluator shall then perform that action,

	observe that it is allowed, sever connection with the Policy Management product, define the new policy during that outage, re-establish the connection, wait for the interval defined by FCO_NRR.2.3, perform the same action again, and observe that it is no longer allowed.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator tested this activity by creating a rule to allow access to a file and attaching it to the policy for an Agent on a Windows and Linux endpoint. Once the Agents on the Windows and Linux endpoints consumed the policy, the evaluator attempted to access the file on each Agent's endpoint system and access was allowed. Then the evaluator severed the connection between the Agents and the App Control Server and update the rule to now block access to the same file. The evaluator then fixed the connection between the Agents and the App Control Server, and waited for the Agents to consume the configuration list with the updated rule. The evaluator attempted to access the file on each Agent's endpoint system and access was now blocked. The evaluation team determined that the Agents will enforce the latest policy configured once an Agent re-establishes communication with the App Control Server after an outage.
Test Results	Pass
Execution Method	Manual

4.3.1.8 TOE Access

Test Case Number	024A
SFR	FTA_TSE.1
Test Objective	The evaluator shall test this capability by performing positive and negative testing for each attribute that can be used to conditionally allow session establishment. For example, if a time of day restriction applies, the evaluator shall successfully log on during an acceptable time and shall be prevented from logging on during an unacceptable time.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator satisfied this assurance activity by configuring a specific Agent's configuration in the Console based upon the Agent's hostname and within the configuration specify to block authentication of a client user based upon their username. The evaluator then attempted to authenticate to the endpoint system with the configured Agent as a different client user than the one that was defined in the Agent's configuration and session establishment (i.e., authentication function) was granted. The evaluator then attempted to authenticate to the endpoint system with the configured Agent as the client user that was defined in the Agent's configuration and session establishment (i.e., authentication function) was denied. The evaluator determined that the client user's username attribute was being used to determine if session establishment (i.e., authentication function) was allowed or denied. The evaluator then attempted to authenticate to an endpoint system where the Agent does not have the session establishment (i.e., authentication function) configuration as the client user that was defined in the other Agent's configuration and session establishment (i.e., authentication function) was allowed. The evaluator determined that the endpoint system's hostname attribute for the Agent was being used to determine if session establishment (i.e., authentication function) was allowed or denied.
Test Results	Pass

Execution Method	Manual

4.3.1.9 Trusted Paths/Channels

Test Case Number	025A
SFR	FTP_ITC.1 – TD0576
Test Objective	Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful. Further assurance activities are associated with the specific protocols. For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connections between Agents and the App Control Server for all of the tests performed. The evaluator started a packet capture between the Agents and the App Control Server. The evaluator then created a new policy on the App Control Server and assigned it to the Agent on a Linux and Windows endpoint system. The evaluator then captured the traffic between the Agents and the App Control Server upon the Agents' next poll which would include the newly created policy. The evaluator observed for each connection that it was between an Agent and the App Control Server, was initiated by the Agent, and that the communication used TLS/HTTPS (channel data is not sent in plaintext). For these reasons, the evaluator determined Test 1, 2, and 3 for the ESM_AC_PP's iteration of FTP_ITC.1 have been satisfied.
Test Results	Pass
Execution Method	Manual

Test Case Number	026A
SFR	FTP_ITC.1 – TD0576
Test Objective	Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities. Further assurance activities are associated with the specific protocols. For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connections between Agents and the App Control Server for all of the tests performed. The evaluator started a packet capture between the Agents and the App Control Server. The evaluator then created a new policy on the App Control Server and assigned it to the Agent on a Linux and Windows endpoint system. The evaluator then captured the traffic between the Agents and the App Control Server upon the Agents' next poll which would include the newly

	created policy. The evaluator observed for each connection that it was between an Agent and the App Control Server, was initiated by the Agent, and that the communication used TLS/HTTPS (channel data is not sent in plaintext). For these reasons, the evaluator determined Test 1, 2, and 3 for the ESM_AC_PP's iteration of FTP_ITC.1 have been satisfied.
Test Results	Pass
Execution Method	Manual

Test Case Number	027A
SFR	FTP_ITC.1 – TD0576
Test Objective	Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext. Further assurance activities are associated with the specific protocols. For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connections between Agents and the App Control Server for all of the tests performed. The evaluator started a packet capture between the Agents and the App Control Server. The evaluator then created a new policy on the App Control Server and assigned it to the Agent on a Linux and Windows endpoint system. The evaluator then captured the traffic between the Agents and the App Control Server upon the Agents' next poll which would include the newly created policy. The evaluator observed for each connection that it was between an Agent and the App Control Server, was initiated by the Agent, and that the communication used TLS/HTTPS (channel data is not sent in plaintext). For these reasons, the evaluator determined Test 1, 2, and 3 for the ESM_AC_PP's iteration of FTP_ITC.1 have been satisfied.
Test Results	Pass
Execution Method	Manual

Test Case Number	028A
SFR	FTP_ITC.1 – TD0576
Test Objective	Test 4: The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected. Further assurance activities are associated with the specific protocols. For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connections between Agents and the App Control Server for all of the tests performed. The evaluator started a packet capture between the Agents and the App Control Server. The evaluator physically interrupted the connection between the Agents and App Control Server by removing the ethernet

	cable to the App Control Server's machine, waited a few minutes for the TCP connection to timeout, and then reconnected the ethernet cable. The evaluator then captured the traffic between the Agents and the App Control Server being reestablished upon each Agent's next poll. The evaluator observed for each connection that it was between an Agent and the App Control Server, was initiated by the Agent, and that the communication was appropriately protected using TLS/HTTPS.
Test Results	Pass
Execution Method	Manual

4.3.2 ESM_PM_PP Security Functional Requirements

4.3.2.1 Enterprise Security Management

Test Case Number	001P
SFR	ESM_ACD.1
Test Objective	The evaluator shall test this capability by using the TOE to create a policy that uses the full range of subjects, objects, operations, and attributes and sending it to a compatible Access Control product for consumption. The evaluator will then perform actions that are mediated by the Access Control product in order to confirm that the policy was applied appropriately. The evaluator will also verify that a policy identifier is associated with a transmitted policy by querying the policy that is being implemented by the Access Control product.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the management of Agents (i.e., Access Control products) by the App Control Server and Console (i.e., together being the Policy Management product) for all of the tests performed. The ESM_AC_PP has Table 6 (incorrectly referenced as Table 15 in the assurance activity) defined which has been defined in the Security Target through Tables 6-2 and 6-3 which will be used as the basis for discussion of this testing assurance activity. Tables 6-2 and 6-3 expand on the original table's concept of a mapping between subjects, objects, and operations by introducing another type of subject (i.e., processes) in Table 6-3 and adding the subjects attributes and object attributes to both tables. Tables 6-2 and 6-3 now depict all subject, object, operation, and attribute rule combinations that require testing to address this assurance activity, with one addition and one note. Additionally, the attribute hostname can be used to restrict a rule to only apply to an endpoint system based upon its hostname matching the hostname(s) defined within the rule. Note that Active Directory Users, AD Group Name, Authentication Function, and Login are not a combination for creating access control policies because AD Group Name is not a credential for authentication to an endpoint system. The evaluator created a single policy and verified that an audit record was generated for the policy's creation. The evaluator created rules for all subject, object, operation, and attribute combinations defined in Tables 6-2 and 6-3 from the Security Target. The evaluator also created rules focused on the hostname attribute defined and it was processed in rules with subjects using the username attribute, all objects using the name and approved status attributes, and all operations. Through the process of creating each rule, the rule was assigned to the single policy. The evaluator then assigned the policy to all Agents and waited for the Agents to consume the policy. The evaluator then queried the Computers table to verify the

	policy is being implemented by each Agent which is confirmed with the policy's name (i.e., policy identifier) being listed on each Agent's row and under the Policy column. For each rule created, the evaluator performed the following general steps to positively and negatively test the rule: 1. Enabled the rule and waited for the Agents to consume their policy's updated configuration list with the enabled rule a. If the rule is testing the 'Approved Status' attribute for a File Object, verify or update the File Object's 'Approved Status' to match the value (i.e., Approved, Banned, Unapproved) identified in the rule 2. Access an Agent protected endpoint system that would enforce the rule selected; note the rule may not apply to all Agents that consumed the policy to which the rule applies due to the different operating systems (i.e., Windows versus Linux) and the hostname attribute a. Authenticate as a subject who has their attribute defined in the rule OR start a process on the endpoint system which would be the subject defined in the rule based upon its attribute b. Either as the subject or by proxy having the process be the subject, perform the operation defined by the rule on the object defined in the rule based upon its attribute(s) 3. Verify that the rule was enforced and the operation on the object by the subject was blocked by the Agent 4. Repeat step 2 to perform an operation on the object by a subject on an Agent protected endpoint system but change an attribute for the subject, object, or hostname to make the event not match the rule (e.g., login to the endpoint system as a client user whose username does not match the rule) 5. Verify that the rule was not enforced and the operation on the object by the subject was allowed by the Agent
Test Results	Pass
Execution Method	Manual

Test Case Number	002P
SFR	ESM_ACT.1
Test Objective	The evaluator shall test this capability by obtaining one or more compatible Access Control products and configuring the TOE to manage them. Then, following the procedures in the operational guidance for both the TOE and the Access Control product, the evaluator shall create a new policy and ensure that the new policy defined in the by the TSF is successfully transmitted to, consumed by, and enforced in an Access Control product, in accordance with the circumstances defined in the SFR. In other words, (a) if the selection is completed to transmit after creation of a new policy, then the evaluator shall create the new policy and ensure that, after a reasonable window for transmission, the new policy is installed; (b) if the selection is completed to transmit periodically, the evaluator shall create the new policy, wait until the periodic interval has passed, and then confirm that the new policy is present in the Access Control component; or

	(c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator shall create the policy, use the Secure Configuration Management component to request transmission, and the confirm that the Access Control component has received and installed the policy. If the ST author has specified "other circumstances", then a similar test shall be executed to confirm transmission under those circumstances. The evaluator shall then make a change to the previously created policy and then repeat the previous procedure to ensure that the updated policy is transmitted to the Access Control component in accordance with the SFR-specified circumstances. Lastly, as updating a policy encompasses deletion of a policy, the evaluator shall repeat the process a third time, this time deleting the policy to ensure it is removed as an active policy from the Access Control component. The evaluator shall repeat this test for a representative sample of Access Control products that can be managed by the TOE. For example, if the TOE provides the ability to manage groups of host-based access control endpoints, the evaluator shall create different groups such that each supported platform is included in at least one group and verify that group members will appropriately consume policies when instructed to do so. Note: This testing will likely be performed in conjunction with the testing of ESM_ACD.1.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the management of Agents (i.e., compatible Access Control products) by the App Control Server for all of the tests performed. The following test was performed for both Agents on Windows machines and Agents on a Linux machines which are all of the types of Access Control products that can be managed by the App Control Server in the evaluated configuration. The evaluator created a new policy (e.g., policy1), created a new rule (e.g., rule1), and assigned rule1 to policy1. Rule1 specified that a specific client user (e.g., user1) was blocked from creating files within a specific path (i.e., directory). The evaluator then assigned policy1 to an Agent (e.g., Agent1) on an endpoint system and waited for Agent1 to consume policy1. The evaluator as user1 authenticated to the endpoint system protected by the Agent1 and verified that user1 was blocked from creating a file in the path specified in policy1's rule1. The evaluator as a different client user (e.g., user2) authenticated to the endpoint system protected by the Agent1 and verified that user2 was allowed to create a file in the path specified in policy1's rule1. The evaluator then modified rule1 to change user1 to user2 and waited for the Agent to consume policy1's updated configuration list with rule1. The evaluator then attempted to perform the same create file operation, within the same path, on the same endpoint system protected by Agent1 with user1 and then user2. This time user1's operation was allowed and user2's operation was blocked. The evaluator determined this verified that a policy and associated rule are enforced based upon the client user's username when defined in a rule. The evaluator then moved the Agent1 to a different policy (e.g., policy2) without rule1 assigned and deleted policy1. The evaluator as user1 authenticated to the endpoint system protected by the Agent1 and verified that user1 was allowed to create a file in the path specified in rule1. The evaluator created a new policy (e.g., policy3) and assigned rule2 to policy3. Rule2 specified that a specific client user (e.g., user1) was blocked creating files within a specific path (i.e., directory) on specific endpoint systems by their hostname (i.e., Agent1's and Agent2's endpoint systems hostnames). The evaluator then assigned policy3 to two Agents (e.g., Agent1, Agent2) on endpoint systems of the same operating system and waited for the Agents to consume policy3. The

	evaluator as user1 authenticated to the endpoint systems protected by Agent1 and Agent2, and verified that user1 was blocked from creating a file in the path specified in policy3's rule2 on both endpoint systems. The evaluator modified rule2 to remove Agent2's endpoint system hostname from the rule and waited for the Agents to consume policy3's updated configuration list with rule2. The evaluator as user1 authenticated to the endpoint systems protected by Agent1 and Agent2, and verified that user1 was blocked from creating a file in the path specified in policy3's rule2 on only Agent1 and the operation was allowed on Agent2's endpoint system. The evaluator determined this verified that a policy and associated rule are enforced based upon the Agent's endpoint system hostname when defined in a rule. The evaluator then moved the Agent1 and Agent2 to a different policy (e.g., policy2) without rule2 assigned and deleted policy3. The evaluator as user1 authenticated to the endpoint systems protected by Agent1 and Agent2, and verified that user1 was allowed to create a file in the path specified in rule2 on both endpoint systems.
Test Results	Pass
Execution Method	Manual

Test Case Number	003P
SFR	ESM_ATD.1
Test Objective	The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.
Test Instructions	Execute this test per the test steps. This assurance activity is tested in conjunction with [PM] ESM_ACD.1 (Test Case 001P).
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the management of Agents (i.e., Access Control products) by the App Control Server and Console (i.e., together being the Policy Management product) for all of the tests performed. The ESM_AC_PP has Table 6 (incorrectly referenced as Table 15 in the assurance activity) defined which has been defined in the Security Target through Tables 6-2 and 6-3 which will be used as the basis for discussion of this testing assurance activity. Tables 6-2 and 6-3 expand on the original table's concept of a mapping between subjects, objects, and operations by introducing another type of subject (i.e., processes) in Table 6-3 and adding the subjects attributes and object attributes to both tables. Tables 6-2 and 6-3 now depict all subject, object, operation, and attribute rule combinations that require testing to address this assurance activity, with one addition and one note. Additionally, the attribute hostname can be used to restrict a rule to only apply to an endpoint system based upon its hostname matching the hostname(s) defined within the rule. Note that Active Directory Users, AD Group Name, Authentication Function, and Login are not a combination for creating access control policies because AD Group Name is not a credential for authentication to an endpoint system. The evaluator created a single policy and verified that an audit record was generated for the policy's creation. The evaluator created rules for all subject, object, operation, and attribute combinations defined in Tables 6-2 and 6-3 from the Security Target. The evaluator also created rules focused on the hostname attribute defined and it was processed in rules with subjects using the username attribute, all

	objects using the name and approved status attributes, and all operations. Through the process of creating each rule, the rule was assigned to the single policy. The evaluator then assigned the policy to all Agents and waited for the Agents to consume the policy. The evaluator then queried the Computers table to verify the policy is being implemented by each Agent which is confirmed with the policy's name (i.e., policy identifier) being listed on each Agent's row and under the Policy column. For each rule created, the evaluator performed the following general steps to positively and negatively test the rule: 1. Enabled the rule and waited for the Agents to consume their policy's updated configuration list with the enabled rule 2. Accessed an Agent protected endpoint system that would enforce the rule selected; note the rule may not apply to all Agents that consumed the policy to which the rule applies due to the different operating systems (i.e., Windows versus Linux) and the hostname attribute a. Authenticate as a subject who has their attribute defined in the rule OR start a process on the endpoint system which would be the subject defined in the rule based upon its attribute b. Either as the subject or by proxy having the process be the subject, perform the operation defined by the rule on the object defined in the rule based upon its attribute(s) 3. Verify that the rule was enforced and the operation on the object by the subject was blocked by the Agent 4. Repeat step 2 to perform an operation on the object by a subject on an Agent protected endpoint system but change an attribute for the subject, object, or hostname to make the event not match the rule (e.g., login to the endpoint system as a client user whose username does not match the rule) 5. Verify that the rule was not enforced and the operation on the object by the subject was allowed by the Agent
Test Results	Pass
Execution Method	Manual

Test Case Number	004P
SFR	ESM_ATD.2
Test Objective	The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.
Test Instructions	Execute this test per the test steps. This assurance activity is tested in conjunction with [PM] ESM_ACD.1 (Test Case 001P).
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the management of Agents (i.e., Access Control products) by the App Control Server and Console (i.e., together being the Policy Management product) for all of the tests performed. The ESM_AC_PP has Table 6 (incorrectly referenced as Table 15 in the assurance activity) defined which has

	been defined in the Security Target through Tables 6-2 and 6-3 which will be used as the basis for discussion of this testing assurance activity. Tables 6-2 and 6-3 expand on the original table's concept of a mapping between subjects, objects, and operations by introducing another type of subject (i.e., processes) in Table 6-3 and adding the subjects attributes and object attributes to both tables. Tables 6-2 and 6-3 now depict all subject, object, operation, and attribute rule combinations that require testing to address this assurance activity, with one addition and one note. Additionally, the attribute hostname can be used to restrict a rule to only apply to an endpoint system based upon its hostname matching the hostname(s) defined within the rule. Note that Active Directory Users, AD Group Name, Authentication Function, and Login are not a combination for creating access control policies because AD Group Name is not a credential for authentication to an endpoint system. The evaluator created a single policy and verified that an audit record was generated for the policy's creation. The evaluator created rules for all subject, object, operation, and attribute combinations defined in Tables 6-2 and 6-3 from the Security Target. The evaluator also created rules focused on the hostname attribute defined and it was processed in rules with subjects using the username attribute, all objects using the name and approved status attributes, and all operations. Through the process of creating each rule, the rule was assigned to the single policy. The evaluator then assigned the policy to all Agents and waited for the Agents to consume the policy. The evaluator then queried the Computers table to verify the policy is being implemented by each Agent which is confirmed with the policy's name (i.e., policy identifier) being listed on each Agent's row and under the Policy column. For each rule created, the evaluator performed the following general steps to positively and negatively test the rule: 1. Enabled the rule and waited for the Agents to consume their policy's updated configuration list with the enabled rule 2. Accessed an Agent protected endpoint system that would enforce the rule selected; note the rule may not apply to all Agents that consumed the policy to which the rule applies due to the different operating systems (i.e., Windows versus Linux) and the hostname attribute a. Authenticate as a subject who has their attribute defined in the rule OR start a process on the endpoint system which would be the subject defined in the rule based upon its attribute b. Either as the subject or by proxy having the process be the subject, perform the operation defined by the rule on the object defined in the rule based upon its attribute(s) 3. Verify that the rule was enforced and the operation on the object by the subject was blocked by the Agent 4. Repeat step 2 to perform an operation on the object by a subject on an Agent protected endpoint system but change an attribute for the subject, object, or hostname to make the event not match the rule (e.g., login to the endpoint system as a client user whose username does not match the rule) 5. Verify that the rule was not enforced and the operation on the object by the subject was allowed by the Agent

Test Results	Pass
Execution Method	Manual

Test Case Number	005P
SFR	ESM_EAU.2
Test Objective	The evaluator shall test this capability by accessing the TOE without having provided valid identification and authentication information and observe that access to the TSF is subsequently denied. If any IT entities authenticate to the TOE, the evaluator shall instruct these IT entities to provide invalid identification and authentication information and observe that they are not able to access the TSF. Note that positive testing of the identification and authentication is assumed to be tested by other requirements because successful authentication is a prerequisite to manage the TSF (and possibly for the TSF to interact with external IT entities).
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator satisfied this assurance activity by providing invalid identification and authentication information to the TOE resulting in a denial of access. The invalid authentication information included an invalid username for a TOE defined user, an invalid password for a TOE defined users, an invalid username for an Active Directory (AD) user, and an invalid password for an AD user. The evaluator also provided valid authentication information for a TOE defined user and AD user which resulted in successful authentication to the TOE for both users. The TOE does not have any IT entities authenticate to it, and this portion of the testing assurance activity was not performed.
Test Results	Pass
Execution Method	Manual

Test Case Number	006P
SFR	ESM_EID.2
Test Objective	There are no Test Assurance Activities for this requirement defined within ESM_PM_PP.
Test Instructions	N/A
Test Steps and Rationale	N/A
Test Results	Pass
Execution Method	Manual

4.3.2.2 Security Audit

Test Case Number	007P
SFR	FAU_GEN.1
Test Objective	The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST. This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is

	defined, the corresponding audit record should correctly identify the policy that was defined.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	Refer to Test Case 002A.
Test Results	Pass
Execution Method	Manual

Test Case Number	008P
SFR	FAU_SEL_EXT.1
Test Objective	The evaluator shall test this capability by configuring a compatible Access Control product to have: - All selectable auditable events enabled - All selectable auditable events disabled - Some selectable auditable events enabled For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded by the Access Control product. If this SFR is iterated, the evaluator shall repeat these activities for each iteration of the SFR, substituting the appropriate external entity for "Access Control product" where appropriate.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the management of Agents (i.e., Access Control products) by the App Control Server and Console (i.e., together being the Policy Management product) for all of the tests performed. The TOE performs selectable audit based upon administrative users defining rules and specifying that events triggering the rules need to be audited. **All selectable auditable events enabled:** Through the course of the evaluator testing ESM_ACD.1, FDP_ACC.1(1), and FDP_ACF.1(1) by performing Test Case 001P, all administrative user generated rules for all subject, object, operation, and attribute combinations that were claimed by the evaluation through Security Target Tables 6-2 and 6-3 have been tested. These rules resulted in an audit record being generated when the rule was enforced, and the audit record was confirmed by the evaluator. The evaluator also confirmed that it was due to the rule that the audit record was generated because when the subject, object, operation, and attribute combination did not exactly match the rule, the rule was not enforced, and no audit record was generated. Therefore, the evaluator has completed the testing for all selectable auditable events enabled. **All selectable auditable events disabled:** On the Console, the evaluator ensured all administrative user generated rules were disabled or disabled the rule so that only rules that are prepackaged with the TOE are enabled. Next the evaluator created the 'No Selectable Audit' policy, assigned it to all Agents, and waited for the Agents to consume the new policy. The evaluator then accessed a Windows and a Linux endpoint system protected by an Agent and attempted to kill the Agent's process on each endpoint system. The evaluator then logged into the Console and verified that audit records were created for the Agents policy change and attempting to kill the Agent's process on each endpoint system. The evaluator determined that when all selectable auditable events are disabled, based upon the administrative user generated rules being disabled, that the TOE still performs auditing of events that are not selectable. **Some selectable auditable events enabled:**

	For an Agent on a Windows and Linux endpoint system, the evaluator conducted the following 'some selectable audit events enabled' test. The evaluator created four rules: all rules were created disabled, each rule identified a different object, two of the rules were applicable to all subjects, one of the rules was specific to a client user by their username, and one of the rules was specific to a process by their process name. The evaluator then moved the Agent to a new policy. On the endpoint system protected by the Agent, in a shared directory between multiple users, create five files with different names, four of the files' names should match the object names defined in the four rules. The evaluator then performed an action which would have trigged one of the rules applicable to all subjects, if it were enabled, and confirmed that an audit record was not generated. The evaluator then enabled that rule and waited for the Agent to consume the updated configuration list. The evaluator then performed the same action on the endpoint and this time the rule was enforced by the Agent and an audit record was created. The evaluator then performed an action which would have trigged the rule applicable to a specific user subject, if it were enabled, and confirmed that an audit record was not generated. The evaluator then enabled that rule and waited for the Agent to consume the updated configuration list. The evaluator then performed the same action on the endpoint with the client user whose username was within the rule and with a client user with a different username. This time the rule was enforced by the Agent for the user whose username matched the rule and an audit record was created for the enforcement but there was no enforcement nor audit record for the user whose username did not match the rule. The evaluator then performed an action which would have trigged the other rule that is applicable to all subjects, if it were enabled, and confirmed that an audit record was not generated. The evaluator then enabled that rule and waited for the Agent to consume the updated configuration list. The evaluator then performed the same action on the endpoint and this time the rule was enforced by the Agent and an audit record was created. The evaluator then performed an action which would have trigged the rule applicable to a specific process subject, if it were enabled, and confirmed that an audit record was not generated. The evaluator then enabled that rule and waited for the Agent to consume the updated configuration list. The evaluator then performed the same action on the endpoint with the process whose process name was within the rule and with a process with a different process name. This time the rule was enforced by the Agent for the process whose process name matched the rule and an audit record was created for the enforcement but there was no enforcement nor audit record for the process whose process name did not match the rule. The evaluator determined based upon performing the 'some selectable audit events enabled' test that the selectable audit worked as described because audit records would only be generated for enabled rules and when the rule is enforced because the subject, object, operation, attribute combination was a match to the rule.
Test Results	Pass
Execution Method	Manual

Test Case Number	009P
SFR	FAU_STG_EXT.1 – TD0066 & TQ1196
Test Objective	The evaluator shall test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit

	storage contain identical data. The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one. If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.). Lastly, the described loss minimization mechanisms must be tested to ensure that they behave as documented.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	Per the Section 8.2.4 of Security Target, Section 8 of the AGD, and the results of the testing, the evaluator knows that different types of audit records are stored in the local log files and the SQL Server Database. Therefore, there is no scenario where audit reconciliation is possible between the audit logs (TOE-internal storage) and the SQL Server Database. As the App Control Server and Console rely on the SQL Server Database to function as well as to write audit records to, the test could not be performed as described. The evaluator received guidance from NIAP through Technical Query #1196 and the following test was performed to verify that no audit data is lost when the connection to the SQL Server Database is unavailable because no audit data could be generated by the App Control Server and no audit data could be received from Agents. The evaluator observed the last audit record recorded to the SQL Server Database through the Console and then shutdown the SQL Server Database. The evaluator then attempted to perform actions in the Console and confirmed its functionality was disabled. The evaluator then restarted the SQL Server Database, authenticated to the Console, verified no audit records were recorded to the SQL Server Database while it was shut down, and that auditing to the SQL Server Database has resumed. The evaluator also verified through conducting test case 025A that audit data which is sent between remote IT entities (i.e., Agents to App Control Server) are protected within TLS/HTTPS.
Test Results	Pass
Execution Method	Manual

4.3.2.3 Identification and Authentication

Test Case Number	011P
SFR	FIA_USB.1
Test Objective	The evaluator shall test this capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance. Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent

	with their externally-defined attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to policy information, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF that they do not have write access to policy information. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and used in order to determine what the user is able to do.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The configuration of the TSF to accept user information from Active Directory (i.e., external sources) was completed during the initial installation and configuration of the TOE. The evaluation team also created three Active Directory user groups and a user was created in each of these groups. The evaluator then created a User Role Mapping for the three Active Directory user groups being assigned one each to the default roles of Administrator, Power User, and Read Only. The evaluator then authenticated to the Console with the Active Directory user within the Active Directory user group assigned to each of these roles and verified the authentication was successful by gaining access to the Console's post authentication functions. The evaluator then verified that each authenticated Active Directory user was only able to access functions allowed by their respective role assignment to the Active Directory user group they are within. The evaluator then deleted the three User Role Mappings that were created. The evaluator determined that the user authorizations allowed to each Active Directory user were consistent with their externally-defined Active Directory user group attribute as well as the configuration of the TSF's access control policy based upon their role. The evaluator then created a User Role Mapping for the three Active Directory users' usernames being assigned one each to the default roles of Administrator, Power User, and Read Only. The evaluator then authenticated to the Console with the Active Directory users assigned to each role by username and verified the authentication was successful by gaining access to the Console's post authentication functions. The evaluator then verified that each authenticated Active Directory user was only able to access functions allowed by their respective role assignment to their Active Directory username. The evaluator determined that the user authorizations allowed to each Active Directory user were consistent with their externally-defined Active Directory username attribute as well as the configuration of the TSF's access control policy based upon their role.
Test Results	Pass
Execution Method	Manual

4.3.2.4 Security Management

Test Case Number	012P
SFR	FMT_MOF.1
Test Objective	The evaluator shall test this function by accessing the TSF using one or more appropriately privileged administrative accounts and determining that the management functions as described in the ST and operational guidance can be managed in a manner that is consistent with any instructions provided in the operational guidance. If the TSF can be configured by an authorized and

	compatible Secure Configuration Management product, the evaluator shall also configure such a product to manage the TSF and use this product to perform the defined management activities. In addition, any access restrictions to this behavior should be enforced in a manner that is consistent with the relevant documentation. The evaluator shall test this by attempting to perform a sampling of the available management functions using one or more unprivileged accounts to observe that the activities are rejected or unavailable
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	Throughout the course of performing all of the testing assurance activities specified by the SFRs defined within the Security Target, the evaluator managed the TOE via the Console interface with multiple administrative user accounts with roles assigned to a local TOE username, an Active Directory group name, and an Active Directory username. The evaluator also confirm that the testing was performed as described in the Security Target and AGD as directed per the testing assurance activities. The configuration of the TSF to accept user information from Active Directory (i.e., external sources) was completed during the initial installation and configuration of the TOE. The evaluation team also created three Active Directory user groups and a user was created in each of these groups. The evaluator then created a User Role Mapping for the three Active Directory user groups being assigned one each to the default roles of Administrator, Power User, and Read Only. The evaluator then authenticated to the Console with the Active Directory user within the Active Directory user group assigned to each of these roles and verified the authentication was successful by gaining access to the Console's post authentication functions. The evaluator then verified that each authenticated Active Directory user was only able to access functions allowed by their respective role assignment to the Active Directory user group they are within. The evaluator then deleted the three User Role Mappings that were created. The evaluator determined that the user authorizations allowed to each Active Directory user were consistent with their externally-defined Active Directory user group attribute as well as the configuration of the TSF's access control policy based upon their role. The evaluator then created a User Role Mapping for the three Active Directory users' usernames being assigned one each to the default roles of Administrator, Power User, and Read Only. The evaluator then authenticated to the Console with the Active Directory users assigned to each role by username and verified the authentication was successful by gaining access to the Console's post authentication functions. The evaluator then verified that each authenticated Active Directory user was only able to access functions allowed by their respective role assignment to their Active Directory username. The evaluator determined that the user authorizations allowed to each Active Directory user were consistent with their externally-defined Active Directory username attribute as well as the configuration of the TSF's access control policy based upon their role. Finally, the evaluator authenticated to the Console with an administrative user with the Power User role and verified that this administrative user could not modify user roles or change Active Directory settings. The evaluator then repeated this for an administrative user with the Read Only role. Through this the evaluator confirmed that an administrative user could not bypass the privileges defined through role assignment by attempting to elevate their own privileges through the TOE or through Active Directory. The TOE cannot be configured by an authorized and compatible Secure

	Configuration Management Product, and this portion of the testing assurance activity was not performed.
Test Results	Pass
Execution Method	Manual

Test Case Number	013P
SFR	FMT_MOF_EXT.1
Test Objective	The evaluator shall also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities: - Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior - Repository for audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository - Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP. - Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP. - Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied. Once this has been done, the evaluator shall reconfigure the TOE so that it is no longer authorized to manage the Access Control product. The evaluator shall then attempt to perform management functions using the TOE and observe that this is either disallowed or that the option is not even present
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the management of Agents (i.e., Access Control products) by the App Control Server and Console (i.e., together being the Policy Management product) for all of the tests performed. Through the Console, the evaluator modified the behavior of the functions of the TOE, verified the function was modified and performed other actions which confirmed that the TOE operated per the manner it was configured. The evaluator performed testing to modify the items below. **A portion of this assurance activity is satisfied with other test cases. For those portions, below is a mapping of the test cases that satisfy that portion.** **Audited Events**: This portion of the assurance activity is satisfied by Test Case 003A. **Repository for trusted audit storage**:

	The evaluator placed the TOE into configuration two, which is strictly a test configuration, before conducting this test. This was accomplished by setting up a second SQL database and configuring the TOE to use it as a second audit repository. Once configured, the evaluator logged into the Console, confirmed that log in event was sent to the second SQL database. The evaluator then disabled the TOE's configuration to use the second SQL database. The evaluator logged into the Console again and verified that this audit event was not written to the disconnected second SQL database. This audit record was still written to the SQL Server Database. **Access Control SFP**: This portion of the assurance activity is satisfied by Test Case 002P. **Policy being implemented by the TSF**: This portion of the assurance activity is satisfied by Test Case 002P. **Access Control SFP behavior to implement in the event of communications outage**: This portion of the test case is satisfied by Test Case 020A. The last portion of the assurance activity was satisfied by performing the following test with an Agent on a Linux endpoint system and an Agent on a Windows endpoint system. The evaluator created a rule, assigned the rule to the Agent's policy, and waited for the Agent to consume the updated configuration list with the rule. On the Agent's endpoint system, the evaluator performed an operation on an object that matched the rule. This was blocked by the Agent and an audit record for the block was created. On the Agent, the evaluator used the dascli utility to disconnect the Agent which would stop the Agent from polling and being managed by the App Control Server. The evaluator confirmed that the Agent recognized its disconnected status and after a few minutes confirmed that the App Control Server also recognized that the Agent was now disconnected. The evaluator then deleted the rule created earlier. The evaluator verified that the App Control Server was not able to manage the Agent by providing the Agent the latest configuration list. The evaluator further verified the Agent was not being managed by performing the same operation on the same object that matched the rule and confirming the Agent still enforced the rule. The evaluator determined that the App Control Server could no longer manage the Agent.
Test Results	Pass
Execution Method	Manual

Test Case Number	014P
SFR	FMT_MSA_EXT.5
Test Objective	The evaluator shall test this capability by defining policies that contain the contradictions indicated in the operational guidance and observing if the TSF responds by detecting the contradictions and reacting in the manner prescribed in the ST. If the TSF behaves in a manner that prevents contradictions from occurring, the evaluator shall review the operational guidance in order to determine if the mechanism for preventing contradictions is described and if this feature is communicated to administrators. This feature shall be tested in conjunction with a compatible Access Control product; in other words, if the TOE has a mechanism that prevents contradictions (for example, if a deny rule always supersedes an allow rule), then correct enforcement of such a policy by a compatible Access Control product is both a

	sufficient and a necessary condition for demonstrating the effectiveness of this mechanism.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator satisfied this assurance activity by creating rules through the Console which allow and block access to a directory and by doing so, assigned them to an Agent's policy for a Linux and Windows endpoint system. The evaluator ranked the allow access rule to be processed before the block access rule in the rule ranking which prevents a contradiction from occurring per Section 7.3.3.7 of the AGD. The evaluator waited for the Agents (i.e., Access Control products) to poll and process the latest configuration list of rules, and then verified that a client user was allowed to create a file in the specified directory on each of the respective endpoint systems. The evaluator then ranked the block access rule to be processed before the allow access rule in the rule ranking. The evaluator waited for the Agents (i.e., Access Control products) to poll and process the latest configuration list of rules, and then verified that a client user was blocked from creating a file in the specified directory on each of the respective endpoint systems.
Test Results	Pass
Execution Method	Manual

Test Case Number	015P
SFR	FMT_SMF.1
Test Objective	The evaluator shall test this capability by accessing the TOE and verifying that all of the defined management functions exist, that they can be performed in the prescribed manner, and that they and accomplish the documented capability.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	This test is satisfied with the testing of other test cases within this test plan. A mapping of each function has been provided in the table below this test case. This mapping provides the defined management functions listed in the Security Target and the test case that the functions are performed. Each function was performed in the prescribed manner as instructed in the AGD. The mapping is not an exhaustive list of all instances were these management functions were performed throughout the testing but a single instance of the management function being performed to verify that each function exists, that it can be performed in the prescribed manner, and that it accomplishes the documented capability. The evaluator has determined that based upon testing all other SFR assurance activities claimed that the management functions accomplished their capability.
Test Results	Pass
Execution Method	Manual

Management Activity	Test Case
Creation of policies	001P
Transmission of policies	002P
Definition of object attributes Association of attributes with objects	001P
Definition of subject attributes Association of attributes with subjects	003A
Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	005P Note that this is N/A to the TOE. No IT entities authenticate to the TOE.

Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	005P Note that this is N/A to the TOE. No IT entities authenticate to the TOE.
Configuration of auditable events	003A
Configuration of auditable events for defined external entities	003A
Configuration of external audit storage location	012A
Definition of default subject security attributes, modification of subject security attributes	011P
Configuration of the behavior of other ESM products	001P
Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)	014P
Management of the users that belong to a particular role	016P
Maintenance of the banner	022P

Test Case Number	016P
SFR	FMT_SMR.1
Test Objective	The evaluator shall test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles. If the TSF provides the capability to define additional roles, the evaluator shall create at least one new role and ensure that a user can be assigned to it. Since other assurance activities for management requirements involve the evaluator assuming different roles on the TOE, it is possible that these testing activities will be addressed in the course of performing these other assurance activities.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator satisfied this assurance activity by authenticating to the Console, creating administrative users, and assigning the administrative users to the different default roles of the TOE in the manner prescribed by the operational guidance (Sections 7.1.4 and 7.1.5 of the AGD). The evaluator authenticated to the TOE as each of the administrative users assigned to the different default roles and ensured that the role was in fact assigned to the administrative user. The evaluator then authenticated to the Console, created a custom role, and assigned it to an administrative user by creating a new administrative user. The evaluator authenticated to the TOE as the administrative user assigned to the custom role and ensured that the role was in fact assigned to the administrative user.
Test Results	Pass
Execution Method	Manual

4.3.2.5 Protection of the TSF

Test Case Number	017P
SFR	FPT_APW_EXT.1
Test Objective	The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator as an administrator of the underlying Windows operating system accessed the SQL Database Server with a database management utility and performed a query on the user table. The returned rows had a hash in the

	"password" column and a random value in the "salt" column for all users. The evaluator attempted to repeat these steps as a user that was not an administrator, and that user was not able to access the user information in the SQL Database Server. The evaluator as domain administrator accessed the Active Directory and extract the user information. The extracted information had a hash under each user's secrets. The evaluator attempted to repeat these steps as a user that was not the domain administrator, and that user was not able to access the user information in Active Directory.
Test Results	Pass
Execution Method	Manual

4.3.2.6 TOE Access

Test Case Number	019P
SFR	FTA_SSL.3
Test Objective	The evaluator shall test this capability by following the operational guidance to configure several different values for the inactivity time period referenced in the component; these shall consist at least of the minimum and maximum allowed values as specified in the operational guidance, as well as one other value. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator tested the inactivity values of 1, 3, and 120 minutes which included the minimum and maximum values as specified in the operational guidance (Section 7.1.3 of the AGD). After setting each inactivity value, the evaluator established a remote session to the Console, performed no additional actions via the Console, and observed the session terminated according to the inactivity value that was set. The evaluator also confirmed that an audit record was generated for the all three session termination events.
Test Results	Pass
Execution Method	Manual

Test Case Number	021P
SFR	FTA_SSL.4
Test Objective	The evaluator shall test this capability by establishing a session with the TOE using an administrative interface. The evaluator then follows the operational guidance to exit or log off of the session and observes that the session has been terminated. If applicable, the evaluator shall repeat this test for each administrative interface that is supported by the TOE.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator performed this test by establishing a remote session with the TOE by authenticating to the Console and then ended the session according to the steps described in the operational guidance (Section 7.1.2 of the AGD).
Test Results	Pass
Execution Method	Manual

Test Case Number	022P
SFR	FTA_TAB.1
Test Objective	If the banner is not displayed by default, the evaluator shall configure the TOE in accordance with the operational guidance in order to enable its display. The evaluator shall then attempt to access the TOE and verify that a TOE banner exists.

	If applicable, the evaluator will also attempt to use the functionality to modify the TOE access banner as per the standards defined in FMT_SMF.1 and verify that the TOE access banner is appropriately updated.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator performed this test by using the TOE in accordance with the operational guidance (Section 7.2 of the AGD) to create the login banner via the Console. The evaluator logged out and then accessed the login page to view the login banner that was originally set. The evaluator then authenticated to the Console and modified the banner as per the standards defined in FMT_SMF.1 (Section 7.2 of the AGD). The evaluator logged out and then accessed the login page to view the login banner that was originally updated. In each instance, the evaluator verified that the banner displayed and was updated appropriately.
Test Results	Pass
Execution Method	Manual

4.3.2.7 Trusted Paths/Channels

Test Case Number	023P
SFR	FTP_ITC.1 – TD0576
Test Objective	Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful. Further assurance activities are associated with the specific protocols. For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator tested the connection between the Agents and the App Control Server for this tested under test case 025A (which covers 026A and 027A testing assurance activities as well). The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connection between the App Control Server and Active Directory for all of the tests performed. The evaluator started a packet capture between the App Control Server and Active Directory. The evaluator then authenticated to the Console with a user defined in the Active Directory Server. The evaluator observed for the connection between the App Control Server and Active Directory, that it was initiated by the App Control Server and that the communication used TLS (channel data is not sent in plaintext). For these reasons, the evaluator determined Test 1, 2, and 3 for the ESM_PM_PP's iteration of FTP_ITC.1 have been satisfied.
Test Results	Pass
Execution Method	Manual

Test Case Number	024P
SFR	FTP_ITC.1 – TD0576
Test Objective	Test 2: For each protocol that the TOE can initiate as defined in the requirement,

	the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities. Further assurance activities are associated with the specific protocols. For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator tested the connection between the Agents and the App Control Server for this tested under test case 025A (which covers 026A and 027A testing assurance activities as well). The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connection between the App Control Server and Active Directory for all of the tests performed. The evaluator started a packet capture between the App Control Server and Active Directory. The evaluator then authenticated to the Console with a user defined in the Active Directory Server. The evaluator observed for the connection between the App Control Server and Active Directory, that it was initiated by the App Control Server and that the communication used TLS (channel data is not sent in plaintext). For these reasons, the evaluator determined Test 1, 2, and 3 for the ESM_PM_PP's iteration of FTP_ITC.1 have been satisfied.
Test Results	Pass
Execution Method	Manual

Test Case Number	025P
SFR	FTP_ITC.1 – TD0576
Test Objective	Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext. Further assurance activities are associated with the specific protocols. For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator tested the connection between the Agents and the App Control Server for this tested under test case 025A (which covers 026A and 027A testing assurance activities as well). The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connection between the App Control Server and Active Directory for all of the tests performed. The evaluator started a packet capture between the App Control Server and Active Directory. The evaluator then authenticated to the Console with a user defined in the Active Directory Server. The evaluator observed for the connection between the App Control Server and Active Directory, that it was initiated by the App Control Server and that the communication used TLS (channel data is not sent in plaintext). For these reasons, the evaluator determined Test 1, 2, and 3 for the ESM_PM_PP's iteration of FTP_ITC.1 have been satisfied.

Test Results	Pass
Execution Method	Manual

Test Case Number	026P
SFR	FTP_ITC.1 – TD0576
Test Objective	Test 4: The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected. Further assurance activities are associated with the specific protocols. For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator tested the connection between the Agents and the App Control Server for this tested under test case 028A. The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connection between the App Control Server and Active Directory for all of the tests performed. The evaluator physically interrupted the connection between the App Control Server and Active Directory by removing the ethernet cable to the Active Directory's machine. The evaluator then attempted to authenticate to the Console with a user defined in the Active Directory Server which failed due to being unable to verify the credentials against Active Directory. The evaluator reconnected the ethernet cable to the Active Directory's machine. The evaluator started a packet capture between the App Control Server and Active Directory. The evaluator then authenticated to the Console with a user defined in the Active Directory Server. The evaluator observed the connection was between the App Control Server and Active Directory, that it was initiated by the App Control Server and that the communication used TLS. For these reasons, the evaluator determined Test 4 for the ESM_PM_PP's iteration of FTP_ITC.1 have been satisfied.
Test Results	Pass
Execution Method	Manual

Test Case Number	027P
SFR	FTP_TRP.1 – TD0576
Test Objective	The evaluator shall perform the following set of tests and where applicable, repeat for each remote administration method: Test 1: The evaluator shall ensure that communications using each protocol with each authorized IT entity, including each remote administration method, is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful. For distributed TOEs, regardless of the tests performed, the evaluator shall perform tests on all TOE components according to the mapping of trusted paths to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connection between the Console and a remote

	administrative user via a web browser. The evaluator started a packet capture between the App Control Server and the web browser. The evaluator then accessed the login page and authenticated to the Console. The evaluator observed for the connection between the App Control Server and the web browser that it was initiated by the web browser and that the communication used TLS/HTTPS (channel data is not sent in plaintext). The evaluator confirmed that an audit record was created for 'all attempted uses of the trusted path functions'. For these reasons, the evaluator determined Test 1 and 3 for FTP_TRP.1 have been satisfied.
Test Results	Pass
Execution Method	Manual

Test Case Number	028P
SFR	FTP_TRP.1 – TD0576
Test Objective	The evaluator shall perform the following set of tests and where applicable, repeat for each remote administration method: Test 2: For communications using each protocol with each authorized IT entity and method of remote administration supported, the evaluator shall follow the guidance documentation to ensure that there is no available interface that can be used by a remote user to establish a remote administrative session without invoking the trusted path. For distributed TOEs, regardless of the tests performed, the evaluator shall perform tests on all TOE components according to the mapping of trusted paths to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator performed this test by conducting a remote port scan on the machine running the Console and App Control Server, which revealed that the only TOE user interface was the Console (open port TCP/443). All other open ports were TOE interfaces but non-user interfaces and/or non-TOE interfaces. The evaluator confirmed that the TOE was unable to be remote administered without invoking the trusted path via the Console on TCP port 443 using HTTPS/TLS by attempting to access the Console with only HTTP which failed. The evaluation team determined that the Console was the only user interface and that access to it required the use of HTTPS/TLS.
Test Results	Pass
Execution Method	Manual

Test Case Number	029P
SFR	FTP_TRP.1 – TD0576
Test Objective	The evaluator shall perform the following set of tests and where applicable, repeat for each remote administration method: Test 3: The evaluator shall ensure that for communications of each protocol with each authorized IT entity, and for each method of remote administration, the channel data is not sent in plaintext. For distributed TOEs, regardless of the tests performed, the evaluator shall perform tests on all TOE components according to the mapping of trusted paths to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of

	the AGD which configured the connection between the Console and a remote administrative user via a web browser. The evaluator started a packet capture between the App Control Server and the web browser. The evaluator then accessed the login page and authenticated to the Console. The evaluator observed for the connection between the App Control Server and the web browser that it was initiated by the web browser and that the communication used TLS/HTTPS (channel data is not sent in plaintext). The evaluator confirmed that an audit record was created for 'all attempted uses of the trusted path functions'. For these reasons, the evaluator determined Test 1 and 3 for FTP_TRP.1 have been satisfied.
Test Results	Pass
Execution Method	Manual

Test Case Number	030P
SFR	FTP_TRP.1 – TD0576
Test Objective	The evaluator shall perform the following set of tests and where applicable, repeat for each remote administration method: Test 4: The evaluators shall ensure that, for each protocol and remote administration method combination tested during Test 1, the connection is physically interrupted. The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected. For distributed TOEs, regardless of the tests performed, the evaluator shall perform tests on all TOE components according to the mapping of trusted paths to TOE components in the Security Target.
Test Instructions	Execute this test per the test steps.
Test Steps and Rationale	The evaluator installed and configured the TOE per the procedures in Section 6 of the AGD which configured the connection between the Console and a remote administrative user via a web browser. The evaluator started a packet capture between the App Control Server and the web browser. The evaluator then accessed the login page. The evaluator physically interrupted the connection between the App Control Server and the web browser by removing the ethernet cable to the App Control Server's machine. The evaluator waited until the connection had RST messages occurring and then reconnected the ethernet cable to the App Control Server. The evaluated then authenticated to the Console and confirmed that an audit record was created for 'all attempted uses of the trusted path functions'. The evaluator reviewed the communications in the packet capture confirming that no plaintext data was transmitted and that the communications were appropriately protected with TLS.
Test Results	Pass
Execution Method	Manual

5 Evaluation Activities for SARs

This section addresses assurance activities that are defined in the *Protection Profile for Enterprise Security Management Access Control version 2.1* [ESM_AC_PP] and *Protection Profile for Enterprise Security Management Policy Management version 2.1* [ESM_PM_PP] that correspond with Security Assurance Requirements.

ADV_FSP.1 – *"There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described for each SFR, and*

for other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided. For example, if the TOE provides the capability to configure the key length for the encryption algorithm but fails to specify an interface to perform this function, then the assurance activity associated with FMT_SMF would fail.

The evaluator shall verify that the TOE functional specification describes the set of interfaces the TOE intercepts or works with. The evaluator shall examine the description of these interfaces and verify that they include a satisfactory description of their invocation."

Section 2 of the Security Target describes the purpose and method of use for each security relevant TSFI by enumerating all security relevant interfaces:

- E1: Remote administration to the App Control Console using TLS/HTTPS provided by OS. The console is an IIS application. Administrative users can access the Console remotely using TLS/HTTPS via E1 and authenticate to the TOE with locally defined users and/or AD users.

- E2: Local client interface. Each endpoint has methods for client users to access the underlying endpoint operating system which is depicted as the E2 interface in Figure 1. The E2 interface does not interact with the TOE directly but instead the TOE will make access control decisions based upon the Agent's policy when client users attempt to perform operations on objects located on the endpoint over this interface.

- E3: TLS connection to the Active Directory. The E3 connection is established over TLS between the TOE's operating system and the AD's operating system.

- E4: TLS/HTTPS between Agent and Server. One or more App Control Agents (Agents) initiate communication via E4 with the Server using TOE's operating systems' TLS/HTTPS to receive updated configuration lists from the Server, send information about new objects to the Server, and send/receive other information needed to perform its host-based access control functionality on endpoint systems.

The evaluation team found that each TSFI's method of use has been given. For these reasons, the evaluation team considers this activity satisfied.

AGD_OPE.1 – *"Some of the contents of the operational guidance will be verified by the assurance activities with each SFR. The following additional information is also required.*

The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE."

Section 5.4 of the AGD states The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
Section 6.1.2 of the AGD specifically states for the Server: **NOTE:** Use of cryptographic engines provided by other underlying operating systems were not evaluated nor tested during the Common Criteria evaluation of the TOE.
Section 6.2.2 of the AGD specifically states for the Agents: **NOTE:** Use of cryptographic engines provided by other underlying operating systems were not evaluated nor tested during the Common Criteria evaluation of the TOE.

AGD_PRE.1 – *"As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately*

addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST."

Section 5.4 of the AGD contains instructions for the Security Administrator to ensure that the operational environment will fulfil its role in supporting the TOE. These instructions match the assumptions for the TOE's operational environment in Section 4.3 of the ST.

For the operational environment requirements for the Server:

Section 6.1.1 of the AGD addresses the joining of the App Control server to the Active Directory Domain and the installation and configuration of the required SQL Server Database.

Section 6.1.2 of the AGD addresses the required Microsoft Internet Information Services (IIS) configuration and Windows Defender Firewall Rules. Additionally, the AGD declares that 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 Microsoft Windows 10 and Windows Server 2019 (version 1809) GP OS Operational and Administrative Guidance.

Section 6.1.5 addresses the of the App Control Server configuration for enabling the integration of the Active Directory.

For the operational environment requirement of the host OS for the Agent:

Section 6.2.2 of the AGD addresses the underlying OS: The underlying operating systems must be configured in a manner consistent with their Common Criteria evaluations by referencing the configuration procedures described in Microsoft Windows 10 and Windows Server (version 1903) GP OS Operational and Administrative Guidance and the Red Hat Enterprise Linux 7.6 CC Guidance Version 1.4, dated June 19, 2020 respectively.

ALC_CMC.1 – *"The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product."*

The evaluation team verified that the Security Target (ST), TOE, Vendor documentation, and Supplemental Administrative Guidance (AGD) were labeled consistently to correctly identify the documentation and software versions in the CC evaluation.

The AA for this SFR requires the evaluator (1) to check the ST to ensure it contains an identifier that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall (2) check the AGD and TOE samples received for testing to ensure that the version number is consistent with that in the ST. For (1) the ST meets the AA in section 1.2 called TOE Reference where it is stated the TOE is VMware Carbon Black App Control. This is consistent with the vendor's marketing materials for the product and how the product identifies itself, both during installation and once installed. For (2), the AGD in sections 1 and 2 clearly identifies VMware Carbon Black App Control version 8.8.2 as the TOE.

ALC_CMS.1 – *"The 'evaluation evidence required by the SARs' in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component."*

The evaluation team verified that the Security Target (ST), TOE, Vendor documentation, and Supplemental Administrative Guidance (AGD) were labeled consistently to correctly identify the documentation and software versions in the CC evaluation.

The evaluation team found the VMware Carbon Black User Guides clearly indicate the software version (8.8) on the first page. The vendor releases user documentation to the major.minor level versioning detail.

- Server Installation Guide VMware Carbon Black App Control 8.8, dated 8 December 2021
- Operating Environment Requirements VMware Carbon Black App Control 8.8, dated 8 December 2021
- SQL Server Configuration Guide VMware Carbon Black App Control 8.8, dated 8 December 2021
- VMware Carbon Black App Control User Guide Product Version 8.8, Document Version 1.0, dated 6 December 2021

The TOE reference and evidence created for the evaluation, reference the TOE to the third digit 8.8.2:

- VMware Carbon Black App Control v 8.8.2 Supplemental Administrative Guidance, Document Version 1.0, dated February 27, 2022
- VMware Carbon Black App Control v8.8.2 Security Target, Version 1.0, February 27, 2022

The TOE Server software is labeled as 8.8.2 (Main versioning for the product)

- The TOE component Windows Agent is labeled as 8.7.2
- The TOE component Linux Agent is labeled as 8.7.6

The documentation and the TOE software package are labeled in a manner that makes it clear that the end user needs to purchase version 8.8.2 to have the certified version.

ATE_IND.1 – *"The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators shall document in the test plan that each applicable testing requirement in the ST is covered.*

The Test Plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification shall address the differences between the tested platform and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale shall be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH).

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (that could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that

resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a 'fail' and 'pass' result (and the supporting details), and not just the 'pass' result."

The evaluation team has produced a Test Plan and a Test Report, which define the subset for testing that covered all test assurance activities from ESM_AC_PP and ESM_PM_PP for the SFRs claimed. This subset is a combination of vendor developed functional tests and independently devised functional tests. Note that although the vendor provided functional tests, all tests were executed by the lab evaluators. These tests are sufficiently detailed for the tests to be reproducible because they contain:

- Test purpose
- Ordering dependencies, if applicable
- Test setup
- Step-by-step procedures
- Expected results (Pass/Fail Criteria)
- Clean up activities

There was no sampling of testing, as all required test assurance activities were preformed against the TOE for the VMware Carbon Black App Control that was claimed in the Security Target. The evaluation team configured the TOE for testing according to the *VMware Carbon Black App Control Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The test plan incorporates a detailed chart that lists all required elements to identify the composition of a device that has been provided in Section 4.1.1 of this document.

The Results are recorded in a proprietary Test Matrix in which columns indicate Verdict, Date, and list of supplied evidence such as screenshots, audit records, and network captures. This information is sufficient to provide assurance that the external interfaces and the TOE performs all functions as defined by the ESM_PM_PP and the ESM_AC_PP assurance activities.

AVA_VAN.1 – *"As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in this category of ESM application in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated."*

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the ESM_AC_PP and ESM_PM_PP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

<u>General Terms</u>
Carbon Black
Carbon Black App Control (8.8)
VMware App Control (8.8)
Host Based Access Control

<u>Server/Console Libraries</u>
ASP.NET AJAX ASP.NET AJAX (2020.2.617.45 Telerik) BOOST (1.74)

jQuery (3.5.1)
jQuery_ui (1.13.0)
nghttp2 (1.43)
PHP (7.4.27)
PEAR (1.10.12)
SimpleSAML.php (1.18.7)
Yara (4.1.1)
Zlib (1.2.11)

Agent Library
BOOST (1.69 Linux, 1.59 Windows)
wxWidget (3.1.3 Linux, 3.0.2 Windows)
Minizip (1.1-5 Linux)
Zlib (1.2.11 Windows)
7-zip (19.0 Windows)
SQLite (3.35 Linux, 3.30.1 Windows)

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources (updated: February 7, 2022). The following public vulnerability sources were searched:

a) NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
b) Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/
https://www.cvedetails.com/vulnerability-search.php
c) US-CERT: http://www.kb.cert.org/vuls/html/search
g) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
h) Offensive Security Exploit Database: https://www.exploit-db.com/
i) Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

Upon the completion of the vulnerability analysis research, the team had identified generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Port Scanning

Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration.

- Virus scan (ClamAV)

The test is to ensure that there is no malicious code included in the software for any of the TOE components.

- Web Interface Vulnerability Identification (Burp Suite Pro)

The test is to identify possibly vulnerabilities by scanning the web application with the desired tool that is specifically designed to identify OWASP vulnerabilities. The results provide an exploitability factor (easy, average, and difficult). Further testing is dependent on findings.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

6 Conclusions

The TOE was evaluated against the ST and has been found by this evaluation team to be conformant with the ST. The overall verdict for this evaluation is: Pass.

7 Glossary of Terms

Acronym	Definition
AC	Access Control
AD	Active Directory
CC	Common Criteria
CL	Configuration List
CLI	Command-Line Interface
ESM	Enterprise Security Management
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IIS	Internet Information Services (Microsoft)
NIAP	National Information Assurance Partnership
OS	Operating System
PM	Policy Management
PP	Protection Profile
RBG	Random Bit Generator
SCM	Service Control Manager
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

Table 7-1: Acronyms

Term	Definition
Admin	An administrative user who is assigned the 'Administrator' role on the TOE and has the ability to manage the TSF. An Admin using the Console is considered a TOE administrative user.
Administrative User	Administrative users access the TOE via the Console and are authorized to manage the TOE and its data. The TOE defines the out of the box administrative roles called Read-Only, Power User, and Admin but the TOE also allows the ability to create custom roles.
Client User	An endpoint system user that is considered to be the subject to which the access control policies are applied. Client users are not considered TOE users.
Configuration list	A hierarchal bundle of rules which is consumed by an Agent for making access control decisions.
Policy	The Agent's configuration for making access control decisions.

Table 7-2: Customer Specific Terminology

Term	Definition
Access Control product	The TOE component related to the Security Functional Requirements defined in the Standard Protection Profile for Enterprise Security Management-Access Control, version 2.1. In terms of the TOE, this is the Agent component.
Policy	The set of access control decisions which govern how the TOE will respond to an

	access request. In terms of the TOE, an Agent's policy and configuration list together determine the access control decisions for the TOE on that Agent's endpoint system.
Policy Management product	The TOE component related to the Security Functional Requirements defined in the Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1. In terms of the TOE, this is the Server and Console components.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an administrative user uses to manage it (web browser, terminal client, etc.).
User or TOE user	In a CC context, any individual who has the ability to access the TOE functions or data.

Table 7-3: CC Specific Terminology