VMware Carbon Black App Control v8.8.2

Security Target

ST Version: 1.0
February 27, 2022

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West St
Laurel, MD 20707

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation.

1.1.1 ST Identification

ST Title: VMware Carbon Black App Control v8.8.2 Security Target
ST Version: 1.0
ST Publication Date: February 27, 2022
ST Author: Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this document provides identifying information for the ST and TOE as well as a brief description of the TOE and its associated TOE type.

Chapter 2 describes the TOE in terms of its physical boundary, logical boundary, exclusions, and dependent Operational Environment components.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the threats, assumptions, objectives, and organizational security policies that apply to the TOE.

Chapter 5 defines extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 6 describes the SFRs that are to be implemented by the TSF.

Chapter 7 describes the SARs that will be used to evaluate the TOE.

Chapter 8 provides the TOE Summary Specification, which describes how the SFRs that are defined for the TOE are implemented by the TSF.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1 and 2. These tables are to be used by the reader as a quick reference guide for terminology definitions.

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 1-1: 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 1-2: CC Specific Terminology

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 3. This table is to be used by the reader as a quick reference guide for acronym definitions.

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 1-3: Acronym Definition

1.1.5 References

[1] or [AC] Standard Protection Profile for Enterprise Security Management Access Control, version 2.1 (AC PP)
[2] or [PM] Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1 (PM PP)
[3] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4
[4] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4
[5] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4
[6] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4

1.2 TOE Reference

The TOE is VMware Carbon Black App Control version 8.8.2.

1.3 TOE Overview

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

1.4 TOE Type

App Control is an Enterprise System Management product, specifically access control (AC) and policy management (PM). The TOE is considered to be an enterprise-level product because it can be used to control user access on multiple host systems using centrally defined attributes. The TOE provides host-

based access control by determining what a subject can do on a particular system. The intent of host-based access control is to prevent a subject from performing damaging, or otherwise inappropriate, acts against a host system such as running unauthorized software or modifying its configuration. The TOE also provides policy management through an administrative interface which is used to configure and manage the security policies which are deployed to TOE Agents on host systems for enforcement.

2 TOE Description

App Control is an ESM application that is used to define and enforce access control policies for enforcement on endpoint systems within the enterprise. Access control policies are consumed and enforced by App Control Agent components which are installed on each endpoint system. From the App Control Console interface, an administrative user creates policies and the App Control Server component will then generate a custom App Control Agent installer for each policy. The administrative user will then download the installer file from the web interface on the App Control Server and install it manually on the endpoint systems that will be assigned that policy.

Once installed on an endpoint system, the App Control Agent is able to enforce the rules defined within its access control policy against client users attempting to perform operations on files and processes on the endpoint system. The TOE operates on the principle of whitelisting; in other words, it allows an organization to specify the specific types of files and processes that can be used by a given subject (e.g. client user) on a given endpoint system and block execution of anything else within the purview of its rules.

Policies are written to apply to individual endpoint systems or groups of endpoint systems. Rules can be defined in real-time and can be associated with one or more policies. Whenever a rule is changed, a new bundle of rules (known as a configuration list or CL) is transmitted to the App Control Agents on all endpoint systems. An App Control Agent will immediately enforce any rules it consumes from the CL that matches its policy. By default, the App Control Agents will automatically enforce a set of self-protection rules to prevent an untrusted user from tampering with the TOE's software to block, terminate, modify, or prevent startup (on reboot) of its execution.

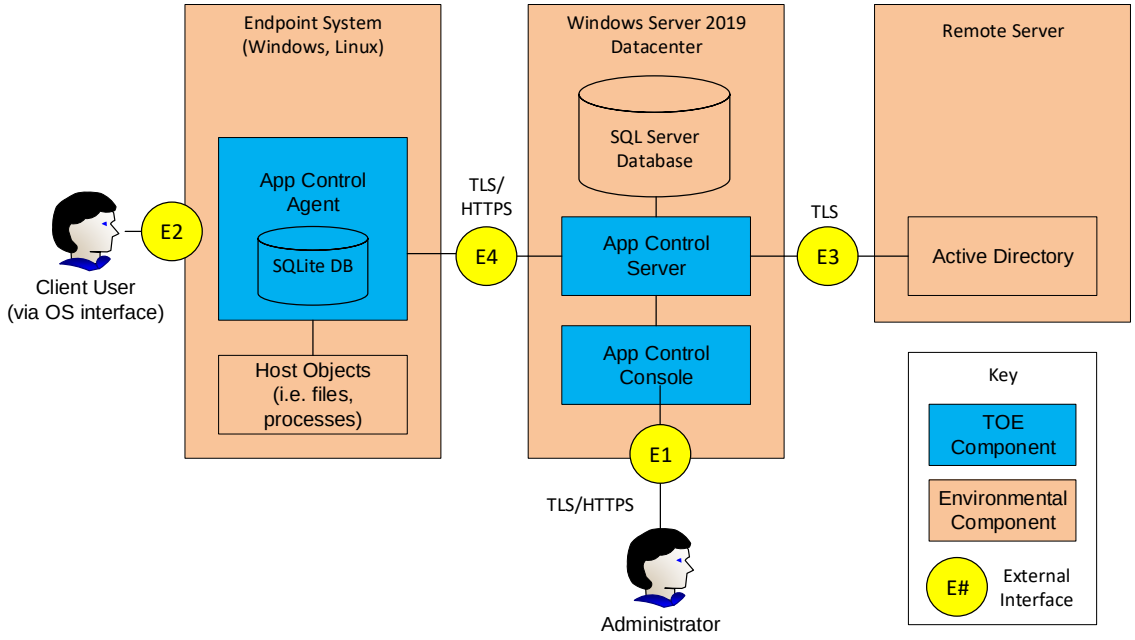

Figure 1: TOE Boundary for App Control

The App Control Console (Console) is an Internet Information Services (IIS) application that is an administrative interface to the App Control Server (Server). 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. When authenticating a TOE administrative user defined in AD, the E3 connection is established over TLS between the TOE's operating system and the AD's operating system. Administrative users can be assigned different levels of privilege to perform management functionality, and can also be limited such that they only have the ability to write rules that are associated with specific policies.

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. 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. Client users are authenticated by the underlying endpoint operating system communicating with the enterprise AD.

In the evaluated configuration, Agents will operate on Windows and Linux platforms, and the Server and Console will run on a Windows platform. All TOE components (Server, Console and the Windows and Linux Agents), depend on their host platform for all cryptographic functionality used to secure remote communication.

2.1 Evaluated Components of the TOE

The following table describes the TOE components in the evaluated configuration:

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

Table 2-1: Evaluated Components of the TOE

2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the TOE's operational environment that must be present for the TOE to be operating in its evaluated configuration:

Component	Definition
Active Directory (AD)	This is an enterprise authentication server. In the evaluated configuration, TOE administrative users can be authenticated against an AD user account. AD is also used for client user identity data on endpoint systems. For endpoint systems running Linux a LDAP client, which is part of the operational environment, is used to map local system account information to network accounts defined in AD (since it is not natively supported on the Linux platforms) o Examples of this include realmd or SSSD. o The TOE's Agent has no awareness of how the user is authenticated by the environment, it just knows the user's claimed identity on the system (e.g., username, UID)
Endpoint System(s)	Any general-purpose computer that has the TOE Agent software installed and that supports TLS/HTTPS communications. Supported operating systems for the evaluation include Windows and Linux. These operating systems provide all cryptography for the TOE Agents to communicate with the TOE's App Control Server. Users of the endpoint systems are considered 'client users'. 'Client users' are users that are considered the subjects to which the access control policies are applied and are not considered TOE users. Refer to Section 2.4.1 for these machines' specifications.
Management Workstation	Any general-purpose computer that is used by an administrative user to remotely manage the TOE via the Console. The management workstation requires a web browser which supports HTTPS (Google Chrome 36 or higher supported, recommend latest version) to access the Console.
SQL Server Database	The TOE requires a pre-installed instance of Microsoft SQL Server (2012 or higher supported, recommend latest version) on the same machine where App Control Server is installed. Microsoft SQL Server must be configured to use AES-256 encryption method. All TOE configuration data, audit data, and local user data is stored in the database.
Windows Server	A Windows Server that has the TOE App Control Server and App Control Console software installed. The SQL Server Database is also installed on this machine. The Windows Server supports TLS/HTTPS communications. The Windows operating system installed on this machine provides all cryptography required by the TOE's App Control Server and App Control Console components. Refer to Section 2.4.1 for this machine's specifications.

Table 2-2: Components of the Operational Environment

2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with the TOE but are not included in the evaluated configuration. They provide no added security related functionality for the evaluated product. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.3.1 Not Installed

There are no optional components that are omitted from the installation process.

2.3.2 Installed but Requires a Separate License

There are no excluded components that are installed and require a separate license.

2.3.3 Excluded from the Evaluated Configuration

The following are considered to be out of the scope of this evaluation.

- Server database encryption – The key used to encrypt the SQL Server database is protected by the OS; App Control has no role in this.
- Firewall/IIS configuration – The console/server is installed on Microsoft IIS, which is assumed to be hardened in an appropriate manner for the customer's environment. Similar, Windows Defender or another firewall can be assumed to be in place to limit network exposure of the server. The TOE cannot exert any control over the configuration of the underlying server.
- SAML - Support for SAML to facilitate single sign-on from another application in the organization's environment.
- REST API - This is an alternate method of remote management using a custom build management program. This evaluation did not evaluate the REST API or a custom build management console.
- Timed override to endpoint – The Console can be used to generate a one-time token that can be used to locally administer an endpoint for set period of time, known as timed override. This is provided for cases where an endpoint system must have new policy rules applied to it but it is currently deployed in a situation where a persistent connection to the server is not feasible (e.g., submarine or other location with sharply constrained bandwidth).
- App Control Connector – Allows the integration of the App Control Server with one or more network security devices or services. Integration with other network security devices or services is not included in the evaluation boundary.
- Unified Management – Centralized management of multiple App Control Servers. Multiple App Control Servers and centralized management are not included in the evaluation boundary.
- MacOS Agent – Agents can be installed on MacOS endpoints; however, this was not included in the evaluation boundary.
- Two-tier Deployment Architecture – The App Control Server and SQL Server Database could be installed on separate machines in the Two-tier Deployment Architecture. This was not part of the evaluation boundary. The evaluation boundary only includes both the App Control Server and SQL Server Database on the same machine.
- Visibility and Disabled Modes – Policies have different Modes of operation that can be configured. To enforce the functionality described by the ST, all policies must be in Control Mode. Visibility Mode and Disabled Mode are not included within the evaluation.
- Rule Types – The product has multiple types of rules that can be generated by administrative users. The only rules covered by this evaluation are Custom Software Rules, Memory Rules, Registry Rules, and Rapid Configs. Rules of any other name are not included within the evaluation.
- The broad set of vendor documentation covers a large number of product features. However, only those features and capabilities discussed in the specific sections of the 'VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0' document was evaluated as part of this evaluation. Product functionality discussed within the broader vendor documents and not directly referenced by the 'VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0' document was not evaluated as part of this evaluation.

2.4 Physical Boundary

2.4.1 Hardware

The TOE does not include the hardware or operating systems of the machines on which it is installed. The following table lists the hardware and operating systems of the machines used for the evaluation. The administrative users are advised to update the TOE component's underlying operating systems to the latest patched versions provided by the operating systems' vendors.

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

Table 2-3: Evaluated Component's Host System Configurations

2.4.2 Software

The TOE consists of the following software components:

- The App Control Server and App Control Console are software version 8.8.2.
- The App Control Agent for Windows operating systems is software version 8.7.2.
    - Uses a database built off of SQLite version 3.30.1.
- The App Control Agent for Linux operating systems is software version 8.7.6.
    - Uses a database built off of SQLite version 3.35.

The Agent software is not purchased separately. The Agent software is uploaded to the App Control Server which will then generate a custom App Control Agent installer for each policy.

2.5 Logical Boundary

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Enterprise Security Management
- Security Audit
- Communications
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access
- Trusted Path/Channels

2.5.1 Enterprise Security Management

The TOE provides the ability to define access control policies for consumption by Agents for enforcement. The TOE maintains security attributes that belong to an individual object as well as individual subjects. Through the TOE's Console interface, administrative users create policies and configuration lists of rules which define whether or not a subject is allowed or denied the ability to perform an operation on an object based upon the attributes defined within the rule applied to the authorization request. The Server is responsible for deploying the new policies and configuration lists to the Agents for enforcement. The Agents will immediately enforce any new policies and configuration lists it receives.

The Agents rely on their underlying operating system and its communication with an Active Directory for the identification of client user subjects and the operating system for the identification of process subjects. The Console requires identification and authentication of the TOE's administrative user which is accomplished via a local username/password mechanism or the AD server.

2.5.2 Security Audit

The Agent generates records of auditable events and either transmits the audit events to the Server over TLS provided by the TOE's underlying operating systems or stores the audit events in local audit logs. The Server generates audit records and stores them in local audit logs or an SQL Server Database that resides on the Server's host platform. Additionally, the Server will store all audit events received from the Agent in the SQL Server Database. The ability to select the set of events to be audited can be configured by administrative users defining rules that require or do not require audit events to be generated. Generated audit data is stored in a manner that prevents unauthorized modification or deletion.

2.5.3 Communications

The TOE provides a mechanism that requires the Agent to send a proof of receipt to the Server upon receiving a policy or configuration list. This receipt contains information that relates to the hostname of the Agent's endpoint server and the policy name or configuration list version that was received. This feedback is then verified by the Server.

2.5.4 User Data Protection

The Agent enforces the access control policy received from the Server and the rules applicable to its policy from the configuration lists received from the Server. The TOE's access control Security Function Policy (SFP) defines whether or not a subject is allowed or denied the ability to perform an operation on an object based upon the attributes defined within the rule applied against the authorization request. Each Agent will process rules assigned to their policy in a hierarchical manner, ensuring the lowest numbered rule (i.e. highest ranked hierarchically) is always enforced. By default, the TOE also enforces a self-protection SFP on its Agent's binaries and configuration data.

2.5.5 Identification and Authentication

The TOE requires each administrative user to be successfully identified before allowing any TSF-mediated actions on behalf of that subject. The TOE binds administrative users to their assigned role for restrictive security management enforcement.

2.5.6 Security Management

The TOE's Server maintains the administrative user roles: Read-Only, Power User, Admin, and custom role. Each of these roles has varying levels of privileges which determine what management functions the administrative users are able to perform via the TOE's Console interface which is a web based GUI. Administrative users are able to manage the TOE's own security functions, administrative users, audit events, and the Access Control SFP to include modifying its default configuration.

The TOE has only a single role when the Server is managing one of its Agents called administrator. The Server assumes this role every time an Agent polls the Server and during this connection the Server will send policy and configuration list updates.

2.5.7 Protection of the TSF

The TOE preserves a secure state when an Agent is terminated by immediately restarting the Agent. Agents will maintain policy enforcement by enforcing the last policy received when it is unable to communicate with the Server and can be configured to enforce a different Enforcement Level when this occurs. The Agent relies on its operating system's implementation of TLS to discard traffic in case a replay is detected. The client users' and administrative users' credentials which are needed for TOE operation are stored hashed and encrypted. The TOE also prevents the reading of symmetric keys.

2.5.8 Resource Utilization

In the event of a communication outage between the TOE's Agent and Server, the Agent will enforce the last known policy and configuration list it consumed. Once communications are restored, the Agent will immediately query the Server for the most up-to-date policy and configuration list data, and immediately enforce them.

2.5.9 TOE Access

The TOE displays a customizable warning banner on the Console login page. The TOE will terminate inactive sessions to the Console after an administratively configured amount of time and allows administrative users to terminate their own Console sessions. The TOE also allows the creation of rules which will allow or deny client users the ability to login to endpoint systems.

2.5.10 Trusted Path/Channels

The TOE's evaluated configuration enforces secure communication using TLS and HTTPS from the Agent to the Server, the Server to Active Directory, and administrative users via web browser to Console. The TLS and HTTPS protocols are implemented by the underlying TOE components' operating systems.

3 Conformance Claims

3.1 CC Version

This ST is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 September 2012.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended to include all applicable NIAP and International interpretations through February 27, 2022.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) are conformant to Part 3 to include all applicable NIAP and International interpretations through February 27, 2022.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profiles:

- Standard Protection Profile for Enterprise Security Management-Access Control, version 2.1 (AC PP)
- Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1 (PM PP)

3.5 Package Claims

The TOE claims exact compliance to the *Standard Protection Profile for Enterprise Security Management-Access Control, version 2.1* and the *Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1*.

The TOE claims the following Host-Based Access Control SFRs in the appendices of the AC PP:

- FDP_ACC.1(1)
- FDP_ACC.1(2)
- FDP_ACF.1(1)
- FDP_ACF.1(2)

The TOE claims following optional SFRs that are defined in the appendices of the AC PP:

- FPT_FLS.1
- FTA_TSE.1

The TOE claims following optional SFRs that are defined in the appendices of the PM PP:

- ESM_ATD.1
- ESM_ATD.2
- FTA_SSL.3
- FTA_SSL.4

This does not violate the notion of exact conformance because the PP specifically indicates these as allowable options and provides both the ST author and evaluation laboratory with instructions on how these claims are to be documented and evaluated."

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are in exact conformance with the ESM PM PP and ESM AC PP

3.7 Technical Decisions

The following is the list of NIAP Technical Decisions that are applicable to the ST/TOE and a summary of their impact:

		Changes			Analysis to this evaluation	
TD #	Title	SFR	AA	Notes	NA	Reason
TD0621	Corrections to FCS_TLS_EXT.1 in ESM PPs	X	X	X	X	NA – OE provides all cryptography TD0575 is archived per TD
TD0576	FTP_ITC and FTP_TRP Updated	X	X	X		SFRs claimed as specified
TD0574	Update to FCS_SSH in ESM PPs	X	X	X	X	NA – SSH not claimed by TOE or OE
TD0573	Update to FCS_COP and FCS_CKM in ESM PPs	X	X	X	X	NA – OE provides all cryptography
TD0079	RBG Cryptographic Transitions per NIST SP 800-131A Revision 1	X	X	X	X	NA – OE provides all cryptography
TD0066	Clarification of FAU_STG_EXT.1 Requirement in ESM PPs		X			TSS wording requirement.
TD0055	Move FTA_TAB.1 to Selection-Based Requirement			X		FTA_TAB.1 is claimed as specified
TD0042	Removal of Low-level Crypto Failure Audit from PPs				X	NA – OE provides all cryptography

Table 3-1: Technical Decisions

3.8 Conformance Claim Rationale

The AC PP states the following: "The purpose of an Access Control product is to enforce access control policies." The PM PP states the following: "A TOE that conforms to this PP may be able to define policies that control access to any of a wide variety of resources." The TOE provides the ability to define and enforce access control policies.

The SFRs that were chosen from these PPs include all required SFRs as well as optional SFRs defined as such by the PPs. Therefore, the conformance claim of exact conformance is appropriate.

4 Security Problem Definition

4.1 Threats

This section identifies the threats against the TOE. These threats have been taken from the ESM PM PP and ESM AC PP.

Threat	Threat Definition
T.ADMIN_ERROR [PM]	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.CONDTRADICT [PM]	A careless administrator may create a policy that contains contradictory rules for access control enforcement.
T.DISABLE [AC]	A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data.
T.EAVES [AC, PM]	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FALSIFY [AC]	A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
T.FORGE [AC]	A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.
T.FORGE [PM]	A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
T.MASK [AC, PM]	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.NOROUTE [AC]	A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.
T.OFLOWS [AC]	A malicious user may attempt to provide incorrect policy data to the TOE in order to alter its access control policy enforcement behavior.
T.UNAUTH [AC]	A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.
T.UNAUTH [PM]	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
T.WEAKIA [PM]	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
T.WEAKPOL [PM]	A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

Table 4-1: TOE Threats

4.2 Organizational Security Policies

This section identifies the organizational security policies which are expected to be implemented by an organization that deploys the TOE. These policies have been taken from the ESM PM PP and ESM AC PP.

Policy	Policy Definition
P. BANNER [PM]	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.UPDATEPOL [AC]	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

Table 4-2: Organizational Security Policies

4.3 Assumptions

The specific conditions listed in this section are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the ESM PM PP and ESM AC PP.

Assumption	Assumption Definition
A.INSTALL [AC]	There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.
A.MANAGE [PM]	There will be one or more competent individuals assigned to install, configure, and operate the TOE.
A.ESM [AC, PM]	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.SYSTIME [AC, PM]	The TOE will receive reliable time data from the Operational Environment.
A.USERID [AC, PM]	The TOE will receive identity data from the Operational Environment.
A.CRYPTO [AC, PM]	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.POLICY [AC]	The TOE will receive policy data from the Operational Environment.

Table 4-3: TOE Assumptions

4.4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.4.1 TOE Security Objectives

The ESM PM PP and ESM AC PP defines the following security objectives for the TOE.

Security Objective	Security Objective Definition
O.ACCESSID [PM]	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT [PM]	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH [PM]	The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.BANNER [PM]	The TOE will display an advisory warning regarding use of the TOE.
O.CONSISTENT [PM]	The TSF will provide a mechanism to identify and rectify contradictory policy data.

O.DATAPROT [AC]	The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.
O.DISTRIB [PM]	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
O.INTEGRITY [AC]	The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.
O.INTEGRITY [PM]	The TOE will contain the ability to assert the integrity of policy data.
O.MAINTAIN [AC]	The TOE will be capable of maintaining access control policy enforcement if it is unable to communicate with the Policy Management product which provided it the policy.
O.MANAGE [PM]	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
O.MNGRID [AC]	The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.
O.MONITOR [AC]	The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users).
O.OFLOWS [AC]	The TOE will be able to recognize and discard invalid or malicious input provided by users.
O.POLICY [PM]	The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.
O.PROTCOMMS [AC,PM]	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.RESILIENT [AC]	If the TOE mediates actions performed by a user against resources on an operating system, the system administrator or user shall not be allowed to perform an operation in the Operational Environment that would disable or otherwise modify the behavior of the TOE.
O.ROBUST [PM]	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
O.SELFID [AC]	The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.
O.SELFID [PM]	The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

Table 4-4: TOE Security Objectives

4.4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives:

Objective	Objective Definition
OE.ADMIN [PM]	There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.
OE.INSTALL [AC, PM]	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.

OE.POLICY [AC]	The Operational Environment will provide a policy that the TOE will enforce.
OE.PERSON [PM]	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PROTECT [PM]	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
OE.ROBUST [PM]	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.SYSTIME [AC, PM]	The Operational Environment will provide reliable time data to the TOE.
OE.USERID [AC]	The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF.
OE.USERID [PM]	The Operational Environment shall be able to identify a user requesting access to the TOE.
OE.CRYPTO	The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.

Table 4-5: Operational Environment Objectives

4.5 Security Problem Definition Rationale

The assumptions, threats, OSPs, and objectives that are defined in this ST represent the assumptions, threats, OSPs, and objectives that are specified in the Protection Profile to which the TOE claims conformance. The associated mappings of assumptions to environmental objectives, SFRs to TOE objectives, and OSPs and objectives to threats are therefore identical to the mappings that are specified in the claimed Protection Profile.

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the PPs to which the ST and TOE claim conformance. These extended components are formally defined in the PPs in which their usage is required.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This ST will highlight the operations in the following manner:

- **Assignment:** allows the specification of an identified parameter. Indicated with *italicized* text.
- **Refinement:** allows the addition of details. Indicated with **bold** text.
- **Selection:** allows the specification of one or more elements from a list. Indicated with underlined text.
- **Iteration:** allows a component to be used more than once with varying operations. Indicated with a number inside parentheses (e.g., "(1)").

When multiple operations are combined, such as an assignment that is provided as an option within a selection or refinement, a combination of the text formatting is used.

Text that is formatted in a claimed PP, such as if the PP's instantiation of the SFR has a refinement (bolded font), or a completed assignment (inside brackets), the formatting is not preserved when reproduced in this ST. Only the assignments and selections made by the ST author are within [brackets]. This is so that the reader can easily identify the operations that are performed by the ST author.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Class Name	Claimed by	Component Identification	Component Name
Enterprise Security Management (ESM)	PM	ESM_ACD.1	Access Control Policy Definition
	PM	ESM_ACT.1	Access Control Policy Transmission
	PM	ESM_ATD.1	Object Attribute Definition
	PM	ESM_ATD.2	Subject Attribute Definition
	PM	ESM_EAU.2	Reliance on Enterprise Authentication
	AC	ESM_EID.2	Reliance on Enterprise Identification
	PM	ESM_EID.2	Reliance on Enterprise Identification
Security Audit (FAU)	AC, PM	FAU_GEN.1	Audit Data Generation
	AC	FAU_SEL.1	Selective Audit
	PM	FAU_SEL_EXT.1	External Selective Audit
	AC	FAU_STG.1	Protected Audit Trail Storage (Local Storage)
	AC, PM	FAU_STG_EXT.1	External Audit Trail Storage
Communication (FCO)	AC	FCO_NRR.2	Enforced Proof of Receipt
User Data Protection (FDP)	AC	FDP_ACC.1(1)	Access Control Policy
	AC	FDP_ACC.1(2)	Access Control Policy
	AC	FDP_ACF.1(1)	Access Control Functions
	AC	FDP_ACF.1(2)	Access Control Functions
Identification and Authentication (FIA)	PM	FIA_USB.1	User-Subject Binding

Class Name	Claimed by	Component Identification	Component Name
Security Management (FMT)	PM	FMT_MOF.1	Management of Functions Behavior
	PM	FMT_MOF_EXT.1	External Management of Functions Behavior
	AC	FMT_MOF.1(1)	Management of Functions Behavior
	AC	FMT_MOF.1(2)	Management of Functions Behavior
	AC	FMT_MSA.1	Management of Security Attributes
	AC	FMT_MSA.3	Static Attribute Initialization
	PM	FMT_MSA_EXT.5	Consistent Security Attributes
	AC, PM	FMT_SMF.1	Specification of Management Functions
	AC, PM	FMT_SMR.1	Security Management Roles
Protection of the TSF (FPT)	AC, PM	FPT_APW_EXT.1	Protection of Stored Credentials
	AC	FPT_FLS.1	Failure With Preservation of a Secure State
	AC	FPT_FLS_EXT.1	Failure of Communications
	AC	FPT_RPL.1	Replay Detection
	AC, PM	FPT_SKP_EXT.1	Protection of Secret Key Parameters
Resource Utilization (FRU)	AC	FRU_FLT.1	Degraded Fault Tolerance
TOE Access (FTA)	PM	FTA_TAB.1	TOE Access Banner
	AC	FTA_TSE.1	TOE Session Establishment
	PM	FTA_SSL.3	TSF-initiated Termination
	PM	FTA_SSL.4	User-initiated Termination
Trusted Path/Channels (FTP)	AC, PM	FTP_ITC.1	Inter-TSF Trusted Channel
	PM	FTP_TRP.1	Trusted Path

Table 6-1: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class ESM: Enterprise Security Management

6.3.1.1 *[PM] ESM_ACD.1* *Access Control Policy Definition*

ESM_ACD.1.1 The TSF shall provide the ability to define access control policies for consumption by one or more compatible Access Control products.

ESM_ACD.1.2 Access control policies defined by the TSF shall be capable of containing the following:

Subjects: [*Subjects column in Tables 6-2 and 6-3*]**;** and

Objects: [*Objects column in Tables 6-2 and 6-3*]; and

Operations: [*Operations column in Tables 6-2 and 6-3*]; and

Attributes: [*Subject Attributes and Object Attributes columns in Tables 6-2 and 6-3, and hostname*]

Subjects	Subject Attributes	Objects	Object Attributes	Operations
Active Directory Users	Username, AD Group Name	Processes	Name	Execute | Delete | Terminate
				Change Permissions
		Files	Name, Approved Status	Create | Read | Modify | Delete
				Change Permissions
		Host Configuration	Name	Read | Modify | Delete
		Authentication Function		Login

Table 6-2: Host-based Operations – Active Directory Users

Application Note: The Subject Attribute of AD Group Name does not apply to the subject, object, operation, and attribute combinations for creating access control policies with the Authentication Function Object and Login Operation. This is because AD Group Name is not a credential for authentication to an endpoint system.

Subjects	Subject Attributes	Objects	Object Attributes	Operations
Processes	Process Name	Processes	Name	Execute | Delete | Terminate
				Change Permissions
		Files	Name, Approved Status	Create | Read | Modify | Delete
				Change Permissions
		Host Configuration	Name	Read | Modify | Delete

Table 6-3: Host-based Operations – Processes

ESM_ACD.1.3 The TSF shall associate unique identifying information with each policy.

6.3.1.2 *[PM] ESM_ACT.1* *Access Control Policy Transmission*

ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: [immediately following creation of a new or updated policy].

6.3.1.3 *[PM] ESM_ATD.1* *Object Attribute Definition*

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects: [*Object Attributes columns in Tables 6-2 and 6-3*].

ESM_ATD.1.2 The TSF shall be able to associate security attributes with individual objects.

6.3.1.4 *[PM] ESM_ATD.2* *Subject Attribute Definition*

ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: [*Subject Attributes columns in Tables 6-2 and 6-3]*

ESM_ATD.2.2 The TSF shall be able to associate security attributes with individual subjects.

6.3.1.5 *[PM] ESM_EAU.2* *Reliance on Enterprise Authentication*

ESM_EAU.2.1 The TSF shall rely on [[*TOE username/password*], [*Active Directory username/password*]] for subject authentication.

ESM_EAU.2.2 The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

Application Note: This SFR is related to the TOE's administrative users.

6.3.1.6 *[AC] ESM_EID.2* *Reliance on Enterprise Identification*

ESM_EID.2.1 The TSF shall rely on [[*Active Directory authentication*]], for subject identification.

ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

Application Note: This SFR is related to the endpoint system's client users.

6.3.1.7 *[PM] ESM_EID.2* *Reliance on Enterprise Identification*

ESM_EID.2.1 The TSF shall rely on [[*TOE username/password*], [*Active Directory username/password*]] for subject identification.

ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

Application Note: This SFR is related to the TOE's administrative users.

6.3.2 Class FAU: Security Audit

6.3.2.1 *[AC, PM] FAU_GEN.1 Audit Data Generation*

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions; and
b) All auditable events identified in **Tables 6-4 and 6-5** for the not specified level of audit; and
c) [*no other auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Component	Event	Additional Information
FAU_SEL.1	All modifications to audit configuration	None
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FCO_NRR.2	The invocation of the non-repudiation service	Identification of the information, the destination, and a copy of the evidence provided
FDP_ACC.1(1)	Any changes to the enforced policy or policies	Identification of Policy Management product making the change
FDP_ACC.1(2)	Any changes to the enforced policy or policies	Identification of Policy Management product making the change
FDP_ACF.1(1)	All requests to perform an operation on an object covered by the SFP	Subject identity, object identity, requested operation
FDP_ACF.1(2)	All requests to perform an operation on an object covered by the SFP	Subject identity, object identity, requested operation
FMT_MOF.1	All modifications to TSF behavior	None
FPT_FLS_EXT.1	Failure of communication between the TOE and Policy Management product	Identity of the Policy Management product, reason for the failure
FPT_RPL.1	Detection of replay	Action to be taken based on the specific actions
FTA_TSE.1	Denial of session establishment	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel

Table 6-4: Auditable Events [AC]

Application Note: All audit records from Table 6-4 are generated by the Agents, except audit records for FAU_STG_EXT.1, FTP_ITC.1, and FPT_RPL.1. The FAU_STG_EXT.1 and FTP_ITC.1 audit records are generated by the Server. The FPT_RPL.1 would be audited by the Agent's underlying operating system handling of TLS traffic.

Component	Event	Additional Information
ESM_ACD.1	Creation or modification of policy	Unique policy identifier
ESM_ACT.1	Transmission of policy to Access Control products	Destination of policy

ESM_ATD.1	Definition of object attributes	Identification of the attribute defined
ESM_ATD.1	Association of attributes with objects	Identification of the object and the attribute
ESM_ATD.2	Definition of subject attributes	Identification of the attribute defined
ESM_ATD.2	Association of attributes with subjects	None
ESM_EAU.2	All use of the authentication mechanism	None
FAU_SEL_EXT.1	All modifications to audit configuration	None
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FMT_SMF.1	Use of the management functions	Management function performed
FMT_SMR.1	Modifications to the members of the management roles	None
FTA_SSL.3	All session termination events	None
FTA_SSL.4	All session termination events	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if applicable

Table 6-5: Auditable Events [PM]

Application Note: All audit records from Table 6-5 are generated by the Server.

6.3.2.2 *[AC] FAU_SEL.1* *Selective Audit*

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a. [object identity, user identity, subject identity, host identity, event type];
b. [*no other attributes*]

6.3.2.3 *[PM] FAU_SEL_EXT.1* *External Selective Audit*

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by an ESM Access Control product from the set of all auditable events based on the following attributes:

a. [object identity, user identity, subject identity, host identity, event type]; and
b. [*no other attributes*]

6.3.2.4 *[AC] FAU_STG.1* *Protected Audit Trail Storage (Local Storage)*

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

6.3.2.5 *[AC] FAU_STG_EXT.1 External Audit Trail Storage*

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [*Server, TOE-internal storage*].

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and
b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

6.3.2.6 *[PM] FAU_STG_EXT.1 External Audit Trail Storage*

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [*SQL Server Database, TOE-internal storage*].

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and
b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

6.3.3 Class FCO: Communication

6.3.3.1 *[AC] FCO_NRR.2 Enforced Proof of Receipt*

FCO_NRR.2.1 The TSF shall enforce the generation of evidence of receipt for received policies at all times.

FCO_NRR.2.2 The TSF shall be able to relate the [*hostname, IP address, MAC address*] of the recipient of the information, and the [*policy name, Connected Enforcement Level, Disconnected Enforcement Level, configuration list (CL) version, Agent version*] of the information to which the evidence applies.

FCO_NRR.2.3 The TSF shall provide a capability to verify the evidence of receipt of information to originator given [*connectivity of Agent to originator and up to 90 seconds for the policy data to be transferred and consumed*].

6.3.4 Class FDP: User Data Protection

6.3.4.1 ***[AC] FDP_ACC.1(1)*** ***Access Control Policy***

FDP_ACC.1.1(1) The TSF shall enforce the access control Security Function Policy (SFP) on

- subjects: subset of users from an organizational data store, [*Processes*]; and
- objects: programs, files, host configuration, authentication function, [*none*]; and
- operations: ability to create, read, modify, execute, delete, terminate, or change permissions of objects, ability to use authentication function, [*none*]

6.3.4.2 ***[AC] FDP_ACC.1(2)*** ***Access Control Policy***

FDP_ACC.1.1(2) The TSF shall enforce the self-protection Security Function Policy (SFP) on

- subjects: subset of users from an organizational data store, [*Processes*]; and
- objects: programs, files, host configuration, authentication function, [*none*]; and
- operations: ability to create, read, modify, execute, delete, terminate, or change permissions of objects, ability to use authentication function, [*none*]

6.3.4.3 ***[AC] FDP_ACF.1(1)*** ***Access Control Functions***

FDP_ACF.1.1(1) The TSF shall enforce the access control SFP to objects based on the following: all operations between subjects and objects defined in **Tables 6-2 and 6-3 above** based upon some set of organizational attributes.

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*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*].

FDP_ACF.1.3(1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

Application Note: The TOE has different names for rules depending on the object, as defined in Tables 6-2 and 6-3, being protected. The name of the rules covered by the objects included within the process described under FDP_ACF.1(1) are Custom Software Rules, Memory Rules, Registry Rules, and Rapid Configs.

6.3.4.4 ***[AC] FDP_ACF.1(2)*** ***Access Control Functions***

FDP_ACF.1.1(2) The TSF shall enforce the self-protection SFP to objects based on the following: all operations between subjects and objects based upon some set of organizational attributes.

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: the TOE will not permit requested operations against objects that are defined to be protected unless the acting subject is the individual that was responsible for the TOE's installation and initial configuration.

FDP_ACF.1.3(2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

6.3.5 Class FIA: Identification and Authentication

6.3.5.1 ***[PM] FIA_USB.1*** ***User-Subject Binding***

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*TOE username, AD username, AD Group Name, role*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*user is associated with their assigned role at login, TOE username or AD username or AD group membership are checked for role assignment*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*changes to role assignment and to role's permissions take effect on next action*].

6.3.6 Class FMT: Security Management

6.3.6.1 ***[PM] FMT_MOF.1*** ***Management of Functions Behavior***

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions: [*as listed in the Management Activities column of Table 6-6*] to [*roles identified in the Administrative User Role column of Table 6-6*].

6.3.6.2 ***[PM] FMT_MOF_EXT.1*** ***External Management of Functions Behavior***

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the functions of Access Control products: audited events, repository for audit storage, Access Control SFP, policy version being implemented, Access

Control SFP behavior to enforce in the event of communications outage, [*no other functions*] to [*roles identified in the Administrative User Role column of Table 6-6*].

6.3.6.3 *[AC] FMT_MOF.1(1) Management of Functions Behavior*

FMT_MOF.1.1(1) The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions: audited events, repository for trusted audit storage, access control SFP, policy being implemented by the TSF, access control SFP behavior to enforce in the event of communications outage, [*no other functions*] to an authorized and compatible Policy Management product.

6.3.6.4 *[AC] FMT_MOF.1(2) Management of Functions Behavior*

FMT_MOF.1.1(2) The TSF shall restrict the ability to determine the behavior of the functions: policy being implemented by the TSF, [*no other functions*] to an authorized and compatible Enterprise Security Management product.

6.3.6.5 *[AC] FMT_MSA.1 Management of Security Attributes*

FMT_MSA.1.1 The TSF shall enforce the access control SFP to restrict the ability to [change default, query, modify, delete] the security attributes access control policies, access control policy attributes, implementation status of access control policies to an authorized and compatible Policy Management product.

6.3.6.6 *[AC] FMT_MSA.3 Static Attribute Initialization*

FMT_MSA.3.1 The TSF shall enforce the access control SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the authorized and compatible Policy Management product to specify alternative initial values to override the default values when an object or information is created.

6.3.6.7 *[PM] FMT_MSA_EXT.5 Consistent Security Attributes*

FMT_MSA_EXT.5.1 The TSF shall [only permit definition of unambiguous policies].

FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: [[*automatically resolve the inconsistency*]].

6.3.6.8 *[AC] FMT_SMF.1 Specification of Management Functions*

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: configuration of audited events, configuration of repository for trusted audit storage, configuration of Access Control SFP, querying of policy being implemented by the TSF, management of Access Control SFP

behavior to enforce in the event of communications outage, [*no other management functions*].

6.3.6.9 *[PM] FMT_SMF.1 Specification of Management Functions*

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*management functions defined in Table 6-6*].

Requirement	Management Activities	Administrative User Role	
		Admin	Power
ESM_ACD.1	Creation of policies	X	X
ESM_ACT.1	Transmission of policies	X	X
ESM_ATD.1 (optional)	Definition of object attributes Association of attributes with objects	X	X
ESM_ATD.2 (optional)	Definition of subject attributes Association of attributes with subjects	X	X
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	X	
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	X	
FAU_SEL.1 (optional)	Configuration of auditable events	X	X
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities	X	X
FAU_STG_EXT.1	Configuration of external audit storage location	X	
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	X	
FMT_MOF_EXT.1	Configuration of the behavior of other ESM products	X	X
FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)	X	X
FMT_SMR.1	Management of the users that belong to a particular role	X	
FTA_TAB.1	Maintenance of the banner	X	

Table 6-6: Management Functions Within TOE

6.3.6.10 *[AC] FMT_SMR.1 Security Management Roles*

FMT_SMR.1.1 The TSF shall maintain the roles [*administrator*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.3.6.11 *[PM] FMT_SMR.1 Security Management Roles*

FMT_SMR.1.1 The TSF shall maintain the roles [*Read-Only, Power User, Admin, custom]*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.3.7 Class FPT: Protection of the TSF

6.3.7.1 *[AC, PM] FPT_APW_EXT.1 Protection of Stored Credentials*

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

6.3.7.2 *[AC] FPT_FLS.1* *Failure With Preservation of a Secure State*

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*termination of Agent*].

6.3.7.3 *[AC] FPT_FLS_EXT.1* *Failure of Communications*

FPT_FLS_EXT.1.1 The TSF shall maintain policy enforcement in the following manner when the communication between the TSF and the Policy Management product encounters a failure state: [enforce the last policy received, [*apply the Disconnected Enforcement Level*]].

6.3.7.4 *[AC] FPT_RPL.1* *Replay Detection*

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [*Server*].

FPT_RPL.1.2 The TSF shall perform [*discard traffic*] when replay is detected.

6.3.7.5 *[AC, PM] FPT_SKP_EXT.1 Protection of Secret Key Parameters*

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.3.8 Class FRU: Resource Utilization

6.3.8.1 *[AC] FRU_FLT.1* *Degraded Fault Tolerance*

FRU_FLT.1.1 The TSF shall ensure the operation of enforcing the most recent policy when the following failures occur: restoration of communications with the Policy Management product after an outage.

6.3.9 Class FTA: TOE Access

6.3.9.1 *[PM] FTA_TAB.1* *TOE Access Banner*

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.3.9.2 *[AC] FTA_TSE.1* *TOE Session Establishment*

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [[*Username, hostname*]].

6.3.9.3 *[PM] FTA_SSL.3*	*TSF-initiated Termination*

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after an Authorized Administrator-configurable time interval of session inactivity.

6.3.9.4 *[PM] FTA_SSL.4*	*User-initiated Termination*

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

6.3.10 Class FTP: Trusted Path/Channels

6.3.10.1*[AC] FTP_ITC.1*	*Inter-TSF Trusted Channel*

FTP_ITC.1.1 [1] The TSF shall be capable of using [TLS, HTTPS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: [[*Server*]] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2[2] The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for transfer of policy data, [[*transfer of software updates, transfer of audit data*]].

6.3.10.2*[PM] FTP_ITC.1*	*Inter-TSF Trusted Channel*

FTP_ITC.1.1[3] The TSF shall be capable of using [TLS, HTTPS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: [authentication server, [*Agents*]] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2[4] The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for transfer of policy data, [[*remote administrative user authentication, transfer of audit data, transfer of software updates*]].

[1] TD0576
[2] TD0576
[3] TD0576
[4] TD0576

6.3.10.3 ***[PM] FTP_TRP.1***	***Trusted Path***

FTP_TRP.1.1[5]	The TSF shall be capable of using [HTTPS] to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identifications of its end points and protection of the communicated data from modification, disclosure, and [no other types of integrity or confidentiality violations].
FTP_TRP.1.2	The TSF shall permit remote users to initiate communication via the trusted path.
FTP_TRP.1.3[6]	The TSF shall require the use of the trusted path for initial user authentication and execution of management functions.

6.4 Statement of Security Functional Requirements Consistency

The Security Functional Requirements included in the ST represent all required SFRs specified in the claimed PPs, a subset of the optional requirements, and all applicable selection-based requirements that have been included as specified for the claimed PPs.

Any references to "Access Control product" or "Policy Management product" or "compatible Enterprise Security Management product" that appear in the SFRs are considered to apply to the TSF since the TOE claims conformance to both PPs. The TSF implements both capabilities in a single product.

[5] TD0576
[6] TD0576

7 Security Assurance Requirements

This section identifies the Security Assurance Requirements (SARs) that are claimed for the TOE. The SARs which are claimed are in exact conformance with the ESM PM PP and ESM AC PP.

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 *Developer action elements:*

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

7.1.1.2 *Content and presentation elements:*

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

7.1.1.3 *Evaluator action elements:*

ADV_ FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_ FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

7.2 Class AGD: Guidance Documentation

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 *Developer action elements:*

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 *Content and presentation elements:*

AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 *Evaluator action elements:*

AGD_OPE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 *Developer action elements:*

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.2 *Content and presentation elements:*

AGD_ PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

7.2.2.3 *Evaluator action elements:*

AGD_ PRE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

7.3 Class ALC: Life Cycle Supports

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 *Developer action elements:*

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

7.3.1.2 ***Content and presentation elements:***

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 ***Evaluator action elements:***

ALC_CMC.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.3.2 TOE CM Coverage (ALC_CMS.1)

7.3.2.1 ***Developer action elements:***

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 ***Content and presentation elements:***

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.3.2.3 ***Evaluator action elements:***

ALC_CMS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.4 Class ATE: Tests

7.4.1 Independent Testing - Conformance (ATE_IND.1)

7.4.1.1 ***Developer action elements:***

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 *Content and presentation elements:*

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 *Evaluator action elements:*

ATE_IND.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 *Developer action elements:*

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 *Content and presentation elements:*

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 *Evaluator action elements:*

AVA_VAN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

8 TOE Summary Specification

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR. They include Enterprise Security Management, Security Audit, Communications, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, Resource Utilization, TOE Access, and Trusted Path/Channels.

8.1 Enterprise Security Management

8.1.1 [PM] ESM_ACD.1

The App Control Console interface allows an administrative user to create policies, create rules, and associate rules with policies. Each endpoint system running an App Control Agent is assigned to a single App Control policy based upon the policy specific Agent installer. Policies allow administrative users to organize endpoint systems running the Agents into groups with common security requirements. The policy specifies an access control definition for the endpoint systems to which it has been assigned. The creation of a policy requires the administrative user to define policy settings, including its Connected Enforcement Level and Disconnected Enforcement Level. Note that the rules associated with a policy can be viewed within the policy, but rules are created separately and are then assigned to policies. Each policy has a unique name which is also associated internally by the TOE with a unique numeric identifier.

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

The Enforcement Level choices are:

- High – Only operations on files with the Approved Status of Approved are permitted by the Agent. The Agent blocks all operations on files with the Approved Status of Unapproved or Banned.
- Medium – Operations on files with the Approved Status of Approved are permitted by the Agent. The Agent blocks all operations on files with the Approved Status of Banned. The Agent displays a dialog box that provides client users the option to permit or block the operation on files with the Approved Status of Unapproved.
- Low – Operations on files with the Approved Status of Approved are permitted by the Agent. The Agent blocks all operations on files with the Approved Status of Banned. The Agent permits operations on files with the Approved Status of Unapproved but also records these access control events.

If the Connected Enforcement Level is set to Low, the Disconnected Enforcement Level will also be automatically set to Low. If the Connected Enforcement Level is set to High or Medium, the

administrative user can choose a Disconnected Enforcement Level of High or Medium, and it may differ from the Connected Enforcement Level.

There are two categories of rules that can be managed by an administrative user through the Console: internal and administrative user generated. The internal rules come preloaded with the TOE and the administrative user generated rules are defined by the administrative users. 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. 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. All rules are uniquely identified internally by numeric identifier.

Internal rules apply to all platforms and all can be reviewed by administrative users, but only certain internal rules can be modified by administrative users. One method an internal rule can be modified by an administrative user includes configuring it as either Active (i.e. enabled), Off (i.e. disabled), or Report Only. Report Only will permit the action but will record what would have been blocked if the setting were active. Administrative user generated rules require different sets of data to be specified depending on the type of rule being managed. In addition to specifying any specific subject, object, operation, and attribute information required by the rule, the administrative user will also need to define other necessary information including: the rule's name, if the rule is enabled or disabled, the platform to which the rule applies, rank position of the rule, action (e.g. permit, block), and policies to which the rule applies. Rules can be assigned by the administrative user to all policies (including policies that have not yet been created) or to one or more policies individually.

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

8.1.2 [PM] ESM_ACT.1

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

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

- Send the latest policy to the Agents that enforce that policy
- Send the latest CL of all rules to all Agents; except under the following two conditions:
    - a rule is only applicable to a specific platform (e.g., Linux agents will not receive registry rules)

- the Agent is running an older version of the software and an updated rule is not compatible with the Agent

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

8.1.3 [PM] ESM_ATD.1

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

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

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

Approved Status can be assigned and changed through the TOE's internal logic automatically or specifically defined by an administrative user. An example of the TOE's internal logic is that all files present on an endpoint system during initialization receive the 'local' Approved Status value of Approved, unless the file's 'global' Approved Status has already been set to Banned.

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

8.1.4 [PM] ESM_ATD.2

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. When an administrative user defines a rule, they are able to specify within the rule's subject field the Username(s) and/or AD Group Name(s) to which the rule applies.

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. When an administrative user defines a rule, they are able to specify within the rule's subject field the Process Name(s) to which the rule applies.

8.1.5 [PM] ESM_EAU.2 and [PM] ESM_EID.2

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. In the evaluated configuration, the TOE is configured to verify credentials against an Active Directory instance as well as the TOE's local credential table stored in an SQL Server Database. The TOE will first verify the entered credentials against the Active Directory instance with an LDAP bind request. If the credentials match an Active Directory user, the administrative user will be logged into the Console and will receive the role assigned to the user account based upon their AD username or AD Group Name within the SQL Server Database. If the credentials do not match an Active Directory user but the account exists, the administrative user will fail authentication and not be allowed access to the Console. If the credentials do not match an Active Directory user account, the credentials will then be checked against the local username and password table within the SQL Server Database. If the credentials match a locally defined user account, the administrative user will be logged into the Console and will receive the role assigned to the user account based upon their TOE defined username within the SQL Server Database. If the credentials do not match a locally defined user account, the administrative user will fail authentication and not be allowed access to the Console.

8.1.6 [AC] ESM_EID.2

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. In the evaluated configuration, all client users will be required to identify and authenticate through the endpoint system's operating system login screen which will require them to enter a username and password credentials. 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, which can include determining if the authentication function of the operating system can proceed with logging in the client user. If the credentials do not match an Active Directory user, the client user will fail authentication and not be allowed access to the endpoint system, which occurs completely outside of the TOE's purview.

8.2 Security Audit

8.2.1 [AC, PM] FAU_GEN.1

The TOE's Agent and Server generate audit records when auditable events occur on their respective systems, including the start-up and shutdown of their own audit functions. The Agent generates the audit events defined within Table 6-4 and the Server generates the audit events defined within Table 6-5, with three exceptions. The Server will generate the audit event for FTP_ITC.1 in Table 6-4 which audits the trusted channel connection between the Agent and Server. The Server will generate the audit event for FAU_STG_EXT.1 in Table 6-4 which audits the connection between the Server and the SQL Server Database. The Agent relies on its underlying operating system to provide TLS, replay detection (Table 6-4 FPT_RPL.1) is built into this protocol, and the operating system would be responsible for auditing any rejected TLS traffic which would occur without the TOE's knowledge.

For each auditable event, 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.

8.2.2 [AC] FAU_SEL.1 and [PM] FAU_SEL_EXT.1

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 rules define subjects, objects and operations based upon the attributes defined in ESM_ACD.1 as described below:

- Object identity will be used to determine if an access request will generate an audit based upon the rule using the object's Name or Approved Status attributes.
- User identity will be used to determine if an access request will generate an audit based upon the rule using the client user identity's Username or AD Group Name attributes.
- Subject identity will be used to determine if an access request will generate an audit based upon the rule using the subject identity's Process Name attribute.
- Host identity will be used to determine if an access request will generate an audit based upon the rule using the endpoint system host identity's hostname attribute.
- Event type will be used to determine if an access request will generate an audit based upon the rule defining the type of operation the subject is performing on the object.

8.2.3 [AC] FAU_STG.1

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, refer to Section 8.4.2.

The Agent on the Windows endpoint system maintains two local audit logs (TOE-internal storage) 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.

In the evaluated configuration, the Agent on the Linux endpoint system maintains two local audit logs (TOE-internal storage) with no maximum size limit. 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. The Linux Agent periodically executes a thread that performs the log rotation operation when the file size of the primary log file is greater than or equal to 50 MB. When this condition is met, 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.

8.2.4 [AC] FAU_STG_EXT.1 and [PM] FAU_STG_EXT.1

The Agent generates its own audit data for its events. The Agent writes audit data related to failed connections to the Server in the Agent's audit logs (TOE-internal storage) stored on the underlying operating system. All other SFR related audit data produced by the Agent is sent to the Server over a TLS connection provided by the TOE's underlying operating system. As the connection between an Agent and Server is not continuous, the Agent stores audit events destined for the Server in a buffer (note this is not the Agent's audit logs) before sending them to the Server as well as removes the events from its buffer once they are successfully sent to the Server. The Agent sends its audit events to the Server in batches of every ten events or every 30 seconds (whichever occurs first).

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). Refer to Section 8.2.3 for information on the storage capacity of the Agent's audit logs (TOE-internal storage).

Also, while the connection between the Agent and Server is severed, the Agent will buffer up to 5,000 audit events for sending to the Server. When this cap is exceeded, the Agent will begin deleting the oldest 10% of the audit events in its buffer, until the number of audit events is below the cap. Once the connection is re-established, the Agent will continue to send its buffered audit events to the Server. This includes any audit events that occurred during the communication outage between the Agent and the Server, up to the last audit event previously sent to the Server before the communication outage or the oldest audit event still buffered by the Agent. Therefore, if more than 5,000 audit events occurred during the communication outage, not all audit events that occurred during the communication outage will be audited by the TOE.

The Agent stores audit data related to failed connections to the Server in the Agent's audit logs (TOE-internal storage) and sends all other SFR relevant audit data to the Server. Therefore, these locations do not share the same audit records and there is no scenario where audit reconciliation is possible between the audit logs (TOE-internal storage) and the Server.

The Server generates audit data for events that occur on the Server and Console. The Server writes audit data related to receiving connections from Agents, connecting to the SQL Server Database and connecting to the AD to the Server's audit logs (TOE-internal storage) stored on the underlying operating

system. All other audit data produced by the Server is stored in the SQL Server Database. 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.

If the connection from the Server to the SQL Server Database is severed, no management functions can be performed on the Console as well as all Server functions that would result in audit data being stored in the SQL Server Database cannot be performed. The Server will still attempt to connect to the SQL Server Database and these attempts will be audited to the Server's audit logs (TOE-internal storage). Once the connection is re-established, Console management functionality, Server functionality, and all auditing resumes automatically.

The Server stores audit data related to receiving connections from Agents, connecting to the SQL Server Database and connecting to the AD in the Server's audit logs (TOE-internal storage); otherwise, the Server sends all other SFR relevant audit data to the SQL Server Database. Therefore, these locations do not share the same audit records and there is no scenario where audit reconciliation is possible between the audit logs (TOE-internal storage) and the SQL Server Database.

Administrative users do not have the ability to delete, modify, or manipulate the audit data that resides in the TOE-internal storage or the SQL Server Database 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, refer to Section 8.4.2.

8.3 Communications

8.3.1 [AC] FCO_NRR.2

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. When the Server has policy or CL changes after initial establishment, each applicable Agent will be informed about the updated information upon that Agent's next poll of the Server and the Agent will then pull this information to its configuration. The Server will then wait for a receipt message from each of the applicable Agent(s).

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

An administrative user on the Console can verify the information about the endpoint system and the current status of the Agent's configuration. For each endpoint system, an administrative user can view its hostname, its IP address, its MAC address, policy name consumed by Agent, Connected Enforcement Level consumed by Agent, Disconnected Enforcement Level consumed by Agent, CL version consumed by Agent, the Agent's software version, the current Policy Status (policy and enforcement level issues), and Upgrade Status (Agent software issues).

8.4 FDP: User Data Protection

8.4.1 [AC] FDP_ACC.1(1) and [AC] FDP_ACF.1(1)

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 as well as the hostname attribute which identifies specific endpoint systems. Each Agent has a policy assigned to it and the policy determines which rules within the CL are consumed by the Agent for enforcement on the endpoint system. The TOE has different names for rules depending on the object, as defined in Tables 6-2 and 6-3, being protected. The name of the rules covered by the objects included within the processing of rules described in the next paragraph are Custom Software Rules, Memory Rules, Registry Rules, and Rapid Configs.

When a subject attempts to perform an operation on an object, 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 (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. The access control decisions have the following enforcement on the attempted operation:

- Block – denies the operation being performed
- Permit or Allow – allows the operation being performed
- Report or Report Only – creates an event for the operation being performed (i.e., ultimately allows the operation to proceed)

There are no instances where the access control SFP will explicitly authorize or explicitly deny access of subjects to objects.

Note the TOE is not a complete replacement of the endpoint system operating system's own access control SFP. Therefore, it is possible that an access request does not match any rule within the TOE's access control SFP. In these instances, the TOE makes no decision on the access request and defers to the endpoint system's access control SFP to make a decision on the requested access which occurs outside the TOE.

8.4.2 [AC] FDP_ACC.1(2) and [AC] FDP_ACF.1(2)

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)

When a request occurs based upon an operation among controlled subjects and controlled objects, the Agent will not permit the requested operations against objects that are defined to be protected unless the acting subject is the individual that was responsible for the TOE's installation and initial configuration.

There are no instances where the access control SFP will explicitly authorize or explicitly deny access of subjects to objects.

Note that the ability to use authentication function as part of the TOE's self-protection SFP determines if a client user can even authenticate to the endpoint system. Authentication to the endpoint system is a prerequisite to performing any of the other operations between subjects and objects within the TOE's self-protection SFP; however, the process is the exact same as the access control SFP. Other than the inclusion of the authentication function, the TOE's self-protection SFP is defined by default and enforced upon each Agent's installation.

8.5 FIA: Identification and Authentication

8.5.1 [PM] FIA_USB.1

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

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

8.6 FMT: Security Management

8.6.1 [PM] FMT_MOF.1

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 TOE provides multiple administrative user roles as described in Section 8.6.9 of this ST. 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. Refer to Table 6-6 for a list of management functions and the role an administrative user must have to be able to perform them.

8.6.2 [PM] FMT_MOF_EXT.1

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

The TOE's Agents are configured by the Server based upon the configuration settings defined by the TOE's administrative users through the Console. In the Console, administrative users are able to determine the TOE's current configuration, create Agent installers, manage Agent policies, and manage the CL which together manage the Agent's functions and application of the Access Control SFP on the endpoint system were the Agent is installed. The TOE defines multiple roles for the administrative users and Table 6-6 defines which administrative users' roles have the permissions to perform these functions.

8.6.3 [AC] FMT_MOF.1(1)

The TOE has the ability to determine the behavior of, disable, enable, modify the behavior of the functions:

- audited events – defined within each rule
- repository for trusted 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 being implemented by the TSF – 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

The TOE's Agent is configured by a single Server which assumes the role of administrator when these components are communicating. Beginning with the initial establishment of the Agent to Server communication, as described in Section 8.3.1 of this ST, the Agent will verify that only the TOE's Server is able to manage the Agent. Therefore, as administrative users manage the TOE by changing an Agent's

policy and/or the CL, the Server will communicate with the Agent to perform these management functions.

8.6.4 [AC] FMT_MOF.1(2)

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.

8.6.5 [AC] FMT_MSA.1

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. Beginning with the initial establishment of the Agent to Server communication, as described in Section 8.3.1 of this ST, the Agent will verify that only the TOE's Server is able to manage the Agent. Therefore, as administrative users manage the TOE by changing an Agent's policy and/or the CL, the Server will communicate with the Agent to perform these management functions when each Agent polls the Server.

8.6.6 [AC] FMT_MSA.3

The TOE's access control SFP provides restrictive default values for security attributes. The default Approved Status value for all new inventoried files is Unapproved. An administrative user can configure the TOE to have its internal logic automatically change newly inventoried file's Approved Status to Approved or Banned based upon a variety of settings. Additionally, an administrative user can specifically define the Approved Status for a file. An Agent enforces the administratively configured Connected Enforcement Level and Disconnected Enforcement Level defined within its policy. Therefore, when a new file has the default Approved Status of Unapproved 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. An administrative user must define a policy's Connected Enforcement Level and Disconnected Enforcement Level during its creation and can modify these settings at any time. When a policy is modified, the Server will provide the Agent its updated policy upon its next poll.

8.6.7 [PM] FMT_MSA_EXT.5

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. Each Agent will also process 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.

8.6.8 [AC] FMT_SMF.1 and [PM] FMT_SMF.1

The TOE's Server and Agent components are able to perform their own management functions: configuration of audited events, configuration of repository for trusted audit storage, configuration of Access Control SFP, querying of policy being implemented by the TSF, and management of Access Control SFP behavior to enforce in the event of communications outage. The TOE performs these management functions based upon the configuration of the TOE by its administrative users. 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 TOE provides multiple administrative user roles as described in Section 8.6.9 of this ST. 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. Refer to Table 6-6 for a list of management functions and the role an administrative user must have to be able to perform them.

8.6.9 [AC] FMT_SMR.1 and [PM] FMT_SMR.1

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

The TOE also associates administrative users accessing the TOE via the Console with roles. The TOE supports the following roles: Read-Only, Power User, Admin (specified 'Administrator' within the TOE), 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'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 and one of the administrative users with the Admin role is expected to install the TOE. The TOE 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.

Administrative users are assigned to roles through direct assignment to their username (TOE or Active Directory verified) or as a result of their membership in an Active Directory group as defined by mapped AD Group Name. Active Directory group mappings are applied in a strict hierarchy in the event that an administrative user belongs to multiple AD Group Names; each of which are assigned to different roles. Additionally, an AD Group Name role assignment will take priority over the role assigned to an administrative user by their username.

8.7 FPT: Protection of the TSF

8.7.1 [AC, PM] FPT_APW_EXT.1

Administrative users of the TOE are required to authenticate to the Console with a username and password. The user accounts which are used to verify the administrative users' usernames and passwords are stored in either the SQL Server Database or Active Directory. 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.

Client users are required to authenticate to the endpoint system's operating system with a username and password. The user accounts which are used to verify the client users' usernames and passwords are stored in Active Directory. 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.

8.7.2 [AC] FPT_FLS.1

The TOE will preserve a secure state in the event of an unanticipated termination of an Agent by automatically restarting the Agent.

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

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

8.7.3 [AC] FPT_FLS_EXT.1

The TOE's Agent will always enforce its latest configuration as defined by its policy and CL of rules regardless of if communication with the Server is currently active or not active based upon the Agent's last polling attempt of the Server. An Agent's policy defines two Enforcement Levels: one when the Agent is actively connected to the Server called the Connected Enforcement Level and another when the Agent cannot reach the Server called the Disconnected Enforcement Level. The configuration of these Enforcement Levels can be the same or one may be stricter than the other depending on the manner that the configuring administrative user wants access control enforced on the endpoint system when there is a communication outage between the Agent and Server. Refer to Section 8.1.1 of the ST for more information on Enforcement Levels.

8.7.4 [AC] FPT_RPL.1

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

8.7.5 [AC, PM] FPT_SKP_EXT.1

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.

8.8 FRU: Resource Utilization

8.8.1 [AC] FRU_FLT.1

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.

8.9 FTA: TOE Access

8.9.1 FTA_TAB.1

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.

8.9.2 [AC] FTA_TSE.1

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

8.9.3 [PM] FTA_SSL.3

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

8.9.4 [PM] FTA_SSL.4

Any administrative user can initiate termination from their own interactive Console session by using the Username dropdown and selecting 'Log Out'.

8.10 FTP: Trusted Path/Channels

8.10.1 [AC] FTP_ITC.1

The Agent's channels are logically distinct from each other and do not interfere with the operation of the other channels of communication. 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 are initiated by the Agent. 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.

8.10.2 [PM] FTP_ITC.1

The Server's channels are logically distinct from each other and do not interfere with the operation of the other channels of communication. 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.

8.10.3 [PM] FTP_TRP.1

All administrative users are required to authenticate to the TOE in order to be able to perform any management functions. 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.