CA Privileged Access Manager v2.8 Security Target

Version 2.1

July 10, 2017

CA, Inc.
1 Computer Associates Plaza
Islandia, NY 11749
http://www.ca.com

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

CA, Inc.
1 Computer Associates Plaza
Islandia, NY 11749
http://www.ca.com

REVISION HISTORY

Rev	Description
1.0	August 18, 2014, Initial release
1.1	October 24, 2014, Addressed comments from lab and vendor
1.2	November 9, 2014, Added additional vendor information
1.3	December 3, 2014, Added FTA_SSL.4 to table 11, minor editorial corrections
1.4	December 10, 2014, Addressed AAR issues
1.5	January 17, 2015, Added the HSM as a required OE component
1.6	February 20, 2015, Expanded the TOE boundary to address certifier ORs
1.7	March 3, 2015, Addressed comments from lab
1.8	November 11, 2015, Addressed NIAP comments and vendor updates
1.9	December 4, 2015, Product name change
1.10	March 18, 2016, Updated version information
1.11	April 4, 2016, Updated information concerning hierarchical policies
1.12	June 23, 2016, Corrected DRBG reference
1.13	July 20, 2016, Addressed NIAP comments
2.0	May 5, 2017, Assurance Continuity update
2.1	July 10, 2017, Corrections

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

AES ..... **Advanced Encryption Standard**
AMI ..... **Amazon Machine Instance**
API ..... **Application Program Interface**
DBMS ..... **DataBase Management System**
CAVP ..... **Cryptographic Algorithm Validation Program**
CBC ..... **Cipher Block Chaining**
CC ..... **Common Criteria**
CMVP ..... **Cryptographic Module Validation Program**
CPU ..... **Central Processing Unit**
CSP ..... **Critical Security Parameter**
DHE ..... **Diffie–Hellman Ephemeral**
ESM ..... **Enterprise Security Management**
FIPS ..... **Federal Information Processing Standards**
GB ..... **GigaByte**
GUI ..... **Graphical User Interface**
HMAC ..... **Hash-based Message Authentication Code**
HSM ..... **Hardware Security Module**
HTTPS ..... **HyperText Transfer Protocol Secure**
IP ..... **Internet Protocol**
IT ..... **Information Technology**
LDAP ..... **Lightweight Directory Access Protocol**
MAC ..... **Mandatory Access Control**
NIST ..... **National Institute of Standards and Technology**
OS ..... **Operating System**
PKCS ..... **Public-Key Cryptography Standard**
PM ..... **Policy Manager**
PP ..... **Protection Profile**
RBG ..... **Random Bit Generator**
rDSA ..... **RSA Digital Signature Algorithm**
RFC ..... **Request For Comments**
RSA ..... **Rivest-Shamir-Adleman**
SFA ..... **Socket Filter Agent**
SFP ..... **Security Function Policy**
SFR ..... **Security Functional Requirement**
SHA ..... **Secure Hash Algorithm**
SSL ..... **Secure Socket Layer**
ST ..... **Security Target**
TLS ..... **Transport Layer Security**
TOE ..... **Target of Evaluation**
TSF ..... **TOE Security Function**
VPN ..... **Virtual private Network**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the CA Privileged Access Manager (PAM) Version 2.8.2. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

CA Privileged Access Manager v2.8 Security Target, Version 2.1, dated July 10, 2017

1.2 TOE Reference

CA Privileged Access Manager Version 2.8.2

1.3 TOE Overview

1.3.1 Usage and Major Security Features

PAM enables enterprises to secure the access to critical infrastructure by enforcing configured policies to limit connectivity between users (including privileged users) and targets. The PAM Server acts as the Policy Manager (PM) for the PAM product components, enabling policies to be configured and distributed to access control components.

The PAM Server GUI enables administrators to configure policies controlling what users may access what target devices, and using what access mechanisms (protocols). The policies operate within a "deny all, permit by exception" model. Attributes for users (subjects) and targets (objects) may be defined, and policies specify authorized connections between the configured users and targets. The policies may also specify whether users are permitted to connect to a third system after connecting to a target according to a policy.

Users and administrators may connect to the PAM Server GUI via HTTPS. Credentials required to gain access to the GUI are imported from an enterprise server (such as Active Directory) and saved on PAM Server as salted SHA-512 hashes for validation. The imported credentials are periodically updated from the enterprise server. Credentials supplied by users during login are hashed (SHA-512 with salt) are compared to the saved values by the PAM Server.

After successful login, administrators are provided access to the GUIs for configuration of the server and policies. Both users and administrators have access to a list of targets that they are permitted to connect to, and may activate one or more of those connections via the HTTPS session.

Administrators may also define rules to restrict access to the GUI to specific days and/or times, as well as from specific IP addresses. HTTPS sessions may be terminated by the users; idle sessions are also terminated by the TOE after a configured period of time.

The PAM Server communicates policies and audit configuration information to other product components, such as the Socket Filter Agents executing on target systems. Policies are transmitted to remote components via trusted channels.

Audit records are generated for security relevant events on the TOE. The PAM Server acts as the audit server for its own audit records, so audit records are stored locally. Functionality is provided by the PAM Server for the viewing of audit records by authorized users, but this functionality is outside the scope of this evaluation.

1.3.2 TOE Type

Enterprise Security Management (ESM) Policy Manager

1.3.3 Required Non-TOE Hardware/Software/Firmware

The PAM Server is a set of applications and services executing on a hardened Linux platform. PAM Server is delivered pre-installed on a physical appliance, the X304L (PAM HAH 995).

A Hardware Security Module (HSM) is used by the TOE. The SafeNet Luna PCI-E 1700 must be installed in the PAM X304L appliance. The SafeNet Luna PCI-E 1700 is FIPS 140-2 validated (CMVP #1693). The PAM Server applications and services communicate directly with the HSM using software provided by SafeNet utilizing a PKCS#11 API.

PAM also includes components (outside the TOE boundary) such as the Socket Filter Agents (SFA) that are installed on targets to restrict network connections beyond the target. The PAM Server communicates policies to be enforced to SFA.

Web user credential validation is performed by LDAP v3 servers (including Active Directory).

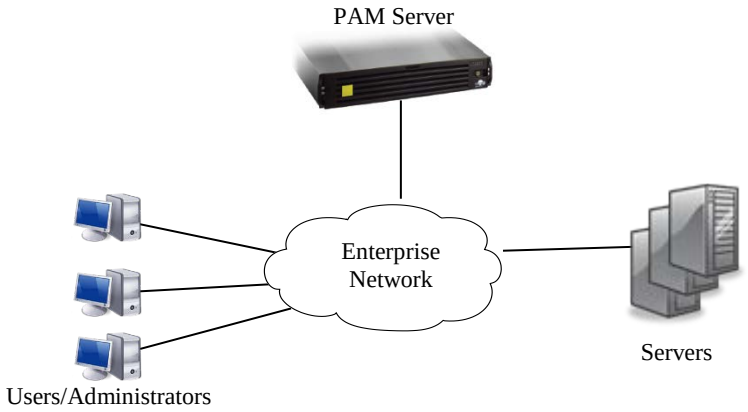
1.4 TOE Description

The PAM Server includes a set of services executing on a hardened Linux platform, the X304L. The PAM Server is one component of the PAM product.

The PAM Server is logically in between the users and servers, mediating access attempts (connections) between the entities. Because the PAM Server is not physically in between the users and servers, it is the responsibility of the Operational Environment to ensure that that all users access the protected servers via PAM. The PAM Server provides the policy management component of the PAM product, along with a portion of the access control aspects of the product.

A typical deployment for these components is shown in the following diagram.

Figure 1 - Typical TOE Deployment



1.4.1 Physical Boundary

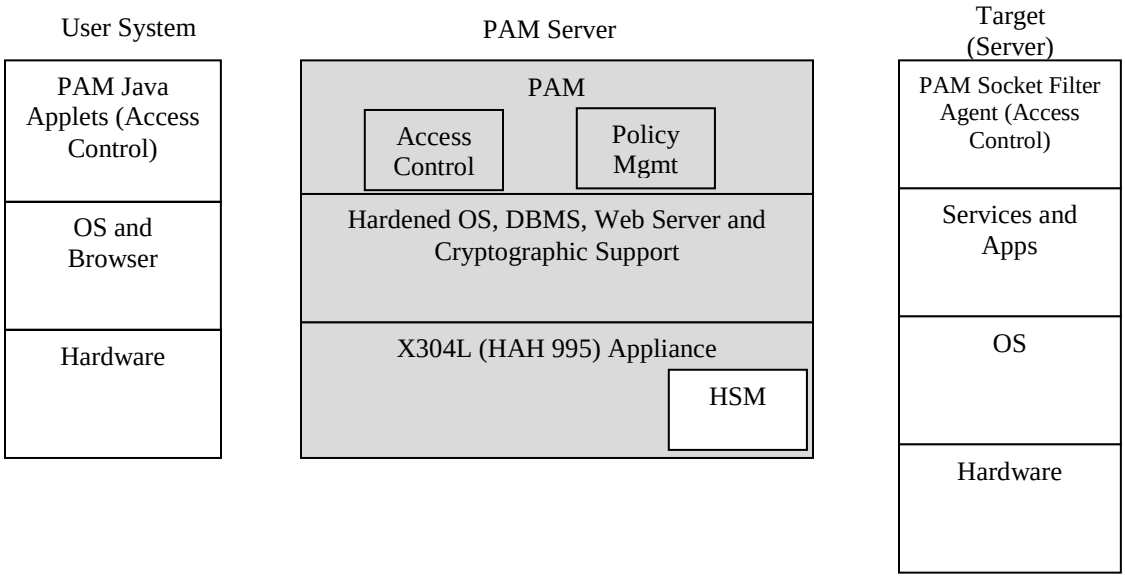
The PAM product includes components that execute on the PAM Server as well as on user systems and servers (targets). For this TOE, the physical boundary of the TOE is the set of services on the PAM Server required for the policy management function, along with the

operating system (OS) and support components required by the services. The TOE boundary is depicted in the following diagram (shaded items are within the TOE boundary).

The services included in the TOE boundary provide the functionality for:

1. Instantiation of the web site to provide user and administrative GUI access to PAM.
2. Policy distribution to the access control components.

Figure 2 - Physical Boundary



The physical boundary includes the following guidance documentation:

1. *CA Privileged Access Manager 2.8 on line documentation (last update April 7, 2017)*
2. *CA Privileged Access Manager Hardware Model X304L Setup Guide (1 December 2015)*
3. *CA Privileged Access Manager Common Criteria Supplement (5 May 2017)*

1.4.2 Logical Boundary

1.4.2.1 Audit

Audit records are generated for security-relevant events and stored on the PAM Server platform.

1.4.2.2 Credential Protection

Since web user credential validation is performed by external credential servers, no user credentials are stored within the TOE. (Note that PAM includes the capability to configure credentials for target logins, but this functionality is excluded from the evaluation and guidance directs administrators to not use this capability.) Keys used by or on behalf of the TOE cannot be read via any TOE interfaces.

1.4.2.3 Management

The TOE provides management capability to enable the TOE to be controlled and monitored. Distinct roles are supported so that management functionality can be restricted to authorized administrators.

1.4.2.4 Policy Management

Administrators configure access control policies for consumption by the PAM access control components to specify the targets that users may connect to. Administrators may configure targets (objects) and users (subjects), and then configure policies to specify what users or user groups may connect to what targets or target groups and using what access mechanisms. Policies are transmitted to access control components on the PAM Server when they are configured, and to the Socket Filter Agent (SFA) access control components when each target connection is established. User credential validation is performed by external servers.

1.4.2.5 Secure Communications

HTTPS is required to be used for all web user sessions. Communication between the PAM Server and the SFAs uses TLS. TLS versions 1.0 and 1.2 are supported; SSL is not supported.

1.4.2.6 Web Session Management

Web sessions are subject to establishment restrictions that may be configured for user accounts by administrators. When a connection is established, a banner message is displayed. Users can terminate their own sessions, and the TOE automatically terminates inactive sessions after a configured period of time.

1.4.2.7 Cryptographic Support

The TOE's cryptographic modules are FIPS PUB 140-2 validated. The TOE's cryptographic algorithms are AES (CBC mod with key sizes of 128 and 256 bits); RSA Digital Signatures (key size 2048); SHA-1, SHA-256, and SHA-384; and HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384 (key size 160 bits). The TOE is capable of generating cryptographic keys. These keys are created, managed and destroyed to provide cryptographic services to the network. Cryptographic keys as well as other CSPs are zeroized when no longer required and the TOE offers a function to zeroize this data on demand.

The cryptographic operations are used with the HTTPS/TLS functionality for user access.

1.5 Evaluated Configuration

The following configuration options must be adhered to:

1. FIPS mode is enabled.
2. Connections to the PAM Server GUI must use HTTPS.
3. Credential validation for web users is performed by external LDAP servers. TLS is enabled for all configured LDAP servers.
4. Credentials for targets are not configured in policies.
5. TOE administrators using the web interface are configured with the Global Administrator role; GUI users are configured with the Standard User role.
6. SFA Monitoring is enabled for all configured Socket Filter Agents.

7. The preconfigured “super” account password is changed during installation (to a secure value) and the account is not used after installation. All administrator access is via user accounts added during installation or operation.
8. Login timeouts (for inactive sessions) are not disabled.

1.6 Functionality Excluded from the Evaluation

The following functionality present in the PAM product was not covered by the evaluation:

1. Access Control and Credential Management functionality.
2. The optional Application-to-Application (A2A) functionality.
3. Redundancy via clustered servers with automatic synchronization.
4. VPNs.
5. In addition to being installed on a physical appliance, PAM is also available as an Amazon Machine Instance (AMI) or as a VMware virtual appliance.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 4, dated September 2012

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

The TOE does not claim conformance to any security functional requirement or security assurance requirement packages.

2.3 Protection Profile Conformance

The TOE claims exact conformance to the Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1, dated October 24, 2013.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption,* threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

Table 1 Assumptions

A.Type	Description
A.CRYPTO	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.
A.ROBUST	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.USERID	The TOE will receive validated identity data from the Operational Environment.

3.3 Threats

Table 2 Threats

T.Type	Description
T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.CONTRADICT	A careless administrator may create a policy that contains contradictory rules for access control enforcement resulting in a security policy that does not have unambiguous enforcement rules.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FORGE	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	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, and authorization mechanisms in order to use the TOE's management functions.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
T.WEAKPOL	A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

3.4 Organisational Security Policies

Table 3 OSPs

P.Type	Description
P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 4 Security Objectives for the TOE

O.Type	Description
O.ACCESSID	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	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	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	The TOE will display an advisory warning regarding use of the TOE.
O.CONSISTENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.
O.CRYPTO	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
O.INTEGRITY	The TOE will contain the ability to assert the integrity of policy data.
O.MANAGE	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
O.POLICY	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	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

4.2 Security Objectives for the Operational Environment

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

Table 5 Security Objectives of the Operational Environment

OE.Type	Description
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing 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.

OE.Type	Description
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
OE.ROBUST	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.USERID	The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF.

5. Extended Components Definition

This section is intended to contain only the extended components and not the extended requirements (requirements based on extended components). The extended requirements should be included in the security requirements and are for all purposes the same as requirements based on components in CC Part 2 or CC Part 3.

5.1 Class ESM: Enterprise Security Management

This ESM class specifies functional requirements that support the definition, consumption, and enforcement of centralized access control, authentication, secure configuration, and auditing policies. The functional requirements defined in this class differ from those defined in CC Part 2 by defining specific methods by which the TSF interacts with the Operational Environment to achieve the goals of Enterprise Security Management.

5.1.1 ESM_ACD Access Control Policy Definition

Family Behavior

The requirements of this family ensure that the TSF will have the ability to authoritatively define access control policies for use in an ESM deployment.

Component Leveling

There is only one component in this family, ESM_ACD.1. ESM_ACD.1, Access Control Policy Definition, requires the TSF to be able to define access control policies for consumption by external Access Control products.

5.1.1.1 ESM_ACD.1 Access Control Policy Definition

The ESM_ACD family defines requirements for defining access control policies. This allows other ESM products to enforce their own security functions by using this attribute data. The ESM_ACD.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define policies that govern the behavior of products that reside external to the TOE.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
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.
Application Note:	*Example source for subject data would be a compatible Identity and Credential Management product.*
	Objects: [***assignment: list of objects that can be used to make an access control decision and the source from which they are derived***]; and
Application Note:	*A host-based example source for objects would be the operating system of the host on which those objects reside.*

Operations: [***assignment: list of operations that can be used to make an access control decision and the source from which they are derived***]; and

Application Note: *A host-based example source for operations would be the operating system of the host on which those objects reside. The operations performed against these objects would be the security-relevant functions of this operating system.*

Attributes: [***assignment: list of attributes that can be used to make an access control decision and the source from which they are derived***].

Application Note: *Example source for attribute data would be a compatible Identity and Credential Management product or the TOE itself.*

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

Management: ESM_ACD.1

The following actions could be considered for the management functions in FMT:

a) Creation and modification of policies.

Audit: ESM_ACD.1

The following actions should be auditable if ESM_ACD.1 Access control policy definition is included in the PP/ST:

a) Minimal: Creation and modification of policies.

5.1.2 ESM_ACT Access Control Policy Transmission

Family Behavior

The requirements of this family ensure that the TSF will have the ability to transfer defined access control policies to other ESM products.

Component Leveling

There is only one component in this family, ESM_ACT.1. ESM_ACT.1, Access Control Policy Transmission, requires the TOE to transmit access control policy data defined by ESM_ACD.1 to compatible and authorized ESM products external to the TSF under conditions defined by the ST author.

5.1.2.1 ESM_ACT.1 Access Control Policy Transmission

The ESM_ACT family defines requirements for transmitting enterprise policy attributes. This allows other ESM products to enforce their own security functions by using attribute data defined by the TSF. The ESM_ACT.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to distribute access control policy data to external entities.

Hierarchical to: No other components.

Dependencies: ESM_ACD.1 Access Control Policy Definition

ESM_ACT.1.1	The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: [selection: choose one or more of: immediately following creation of a new or updated policy, at a periodic interval, at the request of a compatible Secure Configuration Management product, [***assignment: other circumstances***]].
Application Note:	*The intent of this requirement is to ensure that the TSF is transmitting access control policy information to an Access Control product in a timely manner so that there is assurance that it is enforcing an appropriate policy. If the assignment is selected, it must reflect that intent.* *If "at the request of a compatible Secure Configuration Management product" is selected, the ST author must indicate the compatible product(s) which are expected to be present in the evaluated configuration.*

Management: ESM_ACT.1

The following actions could be considered for the management functions in FMT:

a) Specification of the access control policy data to be transmitted.
b) Specification of the circumstances under which this data is transmitted.
c) Specification of the destinations to which this data is transmitted.

Audit: ESM_ACT.1

The following actions should be auditable if ESM ACT.1 Access control policy transmission is included in the PP/ST:

a) Minimal: Transmission of access control policy data to external processes or repositories.

5.1.3 ESM_ATD Attribute Definition

Family Behavior

The requirements of this family ensure that the TSF will have the ability to authoritatively define attributes for Operational Environment attributes that can subsequently be used for access control policy definition and enforcement.

Component Leveling

There are two components in this family, ESM_ATD.1 and ESM_ATD.2. These components are not hierarchical to each other. ESM_ATD.1, Object Attribute Definition, requires the TSF to be able to define some set of policy-related object attributes. ESM_ATD.2, Subject Attribute Definition, requires the TSF to be able to define some set of policy-related subject attributes[1]. In

[1] In other words, attributes are relevant to policies enforced by the access control component. Subjects may have additional attributes that are related to identity and credentials. The ability to manage subject attributes is optional in

both cases, these attributes are expected to be subsequently associated with controlled entities in the Operational Environment for use in handling access control. Examples of object attributes include security labels for use in mandatory access control (MAC) environments and protection levels that can be associated with web pages that reside within an organization's intranet. Examples of subject attributes include clearances or MAC ranges that would be associated with defined identities.

5.1.3.1 ESM_ATD.1 Object Attribute Definition

The ESM_ATD.1 component defines requirements for specification of object attributes. This allows other ESM products to enforce their own security functions by using attribute data defined by the TSF. The ESM_ATD.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define attributes that are associated with objects that reside in the Operational Environment.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
ESM_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual objects: [***assignment*: *list of object security attributes***].
Application Note:	*Object security attributes refer to attributes that may ultimately factor into an access control decision but are not associated with either a user or an access control policy. A TOE that defines access control policies for multi-level security may need to define security labels that can be associated with resources in order for the policy to be applicable to those resources.*
ESM_ATD.1.2	The TSF shall be able to associate security attributes with individual objects.

Management: ESM_ATD.1

The following actions could be considered for the management functions in FMT:

a) Definition of object attributes.
b) Association of attributes with objects.

Audit: ESM_ATD.1

The following actions should be auditable if ESM_ATD.1 Object attribute definition is included in the PP/ST:

a) Minimal: Definition of object attributes.
b) Minimal: Association of attributes with objects.

---

the Policy Management component; a system designer may choose to provide that capability within the Identity and Credential Management component.

5.1.3.2 ESM_ATD.2 Subject Attribute Definition

The ESM_ATD.2 component defines requirements for specification of subject attributes. This allows other ESM products to enforce their own security functions by using attribute data defined by the TSF. In particular, subject attributes might be maintained by an Identity Management component and consumed by the Access Control component. The ESM_ATD.2 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define attributes that are associated with subjects that reside in the Operational Environment.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
ESM_ATD.2.1	The TSF shall maintain the following list of security attributes belonging to individual subjects: [***assignment: list of subject security attributes***].
Application Note:	*Subject security attributes refer to attributes that may ultimately factor into an access control decision and are associated with active entities under the access control policy. A TOE that defines access control policies for multi-level security may need to define security labels that can be associated with users in order for the policy to be applicable to those users.*
ESM_ATD.2.2	The TSF shall be able to associate security attributes with individual subjects.

Management: ESM_ATD.2

The following actions could be considered for the management functions in FMT:

a) Definition of subject attributes.
b) Association of attributes with subjects.

Audit: ESM_ATD.2

The following actions should be auditable if ESM_ATD.2 Subject attribute definition is included in the PP/ST:

a) Minimal: Definition of subject attributes.
b) Minimal: Association of attributes with subjects.

5.1.4 ESM_EAU Enterprise Authentication

Family Behavior

The requirements of this family ensure that the TSF will have the ability to interact with external entities for the purpose of authenticating administrators, users, or other subjects.

Component Leveling

There are four non-hierarchical components in this family, ESM_EAU.1, ESM_EAU.2, ESM_EAU.5, and ESM_EAU.6.

ESM_EAU.1, Enterprise Authentication, requires the TSF to be able to receive authentication requests from a defined set of external entities, validate them by using some protocol, and returning the result of the decision to the requesting entity. ESM_EAU.1 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

ESM_EAU.2, Reliance on Enterprise Authentication, is the opposite of ESM_EAU.1. This allows the TSF to take an authentication performed in the Operational Environment and use it as if the TSF had performed the authentication itself.

ESM_EAU.5, Multiple Enterprise Authentication Mechanisms, allows the TSF to provide multi-factor authentication. ESM_EAU.5 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

ESM_EAU.6, Enterprise Re-authentication, allows the TSF to issue re-authentication challenges for established sessions. ESM_EAU.1 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

Note that ESM_EAU.5 and ESM_EAU.6 were derived from FIA_UAU.5 and FIA_UAU.6, respectively. They were each assigned the same component level as their CC part 2 counterparts to emphasize the similarities.

5.1.4.1 ESM_EAU.2 Reliance on Enterprise Authentication

The ESM_EAU family defines requirements for facilitating enterprise user authentication. This allows other ESM products to enforce their own security functions by using this attribute data. This differs from FIA_UAU.1 and FIA_UAU.2 specified in CC Part 2 because these requirements specifically apply to a user authenticating to the TSF in order to perform activities that are mediated by the TSF. ESM_EAU.2 applies to the ability of the TSF to issue an authentication request that may be directed to the Operational Environment on behalf of a TOE user rather than being forced to perform its own authentication.

Hierarchical to:	No other components.
Dependencies:	ESM_EID.2 Reliance on Enterprise Identification
ESM_EAU.2.1	The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject authentication***], [***assignment: identified Operational Environment component(s) responsible for subject authentication***]] for subject authentication.
Application Note:	*If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.*
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:	*If the TSF uses two different methods for authenticating two*

distinct sets of subjects, the ST author must represent this by creating a different iteration of this SFR for each method.

Management: ESM_EAU.2

The following actions could be considered for the management functions in FMT:

a) Specification of entities used to perform authentication on behalf of the TSF.

Audit: ESM_EAU.2

The following actions should be auditable if ESM_EAU.2 Reliance on enterprise authentication is included in the PP/ST:

- Minimal: All use of the authentication mechanism.

5.1.5 ESM_EID Enterprise Identification

Family Behavior

The requirements of this family ensure that the TSF will have the ability to interact with external entities for the purpose of identifying administrators, users, or other subjects.

Component Leveling

There are two non-hierarchical components in this family, ESM_EID.1 and ESM_EID.2.

ESM_EID.1, Enterprise Identification, requires the TSF to be able to receive identification requests from a defined set of external entities. These identification requests are then used as inputs for enterprise authentication. ESM_EID.1 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

ESM_EID.2, Reliance on Enterprise Identification, is the opposite of ESM_EID.1. This allows the TSF to accept the validity of an identity that was asserted in the Operational Environment.

5.1.5.1 ESM_EID.2 Reliance on Enterprise Identification

The ESM_EID family defines requirements for facilitating enterprise user identification. This allows for the subsequent execution of enterprise user authentication. This differs from FIA_UID.1 and FIA_UID.2 specified in CC Part 2 because these requirements specifically apply to a user presenting identification to the TSF in order to perform activities that are mediated by the TSF. ESM_EID.2 applies to the ability of the TSF to be presented identification from the Operational Environment and to treat this as valid rather than performing its own identification request.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
ESM_EID.2.1	The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject identification***], [***assignment: identified Operational Environment component(s) responsible for subject identification]***] for subject identification.

Application Note: *If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.*

If this SFR is claimed for a TOE that performs host-based access control, it is also acceptable to complete the second assignment with the operating system(s) on which the TOE resides. This prevents a malicious user from attempting to bypass the TSF by creating a new local user on a host system that may not be subject to the TOE's access control policy enforcement.

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: *If the TSF uses two different methods for identifying two distinct sets of subjects, the ST author must represent this by creating a different iteration of this SFR for each method.*

Management: ESM_EID.2

There are no management activities foreseen.

Audit: ESM_EID.2

There are no auditable events foreseen.

5.2 Class FAU: Security Audit

5.2.1 FAU_SEL_EXT.1 External Selective Audit

The FAU_SEL_EXT.1 family defines requirements for defining the auditable events on an external IT entity. Auditable events refer to the situations that trigger audit data to be written as audit data defined in FAU_GEN.1. The FAU_SEL_EXT.1 requirement has been added because CC Part 2 lacks a selectable audit requirement that demonstrates the ability of the TSF to define the auditable events for a specific external entity.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FMT_MTD.1 Management of TSF Data

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by [***assignment: one or more entities in the Operational Environment***] from the set of all auditable events based on the following attributes:

a. [selection: object identity, user identity, subject identity, host identity, event type]; and

b. [***assignment: list of additional attributes that audit selectivity***

is based upon].

Management: FAU_SEL_EXT.1

The following actions could be considered for the management functions in FMT:

a) Specification of the external IT entity that will be configured by the TSF.
b) Specification of the auditable events for an external IT entity.

Audit: FAU_SEL_EXT.1

The following actions should be auditable if FAU_SEL_EXT.1 External selective audit is included in the PP/ST:

a) Minimal: Changes to the set of events that are defined as auditable by the external entity.

5.2.2 FAU_STG_EXT.1 External Audit Trail Storage

The FAU_STG_EXT family defines requirements for recording audit data to an external IT entity. Audit data refers to the information created as a result of satisfying FAU_GEN.1. This pertains to security audit because it discusses how audit data should be handled. The FAU_STG_EXT.1 requirement has been added because CC Part 2 lacks an audit storage requirement that demonstrates the ability of the TSF to write audit data to one or more specific external repository in a specific secure manner, as well as supporting the potential for local temporary storage.[2]

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit Data Generation FTP_ITC.1 Inter-TSF Trusted Channel
FAU_STG_EXT.1.1	The TSF shall be able to transmit the generated audit data to [***assignment: non-empty list of external IT entities and/or "TOE-internal storage"***].
Application Note:	*The term "transmit" is intended to both TOE-initiation of the transfer of information, as well as the TOE transferring information in response to a request from an external IT entity.* *Examples of external IT entities could be an Audit Server ESM component on an external machine, an evaluated operating system sharing the platform with the TOE, or a centralized logging component. Transmission to multiple sources is permitted.*
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.

[2] FAU_STG.1 could have been treated as an optional requirement in the PP. However, as there might be systems that had only local storage, that would have meant FAU_STG_EXT.1 would also need to be optional. Combining both into a single non-optional SFR mandates protected audit storage and transmission, while still supporting an "all-in-one" product that combines ESM capabilities.

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.

Management: FAU_STG_EXT.1

The following actions could be considered for the management functions in FMT:

a) Specification of the external IT entities that will receive generated audit data.

Audit: FAU_STG_EXT.1

The following actions should be auditable if FAU_STG_EXT.1 External audit trail storage is included in the PP/ST:

a) Basic: Establishment and disestablishment of communications with the external IT entities that are used to receive generated audit data.

5.3 Class FCS: Cryptographic Support

5.3.1 FCS_CKM_EXT.4 Cryptographic Key Zeroization

The FCS_CKM_EXT family defines requirements for deletion of cryptographic keys. The FCS_CKM_EXT.4 requirement has been added to provide a higher degree of specificity for key generation than the corresponding requirements in CC Part 2.

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and cryptographic security parameters when no longer required.

Management: FCS_CKM_EXT.4

There are no management actions foreseen.

Audit: FCS_CKM_EXT.4

The following actions should be auditable if FCS_CKM_EXT.4 Cryptographic Key Zeroization is included in the PP/ST:

a) Basic: Failure of the key zeroization process.

5.3.2 FCS_HTTPS_EXT.1 HTTPS

The requirements of this family ensure that the TSF will implement the HTTPS protocol in accordance with an approved cryptographic standard.

There is only one component in this family, FCS_HTTPS_EXT.1. FCS_HTTPS_EXT.1, HTTPS, requires the TOE to implement HTTPS in accordance with a defined standard.

Hierarchical to:	No other components.
Dependencies:	FCS_TLS_EXT.1 TLS
FCS_HTTPS_EXT.1.1	The TSF shall implement the HTTPS protocol that complies with RFC 2818.
FCS_HTTPS_EXT.1.2	The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

Management: FCS_HTTPS_EXT.1

There are no management actions foreseen.

Audit: FCS_HTTPS_EXT.1

The following actions should be auditable if FCS_HTTPS_EXT.1 HTTPS is included in the PP/ST:

a) Basic: Failure to establish a session.
b) Basic: Establishment/termination of a session.

5.3.3 FCS_RBG_EXT.1 Random Bit Generation

The requirements of this family ensure that the TSF will generate random numbers in accordance with an approved cryptographic standard.

There is only one component in this family, FCS_RBG_EXT.1. FCS_RBG_EXT.1, Cryptographic Operation (Random Bit Generation), requires the TOE to perform random bit generation in accordance with a defined standard.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RBG_EXT.1.1	The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulates entropy from [selection: choose one of: (1) one or more independent hardware-based noise sources, (2) one or more independent software-based noise sources, (3) a combination of hardware-based and software-based noise sources.].
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded with a minimum of [selection, choose one of: 128 bits, 256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Management: FCS_RBG_EXT.1

There are no management actions foreseen.

Audit: FCS_RBG_EXT.1

The following actions should be auditable if FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) is included in the PP/ST:

a) Basic: Failure of the randomization process.

5.3.4 FCS_TLS_EXT.1 TLS

The requirements of this family ensure that the TSF will implement the TLS protocol in accordance with an approved cryptographic standard.

There is only one component in this family, FCS_TLS_EXT.1. FCS_TLS_EXT.1, TLS, requires the TOE to implement TLS in accordance with a defined standard.

Hierarchical to:	No other components.
Dependencies:	FCS_COP.1 Cryptographic Operation
FCS_TLS_EXT.1.1	The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: Mandatory Ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA Optional Ciphersuites: [selection: None TLS_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384].

Management: FCS_TLS_EXT.1

There are no management actions foreseen.

Audit: FCS_TLS_EXT.1

The following actions should be auditable if FCS_TLS_EXT.1 TLS is included in the PP/ST:

a) Basic: Failure to establish a session.
b) Basic: Establishment/termination of a session.

5.4 Class FMT: Security Management

5.4.1 FMT_MOF_EXT.1 External Management of Functions Behavior

The FMT_MOF family defines the ability of the TSF to manage the behavior of its own functions. FMT_MOF_EXT extends this capability by defining requirements for managing the behavior of the functions of an external IT entity. In this case, the external IT entity to be managed is an ESM Access Control product. The FMT_MOF_EXT.1 requirement has been added because CC Part 2 lacks a requirement that demonstrates the ability of the TSF to manage functions of entities that are external to the TSF.

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles
Application Note:	*The first assignment is expected to be completed with Access Control product functions that the TSF is capable of managing in addition to what is defined, if any. The second assignment is expected to be completed with one or more roles which are defined in FMT_SMR.1.*
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, [***assignment: other functions***] to [***assignment: the authorized identified roles***].

Management: FMT_MOF_EXT.1

The following actions could be considered for the management functions in FMT:

a) Specification of the external IT entity that will be configured by the TSF.

b) Configuration of the functions of the specified external entities.

Audit: FMT_MOF_EXT.1

There are no auditable events foreseen. The activities defined by this requirement are a subset of the management functions specified in FMT_SMF.1. Because of this, auditing of all management functions that are specified in FMT_SMF.1 is sufficient to address the auditing of FMT_MOF_EXT.1.

5.4.2 FMT_MSA_EXT.5 Consistent Security Attributes

The FMT_MSA family defines the ability of the TSF to manage security attributes. FMT_MSA_EXT extends this capability by defining additional requirements for how these attributes can be managed. FMT_MSA_EXT.5 requires the TSF to enforce the notion of consistent attributes. The ST author must define what constitutes inconsistent attributes and what behavior the TSF exhibits when such inconsistencies are detected. If the TSF is implemented in a manner that prevents inconsistences rather than merely detecting them, this can also be indicated. The FMT_MSA_EXT.5 requirement has been added because CC Part 2 lacks a requirement for defining inconsistent attributes and how the TSF acts to prevent or detect their use.

Hierarchical to: No other components.

Dependencies: FMT_MOF_EXT.1 External Management of Functions Behavior

FMT_MSA_EXT.5.1 The TSF shall [selection: identify the following internal inconsistencies within a policy prior to distribution: [***assignment: non-empty list of inconsistencies***], only permit definition of unambiguous policies].

Application Note: *The most common expected type of inconsistency is the case where one part of a policy allows a subject access to an object and another part denies the same subject access to the same object.*

If the TOE's policy management engine defines an unambiguous hierarchical method of implementing a policy such that no contradictions occur, the ST author indicates that no ambiguous policies can be defined. If this is the case, it is expected that the TSS or operational guidance provides an overview of how contradictory policy is prevented by the TOE.

FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: [selection: issue a prompt for an administrator to manually resolve the inconsistency, [***assignment: other action that ensures that an inconsistent policy is not implemented***]].

Application Note: *If the TOE's policy management engine defines an unambiguous hierarchical method of implementing a policy such that no contradictions occur, FMT_MSA_EXT.5.2 is vacuously satisfied as it is impossible to have inconsistencies to detect.*

Management: FMT_MSA_EXT.5

The following actions could be considered for the management functions in FMT:

a) Specification of inconsistent data to be detected or prevented by the TSF.
b) Specification of actions to be taken by the TSF when inconsistent data is detected.

Audit: FMT_MSA_EXT.5

There are no auditable events foreseen. The activities defined by this requirement are a subset of the management functions specified in FMT_SMF.1. Because of this, auditing of all management functions that are specified in FMT_SMF.1 is sufficient to address the auditing of FMT_MSA_EXT.5.

5.5 Class FPT: Protection of the TSF

5.5.1 FPT_APW_EXT Protection of Stored Credentials

Family Behavior

The requirements of this family ensure that the TSF will protect credential data from disclosure.

Component Leveling

There is only one component in this family, FPT_APW_EXT.1. FPT_APW_EXT.1, Protection of Stored Credentials, requires the TOE to store credentials in non-plaintext form and to prevent the reading of plaintext credentials.

5.5.1.1 FPT_APW_EXT.1 Protection of Stored Credentials

This SFR describes the behavior of the TOE when it must store credentials – either credentials for administrative users or credentials for enterprise users. An explicit requirement was required as there is no equivalent requirement in the Common Criteria. It was based on the requirement defined in the Network Device Protection Profile.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
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.

Management: FPT_APW_EXT.1

There are no management actions foreseen.

Audit: FPT_APW_EXT.1

There are no auditable actions foreseen.

5.5.2 FPT_SKP_EXT Protection of Secret Key Parameters

Family Behavior

The requirements of this family ensure that the TSF will protect credential data from disclosure.

Component Leveling

There is only one component in this family, FPT_SKP_EXT.1. FPT_SKP_EXT.1, Protection of Secret Key Parameters, requires the TOE to ensure that there is no mechanism for reading secret cryptographic data.

5.5.2.1 FPT_SKP_EXT.1 Protection of Secret Key Parameters

This SFR describes the behavior of the TOE when handling pre-shared, symmetric, and private keys, collectively referred to here as secret key parameters. An explicit requirement was required as there is no equivalent requirement in the Common Criteria. It was based on the requirement defined in the Network Device Protection Profile.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Management: FPT_SKP_EXT.1

There are no management actions foreseen.

Audit: FPT_SKP_EXT.1

There are no auditable actions foreseen.

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element.

6.1 TOE Security Functional Requirements

The functional requirements are summarized in Table 6 described in detail in the following subsections.

Table 6 TOE Functional Components

Functional Component	
ESM_ACD.1	Access Control Policy Definition
ESM_ACT.1	Access Control Policy Transmission
ESM_ATD.1	Object Attribute Definition
ESM_ATD.2	Subject Attribute Definition
ESM_EAU.2	Reliance on Enterprise Authentication
ESM_EID.2	Reliance on Enterprise Identification
FAU_GEN.1	Audit Data Generation
FAU_SEL_EXT.1	External Selective Audit
FAU_STG_EXT.1	External Audit Trail Storage
FCS_CKM.1	Cryptographic Key Generation (for Asymmetric Keys)
FCS_CKM_EXT.4	Cryptographic Key Zeroization
FCS_COP.1(1)	Cryptographic Operation (for Data Encryption/Decryption)
FCS_COP.1(2)	Cryptographic Operation (for Cryptographic Signature)
FCS_COP.1(3)	Cryptographic Operation (for Cryptographic Hashing)
FCS_COP.1(4)	Cryptographic Operation (for Keyed-Hash Message Authentication)
FCS_HTTPS_EXT.1	HTTPS
FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
FCS_TLS_EXT.1	TLS

Functional Component	
FIA_USB.1	User-Subject Binding
FMT_MOF.1	Management of Functions Behavior
FMT_MOF_EXT.1	External Management of Functions Behavior
FMT_MSA_EXT.5	Consistent Security Attributes
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_APW_EXT.1	Protection of Stored Credentials
FPT_SKP_EXT.1	Protection of Secret Key Parameters
FPT_STM.1	Reliable Time Stamps
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	TOE Access Banner
FTA_TSE.1	TOE Session Establishment
FTP_ITC.1	Inter-TSF Trusted Channel (Prevention of Disclosure)
FTP_TRP.1	Trusted Path

6.1.1 Class ESM: Enterprise Security Management

ESM_ACD.1 Access Control Policy Definition

Hierarchical to: No other components.

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: [*users (configured by administrators)*]; and

Objects: [*targets (configured by administrators)*]; and

Operations: [*connect to, connect from to another device (fixed in the product)*]; and

Attributes: [*Users: name, role, user group; Targets: IP address/hostname, device group, authorized access methods, authorized services, and filter lists (configured by administrators)*]

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

Dependencies: No dependencies.

ESM_ACT.1 Access Control Policy Transmission

Hierarchical to:	No other components.
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, [*when a user establishes a connection to a target (for SFA filter policies)*]].
Dependencies:	ESM_ACD.1 Access Control Policy Definition
Application Note:	*Immediate transmission applies to access control components on the PAM server.*

ESM_ATD.1 Object Attribute Definition

ESM_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual objects: [*IP address/hostname, device group, authorized access methods, authorized services, and filter lists*].
ESM_ATD.1.2	The TSF shall be able to associate security attributes with individual objects.

ESM_ATD.2 Subject Attribute Definition

Hierarchical to:	No other components.
ESM_ATD.2.1	The TSF shall maintain the following list of security attributes belonging to individual subjects: [*name, role, user group*].
ESM_ATD.2.2	The TSF shall be able to associate security attributes with individual subjects.
Dependencies:	No dependencies.

ESM_EAU.2 Reliance on Enterprise Authentication

Hierarchical to:	No other components.
ESM_EAU.2.1	The TSF shall rely on [[*PAM Server and LDAP servers*]] 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.
Dependencies:	ESM_EID.2 Reliance on Enterprise Identification
Application Note:	*The PAM Server imports credential information (and periodically checks for updates) from a configured LDAP Server. The information retrieved is cached in the PAM Server as a salted SHA-512 hash. Credentials supplied by users and validated against the cached values by PAM Server. Therefore, both the*

LDAP Server and PAM Server are relied upon for subject identification and authentication.

ESM_EID.2 Reliance on Enterprise Identification

Hierarchical to: No other components.

ESM_EID.2.1 The TSF shall rely on [[*PAM Server and LDAP servers*]] 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.

Dependencies: No dependencies.

Application Note: *The PAM Server imports credential information (and periodically checks for updates) from a configured LDAP Server. The information retrieved is cached in the PAM Server as a salted SHA-512 hash. Credentials supplied by users and validated against the cached values by PAM Server. Therefore, both the LDAP Server and PAM Server are relied upon for subject identification and authentication.*

6.1.2 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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 Table 7 for the [not specified] level of audit; *and*

c) [*no other auditable events*].

Table 7 Auditable Events

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

Component	Event	Additional Information
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
FCS_CKM.1	None	None
FCS_CKM_EXT.4	None	None
FCS_COP.1(1)	None	None
FCS_COP.1(2)	None	None
FCS_COP.1(3)	None	None
FCS_COP.1(4)	None	None
FCS_HTTPS_EXT.1	Failure to establish a session	Reason for failure
FCS_RBG_EXT.1	None	None
FCS_TLS_EXT.1	Failure to establish a session	Reason for failure
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
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
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

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*].

Dependencies: FPT_STM.1 Reliable Time Stamps

FAU_SEL_EXT.1 External Selective Audit

Hierarchical to: No other components.

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by [Secure Filter Agents] from the set of all auditable events based on the following attributes:

a) [event type]; and

b) [*no other attributes*].

Dependencies: FAU_GEN.1 Audit Data Generation

FMT_MTD.1 Management of TSF Data

FAU_STG_EXT.1 External Audit Trail Storage

Hierarchical to: No other components.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [*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.

Dependencies: FAU_GEN.1 Audit Data Generation

FTP_ITC.1 Inter-TSF Trusted Channel

6.1.3 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic Key Generation (for Asymmetric Keys)

Hierarchical to: No other components.

FCS_CKM.1.1 *Refinement:* The TSF shall generate *asymmetric* cryptographic keys *used for key establishment* in accordance with:

NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes]

and specified cryptographic key sizes [***equivalent to, or greater than, 112 bits of security***] that meet the following: [***standards defined in first selection***].

Dependencies: [FCS_CKM.2 Cryptographic Key Distribution, or

FCS_COP.1 Cryptographic Operation]

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM_EXT.4 Cryptographic Key Zeroization

Hierarchical to: No other components.

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and cryptographic security parameters when no longer required.

Dependencies: No dependencies.

FCS_COP.1(1) Cryptographic Operation (for Data Encryption/Decryption)

Hierarchical to: No other components.

FCS_COP.1.1(1) *Refinement:* The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES operating in [CBC mode]* and cryptographic key sizes *128-bits, 256-bits, and [no other key sizes]* that meets the following:

- *FIPS PUB 197, "Advanced Encryption Standard (AES)"*
- *[NIST SP 800-38A]*

Dependencies: [FDP_ITC.1 Import of User Data without Security Attributes, or

FDP_ITC.2 Import of User Data with Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

FCS_COP.1(2) Cryptographic Operation (for Cryptographic Signature)

Hierarchical to: No other components.

FCS_COP.1.1(2) *Refinement:* The TSF shall perform *cryptographic signature services* in accordance with a [

(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater]

that meets the following: [

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-3, "Digital Signature Standard"*].

Dependencies: [FDP_ITC.1 Import of User Data without Security Attributes, or

FDP_ITC.2 Import of User Data with Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

FCS_COP.1(3) Cryptographic Operation (for Cryptographic Hashing)

Hierarchical to: No other components.

FCS_COP.1.1(3) *Refinement:* The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm *[SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes*

	[160, 256, 384, 512] bits that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*
Dependencies:	[FDP_ITC.1 Import of User Data without Security Attributes, or FDP_ITC.2 Import of User Data with Security Attributes, or FCS_CKM.1 Cryptographic Key Generation] FCS_CKM.4 Cryptographic Key Destruction

FCS_COP.1(4) Cryptographic Operation (for Keyed-Hash Message Authentication)

Hierarchical to:	No other components.
FCS_COP.1.1(4)	*Refinement:* The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *HMAC-[SHA-1, SHA-256, SHA-384, SHA-512**], key size [160 bits], and message digest sizes [160, 256, 384, 512] bits* that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."*
Dependencies:	[FDP_ITC.1 Import of User Data without Security Attributes, or FDP_ITC.2 Import of User Data with Security Attributes, or FCS_CKM.1 Cryptographic Key Generation] FCS_CKM.4 Cryptographic Key Destruction

FCS_HTTPS_EXT.1 HTTPS

Hierarchical to:	No other components.
FCS_HTTPS_EXT.1.1	The TSF shall implement the HTTPS protocol that complies with RFC 2818.
FCS_HTTPS_EXT.1.2	The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.
Dependencies:	FCS_TLS_EXT.1 TLS

FCS_RBG_EXT.1 Random Bit Generation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RBG_EXT.1.1	The TSF shall perform all random bit generation (RBG) services in accordance with [*NIST Special Publication 800-90 using CTR_DRBG (AES)*] seeded by an entropy source that accumulates entropy from [*one or more independent hardware-based noise sources*].
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded with a minimum of [*256 bits*] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Application Note: *Entropy is provided by the HSM.*

FCS_TLS_EXT.1 TLS

Hierarchical to: No other components.

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
].

Dependencies: FCS_COP.1 Cryptographic Operation

6.1.4 Class FIA: Identification and Authentication

FIA_USB.1 User-Subject Binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*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 attributes must be preconfigured by administrators or logins for the user are rejected; subject attributes are assigned from the user account whose name matches the supplied web user credentials*].

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: [*subject attributes do not change during a session*].

Dependencies: FIA_ATD.1 User Attribute Definition

6.1.5 Class FMT: Security Management

FMT_MOF.1 Management of Functions Behavior

Hierarchical to: No other components.

FMT_MOF.1 The TSF shall restrict the ability to [determine the behavior of, modify the behavior of] the functions**:** [*specified in Table 8*] to [*Global Administrator*].

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

FMT_MOF_EXT.1 External Management of Functions Behavior

Hierarchical to: No other components.

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 [*Global Administrator*].

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

FMT_MSA_EXT.5 Consistent Security Attributes

Hierarchical to: No other components.

FMT_MSA_EXT.5.1 The TSF shall [identify the following internal inconsistencies within a policy prior to distribution: *conflicting user and group policies for SFAs*].

FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: [*connection attempts for a user to a target with a policy with conflicts are prohibited and an error message is displayed to the user*].

Dependencies: FMT_MOF_EXT.1 External Management of Functions Behavior

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*management functions specified in Table 8*].

Dependencies: No dependencies.

Table 8 Management Functions within the TOE

Requirement	Management Activities
ESM_ACD.1	Creation of policies
ESM_ACT.1	Transmission of policies
ESM_ATD.1	Definition of object attributes Association of attributes with objects
ESM_ATD.2	Definition of subject attributes Association of attributes with subjects
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes
FMT_MOF_EXT.1	Configuration of the behavior of other ESM products
FMT_SMR.1	Management of the users that belong to a particular role
FTA_TAB.1	Maintenance of the banner

FMT_SMR.1 Security Management Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [*Global Administrator and Standard User*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of Authentication

6.1.6 Class FPT: Protection of the TSF

FPT_APW_EXT.1 Protection of Stored Credentials

Hierarchical to:	No other components.
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.
Dependencies:	No dependencies.

FPT_SKP_EXT.1 Protection of Secret Key Parameters

Hierarchical to:	No other components.
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.
Dependencies:	No dependencies.

FPT_STM.1 Reliable Time Stamps

Hierarchical to:	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.
Dependencies:	No dependencies.

6.1.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated Termination

Hierarchical to:	No other components.
FTA_SSL.3.1	*Refinement:* The TSF shall terminate a remote interactive session after an [*Authorized Administrator-configurable time interval of session inactivity*].
Dependencies:	No dependencies.

FTA_SSL.4 User-initiated Termination

Hierarchical to:	No other components.
FTA_SSL.4.1	*Refinement:* The TSF shall allow *Administrator*-initiated termination of the *Administrato*r's own interactive session.

Dependencies: No dependencies.

FTA_TAB.1 TOE Access Banner

Hierarchical to: No other components.

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

Dependencies: No dependencies.

FTA_ TSE.1 TOE Session Establishment

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [day, time, [*remote IP address*]].

Dependencies: No dependencies.

6.1.8 Class FTP: Trusted Paths/Channels

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.

FTP_ITC.1.1 *Refinement:* The TSF shall *use [TLS] to* provide a *trusted* communication channel between itself and *authorized IT entities* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 *Refinement:* The TSF shall initiate communication via the trusted channel for *transfer of policy data*, [*communication with LDAP servers*].

Application Note: *Trusted channel communication for transfer of policy data applies to SFAs.*

Dependencies: No dependencies.

FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

FTP_TRP.1.1 *Refinement:* The TSF shall *use [TLS/HTTPS] to* provide a *trusted* communication path between itself and [remote] users that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 *Refinement:* The TSF shall require the use of the trusted path for *initial user authentication, execution of management functions*.

Dependencies: No dependencies.

6.2 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs, the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 9 TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
ESM_ACD.1	No other components.	None	n/a
ESM_ACT.1	No other components.	ESM_ACD.1	Satisfied
ESM_ATD.1	No other components.	None	n/a
ESM_ATD.2	No other components.	None	n/a
ESM_EAU.2	No other components.	ESM_EID.2	Satisfied
ESM_EID.2	No other components.	None	n/a
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_SEL_EXT.1	No other components.	FAU_GEN.1, FMT_MTD.1	Satisfied Satisfied by FMT_MOF.1
FAU_STG_EXT.1	No other components.	FAU_GEN.1, FTP_ITC.1	Satisfied Not satisfied – although FTP_ITC.1 is included in the ST, it does not address this dependency. However, this dependency only applies when sending audit records to a remote entity. This TOE "transmits" audit records to internal storage, so the dependency does not apply
FCS_CKM.1	No other components.	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	Satisfied by FCS_RBG_EXT.1 Satisfied by FCS_CKM_EXT.4
FCS_CKM_EXT.4	No other components.	None	n/a
FCS_COP.1(1)	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	Satisfied by FCS_RBG_EXT.1 Satisfied by FCS_CKM_EXT.4
FCS_COP.1(2)	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	Satisfied Satisfied by FCS_CKM_EXT.4
FCS_COP.1(3)	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	Keys are not required for hashes Satisfied by FCS_CKM_EXT.4
FCS_COP.1(4)	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	Satisfied by FCS_RBG_EXT.1 Satisfied by FCS_CKM_EXT.4

SFR	Hierarchical To	Dependency	Rationale
FCS_HTTPS_EXT.1	No other components.	FCS_TLS_EXT.1	Satisfied
FCS_RBG_EXT.1	No other components.	None	n/a
FCS_TLS_EXT.1	No other components.	FCS_COP.1	Satisfied by FCS_COP.1(1-4)
FIA_USB.1	No other components.	FIA_ATD.1	Satisfied by ESM_ATD.1 and ESM_ASTD.2 (per the PP)
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MOF_EXT.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MSA_EXT.5	No other components.	FMT_MOF_EXT.1	Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by ESM_EID.2 (per the PP)
FPT_APW_EXT.1	No other components.	None	n/a
FPT_SKP_EXT.1	No other components.	None	n/a
FPT_STM.1	No other components.	None	n/a
FTA_SSL.3	No other components.	None	n/a
FTA_SSL.4	No other components.	None	n/a
FTA_TAB.1	No other components.	None	n/a
FTA_TSE.1	No other components.	None	n/a
FTP_ITC.1	No other components.	None	n/a
FTP_TRP.1	No other components.	None	n/a

6.3 TOE Security Assurance Requirements

The assurance requirements are taken from [PM]. The assurance components are summarized in the following table:

Table 10 Assurance Requirements

Assurance Class	Component ID	Component Title
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives
	ASE_REQ.1	Security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Lifecycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

7. TOE Summary Specification

7.1 Security Functions

7.1.1 Audit

Audit records are generated for security-relevant events as specified in the following table.

Table 11 TOE Audit Events

Component	PP Required Event	Corresponding TOE Event
ESM_ACD.1	Creation or modification of policy	Transaction: admin Details: Updated Policy
ESM_ACT.1	Transmission of policy to Access Control products	Transaction: connection Details: *Target identifier*
ESM_ATD.1	Definition of object attributes	Transaction: admin Details: Device Group added successfully or Filter List added successfully
ESM_ATD.1	Association of attributes with objects	Transaction: admin Details: Device added successfully or Device updated
ESM_ATD.2	Definition of subject attributes	Transaction: admin Details: User Group added successfully
ESM_ATD.2	Association of attributes with subjects	Transaction: admin Details: User added successfully or User updated
ESM_EAU.2	All use of the authentication mechanism	Transaction: login Details: User logged in successfully or User login failed
FAU_SEL_EXT.1	All modifications to audit configuration	Transaction: admin Details: Socket Filter Configuration updated
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	
FMT_SMF.1	Use of the management functions	Transaction: admin Details: multiple
FMT_SMR.1	Modifications to the members of the management roles	Transaction: admin Details: User added successfully or User updated
FTA_SSL.3	All session termination events	Transaction: connection Details: Connection closed
FTA_SSL.4	All session termination events	Transaction: connection Details: Connection closed

Component	PP Required Event	Corresponding TOE Event
FTA_TSE.1	Denial of session establishment	Transaction: violation Details: Blocked access
FTP_ITC.1	All use of trusted channel functions	Transaction: login Details: User logged in successfully or User login failed; Transaction: connections Details: Granted access
FTP_TRP.1	All attempted uses of the trusted path functions	Transaction: login Details: User logged in successfully or User login failed; Transaction: violation Details: Blocked access

Audit records are stored on the PAM Server. The TOE does not provide any mechanism to modify audit record contents. Audit records may be automatically or manually deleted via the web GUI by administrators. Automatic purging of audit record files is normally configured to avoid exhausting storage space, and is specified in terms of how long audit records are kept. All records beyond the configured time are periodically deleted. Manual purging also specifies that all audit records up to a specified date be purged. The TOE does not provide any mechanism to delete individual audit records.

Associated SFRs: FAU_GEN.1, FAU_STG_EXT.1, FPT_STM.1

7.1.2 Credential Protection

The PAM Server imports credential information (and periodically checks for updates) from a configured LDAP Server. The information retrieved is saved locally as a salted SHA-512 hash.

Passwords input to the TOE are deleted as soon as they are forwarded to the credential server. (Note that PAM includes the capability to configure credentials for target logins, but this functionality is excluded from the evaluation and guidance directs administrators to not use this capability.)

Credentials for binding to configured LDAP servers are saved by the TOE. The password for the binding is stored in encrypted form. The TOE uses the AES encryption/decryption capability of the HSM (CMVP #1693 for Level 2) in the operational environment to perform this function.

Keys used by or on behalf of the TOE cannot be read via any TOE interfaces. No pre-shared keys, symmetric keys, or private keys are used within the TOE. Secure communication channels are established by the TOE by invoking external libraries (OpenSSL 1.01t and the OpenSSL FIPS 140-2 validated canister 2.0.9 (CMVP #1747)).

Associated SFRs: FPT_APW_EXT.1, FPT_SKP_EXT.1

7.1.3 Management

When a connection to the PAM Server web user interface is established, login credentials are collected and forwarded to an external credential server for validation. If the credentials are invalid, the session is rejected. The user account for the supplied username must also be defined

within the TOE in order to bind the configured role to the session. If the user account corresponding to the supplied credentials does not exist, the session is rejected.

Connections may be established for users (role of Standard User) and administrators (role of Global Administrator). Users (with the Standard User role) are only able to select from authorized connections to targets. Administrators (with the Global Administrator role) have that capability as well as access to the management functions for the TOE. A role does not change once it is bound to a session; if a role is modified while a session is active, it will not take effect for any active sessions.

The management functions specified in Table 8 (FMT_SMF.1) are available to Administrators and only Administrators. The management functions are performed via the web user interface GUIs.

Policies are associated with User and Device pairs, either directly or via inheritance from a User Group or Device Group. For policies pertaining to connections to targets, User policies always take precedence over User Group policies, and Device policies always take precedence over Device Group policies. Because of the strict hierarchy used by CA PAM, conflicting policies are prevented. Policies pertaining to SFAs do not have a hierarchical relationship, so conflicting policies can exist between User (direct) and Group (inherited) policies. User and Group policies are examined before deployment to SFAs. If a conflict exists, an error message is displayed and connections attempts referencing the policy are prohibited.

Associated SFRs: ESM_EID.2, ESM_EAU.2, FIA_USB.1, FMT_MOF.1, FMT_MSA_EXT.5, FMT_SMF.1, FMT_SMR.1

7.1.4 Policy Management

Administrators configure access control policies for consumption by the PAM access control components to specify the targets that users may connect to. Administrators may configure targets (objects) and users (subjects), as well as the attributes for each. Once those entities are configured administrators can configure policies to specify what users may connect to what targets and using what access mechanisms. Users and targets may also be combined into groups, and policies may then be applied to groups rather than individual entities. Policies are identified by unique names; policy versions are identified by time stamp.

The access control components on the PAM Server and the SFAs are compatible access control products. A complete Access Policy is distributed to the access control components on the PAM Server, while just the Socket Filter portion of an Access Policy is distributed to SFAs.

Policies distributed to SFAs include a parameter for whether or not audit records are generated for connections established from the Target to a remote system. This parameter is individually configurable for the Socket Filter portion of each Access Policy.

Administrators may define attributes for subjects (Users) and objects (Targets). The subject attributes that may be defined are:

- Name – specifies a unique name for the subject
- Role – associates a role with the subject
- User group – associates a user group with a subject for permission inheritance

The object attributes that may be defined are:

- IP address/hostname – associates an IP address (directly or indirectly) with each object
- Device group – associates a device group with the object for permission inheritance
- Authorized access methods – specify what access methods may be used to establish a connection to the object
- Authorized services – specify what third party services may be used to establish a connection to the object
- Filter lists – specify either allowed (white list) or disallowed (black list) actions on the objects

Policies may be configured by Administrators to control the following functions of access control components:

- Audited events – specify whether or not SFAs generate audit events for remote connections
- Repository for audit storage – the PAM Server is implicitly the audit storage location
- Access Control policy and version – the policy configured by the Administrator is communicated to the access control components; the version identifier is included in the policy
- Behavior for communication outages – the access control components are either collocated on the PAM Server or are located on Targets (SFAs). For the former, communication outages are moot. For the latter, the same communication path is used to communicate policies as to authorize connections from Users to Targets. Therefore, SFAs inherently fail in a safe mode (no new connections are established) if a communication outage occurs.

Policies are transmitted to access control components on the PAM Server when they are configured, and to the Socket Filter Agent (SFA) access control components when each target connection is established.

In order to connect via the TOE, users must first present valid credentials. The validation of the credentials is performed by the PAM Server using information retrieved from LDAP Servers and saved locally as salted SHA-512 hashes. Credentials presented by users are also hashed and compared to the saved value for the specified user. If invalid credentials are presented, the user session is rejected.

Associated SFRs: ESM_ACD.1, ESM_ACT.1, ESM_ATD.1, ESM_ATD.2, ESM_EID.2, ESM_EAU.2, FAU_SEL_EXT.1, FMT_MOF_EXT.1

7.1.5 Secure Communications

The TOE requires HTTPS/TLS to be used for all web sessions. The TOE initially receives all incoming connection requests and only TLS v1.0, v1.1 and v1.2 are allowed. The cryptographic functionality to support the TLS connections is provided by OpenSSL 1.01t and the OpenSSL FIPS 140-2 validated canister 2.0.9 (CMVP #1747). Client authentication is supported but not required.

Communication between the PAM Server and the SFAs and LDAP servers uses TLS v1.0, v1.1 or v1.2. Connections are initiated by the TOE. The cryptographic functionality to support the HTTPS connections is provided by OpenSSL 1.01t and the OpenSSL FIPS 140-2 validated canister 2.0.9 (CMVP #1747). When acting as the client, certificates are not sent for authentication purposes.

The cryptographic functions specified in FCS_CKM.1 and FCS_COP.1(*) are used during TLS session establishment for:

- Key transport
- Symmetric key generation
- Payload encryption and hashing

Associated SFRs: FTP_ITC.1, FTP_TRP.1

7.1.6 Web Session Management

Web sessions are subject to establishment restrictions that may be configured for user accounts by administrators. Restrictions may be configured for any combination of time of day, day of week, and remote IP address.

When a connection is established, a banner message configured by an administrator is displayed prior to the user initiating the authentication process. Users can terminate their own sessions, and the TOE automatically terminates inactive sessions after a configured period of time (in minutes).

Associated SFRs: FTA_SSL.3, FTA_SSL.4, FTA_TAB.1, FTA_TSE.1

7.1.7 Cryptographic Support

The TOE uses FIPS-approved cryptography that has been implemented in FIPS 140-2 validated cryptographic modules (CMVP cert #1747) for cryptographic operations involving TLS. The HSM in the operational environment is the entropy source. The PAM Server applications and services communicate directly with the HSM using software provided by SafeNet implementing a PKCS#11 API. Entropy bits generated by the HSM is passed directly to the PAM Server applications and services through the SafeNet-provided software without any processing by the operating system's random number generator functionality (e.g. /dev/random).

Cryptographic key destruction by the TOE meets the key zeroization requirements of Key Management Security Level 1 from FIPS PUB 140-2. Keys are destroyed by overwriting the keys with an alternating pattern once; the RSA keys used by the system are overwritten by zeros when the system is reset. The following table describes the key zeroization referenced by FCS_CKM_EXT.4 provided by the TOE. Note that keys maintained within the HSM are not addressed by FCS_CKM_EXT.4 and therefore are not addressed in this section.

Table 12 TOE Key Zeroization

Name	Description of Key	Storage	Destruction
TLS session symmetric key	The symmetric key is used to encrypt the payload of the TLS messages.	SDRAM (plaintext)	Automatically overwritten after the session terminates

Name	Description of Key	Storage	Destruction
RSA keys	Keys used by the overall system, in this context for TLS session establishment.	Flat file on the disk	Automatically zeroized upon system reset.

The TOE does not provide any mechanism for users to read the keys or secrets.

Note that the HSM maintains keys internally for operations it performs (such as encryption of credentials in the database). Those keys never leave the HSM so they are not addressed here.

The following certificates have been issued by the CAVP and are implemented accordingly in the TOE.

Table 13 Cryptographic Module Algorithms

Cryptographic Operations	Cryptographic Algorithim	Key Size	Standards Compliance	Certificate #
Symmetric Encryption and Decryption	AES operating in CBC	128, 256	FIPS PUB 197 (AES) NIST SP800-38A	CAVP Certificate # (3090)
Digital Signature	rDSA	2048	FIPS Pub 186-4	CAVP Certificate # (1581)
Cryptographic Hashing	SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	FIPS Pub 180-3 (SHS)	CAVP Certificate # (2553)
Keyed-Hash message authentication (HMAC)	SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384, 512	FIPS Pub 198-1 (HMAC) FIPS Pub 180-3 (SHS)	CAVP Certificate # (1937)
Random Number Generation	DRBG	256	SP 800-90 AES CTR DRBG	CAVP Certificate # (607)
Asymmetric Key Generation	RSA	2048	NIST SP800-56B	CAVP Certificate # (1581)

The RNG functionality within the TOE is provided by OpenSSL 1.0.1t and the OpenSSL FIPS 140-2 validated canister 2.0.9 (CMVP #1747). Entropy is provided by the HSM; details are provided separately.

For RSA Key Establishment, the TOE implements the following sections of SP800-56B:

- 6
- 6.1
- 6.2
- 6.3

The TOE does not perform any operation marked as “Shall Not” or “Should Not” in SP800-56B. Additionally, the TOE does not omit any operation marked as “Shall.” The following table provides further detail on SP800-56B compliance.

Table 14 SP800-56B Compliance

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
5 Cryptographic Elements	All in section	Yes	N/A
5.1 Cryptographic Hash Functions	All in section	Yes	N/A
5.2 Message Authentication Code (MAC) Algorithm	All in section	Yes	N/A
5.2.1 MacTag Computation	All in section	Yes	N/A
5.2.2 MacTag Checking	All in section	Yes	N/A
5.2.3 Implementation Validation Message	All in section	Yes	N/A
5.3 Random Bit Generation	All in section	Yes	N/A
5.4 Prime Number Generators	Only approved prime number generation methods shall be employed in this Recommendation.	Yes	N/A
5.5 Primality Testing Methods	All in section	Yes	N/A
5.6 Nonces	All in section	Yes	N/A
5.7 Symmetric Key-Wrapping Algorithms	All in section	Yes	N/A
5.8 Mask Generation Function (MGF)	All in section	Yes	N/A
5.9 Key Derivation Functions for Key Establishment Schemes	All in section	Yes	N/A
5.9.1 Concatenation Key Derivation Function (Approved Alternative 1)	All in section	Yes	N/A
5.9.2 ASN.1 Key Derivation Function (Approved Alternative 2)	All in section	Yes	N/A
6 RSA Key Pairs	All in section	Yes	N/A
6.1 General Requirements	All in section	Yes	N/A
6.2 Criteria for RSA Key Pairs for Key Establishment	All in section	Yes	N/A
6.2.1 Definition of a Key Pair	All in section	Yes	N/A
6.2.2 Formats	All in section	Yes	N/A
6.2.3 Parameter Length Sets	All in section	Yes	N/A
6.3 RSA Key Pair Generators	All in section	Yes	N/A

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
6.3.1 RSAKPG1 Family: RSA Key Pair Generation with a Fixed Public Exponent	No shall statements (def of approved key pair generator)	Yes	N/A
6.3.2 RSAKPG2 Family: RSA Key Pair Generation with a Random Public Exponent	No shall statements (def of approved key pair generator)	Yes	N/A
6.4 Assurances of Validity	All in section	Yes	N/A
6.4.1 Assurance of Key Pair Validity	All in section	Yes	N/A
6.4.2 Recipient Assurances of Public Key Validity	All in section	Yes	N/A
6.5 Assurances of Private Key Possession	All in section	Yes	N/A
6.5.1 Owner Assurance of Private Key Possession	All in section	Yes	N/A
6.5.2 Recipient Assurance of Owner's Possession of a Private Key	All in section	Yes	N/A
6.6 Key Confirmation	All in section	Yes	N/A
6.6.1 Unilateral Key Confirmation for Key Establishment Schemes	All in section	Yes	N/A
6.6.2 Bilateral Key Confirmation for Key Establishment Schemes	All in section	Yes	N/A
6.7 Authentication	All in section	Yes	N/A
7 IFC Primitives and Operations	All in section	Yes	N/A
7.1 Encryption and Decryption Primitives	All in section	Yes	N/A
7.1.1 RSAEP	All in section	Yes	N/A
7.1.2 RSADP	All in section	Yes	N/A
7.2 Encryption and Decryption Operations	All in section	Yes	N/A
7.2.1 RSA Secret Value Encapsulation (RSASVE)	All in section	Yes	N/A
7.2.2 RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP)	All in section	Yes	N/A
7.2.3 RSA-based Key-Encapsulation Mechanism with a Key-Wrapping Scheme	All in section	Yes	N/A
(RSA-KEM-KWS)	All in section	Yes	N/A
8 Key Agreement Schemes	All in section	Yes	N/A
8.1 Common Components for Key Agreement	All in section	Yes	N/A

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
8.2 The KAS1 Family	All in section	Yes	N/A
8.2.1 KAS1 Family Prerequisites	All in section	Yes	N/A
8.2.2 KAS1-basic	All in section	Yes	N/A
8.2.3 KAS1 Key Confirmation	All in section	Yes	N/A
8.2.4 KAS1 Security Properties	All in section	Yes	N/A
8.3 The KAS2 Family	All in section	Yes	N/A
8.3.1 KAS2 Family Prerequisites	All in section	Yes	N/A
8.3.2 KAS2-basic	All in section	Yes	N/A
8.3.3 KAS2 Key Confirmation	All in section	Yes	N/A
8.3.4 KAS2 Security Properties	All in section	Yes	N/A
9 IFC based Key Transport Schemes	All in section	Yes	N/A
9.1 Additional Input	All in section	Yes	N/A
9.2 KTS-OAEP Family: Key Transport Using RSA-OAEP	All in section	Yes	N/A
9.2.1 KTS-OAEP Family Prerequisites	All in section	Yes	N/A
9.2.2 Common components	All in section	Yes	N/A
9.2.3 KTS-OAEP-basic	All in section	Yes	N/A
9.2.4 KTS-OAEP Key Confirmation	All in section	Yes	N/A
9.2.5 KTS-OAEP Security Properties	All in section	Yes	N/A
9.3 KTS-KEM-KWS Family: Key Transport using RSA-KEM-KWS	All in section	Yes	N/A
9.3.1 KTS-KEM-KWS Family Prerequisites	All in section	Yes	N/A
9.3.2 Common Components of the KTS-KEM- KWS Schemes	All in section	Yes	N/A
9.3.3 KTS-KEM-KWS-basic	All in section	Yes	N/A
9.3.4 KTS-KEM-KWS Key Confirmation	All in section	Yes	N/A
9.3.5 KTS-KEM-KWS Security Properties	All in section	Yes	N/A

Associated SFRs: FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4).

7.1.7.1 HTTPS

The web user interface uses the HTTPS protocol for secure administrator communications. With respect to the TOE implementation of HTTPS, TLS version 1.2 (RFC 5246) is used to encrypt and authenticate sessions between the remote browser and TOE.

Associated SFRs: FCS_HTTPS_EXT.1

7.1.7.2 TLS

The TOE supports TLS v1.0 and v1.2 with the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA,
- TLS_RSA_WITH_AES_256_CBC_SHA,
- TLS_RSA_WITH_AES_128_CBC_SHA256,
- TLS_RSA_WITH_AES_256_CBC_SHA256.

No TLS extensions are supported.

Associated SFRs: FCS_TLS_EXT.1

8. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Section 2.3 (Protection Profile Conformance).

8.1 Protection Profile Reference

Exact conformance is claimed to the Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1, dated October 24, 2013.

8.2 Protection Profile Variations

The following variations from the PP are present in the ST:

1. T.CONTRADICT is misspelled as T.CONDTRADICT in Table 10. The threat is spelled correctly in the ST.
2. The following optional Assumptions are included: A.CRYPTO, A.ROBUST, and A.SYSTIME.
3. The following optional Objectives are included: O.ROBUST, OE.CRYPTO, OE.ROBUST, and OE.SYSTIME.
4. The following optional SFRs are included: ESM_ATD.1, ESM_ATD.2, FTA_SSL.3, FTA_SSL.4, and FTA_TSE.1.
5. FMT_MTD.1 (which is optional) is identified as a dependency of FAU_SEL_EXT.1 (which is required). Section C.5.1 of the PP states that FMT_MTD.1 should only be included if the TOE provides the ability to manage attributes that are authoritatively defined by an Identity and Credential Management product. Since the TOE does not provide this capability, the ST asserts that the dependency on FMT_MTD.1 is satisfied by FMT_MOF.1 instead.
6. The audit requirements (FAU_GEN.1) for all SFRs of the FCS class have been set to the corresponding audit requirements in the latest Network Device Protection Profile, version 1.1.

9. Mappings and Rationale

9.1 Mapping and Rationale Related to Assumptions

Table 15 Mapping and Rationale Related to Assumptions

Assumptions	Objectives	Rationale
A.CRYPTO – The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.	**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.	It is expected that vendors will typically rely on the usage of cryptographic primitives implemented in the Operational Environment to perform cryptographic protocols provided by the TOE. If the TOE provides its own cryptographic primitives, then this becomes an objective for the TOE rather than for the environment.
A.ESM – The TOE will be able to establish connectivity to other ESM products in order to share security data.	**OE.PROTECT** – One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.	If the TOE does not provide policy data to at least one Access Control product, then there is no purpose to its deployment.
A.MANAGE – There will be one or more competent individuals assigned to install, configure, and operate the TOE.	**OE.ADMIN –** There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.	Assigning specific individuals to manage the TSF provides assurance that management activities are being carried out appropriately.
	OE.INSTALL – Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	Assigning specific individuals to install the TOE provides assurance that it has been installed in a manner that is consistent with the evaluated configuration.
	OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	Ensuring that administrative personnel have been vetted and trained helps reduce the risk that they will perform malicious or careless activity.
A.ROBUST – The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.	**OE.ROBUST** – The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	The ESM deployment as a whole is expected to provide a login frustration mechanism that reduces the risk of a brute force authentication attack being used successfully against the TSF and defines allowable conditions for authentication (e.g. day, time, location). It is expected that if the TSF does not provide this mechanism, then it will receive this capability from

Assumptions	Objectives	Rationale
		elsewhere in the ESM deployment.
A.USERID – The TOE will receive validated identity data from the Operational Environment.	**OE.USERID** – The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF.	It is necessary for the TOE to receive identity data from the Operational Environment so that the TSF is able to properly enforce the consumed access control policy.

9.2 Mapping and Rationale Related to OSPs and Threats

Table 16 Mapping and Rationale Related to OSPs and Threats

OSPs and Threats	Objectives	Rationale
P.BANNER – The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	**O.BANNER –** The TOE will display an advisory warning regarding use of the TOE.	**FTA_TAB.1** The requirement for the TOE to display a banner is sufficient to ensure that this policy is implemented.
T.ADMIN_ERROR – An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	**O.MANAGE –** The TOE will provide Authentication Managers with the capability to manage the TSF.	**FAU_SEL_EXT.1** **FMT_MOF.1** **FMT_MOF_EXT.1** **FMT_SMF.1** By requiring authenticated users to have certain privileges in order to perform different management functions, the TSF can enforce separation of duties and limit the consequences of improper administrative behavior.
	OE.ADMIN – There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.	This objective requires the TOE to have designated administrators for the operation of the TOE. This provides some assurance that the TOE will be managed and configured consistently.
	OE.INSTALL – Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	This objective reduces the threat of administrative error by ensuring that the TOE is installed in a manner that is consistent with the evaluated configuration.
	OE.PERSON – Personnel working as TOE administrators shall be carefully selected and	This objective reduces the threat of administrative error by ensuring that administrators

OSPs and Threats	Objectives	Rationale
	trained for proper operation of the TOE.	have been properly vetted and trained prior to having access to the TOE.
T.CONTRADICT – A careless administrator may create a policy that contains contradictory rules for access control enforcement resulting in a security policy that does not have unambiguous enforcement rules.	**O.CONSISTENT** – The TSF will provide a mechanism to identify and rectify contradictory policy data.	**FMT_MSA_EXT.5** The ability of the TSF to detect inconsistent data and to provide the ability to correct any detected inconsistencies will ensure that only consistent policies are transmitted to Access Control products for consumption.
T.EAVES – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	**O.CRYPTO –** The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	**FCS_CKM.1** **FCS_CKM_EXT.4** **FCS_COP.1(1)** **FCS_COP.1(2)** **FCS_COP.1(3)** **FCS_COP.1(4)** **FCS_RBG_EXT.1** By providing cryptographic primitives, the TOE is able to establish and maintain trusted channels and paths.
	O.DISTRIB – The TOE will provide the ability to distribute policies to trusted IT products using secure channels.	**ESM_ACT.1** **FTP_ITC.1** The TOE will leverage cryptographic tools to generate CSPs for usage within the product and its sensitive connections. The TOE will be expected to use appropriate CSPs for the encryption, hashing, and authentication of data sent over trusted channels to remote trusted IT entities.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_HTTPS_EXT.1** **FCS_TLS_EXT.1** **FPT_SKP_EXT.1** **FTP_ITC.1** **FTP_TRP.1** Implementation of trusted channels ensures that communications are protected from eavesdropping.
	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can	If the Operational Environment is able to perform cryptographic

OSPs and Threats	Objectives	Rationale
	be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	services at the request of the TOE, the TSF is able to establish and maintain a trusted channel when needed.
T.FORGE – 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.	**O.ACCESSID** – The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.	**FTP_ITC.1** Requiring an Access Control product to provide proof of its identity prior to the establishment of a trusted channel from the TOE will reduce the risk that the TOE will disclose authentic policies to illegitimate sources. This reduces the risk of policies being examined for reconnaissance purposes.
	O.CRYPTO – The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	**FCS_CKM.1** **FCS_CKM_EXT.4** **FCS_COP.1(1)** **FCS_COP.1(2)** **FCS_COP.1(3)** **FCS_COP.1(4)** **FCS_RBG_EXT.1** By providing cryptographic primitives, the TOE is able to establish and maintain trusted channels and paths.
	O.INTEGRITY – The TOE will contain the ability to assert the integrity of policy data.	**FTP_ITC.1** Providing assurance of integrity of policy data sent to the Access Control product allows for assurance that the policy the Access Control product receives is the policy that was intended for it.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_HTTPS_EXT.1** **FCS_TLS_EXT.1** **FPT_SKP_EXT.1** **FTP_ITC.1** **FTP_TRP.1** Implementation of a trusted channel between the TOE and an Access Control product ensures that the TOE will securely assert its identity when transmitting data over this channel.

OSPs and Threats	Objectives	Rationale
	O.SELFID – The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.	**FTP_ITC.1** Requiring the TOE to provide proof of its identity prior to the establishment of a trusted channel with an Access Control product will help mitigate the risk of the Access Control product consuming a forged policy.
	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.	If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed.
T.MASK – A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.	**O.AUDIT –** The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.	**FAU_GEN.1** **FAU_STG_EXT.1** **FPT_STM.1** If security relevant events are logged and backed up, an attacker will have difficulty performing actions for which they are not accountable. This allows an appropriate authority to be able to review the recorded data and acquire information about attacks on the TOE.
T.UNAUTH – A malicious user could bypass the TOE's identification, authentication, and authorization mechanisms in order to use the TOE's management functions.	**O.AUTH** – 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.	**ESM_EAU.2** **ESM_EID.2** **FIA_USB.1** **FMT_MOF.1** **FMT_SMR.1** **FPT_APW_EXT.1** **FTA_SSL.3** **FTA_SSL.4** **FTA_TSE.1** **FTP_TRP.1** The Policy Management product is required to have its own access control policy defined to allow authorized users and disallow unauthorized users specific management functionality within the product. Doing so requires the user to be

OSPs and Threats	Objectives	Rationale
		successfully identified and authenticated and to have an established session such that the user is appropriately bound to their assigned role(s).
	O.CRYPTO – The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	**FCS_CKM.1** **FCS_CKM_EXT.4** **FCS_COP.1(1)** **FCS_COP.1(2)** **FCS_COP.1(3)** **FCS_COP.1(4)** **FCS_RBG_EXT.1** By providing cryptographic primitives, the TOE is able to establish and maintain a trusted path.
	O.MANAGE – The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.	**FAU_SEL_EXT.1** **FMT_MOF.1** **FMT_MOF_EXT.1** **FMT_SMF.1** The TOE provides the ability to manage both itself and authorized and compatible Access Control products. The management functions that are provided by the TSF are restricted to authorized administrators so they cannot be performed without appropriate authorization.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_HTTPS_EXT.1** **FCS_TLS_EXT.1** **FPT_SKP_EXT.1** **FTP_ITC.1** **FTP_TRP.1** By implementing cryptographic protocols, the TOE is able to prevent the manipulation of data in transit that could lead to unauthorized administration.
	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	If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain a trusted path when needed.

OSPs and Threats	Objectives	Rationale
	communications.	
T.WEAKIA - A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.	**O.ROBUST** - The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	**FTA_SSL.3** **FTA_SSL.4** **FTA_TSE.1** If the TOE provides session denial functionality, it rejects login attempts made during unacceptable circumstances. If the TOE performs session locking and termination due to administrator inactivity, it decreases the likelihood that an unattended session is hijacked.
	OE.ROBUST – The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	This objective helps ensure that administrative access to the TOE is robust by externally defining strength of secrets, authentication failure, and session denial functionality that is enforced by the TSF.
T.WEAKPOL – A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.	**O.POLICY** – 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.	**ESM_ACD.1** **ESM_ATD.1** **ESM_ATD.2** **FMT_MOF.1** **FMT_SMF.1** The Policy Management product must provide the ability to define access control policies that can contain the same types of access restrictions that the Access Control products which consume the policy can enforce. These policies must be restrictive by default. This will ensure that strong policies are created that use the full set of access control functions of compatible products.

9.2.1 Security Assurance Requirements Rationale

The Security Objectives for the TOE in Section 8.4.1 of the PP were constructed to address threats identified in Section 8.2. The Security Functional Requirements (SFRs) in Section 6.1 of the PP are a formal instantiation of the Security Objectives. The PP draws from the Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.