Symantec Privileged Access Manager 3.3

Security Target

Doc No: 2090-000-D102
Version: 1.8
26 May 2020

Broadcom
520 Madison Avenue
New York, New York, USA
10022

Prepared by:
EWA-Canada
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8 Acronyms, defines the acronyms used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Symantec Privileged Access Manager 3.3 Security Target
ST Version:	1.8
ST Date:	26 May 2020

1.3 TOE REFERENCE

TOE Identification:	Symantec Privileged Access Manager 3.3.0.1085

TOE Developer: Broadcom

TOE Type: Enterprise Security Management Policy Manager

1.4 TOE OVERVIEW

Symantec Privileged Access Manager (PAM) is designed to secure IT resources and facilitate compliance. The PAM appliance prevents security breaches by controlling user access to sensitive resources, enforcing security policies and monitoring and recording privileged user activity across an organization's infrastructure. 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 Web Browser User Interface (Web Browser UI) enables administrators to configure policies that control access between users and target devices. The policies deny access by default and permit access based on allow policies. The attributes for users and targets, and the policies that specify authorized connections between the configured users and targets are defined within PAM.

Users and administrators connect to the PAM Web Browser UI using Hypertext Transfer Protocol Secure (HTTPS). Credentials required to gain access to the Web Browser UI are imported from an enterprise authentication server, such as Active Directory. The credentials are saved on the PAM Server as salted SHA-512 hashes, and are used to authenticate the user. The imported credentials are periodically updated from the enterprise server. Credentials supplied by users during login are subject to the salt and SHA-512 hash operation and the result is then compared to the saved value to determine access to the Web Browser UI.

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

Administrators may also define rules to restrict access to the Web Browser UI 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 (SFAs) executing on target systems. Policies are transmitted to remote components via trusted channels.

Audit records are generated for security relevant events on the TOE and are stored locally.

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Socket Filter Agents (SFAs)	Windows Server 2016	General Purpose Computer Hardware
	Red Hat Enterprise Linux 7.6	General Purpose Computer Hardware
Authentication Server supporting LDAPv3, such as Active Directory	Windows Server 2016	General Purpose Computer Hardware

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The PAM Server provides a set of applications and services executing on a hardened Linux platform. The PAM Server is delivered pre-installed on a physical appliance. The appliance is the Lanner NCA 5210A (404L) running a 64 bit Debian 9.6 operating system, with 64GB RAM, Intel Xeon E3-1275v6 CPU with dual 240GB solid state drive (SSD) units. Logically, the PAM Server is implemented between the users and servers, mediating access between the entities. The Operational Environment is responsible for ensuring that that the protected server resources are accessible only through the PAM server.

A typical TOE deployment is shown in the following diagram.

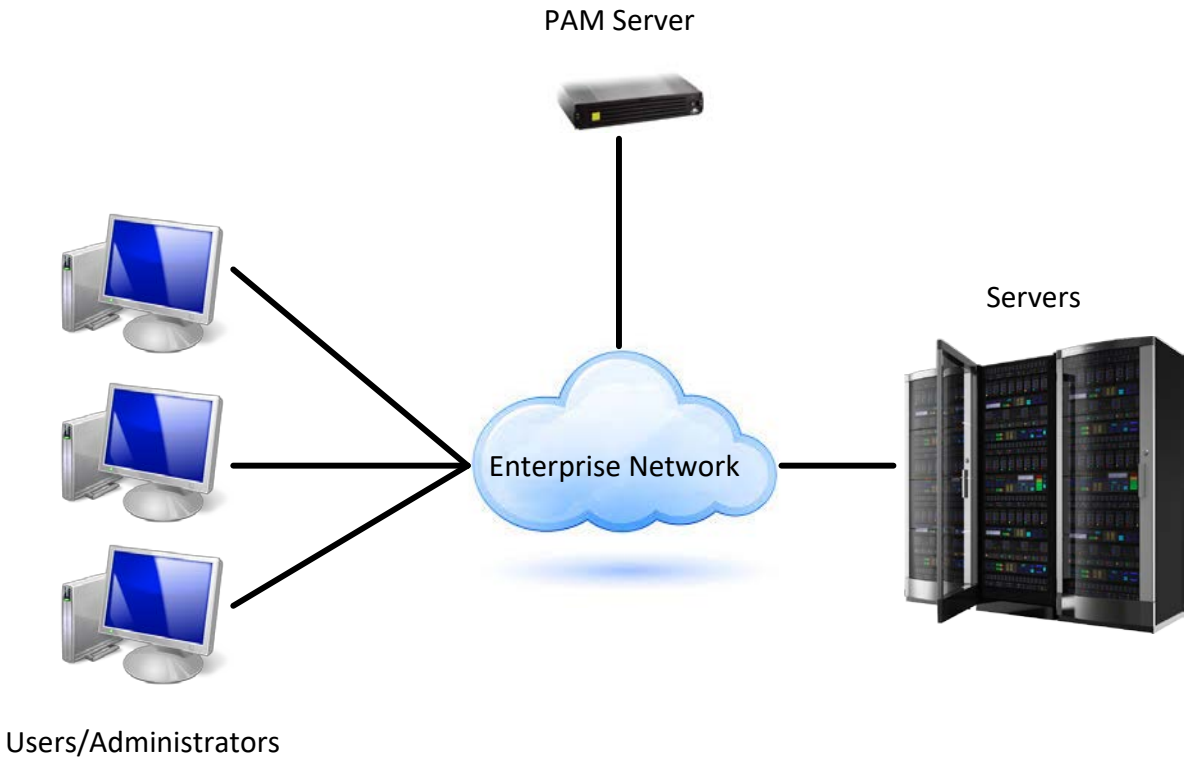

Figure 1 – TOE Diagram

1.5.1.1 TOE Delivery

The TOE is delivered as the Privileged Access Manager 404 appliance with PAM 3.3 software installed. Delivery is via trusted courier.

1.5.1.2 TOE Guidance

The TOE includes the following on line guidance documentation:

- CA Privileged Access Manager – 3.3

The documentation is available to customers at: https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/layer7-privileged-access-management/privileged-access-manager/3-3.html from the Broadcom web site.

1.5.1.3 Evaluated Configuration

The following configuration options must be applied to be in the evaluated configuration:

- FIPS mode must be enabled
- Connections to the PAM Server Web Browser UI must use HTTPS
- Credential validation for web users is performed by an external LDAP server with TLS enabled
- Credentials for targets are not configured in policies

- TOE administrators using the Web Browser UI are assigned the Global Administrator role; other users are assigned the Standard User role
- SFA Monitoring is enabled for all configured Socket Filter Agents
- 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
- Login timeouts (for inactive sessions) are not disabled

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 2 summarizes the logical scope of the TOE.

Functional Classes	Description
Enterprise Security Management	The TOE is able to define and transmit access control policies for the consumption of access control products. The TOE is able to maintain security attributes for individual objects and subjects. The TOE is able to make use of identification and authentication services provided by an enterprise server.
Security Audit	Audit entries are generated for security related events. These events are stored on the TOE. The TOE is able to select which agent events are to be audited.
Cryptographic Support	The TOE includes a Federal Information Processing Standards (FIPS)-validated cryptographic module. This module provides cryptographic support for the Transport Layer Security (TLS) functionality used to protect user connections to the TOE.
Identification and Authentication	Administrators are associated with security attributes that are used to determine access to the TOE.
Security Management	The TOE provides a means to manage the security attributes and policies that are used to determine access between subjects and resources, and to maintain the TOE configuration.
Protection of the TSF	The TOE provides a means to protect sensitive credentials and keys. The TOE provides reliable time stamps.
TOE Access	An advisory warning message banner is presented on user login. Users may terminate an administrative session. Remote interactive sessions terminate after a period of inactivity. The TOE is able to deny session establishment based on day and time.

Functional Classes	Description
Trusted Path/Channel	The communications links between the TOE and remote authorized entities and between the TOE and its remote administrators are protected using TLS.

Table 2 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Access Control and Credential Management functionality
- The optional Application-to-Application (A2A) functionality
- Redundancy via clustered servers with automatic synchronization
- Secure Sockets Layer (SSL) Virtual Private Network (VPN) Service

In the evaluated configuration, PAM is installed on a physical appliance. PAM is also available as a VMWare Open Virtual Appliance (OVA), an Amazon Machine Instance (AMI), or as an Azure Virtual Hard Disk (VHD).

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST claims exact conformance to the Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013 [ESM PM PP]. This claim satisfies the requirement of strict conformance described in Section 2.4 of the [ESM PM PP]. The following Technical Decisions have been taken into consideration:

- 0320 – TLS ciphers in ESM PPs
- 0245 – Updates to FTP_ITC and FTP_TRP for ESM PPs
- 0079 – RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
- 0071 – Use of SHA-512 in ESM PPs
- 0066 – Clarification of FAU_STG_EXT.1 Requirement in ESM PPs
- 0055 – Move FTA_TAB.1 to Selection-Based Requirement
- 0042 – Removal of Low-level Crypto Failure Audit from PPs

PAM is used to configure policy information which is sent to agents for access control enforcement. This makes the TOE an ideal candidate for claiming the [ESM PM PP].

2.3 PACKAGE CLAIM

This Security Target claims a package of Evaluation Assurance Level (EAL)1 augmented, as stated in Section 2.3 of the [ESM PM PP].

2.4 CONFORMANCE RATIONALE

The TOE claims exact conformance to the [ESM PM PP].

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 3 lists the threats addressed by the TOE. Mitigation of the threats is achieved through the instantiation of the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.CONTRADICT	A careless administrator may create a policy that contains contradictory rules for access control enforcement.
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, or authorization mechanisms in order to illicitly 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 robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

Table 3 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the TOE or the operational environment. Table 4 lists the OSP that is presumed to be imposed upon the TOE by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	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.

Table 4 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
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 identity data from the Operational Environment.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	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

Security Objective	Description
	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 or 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.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

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

Table 7 – Security Objectives for the Operational Environment

4.3 SECURITY PROBLEM DEFINITION RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.ADMIN_ERROR	T.CONTRADICT	T.EAVES	T.FORGE	T.MASK	T.UNAUTH	T.WEAKIA	T.WEAKPOL	P.BANNER	A.ESM	A.MANAGE	A.ROBUST	A.USERID
O.ACCESSID				X									
O.AUDIT					X								
O.AUTH						X							
O.BANNER									X				
O.CONSISTENT		X											
O.CRYPTO			X	X		X							
O.DISTRIB			X										
O.INTEGRITY				X									
O.MANAGE	X					X							
O.POLICY								X					
O.PROTCOMMS			X	X		X							
O.ROBUST							X						
O.SELFID				X									
OE.ADMIN	X										X		
OE.INSTALL	X										X		
OE.PERSON	X										X		
OE.PROTECT										X			
OE.ROBUST							X					X	
OE.USERID													X

Table 8 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.	
Objectives:	OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
Rationale:	If the TOE does not provide policy data to at least one Access Control product, then there is no purpose to its deployment.	

Assumption: A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.	
Objectives:	OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.
	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.
	OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
Rationale:	Assigning specific individuals to manage the TSF provides assurance that management activities are being carried out appropriately. Assigning specific individuals to install the TOE provides assurance that it has been installed in a manner that is consistent with the evaluated configuration. Ensuring that administrative personnel have been vetted and trained helps reduce the risk that they will perform malicious or careless activity.	

Assumption: 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.

Objectives:	OE.ROBUST	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
Rationale:	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 elsewhere in the ESM deployment.	

Assumption: **A.USERID**	The TOE will receive identity data from the Operational Environment.	
Objectives:	OE.USERID	The Operational Environment shall be able to identify a user requesting access to the TOE.
Rationale:	The expectation of an ESM product is that it is able to use organizationally-maintained identity data that resides in the Operational Environment.	

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE back to the OSPs applicable to the TOE.

Policy: **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.	
Objectives:	O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
Rationale:	FTA_TAB.1 The requirement for the TOE to display a banner is sufficient to ensure that this policy is implemented.	

4.3.3 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the Operational Environment back to the threats addressed by the TOE.

Threat: **T.ADMIN_**	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

ERROR		
Objectives:	O.MANAGE	The TOE will provide Authentication Managers with the capability to manage the TSF.
	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.
	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.
	OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
Rationale:	O.MANAGE FAU_SEL_EXT.1 FMT_MOF.1 FMT_MOF_EXT.1 FMT_MTD.1 (optional) 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 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 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 This objective reduces the threat of administrative error by ensuring that administrators have been properly vetted and trained prior to having access to the TOE.	

Threat: **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.	
Objectives:	O.CONSISTENT	The TSF will provide a mechanism to identify

		and rectify contradictory policy data.
Rationale:	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.	

Threat: **T.EAVES**	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	
Objectives:	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.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
Rationale:	O.CRYPTO 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 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 FCS_HTTPS_EXT.1 FCS_TLS_EXT.1 FPT_SKP_EXT.1 FTP_ITC.1	

	FTP_TRP.1 Implementation of trusted channels and paths ensures that communications are protected from eavesdropping.

Threat: **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.	
Objectives:	O.ACCESSID	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
	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.INTEGRITY	The TOE will contain the ability to assert the integrity of policy data.
	O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
	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.
Rationale:	O.ACCESSID 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 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 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 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. O.SELFID 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.

Threat: **T.MASK**	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.	
Objectives:	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.
Rationale:	O.AUDIT 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.	

Threat: **T.UNAUTH**	A malicious user could bypass the TOE's identification, authentication, and authorization mechanisms in order to use the TOE's management functions.	
Objectives:	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.CRYPTO	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
	O.MANAGE	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
	O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
Rationale:	O.AUTH ESM_EAU.2 ESM_EID.2 FIA_USB.1 FMT_MOF.1 FMT_SMR.1 FPT_APW_EXT.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 successfully identified and authenticated and to have an established session such that the user is appropriately bound to their assigned role(s). O.CRYPTO 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 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	

	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.

Threat: **T.WEAKIA**	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.	
Objectives:	O.ROBUST	The TOE will provide mechanisms to 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.
Rationale:	O.ROBUST FTA_SSL.3 FTA_SSL.4 FTA_TSE.1 If the TOE applies a strength of secrets policy to user passwords, it decreases the likelihood that an individual guess will successfully identify the password. If the TOE applies authentication failure handling, it decreases the number of individual guesses an attacker can make. 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 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.	

Threat: **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.	
Objectives:	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.
Rationale:	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.	

5 EXTENDED COMPONENTS DEFINITION

This section provides a definition for all the extended components described within the PP, and claimed within this ST.

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.

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

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

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:

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 attributes4. 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.

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 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.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]

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.

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.

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 HTTPS

Family Behavior

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

Component Leveling

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.

5.3.2.1 FCS_HTTPS_EXT.1 HTTPS

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.

Application Note: The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done by adding additional detail in the TSS.

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 Random Bit Generation

Family Behavior

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

Component Leveling

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.

5.3.3.1 FCS_RBG_EXT.1 Cryptographic Operation (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 [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 TLS

Family Behavior

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

Component Leveling

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.

5.3.4.1 FCS_TLS_EXT.1 TLS

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:

[selection:
TLS_RSA_WITH_AES_128_CBC_SHA
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
].

Application Note: *The ST author must make the appropriate selections and assignments to reflect the TLS implementation. The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.*

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_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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***].

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.*

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.*

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_APW_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.

5.6 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of CC Part 2 functional components and extended requirements, as they appear in the [ESM PM PP].

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the same manner used in the claimed protection profile. Every attempt has been made to present the Security Functional Requirements (SFRs) exactly as shown and without correction. As a result, not all operations of the same type are shown using the same conventions.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5.

Class	Identifier	Name
Enterprise Security Management (ESM)	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
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SEL_EXT.1	Selective audit
	FAU_STG_EXT.1	Protected audit trail storage
Cryptographic Support (FCS)	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)

Class	Identifier	Name
	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	Random Bit Generation
	FCS_TLS_EXT.1	TLS
Identification and Authentication (FIA)	FIA_USB.1	User-subject binding
Security Management (FMT)	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
Protection of the TSF (FPT)	FPT_APW_EXT.1	Protection of stored credentials
	FPT_SKP_EXT.1	Protection of secret key parameters
	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners
	FTA_TSE.1	TOE session establishment
Trusted path/channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

Table 9 – Summary of Security Functional Requirements

6.2.1 Enterprise Security Management

6.2.1.1 ESM_ACD.1 Access Control Policy Definition

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.

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.

6.2.1.2 ESM_ACT.1 Access Control Policy Transmission

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: [immediately following creation of a new or updated policy, [***when a user establishes a connection to a target (for SFA filter policies)***]].

6.2.1.3 ESM_ATD.1 Object Attribute Definition

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: [***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.

6.2.1.4 ESM_ATD.2 Subject Attribute Definition

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: [***name, role, user group***].

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

6.2.1.5 ESM_EAU.2 Reliance on Enterprise Authentication

Hierarchical to: No other components.

Dependencies: ESM_EID.2 Reliance on Enterprise Identification

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.

6.2.1.6 ESM_EID.2 Reliance on Enterprise Identification

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

6.2.2 Security Audit (FAU)

6.2.2.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

c) [***no other specifically defined 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

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	Failure of the key generation activity	None
FCS_CKM_EXT.4	Failure of the key zeroization process	Identity of subject requesting or causing zeroization, identity of object or entity being cleared
FCS_COP.1(1)	Failure of encryption or decryption	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted
FCS_COP.1(2)	Failure of cryptographic signature	Cryptographic mode of operation, name/identifier of object being signed/verified
FCS_COP.1(3)	Failure of hashing function	Cryptographic mode of operation, name/identifier of object being hashed
FCS_COP.1(4)	Failure in cryptographic hashing for non-data integrity	Cryptographic mode of operation, name/identifier of object being hashed
FCS_HTTPS_EXT.1	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_RBG_EXT.1	Failure of the randomization process	None
FCS_TLS_EXT.1	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
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

Table 10 – Auditable Events

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***no other audit relevant information***].

6.2.2.2 FAU_SEL_EXT.1 External selective audit

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 [***Socket Filter Agents***] from the set of all auditable events based on the following attributes:

a) [event type]; and

b) [***no other attributes***].

6.2.2.3 FAU_STG_EXT.1 External audit trail storage

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 [***TOE-internal storage***].

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

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

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

6.2.3 Cryptographic Support (FCS)

6.2.3.1 FCS_CKM.1 Cryptographic key generation (for Asymmetric Keys)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

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

- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard")*
- *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***].

6.2.3.2 FCS_CKM_EXT.4 Cryptographic key zeroization

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.3.3 FCS_COP.1(1) Cryptographic operation (for Data Encryption/Decryption)

Hierarchical to: No other components.

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.1.1(1) 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 meet the following:

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

6.2.3.4 FCS_COP.1(2) Cryptographic operation (for Cryptographic Signature)

Hierarchical to: No other components.

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.1.1(2) 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"

6.2.3.5 FCS_COP.1(3) Cryptographic operation (for Cryptographic Hashing)

Hierarchical to: No other components.

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.1.1(3) The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [*SHA-1, SHA-256, SHA-512*] *and message digest sizes [160, 256, 512] bits* that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

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

Hierarchical to: No other components.

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.1.1(4) The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *HMAC-*[*SHA-1, SHA-256*], *key size [256 bits]*, *and message digest sizes* [*160, 256*] *bits* that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."*

6.2.3.7 FCS_HTTPS_EXT.1 HTTPS

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.

6.2.3.8 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 [Hash_DRBG (SHA-256)]] seeded by an entropy source that accumulates entropy from [(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 [256 bits] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

6.2.3.9 FCS_TLS_EXT.1 TLS

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 [TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

[
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

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 user login is rejected; subject attributes are assigned from the user account with the name that matches the supplied 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***].

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of Functions Behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1 The TSF shall restrict the ability to [modify the behavior of] the functions [***functions listed in Table 11***] to [***Global Administrator***].

6.2.5.2 FMT_MOF_EXT.1 External Management of Functions Behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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, [***and no other functions***] to [***Global Administrator***].

6.2.5.3 FMT_MSA_EXT.5 Consistent security attributes

Hierarchical to: No other components.

Dependencies: FMT_MOF_EXT.1 External management of functions behavior

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: [[***prohibit connection attempts from the user to the target and display an error message to the user***]].

6.2.5.4 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [***functions listed in Table 11***].

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

Table 11 – Management Functions within the TOE

6.2.5.5 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_APW_EXT.1 Protection of stored credentials

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.

6.2.6.2 FPT_SKP_EXT.1 Protection of secret key parameters

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.6.3 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.7.2 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.7.3 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.7.4 FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [day, time, [***no other attributes***]].

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

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

points and protection of the channel data from disclosure and detection of modification of the channel data.

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

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

6.2.8.2 FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall **be capable of using [TLS, HTTPS]** to provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification, disclosure**, **and [no other types of integrity or confidentiality violations]**.

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

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

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 12.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_FSP.1	Basic functional specification
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests (ATE)	ATE_IND.1	Independent testing - Conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability survey

Table 12 – Security Assurance Requirements

6.3.1 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST are consistent with the Security Assurance Requirements listed in the claimed Protection Profile and consist of the requirements corresponding to the EAL 1 level of assurance, as defined in the CC Part 3. These assurance requirements were chosen in order to maintain consistency with the ESM PM PP.

6.4 DEPENDENCY RATIONALE

Table 13 identifies the Security Functional Requirements and their associated dependencies. The rationale for unfulfilled dependencies is described in the table.

SFR	Dependency	Dependency Satisfied	Rationale
ESM_ACD.1	None	N/A	
ESM_ACT.1	ESM_ACD.1	✓	
ESM_ATD.1	None	N/A	
ESM_ATD.2	None	N/A	
ESM_EAU.2	ESM_EID.2	✓	
ESM_EID.2	None	N/A	
FAU_GEN.1	FPT_STM.1	✓	
FAU_SEL_EXT.1	FAU_GEN.1	✓	
	FAU_MTD.1	✓	
FAU_STG_EXT.1	FAU_GEN.1	✓	
	FTP_ITC.1	✓	
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM_EXT.4	None	N/A	
FCS_COP.1(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Deemed satisfied by the PP
	FCS_CKM.4	✓	Satisfied by FCS_CKM_EXT.4

SFR	Dependency	Dependency Satisfied	Rationale
FCS_COP.1(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1
	FCS_CKM.4	✓	Satisfied by FCS_CKM_EXT.4
FCS_COP.1(3)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Deemed satisfied by the PP
	FCS_CKM.4	✓	Satisfied by FCS_CKM_EXT.4
FCS_COP.1(4)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Deemed satisfied by the PP
	FCS_CKM.4	✓	Satisfied by FCS_CKM_EXT.4
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	✓	
FCS_RBG_EXT.1	None	N/A	
FCS_TLS_EXT.1	FCS_COP.1	✓	Deemed satisfied by the PP
FIA_USB.1	FIA_ATD.1	x	This SFR is an unfulfilled dependency on FIA_USB.1. It has not been included because the ESM Policy Management product is expected to use user security attributes rather than define them. Any attributes that can be used to define policies should already be defined by a compatible Identity and Credential Management product; if not, they may be defined by the ESM_ATD components.
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MOF_EXT.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FMT_MSA_EXT.5	FMT_MOF_EXT.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	This SFR is an unfulfilled dependency on FMT_SMR.1. ESM_EID.2 satisfies this dependency by providing equivalent functionality.
FPT_APW_EXT.1	None	N/A	
FPT_SKP_EXT.1	None	N/A	
FPT_STM.1	None	N/A	
FTA_SSL.3	None	N/A	
FTA_SSL.4	None	N/A	
FTA_TAB.1	None	N/A	
FTA_TSE.1	None	N/A	
FTP_ITC.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 13 – Functional Requirement Dependencies

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 ENTERPRISE SECURITY MANAGEMENT

7.1.1 Policy Definition

The term 'Provisioning' describes the actions performed by an administrator when configuring the PAM security functionality. Provisioning Privileged Access Manager involves creating records that represent managed objects. Provisioning addresses the managed devices, their properties, and user accounts.

Administrators configure access control policies for consumption by the PAM access control components to specify the devices to which users can connect. Administrators may configure devices and users, as well as the attributes for each. Once those entities are configured administrators can configure policies to specify which users may connect to which targets, and the access mechanisms that may be used. 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 baseline-managed objects in Privileged Access Manager are devices (targets) and users. A policy is the relationship between a device (or device group) and a user (or user group). Essentially, a policy specifies what each user is permitted to do with each device. Optionally, a policy may specify whether to record all or some of the actions performed by a user on a device, permitted or otherwise.

The requirement for compatible access control products is satisfied by the access control components on the PAM server, and by the Socket Filter Agents (SFAs) described in Table 1.

Policies are identified by name and 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 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 connection attempts referencing the policy are prohibited.

TOE Security Functional Requirements addressed: ESM_ACD.1.

7.1.2 Access Control Policy

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 device to a remote system. This parameter is individually configurable for the Socket Filter portion of each Access Policy.

Administrators may define attributes for users and devices. The user attributes that may be defined are:

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

The device attributes that may be defined are:

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

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 communication path used to communicate policies is also used to authorize connections from Users to Targets. Therefore, SFAs inherently fail in a safe mode, that is no new connections are established, in the case of a communication outage.

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

TOE Security Functional Requirements addressed: ESM_ACD.1, ESM_ACT.1, ESM_ATD.1, ESM_ATD.2.

7.1.3 Enterprise Authentication

In order to connect to the Web Browser UI, users in the Standard User or Global Administrator role must first present valid credentials. 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 hashed and compared to the saved value for the specified user. If invalid credentials are presented, the user session is rejected.

TOE Security Functional Requirements addressed: ESM_EAU.2, ESM_EID.2.

7.2 SECURITY AUDIT

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

Requirement	Required Event	Corresponding TOE Auditable 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

Requirement	Required Event	Corresponding TOE Auditable Event
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	Not applicable
FCS_CKM.1	Failure of the key generation activity	Transaction: Common Details: WolfSSL JNI library failure
FCS_CKM_EXT.4	Failure of the key zeroization process	Transaction: Common Details: WolfSSL JNI library failure
FCS_COP.1(1)	Failure of encryption or decryption	Transaction: Common Details: WolfSSL JNI library failure
FCS_COP.1(2)	Failure of cryptographic signature	Transaction: Common Details: WolfSSL JNI library failure
FCS_COP.1(3)	Failure of hashing function	Transaction: Common Details: WolfSSL JNI library failure
FCS_COP.1(4)	Failure in cryptographic hashing for non-data integrity	Transaction: Common Details: WolfSSL JNI library failure
FCS_HTTPS_EXT.1	Failure to establish a session, establishment/ termination of a session	Transaction: Common Details: PAM Client session error
FCS_RBG_EXT.1	Failure of the randomization process	Transaction: Common Details: WolfSSL JNI library failure
FCS_TLS_EXT.1	Failure to establish a session, establishment/ termination of a session	Transaction: Common Details: PAM Client session error
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	Transaction: connection

Requirement	Required Event	Corresponding TOE Auditable Event
	events	Details: Connection closed
FTA_SSL.4	All session termination events	Transaction: connection Details: Connection closed
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

Table 14 – Audit Events

Audit records are stored on the PAM Server in an internal MySQL database. The TOE does not provide any mechanism to modify audit record contents. Audit records may be automatically or manually deleted via the Web Browser UI by Global Administrators. Automatic purging of audit records may be configured to avoid exhausting storage space. Records older than the configured maximum age are periodically deleted. Records may also be manually purged by requesting that all audit records up to an indicated date be deleted. The TOE does not provide a mechanism to delete individual audit records.

The events to be logged by the SFAs may be configured in the Web Browser UI by selecting Configuration > Diagnostics > UI Log and selecting the Log Level. This will determine which events are logged by the SFAs.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_SEL_EXT.1, FAU_STG_EXT.1.

7.3 CRYPTOGRAPHIC SUPPORT

The TOE includes a FIPS 140-2 validated cryptographic module, (Cryptographic Module Validation Program (CMVP) certificate # 3043). This module is called the CA Technologies C-Security Kernel, Software Version 3.11.2. Note that the FIPS validation was performed on an earlier version of the operating system and hardware. The vendor affirms that no source code changes were made to the cryptographic module prior to recompilation into the TOE software for use on the claimed 404 hardware model. The entropy source is assumed to provide 0.5 bits of entropy per one bit sample.

Cryptographic key destruction by the TOE meets the key zeroization requirements of Key Management Security Level 1 from FIPS PUB 140-2. FreeRng_fips is used to destroy Random Number Generation (RNG) Critical Security Parameters (CSPs). Other 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.

Name	Description	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
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

Table 15 – Key Zeroization Requirements

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

The following certificates have been issued by the Cryptographic Algorithm Validation Program (CAVP) and are implemented accordingly in the TOE.

Cryptographic Operation	Cryptographic Algorithm	Key Size	Standard	Certificate
Symmetric Encryption and Decryption	AES operating in CBC mode	128, 256	FIPS PUB 197 (AES) NIST SP800-38A	CAVP Certificate # 4635
Cryptographic Hashing	SHA-1, SHA-256, SHA-512	160 256 512	FIPS Pub 180-4 (SHS)	CAVP Certificate # 3799
Keyed-Hash message authentication (HMAC)	SHA-1, SHA-256	160 256	FIPS Pub 198-1 (HMAC) FIPS Pub 180-4 (SHS)	CAVP Certificate # 3068
Random Number Generation	DRBG	256	SP 800-90 FIPS Pub 180-4	CAVP Certificate # 1561
Asymmetric Key Generation	RSA	2048	FIPS 186-4 NIST SP800-56B	CAVP Certificate # 2530

Table 16 – Cryptographic Algorithms

The RNG functionality within the TOE is provided by an entropy source in the CA Technologies C-Security Kernel. The source is an approved DRBG which generates random strings whose strengths are modified by available entropy.

For RSA Key Establishment, the TOE implements Sections 6, 6.1, 6.2 and 6.3 of SP800-56B.

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.

Section	Statement	Compliance	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	All in section	Yes	N/A

Section	Statement	Compliance	Rationale
Generation Function (MGF)			
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
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	No shall statements (def of approved key pair generator)	Yes	N/A

Section	Statement	Compliance	Rationale
Public Exponent			
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

Section	Statement	Compliance	Rationale
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 (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
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	All in section	Yes	N/A

Section	Statement	Compliance	Rationale
Family			
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

Section	Statement	Compliance	Rationale
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

Table 17 – SP800-56B Compliance

TOE Security Functional Requirements addressed: 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.

7.3.1 HTTPS

The Web Browser UI 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.

TOE Security Functional Requirements addressed: FCS_HTTPS_EXT.1.

7.3.2 TLS

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

- TLS_RSA_WITH_AES_256_CBC_SHA,
- TLS_RSA_WITH_AES_128_CBC_SHA256,
- TLS_RSA_WITH_AES_256_CBC_SHA256.

The ciphersuites for the purposes shown below.

For remote administration:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

For LDAP:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

For communications with Windows SFAs:

- TLS_RSA_WITH_AES_256_CBC_SHA

For communications with Linux SFAs:

- TLS_RSA_WITH_AES_256_CBC_SHA256

The cryptographic functions required to support these ciphersuites are described in Section 6.2.3. No TLS extensions are supported. Client authentication is not implemented in the evaluated configuration.

Communication between the PAM Server and the SFAs and between the PAM Server and the LDAP server uses TLS v1.2.

TOE Security Functional Requirements addressed: FCS_TLS_EXT.1.

7.4 IDENTIFICATION AND AUTHENTICATION

Within the PAM Server, users are associated with role of Standard User or Global Administrator. A user associated with the Standard User role is only able to access and manage the remote devices which have been specifically assigned to that user. Administrators with the Global Administrator role have access to all remoted devices and the management functions for the TOE.

The role is associated with the user when the user account is created. Any change made to a user's role does not take effect while the user is bound to a session; if a role is modified while a session is active, the changes will take effect at the next user login.

Although the product supports 21 predefined roles, only the roles of Standard User and Global Administrator are used in the evaluated configuration.

TOE Security Functional Requirements addressed: FIA_USB.1, FMT_SMR.1.

7.5 SECURITY MANAGEMENT

When a connection to the PAM Server Web Browser UI 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.

The management functions specified in Table 11 are only available to users with the Global Administrator role. Management functions are performed using the Web Browser UI. The management functions provide a means to manage the functionality described in the Enterprise Security Management claims, as well as a means to manage users, roles and access, and audit configuration.

TOE Security Functional Requirements addressed: FMT_MOF.1, FMT_MOF_EXT.1, FMT_SMF.1.

7.5.1 Consistent Attributes

Policies are associated with User and Device pairs, either directly or via inheritance from a User Group or Device Group. When determining whether or

not user access to a device is permitted, User policies always take precedence over User Group policies, and Device policies always take precedence over Device Group policies. Use of this strict hierarchy prevents policy conflicts. 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.

TOE Security Functional Requirements addressed: FMT_MSA_EXT.5.

7.6 PROTECTION OF THE TSF

The PAM Server imports credential information and updates to this information from a configured LDAP Server. The information retrieved is saved locally as a salted SHA-512 hash. Local user passwords are also stored locally as a salted SHA-512 hash.

Passwords that are entered in the Web Browser UI are deleted once they are forwarded to the credential server. It may be noted that the PAM Server provides the capability to configure credentials for target device logins, but this functionality is excluded from the evaluation and guidance directs administrators to not use this functionality in the evaluated configuration.

Credentials for binding to configured LDAP servers are stored by the TOE. The password for the binding is stored in an AES-encrypted form, using the cryptographic functions described in Section 7.3.

Keys used by or on behalf of the TOE cannot be read using TOE interfaces. Ephemeral keys used in support of TLS and HTTPS are not stored. Neither pre-shared keys nor symmetric keys are stored within the TOE. Private keys are stored in an encrypted form, using the cryptographic functions described in Section 7.3. Specifically, the flat file where the private key is stored is encrypted using AES 256.

The TOE includes a system clock which provides reliable time stamps for use in the creation of audit records.

TOE Security Functional Requirements addressed: FPT_APW_EXT.1, FPT_SKP_EXT.1, FPT_STM.1.

7.7 TOE ACCESS

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 and day of week.

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.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_SSL.4, FTA_TAB.1, FTA_TSE.1.

7.8 TRUSTED PATH / CHANNELS

7.8.1 Trusted Channel

Communications between the PAM Server and the SFAs and between the PAM Server and the LDAP servers are protected using TLS v1.2. Connections are initiated by the TOE. The cryptographic functionality required to support the HTTPS connections is described in Section 7.3.

The cryptographic functions specified in Section 6.2.3 are used during TLS session establishment for:

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

TOE Security Functional Requirements addressed: FTP_ITC.1.

7.8.2 Trusted Path

HTTPS/TLS is required to protect administrative sessions using the Web Browser UI. When the remote user requests a session, the TOE ensures that only TLS v1.2 connections are permitted.

TOE Security Functional Requirements addressed: FTC_TRP.1.

8 ACRONYMS

8.1 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
A2A	Application-to-Application
AES	Advanced Encryption Standard
AMI	Amazon Machine Instance
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generation
EAL	Evaluation Assurance Level
EPUB	Electronic Publication
ESM	Enterprise Security Management
ESM PM PP	Standard Protection Profile for Enterprise Security Management Policy Management
FIPS	Federal Information Processing Standards
HMAC	Hash Message Authentication Code
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
OSP	Organizational Security Policy
OVA	VMWare Open Virtual Appliance
PAM	Privileged Access Manager
PDF	Portable Document Format

Acronym	Definition
PM	Policy Manager
PP	Protection Profile
RBG	Random Bit Generation
rDSA	RSA Digital Signature Algorithm
RNG	Random Number Generation
RSA	Rivest, Shamir and Adleman
SDRAM	Synchronous Dynamic Random Access Memory
SFA	Socket Filter Agent
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
VHD	Azure Virtual Hard Disk
VPN	Virtual Private Network

Table 18 – Acronyms