# ASSURANCE ACTIVITY REPORT

# SYMANTEC PRIVILEGED ACCESS MANAGER 3.3

**PREPARED BY**
EWA-Canada, An Intertek Company

**PREPARED FOR**
Canadian Centre for Cyber Security (CCCS) and
National Information Assurance Partnership (NIAP)

**REPORT NO**
2091-000-D008

**DOCUMENT VERSION**
Version 1.2

**DATE**
31 May 2020

# Contents

The Developer of the TOE:
CA Technologies Enterprise Software Division, Broadcom
520 Madison Avenue
New York, New York, 10022
United States of America

**Common Criteria Versions**

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012.

**Common Evaluation Methodology Versions**

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

**Protection Profiles**

- Standard Protection Profile for Enterprise Security Management Policy Management, October 24, 2013, Version 2.1

**NIAP Technical Decisions**

| ITEM | TECHNICAL DECISION TITLE |
|---|---|
| TD0042 | Removal of Low-Level Crypto Failure Audit from PPs |
| TD0055 | Move FTA_TAB.1 to Selection-Based Requirement |
| TD0066 | Clarification of FAU_STG_EXT.1 Requirement in ESM PPs |
| TD0071 | Use of SHA-512 in ESM PPs |
| TD0079 | RBG Cryptographic Transitions per NIST SP 800-131A Revision 1 |
| TD0245 | Updates to FTP_ITC and FTP_TRP for ESM PPs |
| TD0320 | TLS ciphers in ESM PPs |

**Table 1 - NIAP Technical Decisions**

# 1 Introduction

This document presents assurance activity evaluation results of the TOE evaluation. There are three types of assurance activities and the following is provided for each:

1. TOE Summary Specification (TSS) - An indication that the required information is in the TSS section of the Security Target;
2. Guidance - A specific reference to the location in the guidance is provided for the required information; and
3. Test – A summary of the test procedure used and the results obtained is provided for each required test activity.

This Assurance Activities Report contains sections for each functional class and family and sub-sections addressing each of the SFRs specified in the Security Target.

## *1.1 Evidence*

The following is a list of the documents consulted:

- [ST] - Symantec Privileged Access Manager 3.3 Security Target, Version 1.8, 26 May 2020
- [ETProcRes] – Evaluation Test Plan, Procedures and Test Results for ESM PM PP Common Criteria Evaluation of Symantec Privileged Access Manager 3.3, Version 1.6, 31 May 2020
- [EAR] - Symantec Privileged Access Manager 3.3 Entropy Documentation and Assessment, Version 1.8, 6 March 2020
- [HELP] – CA Privileged Access Manager 3.3 Online Help, Version 3.3, Published 2019
- [AGD] - Symantec Privileged Access Manager 3.3 Common Criteria Guidance Supplement, Version 1.3, 29 May 2020
- [CIL] – Symantec Privileged Access Manager 3.3 Configuration List, Version 1.9, 29 May 2020
- [ESM_PM_PP] - Standard Protection Profile for Enterprise Security Management - Policy Management, Version 2.1, October 24, 2013

# 2 Security Functional Requirement Assurance Activities (ESM_PM PP)

This section describes the assurance activities associated with the SFRs defined in the ST and the results of those activities as performed by the evaluation team. The assurance activities are extracted from the ESM PP.

## *2.1 Enterprise Security Management (ESM)*

### 2.1.1 ESM_ACD.1 Access Control Policy Definition

#### 2.1.1.1 TSS Assurance Activity

*The evaluator **shall** do the following:*

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

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

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

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

**Evaluator Assessment:**

As described in section 7.1.2 of the [ST], a complete Access Policy is distributed to the access control components on the PAM Server, while the Socket Filter portion of an Access Policy is distributed to SFAs.

The scope and granularity of the entities to define policies are described in section 7.1.2, this includes name, role, user group, IP address or hostname, device group, access method, services, and filter lists.

The compatible access control products identified in the TSS are the access control components on the PAM Server and the SFAs, this is stated in section 7.1.2.

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. This is further described in section 7.1.1.

#### 2.1.1.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

As specified in the [ST], the access control products are managed and controlled through the deployment of Socket Filter Agents (SFAs). The *Supported Environments* section of the [AGD] defines the supported platforms. The *Set a User-Device Policy* section in the [AGD] describes how access control policies are created and identified by the user and/or device (group).

#### 2.1.1.3 Tests Assurance Activity

*The evaluator **shall** test this capability by using the TOE to create a policy that uses the full range of subjects, objects, operations, and attributes and sending it to a compatible Access Control product for consumption. The evaluator will then perform actions that are mediated by the Access Control product in order to confirm that the policy was applied appropriately. The evaluator will also verify that a policy identifier is associated with a transmitted policy by querying the policy that is being implemented by the Access*

*Control product.*

**Evaluator Assessment:**

The evaluator tested the Access Control policy capability by configuring the TOE to create a policy that uses the full range of subjects, objects, operations, and attributes.

For the access control components of the PAM the policy capabilities consist of the following:

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

For the SFA access control product the policy capabilities consist of the following:

- IP address/hostname – associates an IP address (directly or indirectly) with each object;
- Device group – associates a device group with the object for permission inheritance;
- Filter lists – specify either allowed (white list) or disallowed (black list) actions on the objects.
- Name – specifies a unique name for the subject;
- Role – associates a role with the subject; and
- User group – associates a user group with a subject for permission inheritance.

These policies were sent to Linux and Windows compatible hosts for testing and verification of the policies' implementation.

### 2.1.2 ESM_ACT.1 Access Control Policy Transmission

#### 2.1.2.1 TSS Assurance Activity

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

**Evaluator Assessment:**

Policies are transmitted to access control components on the PAM Server when they are configured and to the Socket Filter Agent (SFA) access control components when each target connection is established, as described in section 7.1.2 of the [ST].

#### 2.1.2.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

The *Provision Access Policies* section in the [AGD] describes the use of SFAs to restrict access control between devices and users. It further explains how once an SFA is deployed and a user connects to a host device, the SFA downloads and enforces the policy. The *Set Up a Policy* section in the [AGD] describes how administrators create and update policies via the Web UI.

#### 2.1.2.3 Tests Assurance Activity

*The evaluator **shall** test this capability by obtaining one or more compatible Access Control products and configuring the TOE to manage them. Then, following the procedures in the operational guidance for both the TOE and the Access Control product, the evaluator **shall** create a new policy and ensure that the new policy defined in the by the TSF is successfully transmitted to, consumed by, and enforced in an Access Control product, in accordance with the circumstances defined in the SFR. In other words,*

*(a) if the selection is completed to transmit after creation of a new policy, then the evaluator **shall** create the new policy and ensure that, after a reasonable window for transmission, the new policy is installed;*

*(b) if the selection is completed to transmit periodically, the evaluator **shall** create the new policy, wait until the periodic interval has passed, and then confirm that the new policy is present in the Access Control component; or*

*(c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator **shall** create the policy, use the Secure Configuration Management component to request transmission, and the confirm that the Access Control component has received and installed the policy. If the ST author has specified "other circumstances", then a similar test **shall** be executed to confirm transmission under those circumstances.*

*The evaluator **shall** then make a change to the previously created policy and then repeat the previous procedure to ensure that the updated policy is transmitted to the Access Control component in accordance with the SFR-specified circumstances. Lastly, as updating a policy encompasses deletion of a policy, the evaluator shall repeat the process a third time, this time deleting the policy to ensure it is removed as an active policy from the Access Control component.*

*The evaluator **shall** repeat this test for a representative sample of Access Control products that can be managed by the TOE. For example, if the TOE provides the ability to manage groups of host-based access control endpoints, the evaluator shall create different groups such that each supported platform is included in at least one group and verify that group members will appropriately consume policies when instructed to do so.*

*Note: This testing will likely be performed in conjunction with the testing of ESM_ACD.1.*

**Evaluator Assessment:**

The evaluator obtained the PAM as well as the Windows and Linux versions of the Socket Filter Agent (SFA). The evaluator followed the guidance to install and configure the PAM to manage the SFAs.

The evaluator then transmitted policies to two different and compatible hosts. These policies were then verified to be enforced. Next the policies were modified and verified to have been transmitted and consumed by the target. When policies were deleted they were no longer applied.

The evaluator verified that the PAM policy was consumed immediately after it was created.

The evaluator verified that the SFA policy was applied when the user associated with the SFA policy accessed the device associated with the SFA policy.

The evaluator used both user groups and device groups and verified that the policies were applied to individual users and devices within the policy groups.

### 2.1.3 ESM_EAU.2 Reliance on Enterprise Authentication

#### 2.1.3.1 TSS Assurance Activity

*The evaluator **shall** check the TSS in order to determine that it describes the TSF as requiring authentication to use and that it describes, for each type of user or IT entity that authenticates to the TOE, the identification and authentication mechanism that is used. The evaluator **shall** also check to ensure that this information is appropriately represented by iterating the SFR for each authentication mechanism that is used by the TSF.*

**Evaluator Assessment:**

Web user authentication is performed by the PAM Server using information retrieved from external 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. This is described in section 7.1.3 of the [ST].

Credentials for binding to configured LDAP servers are stored by the TOE. The password for the binding is stored in an encrypted form, as described in 7.6 of the [ST].

The SFR is represented appropriately.

#### 2.1.3.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

The *How to How to Set up LDAP Servers for User Authentication* section in the [AGD] describes how to configure LDAP devices for providing user authentication. This section further describes the requirement for the administrator to provide valid credentials for the LDAP server in order to connect to the service.

#### 2.1.3.3 Tests Assurance Activity

*The evaluator **shall** test this capability by accessing the TOE without having provided valid identification and authentication information and observe that access to the TSF is subsequently denied. If any IT entities authenticate to the TOE, the evaluator **shall** instruct these IT entities to provide invalid identification and authentication information and observe that they are not able to access the TSF.*

*Note that positive testing of the identification and authentication is assumed to be tested by other requirements because successful authentication is a prerequisite to manage the TSF (and possibly for the TSF to interact with external IT entities).*

**Evaluator Assessment:**

The evaluator tested the authentication capability by configuring the PAM to use an Active Directory Server LDAP connection. Then the evaluator provided an invalid user password and observed that access was denied and then provided a valid user password and observed that access was granted. A second test was performed by first removing the LDAP server certificate for the domain thus invalidating any authentication attempts. The evaluator verified that the TOE could not connect to the LDAP server to validate the user credentials and denied access to the user.

### 2.1.4 ESM_EID.2 Reliance on Enterprise Identification

#### 2.1.4.1 Assurance Activities

*This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.*

**Evaluator Assessment:**

N/A

## *2.2 Security Audit (FAU)*

### 2.2.1 FAU_GEN.1 Audit Data Generation

#### 2.2.1.1 TSS Assurance Activity

*The evaluator **shall** check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records.*

**Evaluator Assessment:**

The auditable events and the audit record contents are summarized in section 7.2 of the [ST], under Table 14 - Audit Events.

#### 2.2.1.2 Guidance Documentation Assurance Activity

*The evaluator **shall** check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record. Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator **shall** check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.*

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

**Evaluator Assessment:**

The *Messages and Log Formats* and *Logging and Reporting Messages* sections in the [AGD] provide a list of auditable events, the associated formats, and a description of the event contents for each audit record.

As per section 1.5 of the [AGD], each audit record may contain the following information: Address, Applet, Date, Time, Details, Device, Device Groups, NAT/Proxy IP, Port, Service, Source IP, Transaction, User Groups, Username.

Only the information appropriate for the record will be included.

#### 2.2.1.3 Tests Assurance Activity

*The evaluator **shall** test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator **shall** then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST.*

*This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator **shall** also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly identify the policy that was defined.*

**Evaluator Assessment:**

Testing of all audit events defined in the ST was performed during the course of the evaluation test plan. All audit components, the event(s), and audit results were compiled in a table located in the evaluator independent test plan [ETProcRes].

### 2.2.2 FAU_SEL_EXT.1 All modifications to audit configuration

#### 2.2.2.1 TSS Assurance Activity

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

**Evaluator Assessment:**

Policies distributed to SFAs include a parameter for whether or not audit records are generated for connections established from the Target to a remote system. The events to be logged by the SFAs may be configured in the Web Browser UI by selecting the Log Level, as described in section 7.2 of the [ST].

#### 2.2.2.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

The *Configure Diagnostic Logs* section in the [AGD] defines the selections for auditable events. Administrators can configure the information being collected by setting the log levels. This is consistent with the description provided in section 7.2 of the [ST].

#### 2.2.2.3 Tests Assurance Activity

*The evaluator **shall** test this capability by configuring a compatible Access Control product to have:*

*- All selectable auditable events enabled*

*- All selectable auditable events disabled*

*- Some selectable auditable events enabled*

*For each of these configurations, the evaluator **shall** perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded by the Access Control product.*

*If this SFR is iterated, the evaluator **shall** repeat these activities for each iteration of the* SFR, substituting the appropriate external entity for "Access Control product" where appropriate.

**Evaluator Assessment:**

By default, logging of third-party access from the target machines is disabled. Following the guidance, the evaluator was able to turn on and off the monitoring of the SFAs. When the monitoring was on, success events for SFAs were auditable and when it was off, the success events for the SFAs did not appear in the

audit log. The option to log only log whitelist or blacklist policies was also examined, satisfying the some selectable auditable events requirement.

### 2.2.3 FAU_STG_EXT.1 Establishment and disestablishment of communications with audit server

#### 2.2.3.1 TSS Assurance Activity

*The evaluator **shall** check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit.*

**Evaluator Assessment:**

Audit records are stored on the PAM Server in an internal MySQL database, as described in section 7.2 of the [ST].

#### 2.2.3.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

The TOE does not communicate with an external repository for audit storage in the evaluated configuration. Therefore, this assurance activity requirement is considered satisfied.

#### 2.2.3.3 Tests Assurance Activity

*The evaluator **shall** test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit storage contain identical data. The evaluator **shall** also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one.*

**Evaluator Assessment:**

The evaluator verified that the audit log was stored locally on the PAM Server. The evaluator was able to save the log file to an external source and then verified that the contents were consistent with the local log store. Two sets of logs are required and can be downloaded individually; session logs and SPFD logs.

## *2.3 Identification and Authentication (FIA)*

### 2.3.1 FIA_USB.1 User-Subject Binding

#### 2.3.1.1 TSS Assurance Activity

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

**Evaluator Assessment:**

As per section 7.4 in the [ST], users are associated with the 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. Administrators with the Global Administrator role have access to all remote 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.

#### 2.3.1.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

The *Import LDAP User Groups* section in the [AGD] specifies that access to the TOE is defined by the LDAP group that the user belongs. The LDAP group member is assigned permissions on the TOE. Upon TOE login, the LDAP user's group is verified and the appropriate permissions are assigned for that session.

#### 2.3.1.3 Tests Assurance Activity

*The evaluator **shall** test this capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator **shall** then perform authentication activities using these methods and validate that authentication is successful in each instance. Based on the defined privileges assigned to each of the subjects, the evaluator **shall** then perform various management tests in order to determine that the user authorizations are consistent with their externally-defined attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to policy information, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF that they do not have write access to policy information. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and used in order to determine what the user is able to do.*

**Evaluator Assessment:**

The Evaluator used an Active Directory server to create a standard user group and an admin group. Using the guidance, the evaluator imported the groups to the TOE and associated the admin group with the global administrator role, and the standard user group with the standard user role. The evaluator then created a user on the Active Directory server and made it a member of the standard user group. The evaluator logged in as the user and verified the standard user permissions were granted. The evaluator then removed the user from the standard user group and made it a member of the admin group. The evaluator logged in and verified that the user had global administrator permissions.

The evaluator verified that a user can be moved from one group to another and inherit the rights granted with the new group assignment.

## *2.4 Security Management (FMT)*

### 2.4.1 FMT_MOF.1 Management of Functions Behavior

#### 2.4.1.1 TSS Assurance Activity

*The evaluator **shall** check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator **shall** also check the TSS to see that it describes the ability of the TSF to perform the required management functions and the authorizations that are required to do this.*

**Evaluator Assessment:**

As per section 7.5 of the [ST], the management functions specified in Table 11 are only available to users with the Global Administrator role, and are performed using the Web Browser UI.

#### 2.4.1.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

Management authority for the TOE is role-based, as specified in the *Configure Users* section of the [AGD]. The *Privileges and Roles* subsection in the [AGD] section further describes each predefined role and the access permissions for each.

#### 2.4.1.3 Tests Assurance Activity

*The evaluator **shall** test this function by accessing the TSF using one or more appropriately privileged administrative accounts and determining that the management functions as described in the ST and operational guidance can be managed in a manner that is consistent with any instructions provided in the operational guidance. If the TSF can be configured by an authorized and compatible Secure Configuration Management product, the evaluator **shall** also configure such a product to manage the TSF and use this product to perform the defined management activities. In addition, any access restrictions to this behavior should be enforced in a manner that is consistent with the relevant documentation. The evaluator **shall** test this by attempting to perform a sampling of the available management functions using one or more unprivileged accounts to observe that the activities are rejected or unavailable.*

**Evaluator Assessment:**

Using the operational guidance, the evaluator assumed the role of global administrator and verified being able to perform the following management functions as defined in the [ST]:

- Creation of policies
- Transmission of Policies
- Definition of object attributes
- Association of attributes with objects
- Definition of subject attributes
- Association of attributes with subjects
- Configuration of auditable events for defined external entities
- Definition and modification of default subject security attributes
- Configuration of the behavior of other ESM products
- Management of the users that belong to a particular role
- Maintenance of the banner

### 2.4.2 FMT_MOF_EXT.1 External Management of Functions Behavior

#### 2.4.2.1 TSS Assurance Activity

*The evaluator **shall** check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator **shall** also check the TSS to see that it summarizes the Access Control product functions that the TOE is able to manage and the authorizations that are required in order to manage these functions.*

**Evaluator Assessment:**

The assignments in the SFR were completed in a manner that is consistent with the guidance provided by the application note(s).

Section 7.5 in the [ST] specifies that only users with a Global Administrator role have the ability to manage the access control product functions. The specific functions are identified in Table 11 – Management Functions within the TOE.

#### 2.4.2.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

Section 1.2 of the [AGD] specifies that administrators using the web interface are configured with the Global Administrator role. Access to the control products is performed through the SFAs. Under Configure Users in the [AGD], subsection *Privileges and Roles* describes the privileges associated with the Global Administrator role required to perform the management functions for these connections.

#### 2.4.2.3 Tests Assurance Activity

*The evaluator **shall** test this capability by deploying the TOE in an environment where there is an Access Control component that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator **shall** use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator shall verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification.*

*The evaluator **shall** also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities:*

*- Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior*

*- Repository for audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository*

*- Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP authorization differs from the original iteration of the SFP.*

*- Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP.*

*- Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied.*

*Once this has been done, the evaluator **shall** reconfigure the TOE so that it is no longer authorized to manage the Access Control product. The evaluator shall then attempt to perform management functions using the TOE and observe that this is either disallowed or that the option is not even present.*

**Evaluator Assessment:**

Modification of the selective audit functionality was performed in FAU_SEL including the verification of audit events being recorded or not based on the configuration of the access control product.

The TOE implements an internal audit storage, of which the administrator can download logs from over the secure HTTPS connection. This is covered in FAU_STG_EXT.1.

Performing actions which are allowed and disallowed by both the Access Control product & TSF Policy is performed in ESM_ACD.1.

The evaluator configured a policy that does not permit a user to access a device if the SFA is not running. The SFA was disabled and the user attempted to login and failed.

### 2.4.3 FMT_MSA_EXT.5 Consistent Security Attributes

#### 2.4.3.1 TSS Assurance Activity

*The evaluator **shall** review the TSS and in order to determine that it explains what potential contradictions in policy data may exist. For example, a policy could potentially contain two rules that permit and forbid the same subject from accessing the same object. Alternatively, the TOE may define an unambiguous hierarchy that makes it impossible for contradictions to occur. If the TOE does not allow contradictory policy to exist, the evaluator shall verify that this assertion has been made in the TSS and that justification is provided to support the assertion.*

**Evaluator Assessment:**

The policies applied by the PAM access control use a “deny all, allow by exception” model, with a hierarchal relationship with User policies taking priority over Group policies. This eliminates the potential for inconsistent policies, as explained in section 7.5.1.

The [ST] further specifies in section 7.5.1 that the policies applied to the 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.

#### 2.4.3.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

As stated in section 1.3 of the [AGD], 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 Symantec 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, connection attempts referencing the policy are prohibited and the following error message is displayed to the user:

Message 20: Error occurred while trying to complete request

#### 2.4.3.3 Tests Assurance Activity

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

**Evaluator Assessment:**

The evaluator conducted this test by creating a user-defined blacklist policy and group-defined whitelist policy for access to the same device. The user was then added to the user group and access to the device was examined. The user was denied access to the device and presented with an error message identifying the policy conflict.

### 2.4.4 FMT_SMF.1 Specification of Management Functions

#### 2.4.4.1 TSS Assurance Activity

*The evaluator **shall** check the TSS in order to determine that it summarizes the management functions that are available.*

**Evaluator Assessment:**

Section 7.5 of the [ST] references Table 11 - Management Functions Within the TOE, as a summary of the available management functions.

#### 2.4.4.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

The [AGD] specifies all management functions and how to perform them. As per Table 11 in the [ST], the following management functions are relevant:

- ESM_ACD.1 (Creation of Policies) – The *Set a User-Device Policy* section in the [AGD] describes how access control policies are created and identified by the user and/or device (group).

- ESM_ACT.1 (Transmission of Policies) – The *Set Up a Policy* section in the [AGD] describes how administrators create and update policies via the Web UI.

- ESM_ATD.1 (Definition of/Association with object attributes) – The *Device Setup* section of the [AGD] specifies how to define and configure the device IP address/hostname, Authorized Access Methods, and Authorized Services. The *Device Group Setup* section specifies how to define and

configure device groups for permission inheritance. The *Set up Command Filter Lists (CFL)* section of the [AGD] specifies how to define and configure white list and black list commands.

- ESM_ATD.2 (Definition of/Association with subject attributes) – The *Configure Users* section of the [AGD] provides instructions on how to define and configure the user attributes Name, Role, and User group.

- FAU_SEL_EXT.1 (Configuration of auditable events for external entities) – The *Configure Diagnostic Logs* section in the [AGD] defines the selections for auditable events. Administrators can configure the information being collected by setting the log levels. This is consistent with the description provided in section 7.2 of the [ST].

- FIA_USB.1 (Definition/Modification of subject security attributes) – The *Import LDAP User Groups* section in the [AGD] specifies that access to the TOE is defined by the LDAP group that the user belongs. The LDAP group member is assigned permissions on the TOE. Upon TOE login, the LDAP user's group is verified and the appropriate permissions are assigned for that session.

- FMT_MOF_EXT.1 (Configuration of the behavior of other ESM products) – Section 1.2 of the [AGD] specifies that administrators using the web interface are configured with the Global Administrator role. Access to the control products is performed through the SFAs. Under Configure Users in the [AGD], subsection *Privileges and Roles* describes the privileges associated with the Global Administrator role required to perform the management functions for these connections.

- FMT_SMR.1 (Management of users/roles) – Section 2.2 of the [AGD] provides instructions on how to assign LDAP users to groups and roles. The *Configure Users* section of the [AGD] provides additional instructions on how to manage user accounts, privileges, groups, and roles.

- FTA_TAB.1 (Maintenance of the banner) – The *Warnings* subsection of the *Apply Global Settings* section in the [AGD] describes how to configure the TOE banner. Under the Warnings tab in the Web UI, administrators can configure the TOE banner to be displayed at the user login page.

#### 2.4.4.3 Tests Assurance Activity

*The evaluator **shall** test this capability by accessing the TOE and verifying that all of the defined management functions exist, that they can be performed in the prescribed manner, and that they and accomplish the documented capability.*

**Evaluator Assessment:**

The evaluator exercised all management functions as specified by FMT_SMF.1 as part of overall product testing. Since each management function could be mapped to a relevant test case exercising such functionality, and all tests passed, the evaluator concluded that all of the management functions must exist, can be performed, and that they accomplish the documented capability.

### 2.4.5 FMT_SMR.1 Security Management Roles

#### 2.4.5.1 TSS Assurance Activity

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

**Evaluator Assessment:**

As per section 7.4 in the [ST], only the roles of Standard User and Global Administrator are used in the evaluated configuration. These roles are consistently reference throughout the ST when discussing how management authorizations are determined.

#### 2.4.5.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

Section 2.2 of the [AGD] provides instructions on how to assign LDAP users to groups and roles. The *Configure Users* section of the [AGD] provides additional instructions on how to manage user accounts, privileges, groups, and roles.

#### 2.4.5.3 Tests Assurance Activity

*The evaluator **shall** test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles. If the TSF provides the capability to define additional roles, the evaluator **shall** create at least one new role and ensure that a user can be assigned to it. Since other assurance activities for management requirements involve the evaluator assuming different roles on the TOE, it is possible that these testing activities will be addressed in the course of performing these other assurance activities.*

**Evaluator Assessment:**

The evaluator tested this capability for both local and LDAP users. For local users, the evaluator toggled between assigning the standard user and global administrator roles, and then verified the access/management permissions by logging into the TOE.

For LDAP users, the test environment setup included two LDAP groups (standard user and admin) each assigned the standard user and global administrator role, respectively. The evaluator toggled between assigning an LDAP user to either group, and then verified the access/management permissions by logging into the TOE.

## *2.5 Protection of the TSF (FPT)*

### 2.5.1 FPT_APW_EXT.1 Protection of Stored Credentials

#### 2.5.1.1 TSS Assurance Activity

*The evaluator **shall** examine the TSS to determine that it details all authentication data, other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the*

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

**Evaluator Assessment:**

As described in section 7.6 of the [ST], credentials for binding to configured LDAP servers are saved by the TOE. The password for binding is stored in encrypted form (AES). As further described in section 7.6 of the [ST], PAM user credentials (local and LDAP) are saved locally as salted SHA-512 hashes.

The TOE uses the AES encryption/decryption (CAVP certificate # 4635) and hashing (CAVP certificate # 3799) capabilities in the CA Technologies C-Security Kernel cryptographic module (CMVP certificate #3043) to perform these functions.

#### 2.5.1.2 Guidance Documentation Assurance Activity

*None. There are no operational guidance activities for this SFR.*

**Evaluator Assessment:**

N/A

#### 2.5.1.3 Tests Assurance Activity

*The evaluator **shall** test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator **shall** similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.*

**Evaluator Assessment:**

The developer provided sufficient evidence of stored passwords being encrypted in the MySQL database. As indicated in the evidence, LDAP binding credentials are encrypted using AES and stored in the "target account" database table. User account credentials (local and LDAP) are saved locally as salted SHA-512 hashes and stored in the "PAM users" database table.

### 2.5.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

#### 2.5.2.1 TSS Assurance Activity

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

**Evaluator Assessment:**

As stated in section 7.6 of the [ST], cryptographic keys used by or on behalf of the TOE cannot be read via any 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 a flat file on disk and encrypted using AES 256.

#### 2.5.2.2 Guidance Documentation Assurance Activity

*None. There are no operational guidance or testing activities for this SFR.*

**Evaluator Assessment:**

N/A

#### 2.5.2.3 Tests Assurance Activity

*None. There are no operational guidance or testing activities for this SFR.*

**Evaluator Assessment:**

N/A

## *2.6 Toe Access (FTA)*

### 2.6.1 FTA_TAB.1 TOE Access Banner

#### 2.6.1.1 TSS Assurance Activity

*The evaluator **shall** check the TSS in order to determine that it discusses the ability of the TSF to display a configurable banner prior to administrator authentication.*

**Evaluator Assessment:**

Section 7.7 in the [ST] discusses the TOEs ability to display a configurable banner message to users prior to initiating the authentication process.

#### 2.6.1.2 Guidance Documentation Assurance Activity

*The evaluator **shall** review the operational guidance to determine how the TOE banner is displayed and configured.*

**Evaluator Assessment:**

The *Warnings* subsection of the *Apply Global Settings* section in the [AGD] describes how to configure the TOE banner. Under the Warnings tab in the Web UI, administrators can configure the TOE banner to be displayed at the user login page.

#### 2.6.1.3 Tests Assurance Activity

*If the banner is not displayed by default, the evaluator **shall** configure the TOE in accordance with the operational guidance in order to enable its display. The evaluator **shall** then attempt to access the TOE and verify that a TOE banner exists. If applicable, the evaluator will also attempt to use the functionality to modify the TOE access banner as per the standards defined in FMT_SMF.1 and verify that the TOE access banner is appropriately updated.*

**Evaluator Assessment:**

The evaluator first enabled the use of a banner page then entered the text to be displayed. At the login screen the TOE properly displayed the new banner text.

## *2.7 Trusted Paths/Channels (FTP)*

### 2.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

#### 2.7.1.1 TSS Assurance Activity

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

**Evaluator Assessment:**

Communication between the PAM Server and the SFAs and between the PAM Server and the LDAP server uses TLSv1.2 as described in section 7.8.1. The protocol listed in the TSS (TLSv1.2) is included in the requirements.

#### 2.7.1.2 Guidance Documentation Assurance Activity

*The evaluator **shall** confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.*

**Evaluator Assessment:**

Section 2.2 of the [AGD] specifies the “Use TLS (LDAPv3 Only)” option for establishing the allowed TLS protocol between the TOE and the LDAP server.

#### 2.7.1.3 Tests Assurance Activity

*The evaluator **shall** perform the following tests:*

*Test 1: The evaluators **shall** ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.*

*Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator **shall** follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities.*

*Test 3: The evaluator **shall** ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.*

*Test 4: The evaluators **shall** ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted[HD1] [MS2] . The evaluator **shall** then ensure that when physical connectivity is restored, communications are appropriately protected.*

*Further assurance activities are associated with the specific protocols.*

*For distributed TOEs, the evaluator **shall** perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.*

**Evaluator Assessments:**

The evaluator triggered communications between the PAM server and the LDAP server (LDAP group Refresh), and between the PAM server and the SFAs (connecting to the target devices). Using a packet capture tool, the evaluator verified the use of TLSv1.2 for all communication paths.

The evaluator then used a packet modification tool to perform a man-in-the-middle attack whereby manipulating/changing the traffic being passed between the PAM server and the LDAP server, and between the PAM server and the SFAs. Using a packet capture tool, and analyzing the TOE behavior, the

evaluator verified that the TOE detected the packet modifications and dropped all connections with the target devices when detected.

### 2.7.2 FTP_TRP.1 Trusted Path

*The evaluator shall repeat the assurance activity for FTP_ITC.1 for each interface and cryptographic protocol that is provided by the TOE for remote administration.*

#### 2.7.2.1 TSS Assurance Activity

*The evaluator **shall** check the TSS to ensure that it identifies the protocol(s) used to establish the trusted path and ensure they are consistent with those declared in the ST. In addition, the evaluator **shall** ensure that the TSS adequately describes the way the trusted communication path is protected.*

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

**Evaluator Assessment:**

As per section 7.8.2 in the [ST], 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. The protocol listed in the TSS (TLSv1.2) is consistent with the requirements.

#### 2.7.2.2 Guidance Documentation Assurance Activity

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

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

**Evaluator Assessment:**

The *Use the UI to Configure the Network Connections* section of the [AGD] specifies that the TOE appliance is shipped with a static IP address and that users can establish an HTTPS session by navigating to https://192.168.98.100/config/ to perform the initial configuration of the TOE. Section 2.2 (Step 4a) of the [AGD] specifies that once configured, users can access the Web UI by navigating to the configured URL (https://ipaddress).

For the purpose of the evaluation, the evaluator used the default IP address (192.168.98.100) for Web UI access.

#### 2.7.2.3 Tests Assurance Activity

*The evaluator **shall** perform the following set of tests and where applicable, repeat for each remote administration method:*

*Test 1: The evaluator **shall** ensure that communications using each protocol with each authorized IT entity, including each remote administration method, is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.*

*Test 2: For communications using each protocol with each authorized IT entity and method of remote administration supported, the evaluator **shall** follow the guidance documentation to ensure that there is no available interface that can be used by a remote user to establish a remote administrative session without invoking the trusted path.*

*Test 3: The evaluator **shall** ensure that for communications of each protocol with each authorized IT entity, and for each method of remote administration, the channel data is not sent in plaintext.*

*Test 4: The evaluators **shall** ensure that, for each protocol and remote administration method combination tested during Test 1, the connection is physically interrupted. The evaluator **shall** then ensure that when physical connectivity is restored, communications are appropriately protected.*

*For distributed TOEs, regardless of the tests performed, the evaluator **shall** perform tests on all TOE components according to the mapping of trusted paths to TOE components in the Security Target.*

*Assurance Activity Note: If data transmitted between the user and the TOE is obfuscated, the trusted path can be assumed to have been established.*

**Evaluator Assessment:**

The evaluator triggered communications between the PAM server and the remote administrator (i.e. logged into the web GUI). Using a packet capture tool, the evaluator verified the use of TLSv1.2 for this communication path.

The evaluator then used a packet modification tool to perform a man-in-the-middle attack whereby manipulating/changing the traffic being passed between the PAM server and the remote workstation. Using a packet capture tool, and analyzing the TOE behavior, the evaluator verified that the TOE detected the packet modification and dropped the connection with the remote administrator as expected.

# 3 Evaluation Activities for Optional Requirements (ESM_PM PP)

## *3.1 Enterprise Security Management (ESM)*

### 3.1.1 ESM_ATD.1 Object Attribute Definition

#### 3.1.1.1 TSS Assurance Activity

*The evaluator **shall** check the TSS to ensure that it describes the object attributes that are defined by the TOE and the purpose for their definition.*

**Evaluator Assessment:**

The object attributes that may be defined by the TOE are described in section 7.1.2 of the [ST], as follows:

- 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

#### 3.1.1.2 Guidance Documentation Assurance Activity

*The evaluator **shall** check the operational guidance to ensure that it provides instructions on how to define and configure the object attributes.*

**Evaluator Assessment:**

The *Device Setup* section of the [AGD] specifies how to define and configure the device IP address/hostname, Authorized Access Methods, and Authorized Services. The *Device Group Setup* section specifies how to define and configure device groups for permission inheritance. The *Set up Command Filter Lists (CFL)* section of the [AGD] specifies how to define and configure white list and black list commands.

#### 3.1.1.3 Tests Assurance Activity

*The evaluator **shall** test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.*

**Evaluator Assessment:**

The evaluator created policies that use all defined attributes and had the PAM and two SFAs (one a Windows SFA and one a Linux SFA) consume the created policies.

On the PAM, when an access method was allowed, the evaluator verified that it was possible to access the associated device. When the same policy was set to deny, the evaluator verified it was no longer available to the user.

The evaluator then defined policies for the SFAs using both blacklists and whitelists. The evaluator verified that a user could access a third party product using the device when a whitelist was applied to the third

party, and could not access the third party product when a blacklist was applied.

The evaluator verified that the defined object attributes within a policy are consumed by the product and the policy was enforced.

### 3.1.2 ESM_ATD.2 Subject Attribute Definition

#### 3.1.2.1 TSS Assurance Activity

*The evaluator **shall** check the TSS to ensure that it describes the subject attributes that are defined by the TOE and the purpose for their definition.*

**Evaluator Assessment:**

The subject attributes that may be defined by the TOE are described in section 7.1.2 of the [ST], as follows:

- 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

#### 3.1.2.2 Guidance Documentation Assurance Activity

*The evaluator **shall** check the operational guidance to ensure that it provides instructions on how to define and configure these attributes.*

**Evaluator Assessment:**

The *Configure Users* section of the [AGD] provides instructions on how to define and configure the user attributes Name, Role, and User group.

#### 3.1.2.3 Tests Assurance Activity

*The evaluator **shall** test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They **shall** then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.*

**Evaluator Assessment:**

The evaluator created policies that use all defined attributes and had the PAM and two SFAs (one a Windows SFA and one a Linux SFA) consume the created policies.

On the PAM, when an access method was allowed, the evaluator verified that it was possible to access the associated device. When the same policy was set to deny, the evaluator verified it was no longer available to the user.

The evaluator then defined policies for the SFAs using both blacklists and whitelists. The evaluator verified that a user could access a third party product using the device when a whitelist was applied to the third party, and could not access the third party product when a blacklist was applied.

The evaluator verified that the defined subject attributes within a policy are consumed by the product and the policy was enforced.

## *3.2 Cryptographic Support (FCS)*

### 3.2.1 FCS_CKM.1 Cryptographic Key Generation (for Asymmetric Keys)

#### 3.2.1.1 TSS Assurance Activity

*In order to show that the TSF complies with 800-56A and/or 800-56B, depending on the selections made, the evaluator shall ensure that the TSS contains the following information:*

*- The TSS **shall** list all sections of the appropriate 800-56 standard(s) to which the TOE complies.*

*- For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options it **shall** be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide rationale for why this will not adversely affect the security policy implemented by the TOE;*

*- For each applicable section of 800-56A and 800-56B (as selected), any omission of functionality related to "shall" or "should" statements shall be described;*

*- Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described.*

**Evaluator Assessment:**

The evaluator has verified that Section 7.3 of the [ST] includes the information required to meet FCS_CKM_EXT.1. This includes a list of all sections of SP800-56B to which the TOE claims conformance or a rationale as to why the section is not claimed.

#### 3.2.1.2 Guidance Documentation Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

#### 3.2.1.3 Tests Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

### 3.2.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

#### 3.2.2.1 TSS Assurance Activity

*The evaluator **shall** check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and critical security parameters used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator **shall** check to ensure that the TSS describes the zeroization procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write").*

**Evaluator Assessment:**

The evaluator reviewed the [ST] and verified that Table 15 in the TSS specifies the keys which reside in the TOE, the storage location, and the means of zeroization. They are as follows:

| 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 |

#### 3.2.2.2 Guidance Documentation Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

#### 3.2.2.3 Tests Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

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

#### 3.2.3.1 TSS Assurance Activity

*None.*

**Evaluator Assessment:**

Section 7.3 of the [ST] specifies that the TOE implements the CA Technologies C-Security Kernel cryptographic module (CMVP certificate # 3043) for all cryptographic operations. Table 16 of the [ST] identifies the cryptographic algorithms associated with each function. CAVP certificate # 4635 is identified for Data Encryption/Decryption.

#### 3.2.3.2 Guidance Documentation Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

#### 3.2.3.3 Tests Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

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

#### 3.2.4.1 TSS Assurance Activity

*None.*

**Evaluator Assessment:**

Section 7.3 of the [ST] specifies that the TOE implements the CA Technologies C-Security Kernel cryptographic module (CMVP certificate # 3043) for all cryptographic operations. Table 16 of the [ST] identifies the cryptographic algorithms associated with each function. CAVP certificate # 2530 is identified for Cryptographic Signatures.

#### 3.2.4.2 Guidance Documentation Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

#### 3.2.4.3 Tests Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

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

#### 3.2.5.1 TSS Assurance Activity

*None.*

**Evaluator Assessment:**

Section 7.3 of the [ST] specifies that the TOE implements the CA Technologies C-Security Kernel cryptographic module (CMVP certificate # 3043) for all cryptographic operations. Table 16 of the [ST] identifies the cryptographic algorithms associated with each function. CAVP certificate # 3799 is identified for Cryptographic Hashing.

#### 3.2.5.2 Guidance Documentation Assurance Activity

**Evaluator Assessment:**

N/A

#### 3.2.5.3 Tests Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

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

#### 3.2.6.1 TSS Assurance Activity

*None.*

**Evaluator Assessment:**

Section 7.3 of the [ST] specifies that the TOE implements the CA Technologies C-Security Kernel cryptographic module (CMVP certificate # 3043) for all cryptographic operations. Table 16 of the [ST] identifies the cryptographic algorithms associated with each function. CAVP certificate # 3068 is identified for Keyed-Hash Message Authentication.

#### 3.2.6.2 Guidance Documentation Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

#### 3.2.6.3 Tests Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

### 3.2.7 FCS_HTTPS_EXT.1 HTTPS

#### 3.2.7.1 TSS Assurance Activity

*The evaluator **shall** check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack. The evaluator **shall** also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes—for each platform identified in the ST—the interface(s) used by the TOE to invoke this functionality.*

**Evaluator Assessment:**

Section 7.3.1 in the [ST] specifies that the Web Browser UI uses the HTTPS protocol for secure administrator communications. It further specifies that the TOE implementation of HTTPS, TLS version 1.2

(RFC 5246) is used to encrypt and authenticate sessions between the remote browser and TOE.

#### 3.2.7.2 Guidance Documentation Assurance Activity

*None. There are no assurance activities to be performed against the operational guidance for this requirement.*

**Evaluator Assessment:**

N/A

#### 3.2.7.3 Tests Assurance Activity

*None. Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.*

**Evaluator Assessment:**

N/A

### 3.2.8 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

#### 3.2.8.1 TSS Assurance Activity

*The evaluator **shall** examine the TSS to ensure it describes the deterministic random bit generation services provided by either the TSF or the TOE environment, including a description of the entropy source.*

**Evaluator Assessment:**

Section 7.3 in the [ST] specifies that random bit generation within the TOE is provided by an entropy source in the CA Technologies C-Security Kernel. A description of the entropy source is provided in the Entropy Assessment Report [EAR], Symantec Privileged Access Manager 3.3 Entropy Documentation and Assessment. The [EAR] provides sufficient details to satisfy the design, justification, operating conditions, and health testing requirements as outlined in Appendix C of the PP.

Table 16 of the [ST] identifies the cryptographic algorithms associated with each function. CAVP certificate # 1561 is identified for Random Bit Generation.

#### 3.2.8.2 Guidance Documentation Assurance Activity

*The evaluator **shall** examine the AGD guidance to ensure it provides clear instructions on how to configure the TOE environment. If any part of the deterministic RBG service is configurable, the evaluator **shall** ensure that the operational guidance provides clear instructions for how to configure them.*

**Evaluator Assessment:**

No part of the deterministic RBG service is configurable; therefore operational guidance and/or instructions are not applicable to this function.

#### 3.2.8.3 Tests Assurance Activity

*Documentation **shall** be produced—and the evaluator **shall** perform the activities—in accordance with Appendix C.9 Entropy Documentation and Assessment. This documentation may be included as a supplemental addendum to the Security Target. The evaluator **shall** also perform the following tests, depending on the standard to which the RBG conforms.*

*The evaluator **shall** perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator **shall** perform 15 trials for each configuration. The evaluator shall also confirm that the operational guidance contains appropriate instructions for configuring the RNG functionality.*

*If the RNG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator **shall** generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90A).*

*If the RNG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator **shall** generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.*

*The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.*

***Entropy input**: the length of the entropy input value must equal the seed length.*

***Nonce**: If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length.*

***Personalization string**: The length of the personalization string must be less then or equal to seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator **shall** use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.*

***Additional input**: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.*

**Evaluator Assessment:**

N/A

## 3.2.9 FCS_TLS_EXT.1 TLS

### 3.2.9.1 TSS Assurance Activity

*The evaluator **shall** check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported, client authentication supported) are specified, and the ciphersuites supported are specified as well. The evaluator **shall** check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator **shall** also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator **shall** perform the following activities:*

*a. Ensure the ST contains a list of representative platforms (hardware and software) compromising the operational environment.*

*b. Check the TSS to ensure it describes-for each platform identified in the ST-the interface(s) used by the TOE to invoke this functionality.*

*c. For each platform identified in the ST, check the OE documentation to ensure the interfaces identified in the previous step exist.*

**Evaluator Assessment:**

Section 7.3.2 in the [ST] specifies that the TOE supports TLS using the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA

These ciphersuites match the ciphersuites specified in the SFR. The TSS further specifies that the TLS

implementation does not support any TLS extensions.

The TSS also specifies that the cryptographic module with certificate #3043 provides the cryptography for the TLS implementation.

The TSS also specifies the uses of each ciphersuite for each communication path, as follows:

- 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_ASE_256_CBC_SHA256

#### 3.2.9.2 Guidance Documentation Assurance Activity

*The evaluator **shall** check the operational guidance to ensure that it contains instructions on configuring the TOE in the Operational Environment so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements or an administrator is expected to deploy a particular client to access the TOE).*

**Evaluator Assessment:**

Section 2.2 of the [AGD] provides instructions for enabling FIPS mode as part of the initial setup activities. This limits the ciphersuites advertised by the TOE.

#### 3.2.9.3 Tests Assurance Activity

*The evaluator **shall** test this capability by establishing a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of a HTTPS session. It is sufficient to observe (on the wire) the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).*

**Evaluator Assessment:**

The evaluator verified that the combined list of available ciphersuites matched the list of ciphersuites specified in the [ST], for each communication path.

The evaluator performed the following tests:

- Using openssl s_client, the evaluator connected to the TOEs management port using each ciphersuite as specified in the requirement. A packet capture tool was also used to verify the successful cipher negotiation.
- On the LDAP server, the evaluator modified the ciphersuites within the local registry and connected to the LDAP server from the TOE using each of the ciphers specified in the requirement. A packet capture tool was also used to verify the successful cipher negotiation.
- Using a packet capture tool, the evaluator connected to each of the SFAs on the target machines

(Windows and Linux), via the PAM server, and verified that the connection was made using the ciphers as specified in the requirement.

## *3.3 Protection of the TSF (FPT)*

### 3.3.1 FPT_STM.1 Reliable Time Stamps

#### 3.3.1.1 TSS Assurance Activity

*The evaluator **shall** check the TSS in order to determine that it discusses the TOE's inclusion of a system clock.*

**Evaluator Assessment:**

Section 7.6 of the [ST] discusses the inclusion of a system clock relied upon for providing reliable time stamps in the creation of audit records.

#### 3.3.1.2 Guidance Documentation Assurance Activity

*The evaluator examines the operational guidance to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the operational guidance instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.*

**Evaluator Assessment:**

The *Configure Date/Time Settings* section of the [AGD] provides instructions for configuring the date and time on the TOE by navigating to **Configuration → Date/Time** in the Web UI. Administrators can configure the date, time, and time zone to set a new clock value.

The TOE supports the use of an NTP server but is not claimed in the evaluated configuration.

#### 3.3.1.3 Tests Assurance Activity

*The evaluator **shall** determine through the evaluation of operational guidance how the TOE initializes and initiates the clock. The evaluator **shall** then follow those instructions to set the clock to a known value, and observe that the clock monotonically increments in a reliable fashion (comparison to a reference timepiece is sufficient). Through its exercise of other TOE functions, the evaluator **shall** confirm that the value of the timestamp is used appropriately. If the TOE supports multiple protocols for establishing a connection with an NTP server, the evaluator **shall** perform this test using each supported protocol claimed in the operational guidance.*

**Evaluator Assessment:**

The Evaluator used a 3rd party time source in testing to verify the TOE maintained its time after adjusting it's time manually to the time source and refreshing it several times. It was also verified that the TOE uses its time source in the recorded time stamps for audit logging.

## *3.4 Toe Access (FTA)*

### 3.4.1 FTA_SSL.3 TSF-initiated Termination

#### 3.4.1.1 TSS Assurance Activity

*The evaluator **shall** check the TSS in order to determine that it discusses how inactivity is handled for remote administrative sessions.*

**Evaluator Assessment:**

The TOE automatically terminates inactive sessions after a configured period of time, as described in section 7.7 of the [ST].

#### 3.4.1.2 Guidance Documentation Assurance Activity

*The evaluator **shall** also check the operational guidance in order to verify that it describes how to set the idle time threshold.*

**Evaluator Assessment:**

The *Basic Settings* subsection of the *Apply Global Settings* section in the [AGD] describes how to set the idle time threshold. Identified as the "Login Timeout" function, administrators can set the threshold from the Basic Settings page in the Web UI.

#### 3.4.1.3 Tests Assurance Activity

*The evaluator shall test this capability by following the operational guidance to configure several different values for the inactivity time period referenced in the component; these shall consist at least of the minimum and maximum allowed values as specified in the operational guidance, as well as one other value. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.*

**Evaluator Assessment:**

The evaluator tested the TOE timeout periods of 1 minute and 5 minutes, and in both cases the administrative session was logged out automatically by the TOE.

### 3.4.2 FTA_SSL.4 User-initiated Termination

#### 3.4.2.1 TSS Assurance Activity

*The evaluator **shall** check the TSS in order to determine that it discusses the ability of an administrator to terminate their own session.*

**Evaluator Assessment:**

Users (including administrators) can terminate their own sessions, as described in section 7.7 of the [ST].

#### 3.4.2.2 Guidance Documentation Assurance Activity

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

**Evaluator Assessment:**

Section 2.2 of the [AGD] specifies that users can terminate their own session with the TOE at any time by selecting the **Log Off** button from the Web UI. The Web UI is the only administrative interface.

#### 3.4.2.3 Tests Assurance Activity

*The evaluator **shall** test this capability by establishing a session with the TOE using an administrative interface. The evaluator then follows the operational guidance to exit or log off of the session and observes that the session has been terminated. If applicable, the evaluator shall repeat this test for each administrative interface that is supported by the TOE.*

**Evaluator Assessment:**

The evaluator verified that the Log Out link provided in the GUI will terminate the administrative session.

### 3.4.3 FTA_TSE.1 TOE Session Establishment

#### 3.4.3.1 TSS Assurance Activity

*The evaluator **shall** examine the TSS to determine that all of the attributes on which a session can be denied are specifically defined.*

**Evaluator Assessment:**

Attributes on which a session can be denied are defined in section 7.7 of the [ST]. Restrictions may be configured for any combination of time of day and day of week.

#### 3.4.3.2 Guidance Documentation Assurance Activity

*The evaluator **shall** examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.*

**Evaluator Assessment:**

Section 1.4 of the [AGD] specifies the method for configuring session restriction attributes on users by defining the access times.

#### 3.4.3.3 Tests Assurance Activity

*The evaluator **shall** test this capability by first fully establishing a session to the TOE. The evaluator then follows the operational guidance to configure the TOE so that that access is denied based on a specific value of the attribute. The evaluator **shall** then attempt to establish a session in contravention to the attribute setting (for instance, the location is denied based upon the time of day). The evaluator **shall** observe that the session establishment attempt fails.*

**Evaluator Assessment:**

The evaluator, using an administrator account, set the access time restrictions on a specific user. The evaluator then attempted to login to the TOE as the restricted user during the restricted access times. The evaluator verified that the user was denied access to the TOE during the defined restriction period.

# 4 Security Assurance Requirement Activities (ESM_PM PP)

## *4.1 Class ASE: Security Target Evaluation*

### 4.1.1 Assurance Activity

*None.*

**Evaluator Assessment:**

N/A

## *4.2 Class ADV: Development*

### 4.2.1 Basic Functional Specification (ADV_FSP.1)

#### 4.2.1.1 Assurance Activity

*There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described for each SFR, and for other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided. For example, if the TOE provides the capability to configure the key length for the encryption algorithm but fails to specify an interface to perform this function, then the assurance activity associated with FMT_SMF would fail.*

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

**Evaluator Assessment:**

The ST and TOE guidance documentation provides specification of the interfaces, and associated management functions in sufficient detail to perform the assurance activities.

## *4.3 Class AGD: Guidance Documentation*

### 4.3.1 Operational User Guidance (AGD_OPE.1)

#### 4.3.1.1 Assurance Activity

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

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

**Evaluator Assessment:**

The *FIPS Mode Activation* section in the [AGD] specifies how to configure the cryptographic module for

FIPS Mode. Only the TOE with the CA Technologies C-Security Kernel, version 3.11.2 cryptographic engine was evaluated.

### 4.3.2 Preparative Procedures (AGD_PRE.1)

#### 4.3.2.1 Assurance Activity

*As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST.*

**Evaluator Assessment:**

The *Deploy the Hardware Appliance* section in the [AGD] specifies how to perform the hardware setup. The *Install and Configure a Socket Filter Agent* section in the [AGD] specifies how to deploy and install SFAs on Windows and Linux/Unix targets. The *Upgrade to Release 3.3* section in the [AGD] specifies how to upgrade/install the PAM software, version 3.3.0.1085. The evaluator has confirmed that the provided guidance adequately addresses all TOE platforms.

## *4.4 Class ALC: Life Cycle Support*

### 4.4.1 Labeling of the TOE (ALC_CMC.1)

#### 4.4.1.1 Assurance Activity

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

**Evaluator Assessment:**

[ST], section 1.3 specifies that the TOE is the Symantec Privileged Access Manager 3.3.0.1085. Section 1.5.1 specifies the TOE hardware as the Lanner NCA 5210A (404L). The evaluator verified the version of the TOE hardware upon delivery and the TOE software upon setup. Both references are consistent with the versions specified in the [ST]. The evaluator also examined the online guidance documentation and the [AGD], and has determined that the version of the TOE specified is consistent with that of the [ST] and sufficiently distinguishes the product.

The developer provided a Configuration List [ALC] identifying each TOE component to satisfy the requirements for ALC_CMS.1. The evaluator examined the [ALC] and has determined that it is consistent with the [ST], user guidance, and the TOE.

### 4.4.2 TOE CM Coverage (ALC_CMS.1)

#### 4.4.2.1 Assurance Activity

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

**Evaluator Assessment:**

Upon examination of the [ST], [ALC], [AGD], and [HELP], the evaluator has determined that the TOE identification is consistent across all evaluation evidence required by the SARs.

## *4.5 Class ATE: Tests*

### 4.5.1 Independent Testing - Conformance (ATE_IND.1)

#### 4.5.1.1 Assurance Activity

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

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

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

*The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test Report (that could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the Report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.*

**Evaluator Assessment:**

The evaluator performed testing on the Symantec PAM version 3.3.0.1085 software deployed on the Lanner NCA 5210A (404L) hardware appliance. The test plan and results are documented in the Evaluation Test Plan, Procedures and Test Results [ETProcRes].

## *4.6 Class AVA: Vulnerability Assessment*

### 4.6.1 Vulnerability Survey (AVA_VAN.1)

#### 4.6.1.1 Assurance Activity

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

**Evaluator Assessment:**

The evaluator performed the following Vulnerability Assessment (VA) activities against the TOE in its evaluated configuration:

- Port Scan (nmap)
- Vulnerability Scan (Nessus)
- Search of the public domain

The evaluator has determined that the evaluated version of the TOE is not susceptible to or impacted by any known vulnerabilities. Results of the VA activities are documented in the [ETProcRes].