Vormetric Data Security Manager Version 6.3 Security Target

Version 3.3
October 7, 2020

Prepared For:

THALES

Evaluated By:

Cygnacom Solutions

1000 Innovation Drive, Ottawa, Ontario, K2K 3E7

Table of Contents

Section **Page**

Figures and Tables

Figures **Page**

Tables **Page**

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

The TOE is the Vormetric Data Security Manager (DSM). The DSM creates, stores, and manages policies that protect data residing on manage hosts. The DSM operates by integrating with an access control product, called Transparent Encryption Agent, installed on the host machines that contain protected data and to specify data access policies that are sent to these agents. Administrators access the DSM through a browser-based user interface.

1.1 *Security Target Reference*

ST Title:	Vormetric Data Security Manager, Version 6.3 Security Target
ST Version:	v3.3
ST Author:	Cygnacom Solutions
ST Date:	October 7, 2020

1.2 *TOE Reference*

TOE Identification:	Vormetric Data Security Manager V6000, Version 6.3 Build 14515
TOE Developer:	Thales DIS CPL USA, Inc.
Evaluation Sponsor:	Thales

1.3 *Conformance Claims*

This TOE is conformant to the following CC specifications:

- *Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002*
  - *Part 2 Conformant with additional extended functional components as specified by the protection profile.*
- *Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003*
  - *Part 3 Conformant with additional assurance activities as specified by the protection profile*

1.4 *Protection Profile Claim*

The TOE claims *exact* conformance to *Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013* [ESM PM PP].

1.5 *Package Claim*

The TOE does not claim to be conformant with any pre-defined packages.

1.6 *Conformance Rationale*

This Security Target (ST) claims exact conformance to only one Protection Profile – the ESM PM PP.

The security problem definition of this ST is consistent with the statement of the security problem definition in the PP, as the ST claims *exact* conformance to the PP and no other threats, organizational security policies, or assumptions are added.

The security objectives of this ST are consistent with the statement of the security objectives in the PP as the ST claims *exact* conformance to the PP and no other security objectives are added.

The security requirements of this ST are consistent with the statement of the security requirements in the PP as the ST claims *exact* conformance to the PP.

1.7 *Technical Decisions*

- TD0320 – TLS ciphers in ESM PPs
    - Removal of mandatory ciphersuites
    - Applied
- TD0245 – Updates to FTP_ITC and FTP_TRP for ESM PPs
    - Mandatory inclusion of protocol SFRs in the ST
    - Applied
- TD0079 – RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
    - Removal of ANS X9.31
    - Not applicable to the evaluation, FCS_RBG_EXT.1 not claimed
- TD0071 – Use of SHA-512 in ESM PPs
    - Added SHA-512 algorithm to FCS_COP.1 selections
    - Applied
- TD0066 – Clarification of FAU_STG_EXT.1 Requirement in ESM PPs
    - External audit reconciliation clarified as optional
    - Applied
- TD0055 – Move FTA_TAB.1 to Selection-Based Requirement

  - Inclusion of FTA_TAB.1 is conditional;

- TD0042 – Removal of Low-level Crypto Failure Audit from PPs
  - Removal of audit events for FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(*), FCS_RBG_EXT.1
  - Applied

2 TOE Description

2.1 *Product Overview*

Vormetric Data Security Manager is a policy-based data protection and encryption system. It provides policy-specified access control and encryption for the following types of data repositories:

- Files and file systems.
- Oracle Database and Microsoft SQL Server Transparent Data Encryption (TDE).
- Applications that use a PKCS11 interface.
- Other data encryption systems – securely stores inventory of symmetric and asymmetric encryption keys and certificates from any application, and tracks key expiration dates.

The active components of Vormetric Data Security are the Vormetric Data Security Manager (DSM[1]), also called the Security Server, and Transparent Encryption Agent, an access control product residing on the host machines containing data to be protected.

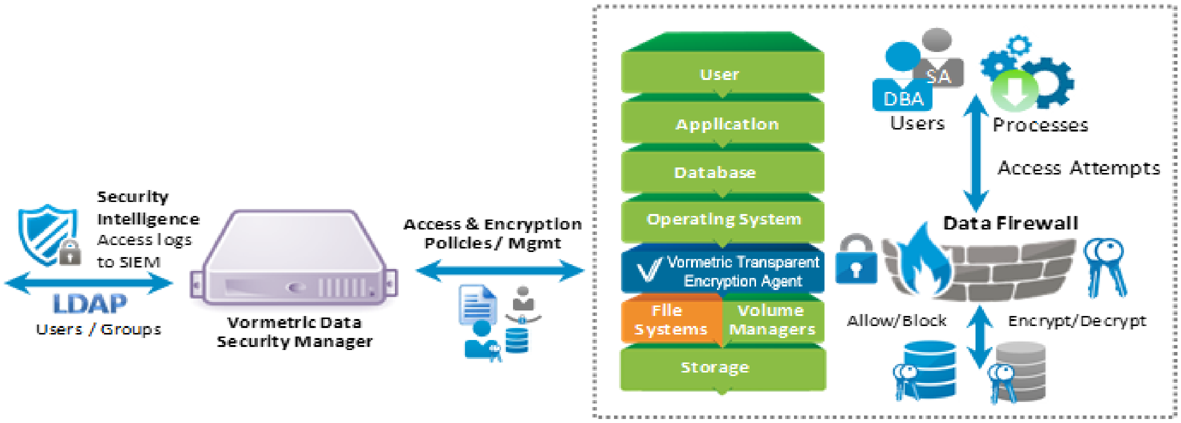

Figure 1: Vormetric Data Security Product

Note 1: DSM is the only component covered by the evaluation.

For Transparent Encryption Agents, the DSM allows administrators to specify data access policies, create new administrators and administrative domains, generate usage reports, register new hosts, access security logs, and perform other management functions.

Administrators access the DSM through a browser-based user interface called the Data Security Remote Administrative Management. The DSM is available as a hardened appliance.

The Vormetric Transparent Encryption Agents are installed on the host machines that contain the data to be protected. The Transparent Encryption Agents manage and implement the security polices stored on the DSM. The DSM manages Transparent Encryption Agents authentication credentials and securely transmits policy data.

2.2 *TOE Overview*

The TOE is the appliance-based Vormetric Data Security Manager (DSM). The TOE includes all DSM appliance hardware and all software installed on the appliance. The TOE hardware appliance model is V6000.

The DSM is the Policy Management product that serves as a trusted source for policy information that is ultimately consumed be the Transparent Encryption Agent (the Access Control product) as defined in [ESM PM PP].

The Transparent Encryption Agent is outside the scope of the ESM PM PP evaluation. The current Transparent Encryption Agent does not meet the definition options identified in ESM PP AC and will therefore not be submitted as a separate evaluation until such a time that the AC definition is updated to allow it into evaluation. This testing conducted in this evaluation will be limited to the Transparent Encryption Agent successfully receiving and loading the policy. The correctness of the enforcement of that policy will not be tested.

2.2.1 Vormetric Data Security Manager (DSM)

2.2.1.1 DSM Software

The Vormetric Data Security Manager (DSM) comprises a policy engine and a central cryptographic key and policy manager. The policies are defined and keys are generated by the DSM and downloaded to the Transparent Encryption Agent through a secure network connection. The policy update requests are evaluated by using agent-system parameters and administrator-defined policy constraints. The AC agents (Transparent Encryption Agents) which run on protected hosts implement policies set by DSM administrators.

Authenticated secure channel is used to protect all communications between the agents and DSM. Vormetric Data Security Manager employs X.509 digital certificates and TLS for agent/server communication as well as communication to domain controller and audit servers.

The DSM administrator configures policies comprised of sets of security rules that must be satisfied in order to allow or deny access. Each security rule evaluates who, what, when, and how protected data is accessed and, if these criteria match, the policy either permits or denies access. Furthermore, the security rule can be constructed to encrypt data in the Transparent Encryption Agent. If the encryption effect on the security rule is matched, the access control component will perform encryption.

The security rules specify:

- Data being accessed: Administrators can configure a mix of files and directories by specifying them individually or by using variables.
- Applications that are authorized: Administrators can specify which executables and tools are permitted to access data.
- The user attempting to access the protected data: Administrators can configure one or more users. Users can be identified by user name, identification number, group, or group number.
- When the data is being accessed: Administrators can configure a range of hours and days of the week to allow access.
- How the data is being accessed: Administrators can configure a security rule that considers how files and directories, and their attributes, are being accessed. The security rule can note attempts to read, write, delete, rename, create, and more.

When the conditions specified in a security rule match, the policy dictates whether to permit or deny access. If encryption is used, the policy can be configured to permit read access but without including the key to decrypt encrypted data. This way the underlying encrypted (unintelligible) data can be backed up.

The DSM also provides auditing capabilities. The Transparent Encryption Agent notifies security administrators of policy violations in near real time. The DSM records all context attributes of an access attempt, enabling traceability of host intrusion and data access events at the application and user level, and maintains an extensive log for detailed forensic analysis. In addition, the DSM provides audit logging to monitor all activities and transactions.

2.2.1.2 DSM Hardware

The V6000 DSM Appliance is a 1u, rack-mountable chassis. Its dimensions are 17”x20.5”x1.75”. Network connectors, a serial console connector, and IPMI connector are on the back. It comes with two auto-switching, 100-240V power supplies. Power connectors are on the back while the power switch is on the front. There are four drive bays but only two bays are populated with disks.

Table 2-1: DSM Appliance Hardware Features

Feature	Description
Hardware Model	V6000
Chassis	1U rack-mountable; 17” wide x 20.5” long x1.75” high (43.18 cm x 52.07cm x 4.5 cm)
Weight	V6000: 21.5 lbs (9.8 kg)
Hard Disk	Dual SAS RAID 1 configured
Serial Port	1; DB-9 RS-232 serial console interface to configure, or log onto, the DSM Appliance.
Ethernet	2x1Gb; Ethernet interface used in the Remote Administrative Management to administer the DSM Appliance and Vormetric Agents. Also used to carry policy evaluation information between the DSM and its agents.
Power Supplies	2 removable 80+certified (100VAC-240VAC/50-60Hz) 400W
Operating Temperature	10° to 35° C (50° to 95° F)
CPU	1 Intel Xeon E5 (6 physical cores)

Memory	16GB

2.2.1.3 Remote Administrative Management

The DSM includes a Web-based interface, referred to as the “Remote Administrative Management”. This interface is used to create policies, configure hosts, and assign keys. The DSM provides a secure connection between itself and the host administering the DSM.

The Remote Administrative Management provides a robust security environment in which administrative control is distributed based upon administrative type. The menus displayed by the Remote Administrative Management and the tasks administrators can perform are dependent upon their administrator type. An administrator is assigned one administrative type and is allowed to perform the tasks for that one administrative type only.

A domain is self-contained environment comprised of policies, keys, hosts, users, and audit records. The configuration data that administrators can see is dependent upon the domain in which they are working. The Remote Administrative Management provides fully separated domains, where the work and configuration data in one domain is invisible to administrators in other domains.

Note: The DSM also includes a Command Line Interface (CLI). The CLI is used to configure the DSM at the system level. An administrator connects to the CLI locally or via SSH. The CLI is a limited Linux command line interface that is used only for installation of the TOE and off-line maintenance. This interface cannot be used to access, import, or export cryptographic keys or authentication credentials. The CLI is a maintenance mode interface and is not included in the scope of the evaluation and is not considered a TSFI.

Note: Vormetric has developed a command line tool called VMSSC, which provides a subset of the administrative functions of the Remote Administrative Management. VMSSC is a separate utility that is not part of the TOE distribution and must be installed separately. VMSSC is not included in the scope of the evaluation.

2.2.1.4 Vormetric Agents

There are several types of Vormetric agents, Transparent Encryption Agent, Key agent for Oracle and SQL Database, and Application Encryption Agent. Vormetric agents come with different installation packages and are not distributed as a part of DSM. All Vormetric Agents are installed on the host machines that contain the data to be protected. The Transparent Encryption Agent enables data-at-rest encryption, file access control, and the collection of security intelligence audit logs. The DSM is capable of producing a policy and the Transparent Encryption Agent can consume and enforce the policy from DSM. The testing conducted in this evaluation is limited to the Transparent Encryption Agent successfully receiving and loading the policy. The correctness of the enforcement of that policy is only coincidentally tested.

The Key Agent for Oracle and SQL database centralize the key storage for Oracle and SQL encryption key while the Application Encryption agent provides a framework to deliver application-layer encryption such as column-level encryption in the database. However, the Key Agent for database and Application Encryption Agent cannot process policy from DSM.

DSM is also capable of registering one external non-Vormetric agent called KMIP client. KMIP client is used to store and retrieve keys from DSM. However, KMIP client is a third-party software and Vormetric does not package or ship KMIP client. This feature is not enabled by default.

2.3 *Physical Scope of the TOE*

The physical boundary of the TOE is the Vormetric Data Security Manager (DSM), which includes:

- The DSM Appliance hardware
- All software installed on the DSM Appliance
    - Remote Administrative Management Interface

Required external access control product components:

- One or more Vormetric Transparent Encryption Agents

The Operational Environment of the TOE includes:

- The web browser that is used for the Remote Administrative Management
- The workstation that hosts the Remote Administrative Management web browser
- The host platforms for the Vormetric Transparent Encryption Agents
- Optional external servers
    - NTP Server (use of an external NTP Server is highly recommended)
    - SMTP Server
    - The DNS server that provides host name resolution service
    - LDAP Authentication Server
    - Syslog Server for external storage of the audit log
    - RSA Authentication Manager and an RSA SecurID device for each administrator
    - External Certificate Authority (CA)

The TOE Boundary is depicted in the following figure:

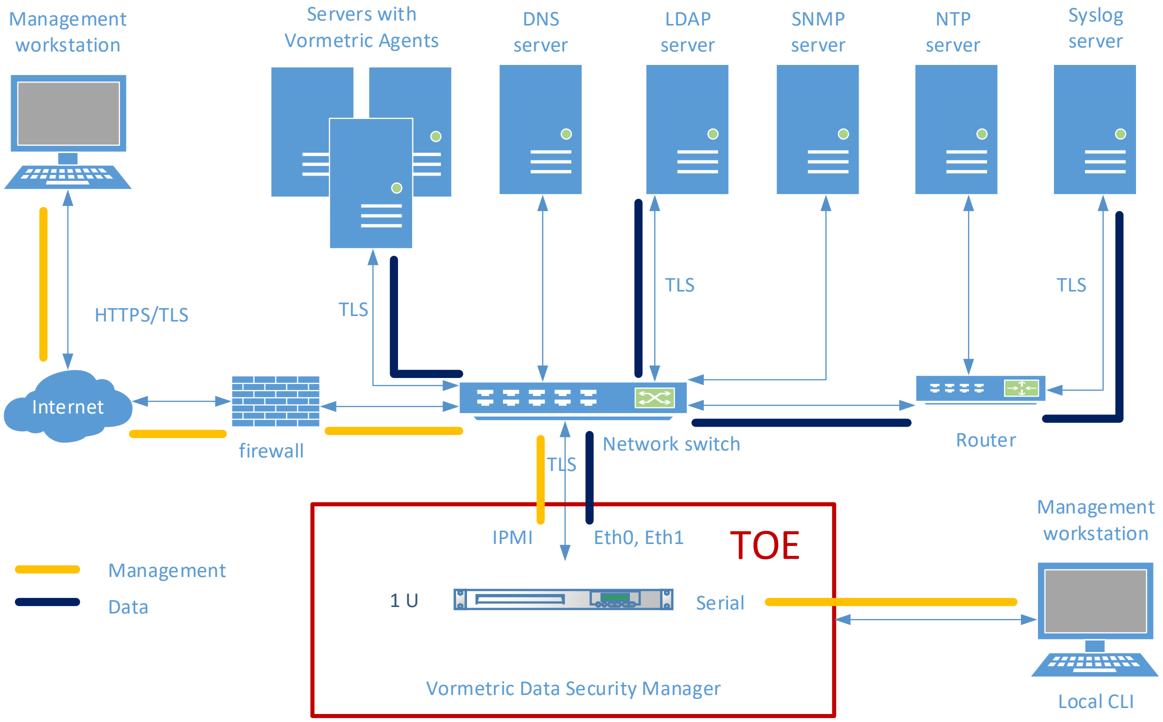

Figure 2: TOE Boundary

2.4 *Protocols and Services Excluded from evaluation*

1. The CLI should be only used for initial configuration and off-line maintenance.
2. CLI over SSH is not evaluated and must be disabled. Local CLI access is not evaluated and the DSM appliance must be physically secured.
3. VMSSC (An external Vormetric command line tool for administering the DSM) - VMSSC is a separate utility that is not part of the TOE distribution and must be installed separately. VMSSC is not included in the scope of the evaluation.
4. Transparent Encryption Agent – This is an external agent that is not a part of TOE distribution. The scope of testing is limited to the Transparent Encryption Agent successfully receiving and loading the policy.
5. SNMP service – Use of the SNMPv1 and SNMPv2 functionality is excluded and it is disabled by default. The use of SNMPv3 with read-only community strings is not restricted in the evaluated configuration; however, it is not evaluated.
6. IPMI – This service offers the same TOE off-line maintenance capability as CLI. IPMI can not be used to import or export DSM cryptographic keys. IPMI service should be disabled in the evaluated configuration.

7. Failover DSM – failover is not restricted in the evaluated configuration; however, it is not evaluated. Failover configuration is disabled by default. This interface uses standard database data replication method. When configured, the database replication does not transmit plaintext data.
8. Auto-backup via SCP and CIFS are not evaluated.
9. Application Encryption Agent – This is an external agent that is not a part of the TOE distribution. The agent functionality is not evaluated.
10. Key Agents for SQL and Oracle Database – These are external agents that are not a part of the TOE distribution. These two agents are not evaluated.
11. KMIP client – This is an external client that is not a part of the TOE distribution. This client is not evaluated.
12. Email notification – email notification is disabled by default. SMTP is not evaluated.
13. Optional RSA Authentication Manager is not evaluated.
14. Optional External Certificate Authority is not evaluated.

2.5 *Logical Scope of the TOE*

The TOE provides the security functionality described in the following subsections.

2.5.1 System Monitoring

The TOE provides the ability to generate audit events In order to identify unauthorized TOE configuration changes and attempted malicious activity against protected objects. The audit trail identifies changes to subject data and usage of the authentication function. The audit data can be stored in an external repository

2.5.2 Robust TOE Access

The TOE implements mechanisms via a configurable password policy that improve security relative to the attempts of unsophisticated attackers to authenticate to the TOE using repeated guesses. The TOE can also enforce an externally-defined LDAP authentication policy. The TOE provides capabilities to terminate established sessions.

2.5.3 Authorized Management

Policy Administrators are designated by the TSF and given various responsibilities for managing the TOE and creating policies. The TSF has its own internal method of enforcing controlled access so that no actions can be performed against it unless the subject is identified, authenticated, and authorized.

2.5.4 Policy Definition

The TSF is able to manage policy attributes that are consistent with the corresponding technology type(s) described in the User Data Protection requirements in the Standard Protection Profile for Enterprise Security Management Access Control. In addition, the TSF is able to detect or prevent inconsistencies in the application of policies so that policies are unambiguously defined. Finally, the TOE is able to identify uniquely policies it creates so that it can be used to determine what policies are being implemented by remote products.

2.5.5 Dependent Product Configuration

The TOE is able to configure the behavior of the functions of the Access Control products that consume the policies it provides. This includes the configuration of what events they audit, what policies they enforce, and how they react in the event of a failure state or lack of connectivity.

2.5.6 Confidential Communications

The TOE uses sufficiently strong and sufficiently trusted encryption algorithms to protect data in transit to and from the TOE. The TOE implements cryptographic protocol to protect these data in transit.

2.5.7 Access Bannering

The TOE displays a banner prior to authentication that defines its acceptable use. This banner provides legal notification for monitoring that allows audit data to be admissible in the event of any legal investigations.

2.5.8 Cryptographic Services

The TOE uses cryptographic primitives (encryption, decryption, random bit generation, etc.) in order to ensure the confidentiality and integrity of the policy data it transmits and to provide trusted communications between itself and the Operational Environment where necessary.

2.6 *TOE Guidance*

The following user guidance document is provided to customers and is considered part of the TOE:

- *Vormetric Data Security Manager (DSM) Common Criteria Addendum, Version 1.2, July 23, 2020*

The documents in the following table were used as reference materials to develop this ST.

Table 2-2: ST Reference Documents

Reference Title	ID
Common Criteria for Information Technology Security Evaluation, CCMB-2012-09-001, Version 3.1, Revision 4, September 2012	[CC]
Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, 24 October 2013	[ESM PM PP]
Vormetric Data Security Platform DSM Administration Guide Release 6 Version v6.3.0 August 21, 2019 v2	[ADMIN]
Data Security Manager (DSM) Common Criteria Addendum, Version 1.2, July 23, 2020	[ADDEND]

3 Security Problem Definition

The U.S. Government Enterprise Security Management Policy Management Protection Profile, [ESM PP PM] provides the following policies, threats and assumptions about the TOE.

3.1 *Threats*

This section identifies the threats applicable to the U.S. Government Enterprise Security Management Policy Management Protection Profile, [ESM PP PM] as specified in the Protection Profile, verbatim.

Table 3-1: TOE Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.CONDTRADICT	A careless administrator may create a policy that contains contradictory rules for access control enforcement.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FORGE	A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.UNAUTH	A malicious user could bypass the TOE’s identification, authentication, or authorization mechanisms in order to illicitly use the TOE’s management functions.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
T.WEAKPOL	A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

3.2 *Organizational Security Policies (OSPs)*

This section identifies the organizational security policies applicable to the Standard Protection Profile for Enterprise Security Management Policy Management [ESM PP PM] as specified in the Protection Profile, verbatim.

Table 3-2: Organizational Security Policies

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

3.3 *Assumptions*

This section identifies assumptions applicable to the Standard Protection Profile for Enterprise Security Management Policy Management [ESM PP PM] as specified in the Protection Profile, verbatim.

Table 3-3: Connectivity Assumptions

Assumption Name	Assumption Definition
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.ROBUST	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME	The TOE will receive reliable time data from the Operational Environment.
A.USERID	The TOE will receive identity data from the Operational Environment.

Table 3-4: Personnel Assumptions

Assumption Name	Assumption Definition
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment.

4.1 *Security Objectives for the TOE*

This section identifies Security Objectives for the TOE applicable to the Standard Protection Profile for Enterprise Security Management Policy Management [ESM PP PM], verbatim.

Table 4-1: TOE Security Objectives

Objective	TOE Security Objective Definition
O.ACCESSID	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.CONSISTENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.
O.CRYPTO	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
O.INTEGRITY	The TOE will contain the ability to assert the integrity of policy data.
O.MANAGE	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
O.POLICY	The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.
O.PROTCOMMS	The TOE will provide protected communication channels or administrators, other parts of a distributed TOE, and authorized IT entities.
O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

4.2 *Security Objectives for the Operational Environment*

This section identifies operational environment security objectives applicable to the Standard Protection Profile for Enterprise Security Management Policy Management [ESM PP PM] as specified in the Protection Profile, verbatim.

Table 4-2: Security Objectives for the Operational Environment

Objective	**Environmental Security Objective Definition**
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
OE.ROBUST	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.
OE.USERID	The Operational Environment shall be able to identify a user requesting access to the TOE.

5 Extended Components Definition

The components listed in the following table have been defined in the Standard Protection Profile for Enterprise Security Management Policy Management [ESM PP PM].

The extended components are denoted by adding "_EXT" in the component name. The extended class is denoted by "ESM_" in the component name.

5.1 *Extended Security Functional Components*

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	ESM_ACD.1	Access Control Policy Definition
2	ESM_ACT.1	Access Control Policy Transmission
3	ESM_ATD.1	Object Attribute Definition
4	ESM_ATD.2	Subject Attribute Definition
5	ESM_EAU.2	Reliance on Enterprise Authentication
6	ESM_EID.2	Reliance on Enterprise Identification
7	FAU_SEL_EXT.1	External Selective Audit
8	FAU_STG_EXT.1	External Audit Trail Storage
9	FCS_CKM_EXT.4	Cryptographic Key Zeroization
10	FCS_HTTPS_EXT.1	HTTPS
11	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
12	FCS_TLS_EXT.1	TLS
13	FMT_MOF_EXT.1	External Management of Functions Behavior
14	FMT_MSA_EXT.5	Consistent Security Attributes
15	FPT_APW_EXT.1	Protection of Stored Credentials
16	FPT_SKP_EXT.1	Protection of Secret Key Parameters

5.1.1 ESM_ACD.1 Access Control Policy Definition

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

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

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

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

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

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

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

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

5.1.2 ESM_ACT.1 Access Control Policy Transmission

Hierarchical to: No other components.

Dependencies: ESM_ACD.1 Access Control Policy Definition.

ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: **[selection: choose one or more of: immideately following creation of a new or updated policy, at a periodic interval, at the request of a compatible Secure Configuration Management product, *[assignment: other circumsntaces]*].**

5.1.3 ESM_ATD.1 Object Attribute Definition

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects: ***[assignment: list of object security attributes].***

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

5.1.4 ESM_ATD.2 Subject Attribute Definition

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: ***[assignment: list of subject security attributes].***

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

5.1.5 ESM_EAU.2 Reliance on Enterprise Authentication

Hierarchical to: No other components.

Dependencies: ESM_EID.2 Reliance on Enterprise Identification.

ESM_EAU.2.1 The TSF shall rely on **[selection: *[assignment: identified TOE compont(s) responsible for subject authentication, [assignment: identified Operational Environment component(s) responsible for subject authentication]*]** for subject authentication.

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

5.1.6 ESM_EID.2 Reliance on Enterprise Identification

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_EID.2.1 The TSF shall rely on **[selection: *[assignment: identified TOE component(s) responsible for subject identification], [assignment: identified Operational Environment component(s) responsible for subject identification]*]** for subject identification.

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

5.1.7 FAU_SEL_EXT.1 External Selective Audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation, FMT_MTD.1 Management of TSF Data.

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

a) **[selection: object identity, user identity, subject identity, host identity, event type]*;*** and
b) ***[assignment: list of additional attributes that audit selectivity is based upon]****.*

5.1.8 FAU_STG_EXT.1 External Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation, FTP_ITC.1 Inter-TSF Trusted Channel.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to ***[assignment: non-empty list of external IT entities and/or "TOE-internal storage"].***

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

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

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

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

5.1.9 FCS_CKM_EXT.4 Cryptographic Key Zeroization

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.1.10 FCS_HTTPS_EXT.1 HTTPS

Hierarchical to: No other components.

Dependencies: FCS_TLS_EXT.1 TLS.

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1

5.1.11 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with **[selection, choose on of: NIST Special Publication 800-90A using [selection: Hash DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)]]** seeded by an entropy source that accumulates entropy from **[selection: a software-based noise source; a hardware-based noise source].**

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of **[selection, choose one of: 128 bits, 256 bits]** of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

Note: Modified by TD0079.

5.1.12 FCS_TLS_EXT.1 TLS

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation.

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols **[selection: TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)]** supporting the following ciphersuites: **[selection:**

- **TLS_RSA_WITH_AES_128_CBC_SHA**
- **TLS_RSA_WITH_AES_256_CBC_SHA**
- **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**
- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA**
- **TLS_RSA_WITH_AES_128_CBC_SHA256**
- **TLS_RSA_WITH_AES_256_CBC_SHA256**
- **TLS_DHE_RSA_WITH_AES_128_CBC_SHA256**
- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA256**
- **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**
- **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**
- **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256**
- **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384**

].

Note: Modified by TD0320.

5.1.13 FMT_MOF_EXT.1 External Management of Functions Behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions, FMT_SMR.1 Security Roles.

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the functions of Access Control products: audited events, repository for audit storage, Access Control SFP, policy version being implemented, Access Control SFP behavior to enforce in the event of communications outage, ***[assignment: other functions]*** to ***[assignment: the authenorized identified roles].***

5.1.14 FMT_MSA_EXT.5 Consistent Security Attributes

Hierarchical to:	No other components.
Dependencies:	FMT_MOF_EXT.1 External Management of Functiona Behaviour

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

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

5.1.15 FPT_APW_EXT.1 Protection of Stored Credentials

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

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.
FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

5.1.16 FPT_SKP_EXT.1 Protection of Secret Key Parameters

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

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

5.2 *Extended Security Functional Components Rationale*

All extended security functional components are sourced directly from the PP and applied verbatim, except where modified by a technical decision.

6 Security Requirements

6.1 *Security Functional Requirements*

Conventions
The following conventions have been applied in this document:

- **Security Functional Requirements –** Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - **Iteration**: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1 (a) and FDP_ACC.1 (b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, "a" and "b".
    - **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold italics and are surrounded by brackets (e.g., ***[assignment]).***
    - **Selection**: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., ***[selection]***).
    - **Refinement**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in <u>***italicized bold and underlined text***</u>.

Note: Operations already performed in the [ESM PP PM] are not identified in this Security Target

- **Application notes** provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

- **Explicitly stated Security Functional Requirements** (i.e., those not found in Part 2 of the CC) are identified "_EXT" or "ESM" in the component name.)

- **Case** - [ESM PP PM] uses an additional convention which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST.

The TOE security functional requirements are listed in Table 6-1. All SFRs are based on requirements defined in Part 2 of the Common Criteria or defined in the Standard Protection Profile for Enterprise Security Management Policy Management [ESM PP PM].

Table 6-1: TOE Security Functional Components

Functional Component		
1	ESM_ACD.1	Access Control Policy Definition
2	ESM_ACT.1	Access Control Policy Transmission
3	ESM_ATD.1	Object Attribute Definition
4	ESM_ATD.2	Subject Attribute Definition
5	ESM_EAU.2 (1)	Reliance on Enterprise Authentication (Password authentication)
6	ESM_EID.2 (1)	Reliance on Enterprise Identification (Password authentication)
7	ESM_EAU.2 (2)	Reliance on Enterprise Authentication (LDAP authentication)
8	ESM_EID.2 (2)	Reliance on Enterprise Identification (LDAP authentication)
9	FAU_GEN.1	Audit Data Generation
10	FAU_SEL.1	Selectable Audit
11	FAU_SEL_EXT.1	External Selective Audit
12	FAU_STG_EXT.1	External Audit Trail Storage
13	FCS_CKM.1	Cryptographic Key Generation (for Asymmetric Keys)
14	FCS_CKM_EXT.4	Cryptographic Key Zeroization
15	FCS_COP.1 (1)	Cryptographic Operation (for Data Encryption/Decryption)
16	FCS_COP.1 (2)	Cryptographic Operation (for Cryptographic Signature)
17	FCS_COP.1 (3)	Cryptographic Operation (for Cryptographic Hashing)
18	FCS_COP.1 (4)	Cryptographic Operation (for Keyed-Hash Message Authentication)
19	FCS_HTTPS_EXT.1	HTTPS
20	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
21	FCS_TLS_EXT.1 (1)	TLS (Syslog and LDAP)
22	FCS_TLS_EXT.1 (2)	TLS (Agents)
23	FCS_TLS_EXT.1 (3)	TLS (Web interface)
24	FIA_AFL.1	Authentication Failure Handling
25	FIA_SOS.1	Verification of Secrets
26	FIA_USB.1	User-Subject Binding
27	FMT_MOF.1	Management of Functions Behavior
28	FMT_MOF_EXT.1	External Management of Functions Behavior
29	FMT_MSA_EXT.5	Consistent Security Attributes
30	FMT_MTD.1	Management of TSF Data
31	FMT_SMF.1	Specification of Management Functions
32	FMT_SMR.1	Security Management Roles
33	FPT_APW_EXT.1	Protection of Stored Credentials
34	FPT_SKP_EXT.1	Protection of Secret Key Parameters
35	FPT_STM.1	Reliable Time Stamps
36	FTA_SSL.3	TSF-initiated Termination
37	FTA_SSL.4	User-initiated Termination
38	FTA_TAB.1	TOE Access Banner
39	FTP_ITC.1	Inter-TSF Trusted Channel
40	FTP_TRP.1	Trusted Path

6.1.1 Class ESM: Enterprise Security Management

6.1.1.1 ESM_ACD.1 Access Control Policy Definition

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

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

Subjects: ***[process accessing GuardPoint]*** and

Objects: ***[resource set, user set, process set, time set];*** and

Operations: ***[create file, read file, write file, remove file, rename file, read file attribute, change file attribute, create directory, read directory, rename directory, remove directory, read directory attribute, change directory attribute, read file security attribute, change file security attribute, read directory security attribute, change directory security attribute, write file appending, link file];*** and

Attributes: ***[file name or path (resource set), user or group (user set), process hashed values (process set), time or day (time set)]***

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

6.1.1.2 ESM_ACT.1 Access Control Policy Transmission

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

6.1.1.3 ESM_ATD.1 Object Attribute Definition

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects: ***[***

Object: Resource Set
Attribute: directory path and/or file name

Object: User Set
Attribute: user name, user id, group name or group id

Object: Process Set
Attribute: hashed value of trusted process binaries

Object: Time Set
Attribute: time and/or day

].

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

6.1.1.4 ESM_ATD.2 Subject Attribute Definition

ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: ***[full path directory location on network host where the Transparent Encryption Agent is installed].***

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

6.1.1.5 ESM_EAU.2 (1) Reliance on Enterprise Authentication (Password authentication)

ESM_EAU.2.1 (1) The TSF shall rely on ***[Vormetric Data Security Manager]*** for subject authentication.

ESM_EAU.2.2 (1) The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

6.1.1.6 ESM_EID.2 (1) Reliance on Enterprise Identification (Password authentication)

ESM_EID.2.1 (1) The TSF shall rely on ***[Vormetric Data Security Manager]*** for subject identification.

ESM_EID.2.2 (1) The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

6.1.1.7 ESM_EAU.2 (2) Reliance on Enterprise Authentication (LDAP authentication)

ESM_EAU.2.1 (2) The TSF shall rely on ***[LDAP Authentication Server]*** for subject authentication.

ESM_EAU.2.2 (2) The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

6.1.1.8 ESM_EID.2 (2) Reliance on Enterprise Identification (LDAP authentication)

ESM_EID.2.1 (2) The TSF shall rely on ***[LDAP Authentication Server]*** for subject identification.

ESM_EID.2.2 (2) The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

6.1.2 Class FAU: Security Audit

6.1.2.1 FAU_GEN.1 Audit Data Generation

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

a) Start-up and shutdown of the audit functions; and
b) All auditable events identified in Table 3 for the not specified level of audit; and
c) ***[no other auditable events].***

Table 6-2: Auditable Events ([ESM PP PM] Table 3.)

Component	Event	Additional Information
ESM_ACD.1	Creation or modification of policy	Unique policy identifier
ESM_ACT.1	Transmission of policy to Access Control products	Destination of policy
ESM_ATD.1	Definition of object attributes	Identification of the attribute defined
ESM_ATD.1	Association of attributes with objects	Identification of the object and the attribute
ESM_ATD.2	Definition of subject attributes	Identification of the attribute defined
ESM_ATD.2	Association of attributes with subjects	None
ESM_EAU.2 (1)	All use of the authentication mechanism	None
ESM_EAU.2 (2)	All use of the authentication mechanism	None
ESM_EAU.2 (3)	All use of the authentication mechanism	None
FAU_SEL_EXT.1	All modifications to audit configuration	None
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FCS_HTTPS_EXT.1	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_TLS_EXT.1	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state	Action taken when threshold is reached
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	None
FIA_SOS.1	Identification of any changes to the defined quality metrics	The change made to the quality metric
FMT_SMF.1	Use of the management functions	Management function performed
FMT_SMR.1	Modifications to the members of the management roles	None
FTA_SSL.3	All session termination events	None

Component	Event	Additional Information
FTA_SSL.4	All session termination events	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***[message ID, the additional information identified in Table 3].***

6.1.2.2 FAU_SEL.1 Selective Audit

FAU_SEL.1.1 **Refinement:** The TSF shall be able to select the set of events to be audited from the set of all auditable events from ***[local definition]*** based on the following attributes:

a) ***[event type];*** and
b) ***[no additional attributes]***

6.1.2.3 FAU_SEL_EXT.1 External Selective Audit

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

a) ***[event type];*** and
b) ***[upload to server checkbox].***

6.1.2.4 FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to ***[external syslog using TLS].***

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

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

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

6.1.3 Class FCS: Cryptographic Support

6.1.3.1 FCS_CKM.1 Cryptographic Key Generation (for Asymmetric Keys)

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

[

- ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***
- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")***

]

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

6.1.3.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

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

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

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

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

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

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

[
(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater
(3) Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater
]

that meets the following:

Case: RSA Digital Signature Algorithm

- FIPS PUB 186-4, “Digital Signature Standard”;

Case: Elliptic Curve Digital Signature Algorithm

- FIPS PUB 186-4, “Digital Signature Standard”;

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

FCS_COP.1.1 (3) **Refinement**: The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm ***[SHA-256, SHA-384, SHA-512]*** and message digest sizes ***[256, 384, 512]*** bits that meet the following: FIPS Pub 180-4, “Secure Hash Standard.”

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

FCS_COP.1.1 (4) **Refinement**: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC***-[SHA-256, SHA-384],*** key size ***[256, 384 key size (in bits) used in HMAC],*** and message digest sizes ***[256, 384]*** bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code”, and FIPS Pub 180-4, “Secure Hash Standard.”

6.1.3.7 FCS_HTTPS_EXT.1 HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1

6.1.3.8 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with ***[NIST Special Publication 800-90A using [CTR_DRBG (AES)]]*** seeded by an entropy source that accumulates entropy from ***[a software-based noise source; a hardware-based noise source].***

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of ***[256 bits]*** of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

6.1.3.9 FCS_TLS_EXT.1(1) TLS (Syslog and LDAP)

FCS_TLS_EXT.1.1(1) The TSF shall implement one or more of the following protocols ***[TLS 1.2 (RFC 5246)]*** supporting the following ciphersuites:

[
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
].

Note: This SFR modified to conform to TD0320.

6.1.3.10 FCS_TLS_EXT.1(2) TLS (Agents)

FCS_TLS_EXT.1.1(2) The TSF shall implement one or more of the following protocols ***[TLS 1.2 (RFC 5246)]*** supporting the following ciphersuites:

[
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
].

Note: This SFR modified to conform to TD0320.

6.1.3.11 FCS_TLS_EXT.1(3) TLS (Web Interface)

FCS_TLS_EXT.1.1(3) The TSF shall implement one or more of the following protocols ***[TLS 1.2 (RFC 5246)]*** supporting the following ciphersuites:

[
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
].

Note: This SFR modified to conform to TD0320.

6.1.4 Class FIA: Identification and Authentication

6.1.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when ***[an administrator configurable positive integer within [1 to 10]]*** unsuccessful authentication attempts occur related to ***[remote administrative management login].***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[met],*** the TSF shall ***[lock the account for an administrator***

configurable period of time].

6.1.4.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet the following:

a) For environmental password-based authentication, the following rules apply:
   1. Passwords shall be able to be composed of a subset of the following character sets: ***[Standard ASCII character set]*** that include the following values ***[alphabet characters: a-z, A-Z, integers: 0-9, and a limited set of special characters: !@#$%^&*(){}[]];*** and
   2. Minimum password length shall settable by an administrator, and support passwords of 16 characters or greater; and
   3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and
   4. Passwords shall have a maximum lifetime, configurable by an administrator; and
   5. New passwords shall contain a minimum of an administrator-specified number of character changes from the previous password; and
   6. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based authentication, the following rules apply:
   1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

6.1.4.3 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

[

- ***Username***
- ***Password***
- ***Role***
- ***Domain***

]

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: ***[user security attributes are associated upon successful identification and authentication].***

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: ***[user security attributes can be changed only by an administrator with type “System Administrator” or “All” through the***

management interfaces of the TOE].

6.1.5 Class FMT: Security Management

6.1.5.1 FMT_MOF.1 Management of Functions Behavior

FMT_MOF.1 The TSF shall restrict the ability to ***[determine the behavior of, modify the behavior of]*** the functions: ***[DSM auditing functions]*** to ***[administrators with type "System Administrator" or "All"].***

6.1.5.2 FMT_MOF_EXT.1 External Management of Functions Behavior

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the functions of Access Control products: audited events, repository for audit storage, Access Control SFP, policy version being implemented, Access Control SFP behavior to enforce in the event of communications outage to ***[administrators with type "Security Administrator", "Domain and Security Administrator", or "All" inside a given domain].***

6.1.5.3 FMT_MSA_EXT.5 Consistent Security Attributes

FMT_MSA_EXT.5.1 The TSF shall ***[identify the following internal inconsistencies with a policy prior to distribution: Rule A: When a newly added or updated security rule is identical to an existing security rule, Rule B: when two security rules have identical security objects but the effects are contradictory (one security rule with permit effect while the other rule has deny effect), Rule C: When a security rule is a superset of subsequent security rule, then the subsequent security rule will not get executed].***

FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: ***[issue a prompt for an administrator to manually resolve the inconsistency].***

6.1.5.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to ***[modify, delete, [add]]*** the ***[authentication data: username and password]*** to ***[administrators with type "System Administrator" or "All"].***

6.1.5.5 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: ***[the management activities listed in Table 6-3].***

Table 6-3: Management Functions within the TOE ([ESM PP PM] Table 4.)

Requirement	Management Activities
ESM_ACD.1	Creation of policies

ESM_ACT.1	Transmission of policies
ESM_ATD.1	Definition of object attributes Association of attributes with objects
ESM_ATD.2	Definition of subject attributes Association of attributes with subjects
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
FAU_SEL.1	Configuration of auditable events
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities
FAU_STG_EXT.1	Configuration of external audit storage location
FIA_AFL.1	Configuration of authentication failure threshold value Configuration of actions to take when threshold is reached Execution of restoration to normal state following threshold action (if applicable)
FIA_SOS.1	Management of the metric used to verify secrets
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes
FMT_MOF_EXT.1	Configuration of the behavior of other ESM products
FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)
FMT_MTD.1	Management of user authentication data
FMT_SMR.1	Management of the users that belong to a particular role
FTA_TAB.1	Maintenance of the banner
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)

6.1.5.6 FMT_SMR.1 Security Management Roles

FMT_SMR.1.1 The TSF shall maintain the roles ***[“System Administrator”, “Domain Administrator”, “Security Administrator”, “Domain and Security Administrator”, “All”].***

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

6.1.6 Class FPT: Protection of the TSF

6.1.6.1 FPT_APW_EXT.1 Protection of Stored Credentials

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

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

6.1.6.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

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

6.1.6.3 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

6.1.7 Class FTA: TOE Access

6.1.7.1 FTA_SSL.3 TSF-initiated Termination

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

6.1.7.2 FTA_SSL.4 User-initiated Termination

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

6.1.7.3 FTA_TAB.1 TOE Access Banner

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

6.1.8 Class FTP: Trusted Paths/Channels

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

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

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

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

Note: This SFR modified to conform to TD0245.

6.1.8.2 FTP_TRP.1 Trusted Path

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

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

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

Note: This SFR modified to conform to TD0245.

6.2 *Security Assurance Requirements for the TOE*

6.2.1 TOE Security Assurance Requirements

This section defines the assurance requirements for the TOE. The assurance activities to be performed by the evaluator are defined in Sections 6 and Appendix C of the Standard Protection Profile for Enterprise Security Management Policy Management dated [ESM PM PP]. The ESM PM PP draws from the CC Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing. The TOE security assurance requirements, summarized in the table below, identify the management and evaluative activities required to address the threats identified in ESM PM PP.

Table 6-4: Assurance Components

Assurance Class	**Assurance Components**	
Development	ADV_FSP.1	Basic Functional Specification
Guidance documents	AGD_OPE.1	Operational User guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability analysis

The following tables state the developer action elements, content and presentation elements and evaluator action elements for each of the assurance components.

Table 6-5: ADV_FSP.1 Basic Functional Specification

Developer action elements	
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
Content and presentation elements	
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
Evaluator action elements	
ADV_ FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_ FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Table 6-6: AGD_OPE.1 Operational User Guidance

Developer action elements	
AGD_OPE.1.1D	The developer shall provide operational user guidance.
Content and presentation elements	
AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
Evaluator action elements	
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 6-7: AGD_PRE.1 Preparative Procedures

Developer action elements	
AGD_PRE.1.1D	The developer shall provide the TOE, including its preparative procedures.
Content and presentation elements	
AGD_ PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_ PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
Evaluator action elements	
AGD_ PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_ PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

Table 6-8: ALC_CMC.1 Labeling of the TOE

Developer action elements	
ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
Content and presentation elements	
ALC_CMC.1.1C	The TOE shall be labeled with its unique reference.
Evaluator action elements	
ALC_CMC.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 6-9: ALC_CMS.1 TOE CM Coverage

Developer action elements	
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
Content and presentation elements	
ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
Evaluator action elements	
ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 6-10: ATE_IND.1 Independent Testing – Conformance

Developer action elements	
ATE_IND.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
ATE_IND.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

Table 6-11: AVA_VAN.1 Vulnerability Survey

Developer action elements	
AVA_VAN.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
AVA_VAN.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

7 TOE Summary Specification

Section 7 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 2.5 Logical Scope of the TOE. The following sub-sections describe how the TOE meets each SFR listed in Section 6.

Table 7-1: Security Functional Requirements Mapped to Security Functions

Security Functions	Sub-Functions	SFRs
System Monitoring	SM-1: System Monitoring	FAU_GEN.1 FPT_STM.1 FAU_SEL.1
	SM-2: Audit Storage	FAU_STG_EXT.1
Robust TOE Access	TA-1: Strength of Secrets	FIA_SOS.1
	TA-2: Authentication Failure	FIA_AFL.1
	TA-3: Session Termination	FTA_SSL.3 FTA_SSL.4
Authorized Management	AM-1: Management I&A	ESM_EAU.2 (1) ESM_EID.2 (1) ESM_EAU.2 (2) ESM_EID.2 (2) ESM_EAU.2 (3) ESM_EID.2 (3) FIA_USB.1 FPT_APW_EXT.1
	AM-2: Management Roles	FMT_MOF.1 FMT_SMR.1
	AM-3: Remote Administration	FTP_TRP.1
Policy Definition	PD-1: Policy Definition	ESM_ACD.1 ESM_ATD.1 ESM_ATD.2 FMT_MOF.1 FMT_MSA_EXT.5 FMT_SMF.1
Dependent Product Configuration	PC-1: TOE Management Functions	FMT_MOF.1 FMT_MTD.1 FMT_SMF.1
	PC-2: Agent Configuration	FAU_SEL_EXT.1 FMT_MOF_EXT.1
Confidential Communications	CC-1: Agent Communications	ESM_ACT.1 FCS_TLS_EXT.1 FCS_HTTPS_EXT.1 FMT_MOF.1 FTP_ITC.1

Security Functions	Sub-Functions	SFRs
	CC-2: User Communications	ESM_EAU.2 (1) ESM_EID.2 (1) ESM_EAU.2 (2) ESM_EID.2 (2) ESM_EAU.2 (3) ESM_EID.2 (3) FCS_HTTPS_EXT.1 FIA_USB.1 FMT_MOF FTP_TRP.1
	CC-3: External Server Communications	FMT_MOF FTP_ITC.1
	CC-4: Key Protection	FPT_SKP_EXT.1
Access Bannering	AB-1: Banner	FTA_TAB.1
Cryptographic Services	CS-1: Crypto	FCS_CKM.1 FCS_CKM_EXT.4 FCS_COP.1 (1) FCS_COP.1 (2) FCS_COP.1 (3) FCS_COP.1 (4) FCS_RBG_EXT.1

7.1 *System Monitoring*

7.1.1 SM-1: Audit Generation

Log files and log data are generated on the DSM and its agents. The TSF generates audit records for the security significant events listed in Table 6-2: Auditable Events ([ESM PP PM] Table 3.). The DSM logs system-level events, such as failed login attempts, a broken network connection, and inoperable DSM database, and application-level events, such as evaluating a policy, applying GuardPoints, and adding administrators.

Application-level Logs
Application-level events from the DSM and the agents are collected in the Message Log and can be viewed in the “Logs” window of the Remote Administrative Management by administrators of type All or Security Administrator with Host role permission. The “Logs” window displays the following information:

Table 7-2: Message Log Information

Column	Description
ID	Entries are numbered in the order in which the DSM enters them into the log database.
Time	The time at which the event occurred. Timestamps are in the form YYYY-MM-DD HH:MM:SS.mm, <Time zone>, where Y=year, M=month, D=day, H=hour, M=minute, S=second, and m=millisecond. Timestamps is relative to the agent for Transparent Encryption Agents. If the DSM and Transparent Encryption Agents are in different time zones, time order

	will not match the event sequences.
Severity	Severity levels are D(ebug), I(nfo), W(arn), E(rror), and F(atal). Severity is configurable and only messages that match the severity level are entered in the log. Log levels are cumulative, so each level includes the levels below it. For example, FATAL logs only fatal messages, whereas WARN logs warning messages, and includes ERROR messages and FATAL messages. Details about the log levels are provided in "Log message levels" on page 478.
Source	The name of the host on which the event took place.
Message	The message associated with the event.

The general format of a Transparent Encryption Agent log entry message is:

> CGP2602I: [SecFS, 0] Level: Policy[policyName?] User[userID?] Process[command?] Access[whatIsItDoing?] Res[whatIsItDoingItTo?] Key[Key Name?] Effect[allowOrDeny? Code (whatMatched?)]

where:

- ***SECFS*** indicates that the message was generated by a Transparent Encryption Agent. You can enter secfs in the Search Message text-entry box in the Logs window to display Transparent Encryption Agent policy evaluation and GuardPoint activity for all configured hosts.
- ***Level*** indicates the importance of the message. For example, AUDIT indicates an informational message, whereas ALARM indicates a critical failure that should not go ignored.
- ***Policy[]*** indicates the name of the policy that is being used to evaluate the access attempt.
- ***User[]*** identifies the system user attempting to access data in the GuardPoint. It typically displays the user name, user ID, and group ID.
- ***Process[]*** indicates the command, script, or utility being executed.
- ***Access[]*** indicates what is being attempted. Access may be read_dir, remove_file, write_file_attr, write_app, create_file, etc. These correspond to the Access methods that you configure in the policy. read_dir corresponds to d_rd. remove_file corresponds to f_rm. And so on.
- ***Res[]*** indicates the object being accessed by Process[].
- ***Key[]*** *indicates the Key name being used*
- ***EFFECT[]*** indicates the rule that matched and, based upon that rule, whether or not the DSM grants access. Rule matching is described below. Access states may be either PERMIT or DENIED.

Note: The TOE also generates system logfiles, which can be viewed on the DSM Appliance using CLI commands; they are not accessible through the TOE's user interfaces. These system logfiles are used only for maintenance and diagnostic purposes only. In addition, the access control product using the Transparent Encryption Agent is outside the scope of the ESM PP PM evaluation.

(FAU_GEN.1)

The audit logs require accurate timestamps: therefore, it is important to synchronize the clocks of all the systems that host the DSM and the agents for accurate time. The DSM appliance has a system clock that can provide the time. The TOE can also be configured to use an NTP server in the Operational Environment. Use of an external NTP server for reliable time is the recommended configuration.

(FPT_STM.1)

The audit events generated by the DSM can be selected by their event type (i.e., severity level). The value of the configured "Logging Level" sets the severity level at which entries are generated, displayed and sent to the syslog server. The choices are DEBUG, INFO, WARN, ERROR, and FATAL. Log levels are cumulative, so each level includes the levels below it. For example, FATAL logs only fatal errors, whereas WARN logs warnings, and includes ERROR and FATAL conditions. The default is INFO.

The "Logging Level" parameter for the DSM can be configured by an administrator of type All or System Administrator via the Remote Administrative Management. The "Logging Level" can be viewed and modified on the "Server" tab of the "Log Preferences" window.

Configuration of the Transparent Encryption Agent logs requires the administrator have the All, Domain and Security, or Security Administrator type with Host role permission, and to be assigned to the agent's domain. Similar to DSM log, the Transparent Encryption agent audit events can be selected by their severity level. The value of the configured "Level" sets the severity level at which audit entries are generated and sent to the DSM. The choices are DEBUG, INFO, WARN, ERROR, and FATAL. Log levels are cumulative; thus, each level includes the levels below it.

The severity "Level" parameter of Transparent Encryption Agent log can be viewed and modified on the "FS Agent Log" tab of a host by All, Domain and Security, or Security Administrator via the Remote Administrative Management. The Transparent Encryption Agent log can be turned off by un-selecting "Upload to Server" checkbox. When "Upload to Server" checkbox is unchecked, the Transparent Encryption Agent will not upload audit logs to DSM.
(FAU_SEL.1)

7.1.2 SM-2: Audit Storage

System-level events are logged in files on the DSM appliance's file system. Application-level events are stored in the DSM database. DSM log messages can also be sent to a syslog server. System Administrators can configure an external syslog server for system-level messages. Domain Administrators can configure an external syslog server for application-level messages

Note: Domain Administrators can configure a domain to send domain-specific events to one (or more) syslog servers. The system-level events configured to be sent to a syslog server by the System Administrator are general application events which to not apply to any particular *domain. Events for all domains and the system-level events can be sent to the same syslog server.*

Transparent Encryption Agent log data can be stored on the local host, sent to a syslog server, or uploaded to the DSM. The “Syslog Server” window in the Remote Administrative Management is used to configure the remote syslog servers to which to send DSM log data. The log data sent to remote syslog servers comprises log data that is generated on the DSM and, when “Upload to Server” is enabled in the “Log Preferences” window, log data that is generated on hosts.

The DSM administrator can configure the DSM to forward log data to a syslog server using TLS transport protocol. A X.509 certificate from syslog server is imported to DSM to provide authentication to syslog server. If syslog server becomes temporarily unavailable, the syslog messages will not be forwarded to the syslog server. When the connection is re-established there is no reconciling the differences between the syslog server and the local audit records. The local audit logs has maximum of 100,000 records and the records are stored in a local database. If the connection to syslog is down for extended period of time, the local copy of the audit log could have rotated and overwriting the audit records that have not been off loaded to the syslog server. To mitigate potential audit log loss due to connectivity issues, the TOE implements support for multiple redundant syslog servers. When a syslog server becomes unavailable, the DSM will continue to forward audit logs to the surviving syslog servers.

Note: A default syslog port number is not provided. While there is no default port for syslog data transmission via TCP, port 1514 has been used successfully.

(FAU_STG_EXT.1)

7.2 *Robust TOE Access*

7.2.1 TA-1: Strength of Secrets

The TSF always enforces the following rules for administrator passwords:

- An administrator password can contain standard ASCII alphabet characters (a-z, A-Z), integers (i.e., 0-9), and a limited set of special characters (!@#$%^&*(){}[]). Blank spaces are not supported.

- The individual elements in this combination of characters cannot occur in adjacent sequence. That is, a password cannot contain two instances of the same element if they are next to each other. For example, “mississippi" will not be accepted, but “misSisSipPi” will.

The additional password restraints listed in the following table can configured by an administrator of type All or Security Administrator with the Host role.

Table 7-3: Password Policy Parameters

Parameter	Description

Parameter	Description
Password Duration	The number of days set by an administrator after which the password will expire. The range is between 6 and 365. The default is 90. The password expiration interval is applied globally to each administrator account. If the administrator does not change the password prior to expiration, the administrator must reset the password immediately the next time s/he attempts to log in; otherwise the Remote Administrative Management will not start. Password Duration must be set to a value greater than Password Expiration Notification. For example, if Password Duration is set to 90 days, then the Password Expiration Notification must be set to 89 days or less.
Password History	The same password cannot be used more than once per the set value of the password history. The default is 4. Setting the value to 0 permits reuse of the current password.
Minimum Password Length	The minimum number of characters that must be in the password. The range is between 8 and the operating system limit. The default is 8.
Password Expiration Notification	The number of days prior to password expiration at which to begin to notify the administrator that their password is about to expire. The range is between 6 and 31. The default is 31.
Require Uppercase	When enabled, requires at least one uppercase alphabet character (i.e., A-Z) in the administrator password. Enabled by default.
Require Numbers	When enabled, requires at least one integer (i.e., 0-9) in the administrator password. Enabled by default.
Require Special Characters	When enabled, requires at least one of accepted special characters (!@#$%^&*(){}[]) in the administrator password. Enabled by default.
Ignore Login Username Case	Handle login username as case insensitive. Enabled by default.

If an administrator forgets his or her password, another administrator can reset the password. When a password is changed, the password enters an “expired” state. The administrator must enter a new password the next time s/he logs into the TOE.

Password changes and the administrators performing those changes are audited and logged.

(*FIA_SOS.1)*

7.2.2 TA-2: Authentication Failure

The TSF enforces authentication failure handling for the Remote Administrative Management user interface.

After a configured number of failed authentication attempts, the TOE locks the user account for a configurable period of time and ignore all further login attempts using that account. The default number of attempts is 3, and the default user lockout is 60 minutes. The locked user account automatically re-enabled after lockout period, or can be manually reset by the administrator.

The parameters used for authentication failure can be configured by an administrator of type All or Security Administrator with the Host role:

- **Maximum Number of Login Tries:** The maximum number of unsuccessful login attempts before disabling the user interfaces for a set interval of time. The default number of tries allowed is 3. This lockout only applies to the account that is exceeding failed login attempts

- **User Lockout Time:** The interval to wait before re-enabling the user interfaces and allowing administrators to login. The default is 60 minutes

(FIA_AFL.1)

7.2.3 TA-3: Session Termination

A Remote Administrative Management user can terminate his/her web session at any time by clicking the “Log Out” text that is located in the top-right corner of the Remote Administrative Management banner.

(FTA_SSL.4)

The TSF enforces an inactivity timeout for Remote Administrative Management sessions. After a specified time interval of inactivity, the user will be automatically logged out of the Remote Administrative Management Web session. Any unsaved changes made by that administrator will be discarded. The Remote Administrative Management Timeout period can be set by an administrator of type All or Security Administrator with Host role permission. The timeout interval can be set to: 5 minutes, 20 minutes, 1 hour, 2 hours, or 8 hours. The default is 1 hour. When an administrator changes the Remote Administrative Management interface timeout value, the new timeout value will only apply to subsequent administrator login sessions and not to the existing administrator session.

(FTA_SSL.3)

7.3 *Authorized Management*

7.3.1 AM-1: Management I&A

The TSF enforces two methods of user authentication for all authorized administrators of the TOE:

1. Password Authentication
2. LDAP Authentication

Password Authentication
Password authentication of users is done solely by the TSF. This method uses a static (constant) password that changes only when a DSM administrator manually changes it.

An administrator must enter his/her username and password in the text-entry boxes of the Remote Administrative Management login screen. The TSF will check the entered identification and authentication data again that stored in the user's account before allowing any access to the functionality of the Remote Administrative Management.

(ESM_EAU.2 (1), ESM_EID.2 (1))

Static passwords are stored in the DSM database protected by PBKDF2 (Password-Based Key Derivation Function 2) as specified in RFC 8018.

(FPT_APW_EXT.1)

LDAP Authentication
The Vormetric DSM allows for integration with Directory Access Protocol (LDAP) directory services. This feature allows the DSM Administrator to import user criteria instead of recreating it from scratch. The DSM uses TLS to protect communications between itself and LDAP Authentication Server. A X.509 certificate from LDAP server is imported to DSM to provide authentication to LDAP server.
Note: If a Login Name already exists in the Vormetric DSM database, the Import function will not overwrite existing users with the same login name.

The external LDAP authentication server can also be used to authenticate administrators of the TOE. For LDAP authentication, an LDAP authentication object must be created to provide user authentication services. The System Administrator must:

- define settings for the connection to the LDAP server
- select the directory context
- define search criteria used to retrieve user data from the server

As with static password authentication, users must enter their username and password on the Remote Administrative Management login screen and be successfully authenticated by the LDAP server before being allowed access to the management functions of the TOE.

(ESM_EAU.2 (2), ESM_EID.2 (2))

Once a user has been successfully identified and authenticated by the TSF, the following attributes stored in the user's account are associated with the user's session:

- Username
- Password
- Role
- Domain

These security attributes are used to associate the subject with the user.

New user accounts can be added by an administrator of type System Administrator or All. All users may change their own password. Only an administrator of type System Administrator or All can change another user's password

If an administrator is currently running an active Remote Administrative Management session when the System Administrator changes his or her password, the Remote Administrative Management session is immediately terminated and the administrator must log in again.

When an administrator of type System Administrator or All changes the password of an administrator of type Domain Administrator, Security Administrator, or All, the Domain Administrator, Security Administrator, or All account is disabled in every domain of which it is a member, and it must be reassigned to the domain by a different administrator of type Domain Administrator, Domain and Security Administrator, or All before the administrator can enter a domain. A disabled administrator can log onto the DSM, but the domain selection radio buttons are opaque and cannot be selected, so the administrator cannot enter any domain and cannot modify the DSM configuration.

In the case of changed passwords, the Domain Administrator, Security Administrator, or All account must be added back into every domain of which it is a member.
The System Administrator can delete domains or change their description. The Domain Administrator adds and removes Security Administrators and other Domain Administrators to and from domains.

(FIA_USB.1)

7.3.2 AM-2: Management Roles

The administrative functionality of the TOE is based upon an authorized user's administrative type, which equates to the CC definition of a role. The menus displayed by the Remote Administrative Management and the tasks administrators can perform through the Remote Administrative Management are dependent upon their administrator type.

Roles in the Vormetric Data Security Manager apply to Administrative Domains. A domain is self-contained environment comprised of policies, keys, hosts, users, and audit records. The configuration data that administrators can see is dependent upon the domain in which they are working. The Remote Administrative Management provides fully separated domains, where the work and configuration data in one domain is invisible to administrators in other domains.

Administrative tasks are performed in each domain based upon each administrator's assigned role in that domain.

Segmenting administrative functions by type ensures that one administrator cannot control the entire data security process. The TOE implements the following administrator types for administrative access control:

- **System Administrator:** Top-level administrator who creates domains and administrative accounts, and adds one administrator to each domain. Other than assigning one administrator to a domain, the System Administrator has no window into domains or access to protected data.
- **Domain Administrator:** Assigns administrators to domains. The Domain Administrator also configures additional access constraints for administrators of type Security Administrator. The Domain Administrator cannot remove administrators or domains. In addition, the Domain Administrator does not have access to guarded data.
- **Security Administrator:** This administrator performs most of the data protection work. This administrator creates keys, policies, configures hosts, and applies GuardPoints. This administrator is not aware of the System and Domain Administrators. Security Administrators can be configured with one or more permissions, which further limit their administrative capabilities. The permissions are applicable only in the current domain. A Security Administrator can be assigned different permissions in different domains. The following permissions may be assigned to a Security Administrator:
    - ***Audit***: The audit permission can only view log data.
    - ***Key***: The key permission can create, edit, and delete local key-pairs, public keys only, and key groups. It can also view log data.
    - ***Policy:*** The policy permission can create, edit, and delete policies. It can also view log data.
    - ***Host:*** The host permission can configure, modify, and delete hosts and host groups. It can also view log data. The Challenge & Response permission is automatically selected when the Host role is selected.
    - ***Challenge & Response:*** The Challenge & Response permission must be enabled for a Security Administrator to display the Host Password Challenge & Response window. The window is used to enter a challenge string and display the response string. The response string is a temporary password that the system user enters to decrypt cached encryption keys when there is no connection to the DSM.

      The Challenge & Response permission is automatically enabled when the Host permission is enabled. You may disable the Host permission afterwards to leave just the Challenge & Response role enabled. With just this permission enabled, the Security Administrator has access to the Dashboard, Domains->Switch Domains, and Hosts->Host Password Challenge & Response menus only.
- **Domain and Security Administrator:** This administrator can perform the tasks of both the System Administrator and the Domain Administrator.
- **All**: This administrator can perform the tasks of all three of the administrative types combined.

An administrator is assigned one administrative type and is allowed to perform the tasks for that one administrative type only.

Administrators may be added and existing administrator attributes may be modified by administrators of type System Administrator or All.

Note: The Vormetric DSM also has the concept of a Network Administrator role, which performs network and system configuration using only the management functions of the CLI. The CLI is used only for off-line maintenance and initial configuration of the TOE and is not part of the scope of the evaluation. Therefore, the Network Administrator is not involved with the run-time administration of the TOE and is not considered a TOE administrator.

(FMT_SMR.1)

Only administrators of type System Administrator or All have the ability to determine and modify the behavior of the TOE's auditing functions

A complete listing of the management functions available to each administrative type is shown in Table 7-6: DSM Management Functions by Administrator Type.

(FMT_MOF.1)

7.3.3 AM-3: Remote Administration

The TSF secures the remote interactive sessions of administrative users of the Remote Administrative Management user interface using TLS/HTTPS.

(FTP_TRP.1)

7.4 *Policy Definition*

7.4.1 PD-1: Policy Definition

The access control policies defined in the DSM are used to protect system files, data files and folders, and applications residing on network hosts. The Vormetric Transparent Encryption Agent installed on the host enforces these policies. The access control policies managed by the DSM are associated with GuardPoints, which are the starting points at which to apply policies. A GuardPoint is a location in the Transparent Encryption Agents host's file system hierarchy where everything underneath has the policy applied to it. The Transparent Encryption Agent intercepts any attempt to access anything in the GuardPoint and uses policies obtained from the DSM to grant or deny the access attempt.

These policies can be created, deleted and modified by administrators of type All, Domain and Security, or Security Administrator with Policy role permission in the domain.

The Remote Administrative Management provides two methods of composing a Transparent Encryption Agent policy:

1. The Policy Wizard, accessed by the "Policies->Policy Wizard" menu, can be used to create simple policies.

2. The Policy Composer, accessed by “Policies” in the Remote Administrative Management menu bar, constructs and configures detailed Transparent Encryption Agent policies.

Note: Only the Policy Definition is evaluated. Policy enforcement of the Transparent Encryption Agent is out of evaluation scope.

(FMT_MOF.1, FMT_SMF.1)

The TOE is capable of creating the policy and the Access Control product (Transparent Encryption Agent) is capable of consuming the policy. The Access Control elements contain the following.

- Subjects: *Process accessing GuardPoint*
- Objects: *resource set, user set, process set, time set*
- Operations: *create file, read file, write file, remove file, rename file, read file attribute, change file attribute, create directory, read directory, rename directory, remove directory, read directory attribute, change directory attribute, read file security attribute, change file security attribute, read directory security attribute, change directory security attribute, write file appending, link file.*
- Attributes:
    - *File name or path (resource set)*
    - *User or group (user set)*
    - *Process hashed values (process set)*
    - *Time or day (time set)*

Policies are identified by a policy name and a version number and are composed of security rules. A security rule defines the users or user groups authorized to have specified access to specific files and directory paths for a designated period of time. The rule defines who is accessing data, what are they doing with the data, where the data is located, when the Security Rule is applicable, and how the data can be accessed.

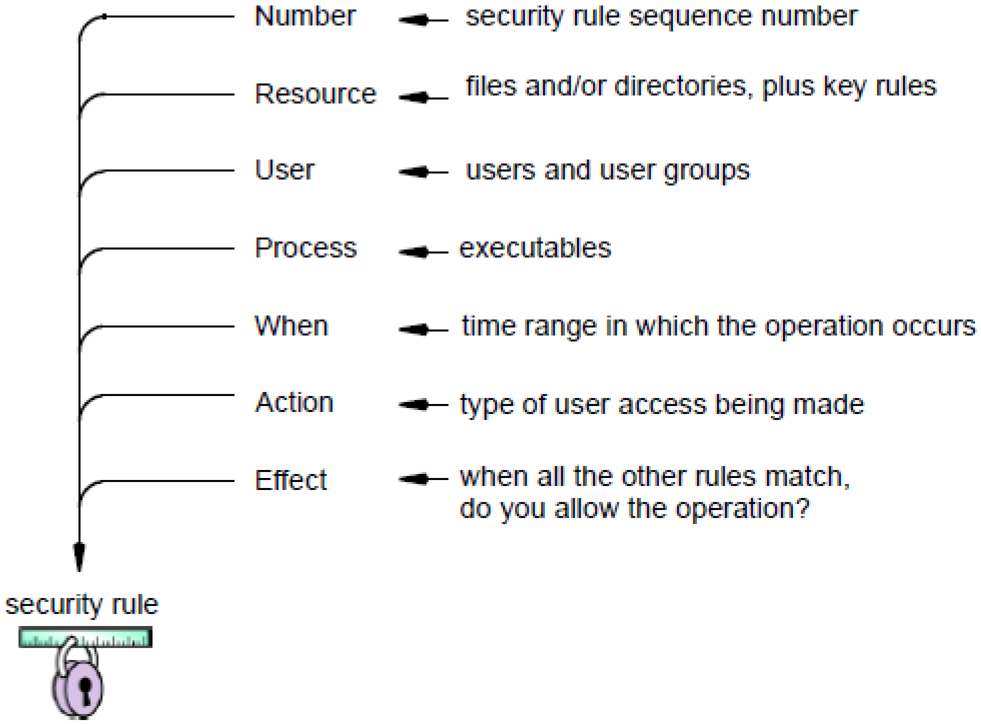
Number
security rule sequence number
Resource
files and/or directories, plus key rules
User
users and user groups
Process
executables
When
time range in which the operation occurs
Action
type of user access being made
Effect
when all the other rules match,
do you allow the operation?
security rule

Figure 3: Security Rule Structure

A Security Rule is composed of the following elements:

Sequence Number

If the policy contains more than one security rule, the security rules are executed in sequential order. The rules that make up the policy are evaluated in order from top to bottom, and the first matching rule's effect is applied. The sequential processing stop at the first match of security rule. The effect applies to first security rule that matches completely on resource set, user set, process set, when set, and actions. The policy engine discards any partial matches of object sets in the security rule and continues to evaluate the subsequent security rule. If none of the security rule matches, then policy engine will deny access to the GuardPoint. In addition, the sequence number is also used for indicating security rule in the policy conflict error message.

Resource Set

A resource specifies the files and directories to which to apply the security rule. A resource set is a collection of directories, files, or both, to be protected. A resource may be a combination of a directory and a file, and include variables and patterns to specify a set of resources.

If a resource set is not configured for a security rule then all files and directories in the GuardPoint are assumed.

User Set

A user defines the security context of who is accessing resource files and directories. A user set is a collection of individual users. User sets are reusable. Any user set in the current Security Server configuration can be used by any other policy.

A user can be identified using a combination of one or more attributes. A specific user can be identified using the user name, user identification number, and user group number, or, multiple users can be identified by group affiliation alone. There are other attributes that can specify the individual, or group of individuals, affected by the security rule.

User identification is optional. If user(s) are not defined in the security rule, then user identification is not used to determine access permissions.

Process Set

A process set is a collection of executables. These are any programs, utilities, or scripts that can be executed on the host system that need to access data within a set GuardPoint. Process sets are reusable. Any process set in the current Security Server configuration can be used by any other policy. Processes can be signed or unsigned. Signing a process is a means to verify that the executable has not been tampered.

When an executable attempts to access data in a GuardPoint, and processes are configured, the executable is verified against the Process rule. When signature matching is used, the signature of the executable is compared against the equivalent signature in the Security Server database. When file path and name are used, the path and name of the executable are compared against the path and name in the process set.

Time Constraint (when)

A security rule can include time constraints to limit access based upon time, day of the week, calendar date, or a combination of these.

By default, there is no time constraint. Other rules permitting, data can be accessed at any time.

Access Method (action)

An “action” is an attempt to access protected data in some way. The Policy Composer provides a range of access methods to specify precisely the action required to match the security rule. The action is identified, evaluated, and used as a factor in determining whether or not to grant access.

Specifying an access method is optional. If an access method is not defined, the default all_ops, or “all operations”. The allowed actions are described below:

Table 7-4: Security Rule Actions

Action	Description
all_ops	All operations. That is, any attempt to access the data in any way. This is the default if no action is specified.
d_chg_att	Change directory attributes (e.g., chown usr dir1).

Action	Description
d_chg_sec	Pertains to attempts to change any security property of a Windows folder, such as you would on the Security tab of the Properties window.
d_mkdir	Make a new directory (e.g., mkdir dir1 dir2) tar.
d_rd	View directory contents (e.g., ls dir; cd dir).
d_rd_att	Read the attributes of a directory (e.g., ls -la dir1).
d_chg_attr	Change directory attributes (e.g., chmod).
d_rd_sec	Pertains to attempts to view the security properties of a Windows folder, such as those on the Security tab of the Properties window.
d_chg_sec	Pertains to attempts to view the security properties of a directory
d_ren	Rename a directory (e.g., mv dir1 dir2).
d_rmdir	Delete a directory (e.g., rm -r dir1).
f_chg_att	Change file attributes (e.g., chmod).
f_chg_sec	Pertains to attempts to change any security property of a Windows file, such as those on the Security tab of the Properties window.
f_cre	Create a new file.
f_link	Link to a file (e.g., ln file_name link_name).
f_rd	Read a file.
f_rd_att	Read the attributes of a file (e.g., ls -l file).
f_rd_sec	Pertains to attempts to view the security properties of a Windows file, such as those on the Security tab of the Properties window.
f_ren	Rename a file.
f_rm	Delete a file.
f_wr	Write to an existing file.
f_wr_app	Append data to a file.
key_op	Key operations. This requires 2 keys. One key is specified in the Key Selection Rules tab and the other in the Data Transformation Rules tab of the Policy Composer. Key Selection keys are the encryption keys for the current security rule. Data Transformation keys are used to migrate data from an encrypted form to a non-encrypted form or to change the encryption keys used to access the data.
Read	This method is a collection of the preceding methods that are related to reading files, directories, and their attributes. This method comprises f_rd, f_rd_att, f_rd_sec, d_rd, d_rd_attr, and d_rd_sec.
Write	This method is a collection of the preceding methods that are related to writing to files, directories, and their attributes. This method comprises f_wr, f_cre, f_ren, f_rm, f_link, f_chg_attr, f_chg_sec, d_ren, d_chg_att, d_chg_sec, d_mkdir, and d_rmdir.

Effect

An “effect” determines the access to allow. An effect is applied when the conditions set in a security rule are matched. An effect is required for a security rule. An effect must be configured before a security rule can be added to a policy. The following table describes the available effects:

Table 7-5: Security Rule Effects

Effect	Description

Effect	Description
apply_key	Applies an encryption key to data in a GuardPoint. When applied, data copied into the GuardPoint is encrypted with the key specified in the Key Selection Rules tab and data that is accessed in the GuardPoint is decrypted using the same key. If apply-key is selected, the key rules to apply for encrypting and decrypting the resources must be specified through the Policy Composer.
Audit	Used in conjunction with *permit* or *deny*, *audit* creates an entry in the Message Log that describes what is being accessed, when it is being accessed, the security rule being applied, and other statistical information that can help to evaluate the performance and efficacy of the security configuration
Deny	Deny the access attempt to the resource. For example, an effect can be specified that denies any attempt to access a resource. *permit* and *deny* cannot be used in the same effect.
Permit	Grant the access attempt to the resource. For example, an effect can be specified that allows writing to a directory. *permit* and *deny* cannot be added to the same effect.

(ESM_ACD.1, ESM_ATD.1, ESM_ATD.2)

The DSM detects definition of ambiguous policies during creation and issues a prompt for an administrator to manually resolve the inconsistency. The rules that make up the policy are evaluated in order from top to bottom, and the first matching rule's effect is applied. As an added layer of protection, a sanity check on various policy parameters is performed when the policy is updated. The Policy Composer in DSM provides a warning to user for potential security rule conflicts in the policy. The Policy Composer in DSM identifies three internal inconsistencies with policy prior to distribution. Rule A: When a newly added or updated security rule is identical to an existing security rule, the Policy Composer gives out a warning message and specifying conflicting rule numbers in the message. Rule B: Policy Composer also gives out warning when two security rules have identical security objects but the effects are contradictory (one security rule with permit effect while the other rule has deny effect). Rule C: If a security rule is a superset of subsequent security rule, then the subsequent security rule will not get executed. The Policy Composer detects the superset security rule and gives out warning message for the subsequent security rule.

The Policy Composer allows the TOE administrator to define detailed policies to enforce robust file access control on network hosts.

The following policy assertions are covered by the evaluation.

Access control assertions. The following subset of access control assertions are evaluated:

i. **Limit service scope**

Enable restricting service access by resource set. The security policy applies to a GuardPoint normally includes all files and all sub-directories, However, the service scope can be limited by applying resource set in the policy to limit the policy control to a specific file or sub-directory. The Transparent Encryption Agent will check the resource set to determine the scope of the service.

GuardPoint: /home/test1
Policy:
Security Rule 1: Resource=/home/test1/dir1, Action=all_ops, Effect=permit, apply key, audit
Security Rule 2: effect=permit audit
Key Rule 1: AES-256

The policy will only encrypt files in directory /home/test1/dir1. The rest of the subdirectories inside the GuardPoint will not get encrypted.

ii. **Authenticate user or group.**
Enable restricting service access by user set. The Transparent Encryption Agent requires specified user and/or groups to be authenticated against trusted identity in the user set before granting the access request.

GuardPoint: /home/test2
Policy:
Security Rule 1: User=ROOT Action=all_ops, Effect=permit, audit
Security Rule 2: User=CFO action=all_ops, effect=permit, apply key, audit
Security Rule 3: effect=deny, audit
Key Rule 1: AES-256

The policy grants users in the CFO user set to encrypt and decrypt files. It allows ROOT user set to view files in the GuardPoint but it does not allow ROOT user set to decrypt encrypted contents. Finally, it denies all users that are not in either ROOT or CFO user set.

iii. **Authenticate against process identity.**
Enable restricting service access by process set. When Transparent Encryption Agent receive a request for file operation access, it will validate the calling process with a known authorized signature in the policy before allowing the access to proceed.

GuardPoint: /home/test3
Policy:
Security Rule 1: Process=TRUST set, Action=all_ops, Effect=permit, apply key, audit
Security Rule 2: effect=deny, audit
Key Rule 1: AES-256

The policy only allows trusted signed processes in the TRUST process set to access encrypted contents. Other unauthorized processes will get denied when accessing the GuardPoint.

iv. **Service availability to time and days.**
Enable restricting service access by a time set. When the Transparent Encryption Agent receives a request for file operation access, it will check the time and/or restriction in the policy before allowing the access to proceed.

GuardPoint: /home/test4
Policy:
Security Rule 1: When=time set, Action=all_ops, Effect=permit, apply key, audit
Security Rule 2: effect=deny, audit
Key Rule 1: AES-256

The policy allows file access in the GuardPoint specified by the time set. Access will not be granted if accessing outside the defined time interval.

(FMT_MSA_EXT.5)

7.5 *Dependent Product Configuration*

7.5.1 PC-1: TOE Management Functions

Once a user has been successfully identified and authenticated by the TSF, the attributes stored in the user's account are associated with the user's session. The management functions available to a TOE user are determined by the administrator type attribute (and role for Security Administrators) For Example:

Only administrators of type System Administrator or All have the ability to determine and modify the behavior of the TOE's auditing functions

Only administrators of type System Administrator or All have the ability modify, delete and add authentication data in the user accounts.

A complete listing of the management functions available to each administrative type is shown in Table 7-6: DSM Management Functions by Administrator Type.

Table 7-6: DSM Management Functions by Administrator Type

Administrator Type	Management Functions
ANY Administrator Type	Login to TOE
	Logout of TOE
	Change own password
	Export DSM database configuration data (data exported depends on administrator type)
	Generate and view reports (reports available depends on administrator type)
	Display DSM version number
System Administrator Or All	Upload license file
	Allocate licenses and hours to a domain
	Generate and view system-level license reports
	Create, modify, and delete TOE administrators
	Reset administrator passwords
	Configure LDAP
	Import and select LDAP administrators

Administrator Type	Management Functions
	Export administrators
	Add and delete domains
	Generate self-signed certificate
	Install certificate (from CA or self-signed)
	View and export message log
	Set DSM log preferences
	Configure syslog server
	Enable and configure syslog server for system-level messages
	Export DSM system logs
	Enable email notification for log messages
	Set system preferences
	Configure password policy
	Backup and restore DSM configuration
	Configure SNMP
	Upgrade DSM software
	Assign first Doman Administrator to domain
	View logs
Domain Administrator **Or** **Domain and Security Administrator** **Or** **All**	Generate and view domain license reports
	Add administrator to a domain
	Remove administrator from a domain
	Configure Security Administrator roles
	Enable and disable administrator account in current domain
	Switch between domains
	Configure syslog messaging
	Backup and restore domain configuration
	View system preference
	View logs
Security Administrator **Or** **Domain and Security Administrator** **Or** **All**	View agent audit log data
	Set agent log preferences
	Switch between domains
	Create, edit, and delete local key-pairs, public keys only, and key groups
	Create, edit, and delete key templates
	Export and import public or symmetric keys
	Create, edit, display and delete policies
	Export and import policies
	Configure file system security rules
	Configure resource sets, user sets and process sets
	Configure, modify and delete hosts and host groups
	Configure policy time constraints
	Configure access methods (actions)
	Configure security rule effects
	Configure security rule encryption
	Set host locks
	Update host certificates
	Apply GuardPoint to Transparent Encryption Agent host
	Delete GuardPoint from Transparent Encryption Agent host
	Change Transparent Encryption Agent host password
	Manage certificate vault
	Generate certificate report

Administrator Type	Management Functions
	Create, delete, add files to, sign file in, and delete signature from signature set
	Set Remote Administrative Management display preferences

User account data is stored in the DSM configuration database (CGSSDB), which is an embedded Postgres database installed on the DSM appliance. CGSSDB is an internal component and the database is stored in the local disk. CGSSDB also contains all the policies, host configurations, and keys that are used in the Vormetric Data Security Remote Administrative Management. There is no direct access to the CGSSDB from the TOE user interfaces. CGSSDB is copied in a DSM backup A DSM backup is a means to restore the DSM configuration if a configuration change or upgrade produces undesirable results.

(FMT_MOF.1, FMT_MTD.1, FMT_SMF.1)

7.5.2 PC-2: Agent Configuration

Only administrators of type Security Administrator, Domain and Security Administrator, or All have the ability to query or modify the following functions of the Transparent Encryption Agents:

- Audited events type – logging level
- Repository for audit storage
- Access Control SFP
- Policy version being implemented
- Access Control SFP behavior to enforce in the event of communications outage
- Key settings and attributes

(FAU_SEL_EXT.1, FMT_MOF_EXT.1)

7.6 *Confidential Communications*

The following table specifies the required ports that must be accessible to ensure reliable communication between the DSMs and the hosts that run agent software, and between the TOE and required Operational Environment components. The protocol implementation splits the EC and RSA into different ports. Moreover, it splits the communications and audit trails with agents.

Table 7-7: Ports and Protocols for External Communications

Inbound Port	Outbound Port	Communication Direction	Description	Protocol
	123	DSM --> NTP Server	Default UDP/IP port for the Network Time Protocol (NTP).	NTP v4 RFC 5905
	1514	DSM --> Syslog Server	Although there is no assigned port for Syslog via TCP/IP, this is a recommended port.	TLS

Inbound Port	Outbound Port	Communication Direction	Description	Protocol
	7024	DSM → Agent	Default TCP/IP listening port of a host running agent software. The DSM initiates communication to the agent software through this port, and sends policies and protection methods to the host through this port. This port is configurable in the Remote Administrative Management interface.	TLS
8443		Agent → DSM	TCP/IP port through which the agent communicates with the DSM using RSA.This mode is configurable alternative to the the DSM → Agent.	TLS
8444		Agent → DSM	TCP/IP port used to upload agent logs to the DSM using RSA.	TLS
8445		Workstation → DSM	TCP/IP port used to connect the Remote Administrative Management Web browser to the DSM via a secure HTTPS connection using RSA.	HTTPS
8446		Agent → DSM	TCP/IP port through which the agent communicates with the DSM using Elliptic Curve Cryptography.	TLS
8447		Agent → DSM	TCP/IP port used to upload agent logs to the DSM using Elliptic Curve Cryptography.	TLS
8448		Workstation → DSM	TCP/IP port used to connect the Remote Administrative Management Web browser to the DSM via a secure HTTPS connection using Elliptic Curve Cryptography.	HTTPS
8448, 8445		Agent → DSM	Used once per agent to perform the initial certificate exchange between an agent host and DSM	HTTPS
	389 or 636	DSM → LDAP Server	Used for LDAP authentication of DSM administrators	TLS, RFC 4511
	53	DSM → DNS Server	UDP port used for IP address resolution	RFC 1035

Note: When remotely managing DSM, if you don’t specify a port in the browser URL and connect to a default port 443 the DSM will forward to port 8445 or 8448 depending on the selected cipher.

7.6.1 CC-1: Agent Communications

The access control policies managed by the DSM are associated with GuardPoints, which are the starting points at which to apply policies. A GuardPoint is a location in the Transparent Encryption Agents host's file system hierarchy where everything underneath has the policy applied to it. The Transparent Encryption Agent intercepts any attempt to access anything in the GuardPoint and uses policies obtained from the DSM to grant or deny the access attempt.

Security Administrators create policies, configure hosts, and apply GuardPoints. Policy data is securely transmitted to the Transparent Encryption Agents immediately after a policy is created or modified via the Remote Administrative Management. By default, when transmitting policy data DSM acts as a TLS client and Agent is acts as a TLS server. As part of TLS establishment, DSM verifies Agent's digital certificate.

(ESM_ACT.1, FMT_MOF.1)

The creation of digital certificates used to authenticate the DSM and each Transparent Encryption Agent is called the "registration" process, and communication to the DSM is in the clear and over HTTP. The Agent creates an RSA key pair and a certificate signing request (CSR) that contains the public key. The CSR is sent to the DSM via HTTP on port 8080. The DSM verifies that the host is known and that registration is expected (i.e. a whitelisting approach), and then signs the CSR, producing a trusted digital certificate that is returned to the agent along with the CA public certificate. The operator at the agent verifies the fingerprint of the CA certificate returned against the value on the DSM dashboard, and a security administrator on the DSM verifies the fingerprint of the new certificate against one displayed for that agent.

DSM and Transparent Encryption Agent secure communications uses TLS. Upon startup of agent, the DSM is queried for key and policy information. When policy or configuration changes are made on the DSM, the DSM initiates the communications with the Transparent Encryption Agent and sends updated policies. The Agent sends status updates and the audit data of Agent's auditable events back to the DSM.

(FCS_TLS_EXT.1(2), FCS_HTTPS_EXT.1, FTP_ITC.1)

FCS_HTTPS_EXT1: The HTTPS protocol conforms to RFC 2818. DSM has an application server to provide the web service through HTTPS, and this application server uses Java/JSSE/JCE for the HTTPS implementation. AES CBC mode supporting key size of 128 bits and 256 bites are being used for encryption and decryption.

FCS_TLS_EXT.1(2) TLS (Agent) : is implemented using TLS 1.2 (RFC 5246). This version of TLS supports the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

For ECC communications, DSM supports TLSv1.2. For RSA communications, which is used only with legacy Agents DSM supports TLSv1.2.

7.6.2 CC-2: User Communications

The TSF enforces two methods of user authentication for all authorized administrators of the TOE:

1. Password Authentication
2. LDAP Authentication

Once a user has been successfully identified and authenticated by the TSF, the attributes stored in the user's account are associated with the user's session. (See Section 7.3.1 AM-1: Management I&A). TLS/HTTPS protocol is used for securing remote administration of the TOE.

(ESM_EAU.2, ESM_EID.2, FIA_USB.1)

Only administrators of type System Administrator or All have the ability modify, delete and add authentication data in the user accounts.

(FMT_MOF.1)

The TSF secures the remote interactive sessions of administrative users of the Remote Administrative Management user interface using TLS/HTTPS.

The HTTPS protocol implemented for the user sessions complies with RFC 2818 and is implemented using TLS 1.2(RFC 5246). This version of TLS supports the following ciphersuites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

For all ECC communications, DSM supports TLSv1.2. For all RSA communications, DSM supports TLSv1.2. AES CBC mode supporting key size of 128 bits and 256 bites are being used for encryption and decryption.

The TOE also supports digital signatures used to protect remote management and cryptographic hash to secure update capabilities of the TOE. The certificate presented to the web browser initially is signed by a certificate authority (CA) that is internal to the DSM. It is possible to replace this certificate with one signed by a public CA (certificate authority).

(FCS_TLS_EXT.1(3), FCS_HTTPS_EXT.1, FTP_TRP.1)

7.6.3 CC-3: External Server Communications

The TOE can be configured for communications with the following servers in the Operational Environment:

- NTP Server – to supply reliable timestamps. NTP does not support authentication.
- Syslog Server – for external storage of audit records using TLS
- LDAP Server – for external authentication of TOE administrators using TLS
- SMTP Server – to send email notifications of log events
- DNS Server – for IP address resolution
- Transperent Encryption Agent – policy transmission

Configuration of NTP, Syslog, LDAP, SMTP and DNS external servers is optional.

The NTP and DNS servers are configured with the CLI during the initial network configuration of the TOE or during off-line maintenance.

The Syslog, SMTP, and LDAP servers are enabled and configured and Transperent Encryption Agent enrolled by System Administrators via the Remote Administrative Management (web based) interface. The TOE uses TLS to protect communication between itself and components in the operational environment – Agents, Syslog, and LDAP servers.

The external servers use the ports and protocols specified in Table 7-7: Ports and Protocols for External Communications. The TOE initiates and controls the communications with each of these servers.

FCS_TLS_EXT.1(1) TLS (Syslog and LDAP) : is implemented using TLS 1.2 (RFC 5246). This version of TLS supports the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

(FCS_TLS_EXT.1(1), FMT_MOF.1, FTP_ITC.1)

7.6.4 CC-4: Key Protection

All key material is stored encrypted in the DSM database. No interfaces for unencrypted key material are provided. There is no general access to the database. Remote Administrative Management operations on keys (e.g. reissue) do not expose key material. For PKI, only non-secret public keys are exposed.

The encryption key for the key material in the DSM database is stored in a keystore protected by the operating system apart from the database, which is itself encrypted and otherwise protected inside the DSM. There is no general access to the underlying operating system, the CLI is limited and does not provide root access. Key material is sent to the Transparent Encryption Agent over TLS and is never exposed in plaintext.

(FPT_SKP_EXT.1)

7.7 *Access Bannering*

7.7.1 AB-1: Banner

The TOE implements a warning and consent message regarding unauthorized use of the TOE that is displayed by the Remote Administrative Management before presenting the login screen. The text of the banner can be modified by Security Administrators via the Remote Administrative Management. A default banner messaging is presented to the user prior to logging to the TOE.

(FTA_TAB.1)

7.8 *Cryptographic Services*

7.8.1 CS-1: Crypto

The TOE generates asymmetric cryptographic keys that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)” used for key establishment in accordance with NIST Special Publication 800-56B Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography” for key establishment schemes and specified cryptographic key sizes equivalent to, or greater than, 112 bits of security.

DSM (the TOE) uses SHA algorithms in two areas:

1. Power on FIPS integrity check of the DSM SW executables: HMAC-SHA-256 is used for integrity checks.
2. Communication with the Vormetric Transparent Encryption Agents and Web Browsers (Remote Administrative Management): This communication is done using TLS in one of two modes:
    a) RSA: The Cipher suite is used with SHA-256 or SHA-384 algorithms
    b) ECC: The Cipher suite is used with SHA-256 or SHA-384 algorithms

The DSM (TOE) is configured to support both RSA and ECC or just ECC alone. The DSM utilizes Java v8.0 and OpenSSL v1.0.2 to provide cryptographic functions.

The following table summarizes the keys generated by the DSM and CSPs (Critical Security Parameters):

Table 7-8: DSM Key Generation

Key		*Generation Input*	*Storage*	*Zeroization*	*Use*
Passwords		User generated	Hard disk (secured with PBKDF2)	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Passwords are used to authenticate the administrator login
800-90A CTR_DRBG "V"		Internally gathered	in RAM	Zeroized every time a new random number is generated. Zeroized by overwritten with new value.	DRBG initialization
800-90A CTR_DRBG "Key"		Internally gathered	in RAM	Zeroized every time a new random number is generated. Zeroized by overwritten with new value.	DRBG initialization
HMAC Integrity Key (HMAC-SHA 256-bit with 256-bit key)		At vendor facility	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Protects the integrity of the module
Certificate Authority Key (for TLS Server)	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Signs certificates used when the DSM acts as a TLS server

Key		Generation Input	Storage	Zeroization	Use
	2048-bit RSA	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Signs certificates used when the DSM acts as a TLS server
Certificate Authority Key (for TLS Client)	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Signs certificates used when the DSM acts as a TLS client
	2048-bit RSA	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Signs certificates used when the DSM acts as a TLS client.
Server Key (for TLS Server)	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Identifies the DSM in a TLS session when it acts as a TLS server; Key establishment methodology provides 128 or 192 bits of encryption strength.

Key		***Generation Input***	***Storage***	***Zeroization***	***Use***
	2048-bit RSA	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Identifies the DSM in a TLS session when it acts as a TLS server; Key establishment methodology provides 112 bits of encryption strength.
Server Key (for TLS Client)	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Identifies the DSM in a TLS session when it acts as a TLS client; Key establishment methodology provides 128 or 192 bits of encryption strength.
	2048-bit RSA	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Identifies the DSM in a TLS session when it acts as a TLS client; Key establishment methodology provides 112 bits of encryption strength.
Web Console Key	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Identifies the DSM to a web browser: https TLS requests. Key establishment methodology provides 128 or 192 bits of encryption strength.

Key		Generation Input	Storage	Zeroization	Use
	2048-bit RSA	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Identifies the DSM to a web browser: https TLS requests. Key establishment methodology provides 112 bits of encryption strength.
TLS Session Keys AES 256		Generated internally using a DRBG compliant to NIST SP 800-90A	In RAM	Keys in RAM will be zeroized upon rebooting the appliance. Zeroized by power cycling the module.	Negotiated as part of the TLS handshake. Keys are exchanged using ECDHE or RSA (depends on cryptography supported by the communicating entities)
TLS HMAC Keys HMAC-SHA-256 / HMAC-SHA-384		Generated internally using a DRBG compliant to NIST SP 800-90A	In RAM	Keys in RAM will be zeroized upon rebooting the appliance. Zeroized by power cycling the module.	Used as part of TLS cipher suites
TLS Key Exchange ECDHE 256-bits ECDHE 384-bits SHA-256, SHA-384, SHA-512		Generated internally using a DRBG compliant to NIST SP 800-90A	In RAM	Keys in RAM will be zeroized upon rebooting the appliance. Zeroized by power cycling the module.	Negotiated as part of the TLS handshake using elliptical curve.
Master Key (KEK) AES 256		Generated internally using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Protects the Protection Key

Key	Generation Input	Storage	Zeroization	Use
Protection Key AES 256	Generated internally using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Protects symmetric file system keys, RSA keys for database backups, password hashes, server backup keys
Domain Key AES 256	Generated internally using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	The domain key is encrypted by the protection key and is used to protect symmetric file system keys, vault keys, RSA keys for agent database backups, password hashes, backup wrapper keys for a defined domain.
Server Backup Key AES 256	Generated internally using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Protects DSM backups
Agent Public Key RSA 2048 bits public key	External Vormetric transparent encryption agent generated using DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Protect a single-use File System Key Protection Key for transport.
Vormetric Upgrade Verification Key RSA 2048 bits public key	External generated using a DRBG compliant to NIST SP 800-90A and preloaded.	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Used to verify the uploaded upgrade package

Key	*Generation Input*	*Storage*	*Zeroization*	*Use*
Symmetric File System Keys AES 128 and 256	Generated internally using a DRBG compliant to NIST SP 800-90A	hard disk	Via factory reset command, maintenance config load default. Zeroized by overwriting once with zeros and formatting the disk volume.	Encryption keys used by Transparent Encryption agent. The File System Keys are encrypted using the Domain Key before being stored.

Keys and CSP's are not exposed through normal interfaces.

FCS_CKM.1

All key material can be zeroized by any administrator with the Network Administrator role via the dedicated CLI command "maintenance config load default" or general factory reset. When this action is performed, all key material and CSPs are removed; everything on the disk is wiped except for a 'restore' partition. The TOE then reboots in a state that is indistinguishable from the state in which it was shipped to the customer.

FCS_CKM_EXT.4

The DSM performs all random bit generation (RBG) services in accordance with NIST Special Publication 800-90A using CTR_DRBG (AES) seeded by an entropy source that accumulates entropy from a combination of hardware-based and software-based noise sources.

The DSM uses a modified version of the Linux random number generator, which is part of the OS kernel. Entropy bits are added to the primary pool from external sources, such as disk I/O operations and the RdRand instruction provided by the Intel CPU. (Detailed report of entropy analysis documented in the EAR.)

FCS_RBG_EXT.1

The following table summarizes the cryptographic operations performed by the TOE that have not been covered in other sections of the TSS.

Table 7-9: DSM Cryptographic Operations

Security Function	**Cryptographic Algorithm**	**Standard**	**CAVP Certificate**	
			Java	**OpenSSL**
Symmetric Encryption/Decryption	AES: (CBC Mode, Encrypt/Decrypt, Key Size = 128, 256; GCM Mode, Encrypt/Decrypt, Key Size = 128, 256)	FIPS PUB 197, "Advanced Encryption Standard (AES)" NIST SP 800-38A NIST SP 800-38D	C1389	

Security Function	**Cryptographic Algorithm**	**Standard**	**CAVP Certificate**	
			Java	**OpenSSL**
	AES: (CBC Mode, Encrypt/Decrypt, Key Size = 128, 256; GCM Mode, Encrypt/Decrypt, Key Size = 128, 256)	FIPS PUB 197, “Advanced Encryption Standard (AES)” NIST SP 800-38A NIST SP 800-38D		C1377
Cryptographic Hashing	SHA-256, SHA-384	FIPS Pub 180-4, “Secure Hash Standard.”	C1389	C1377
	SHA-512 – is used only for signature hashing during ECDHE key exchange	FIPS Pub 180-4, “Secure Hash Standard.”	C1389	
Keyed-Hash Message Authentication	HMAC-SHA-256, HMAC-SHA-384	FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code”	C1389	
	HMAC-SHA-256 – used for firmware integrity check	FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code”		C1377
RSA Key Generation	Key Generation for FIPS PUB 186-4 RSA Schemes 2048, 3072 bits	FIPS PUB 186-4, “Digital Signature Standard”		C1377
RSA Cryptographic Signature	RSA Digital Signature Algorithm (rDSA) (2048 bit key size)	FIPS PUB 186-4, “Digital Signature Standard”		C1377
EC Key Generation	Key Generation for Elliptic Curve Cryptography FIPS PUB 186-4 EC Schemes P-256, P-384	FIPS PUB 186-4, “Digital Signature Standard”	C1389	
Elliptical Curve Cryptographic Signature	ECDSA Elliptic Curve Digital Signature Algorithm (message digest size 256, 384 bits)	FIPS PUB 186-4, “Digital Signature Standard”	C1389	
Random Bit Generation	CTR_DRBG (AES-256) random bit generation	NIST SP 800-90A		C1377
Key Derived Function (KDF)	Key generation for TLS 1.2 session	NIST SP 800-135	C1389	C1377

The TOE uses Java/JSSE/JCE for AES encryption, AES decryption, hashing (SHA-256, SHA-384, SHA-512), elliptical curve cryptographic signature (ECDSA), key-hash message authentication (HMAC-SHA-256, HMAC-SHA-384), and TLS 1.2. SHA-512 is used only for signature hashing during ECDHE key exchange. OpenSSL is used for module integrity check (HMAC-SHA-256), RSA, and random number generation (DRBG). The TOE has implemented a Java provider that hooks into OpenSSL's DRBG routine for generating random numbers. This Java provider ensures that all Java/JSSE/JCE calls to generate random numbers will go through the same OpenSSL DRBG routine. The OpenSSL DRBG routine utilizes CTR_DRBG and AES block cipher to generate random numbers. Separate CAVP certificates are needed for OpenSSL implementation of AES for DRBG and OpenSSL implementation of HMAC-SHA-256. Figure 4 illustrate illustrates the components that utilize OpenSSL.

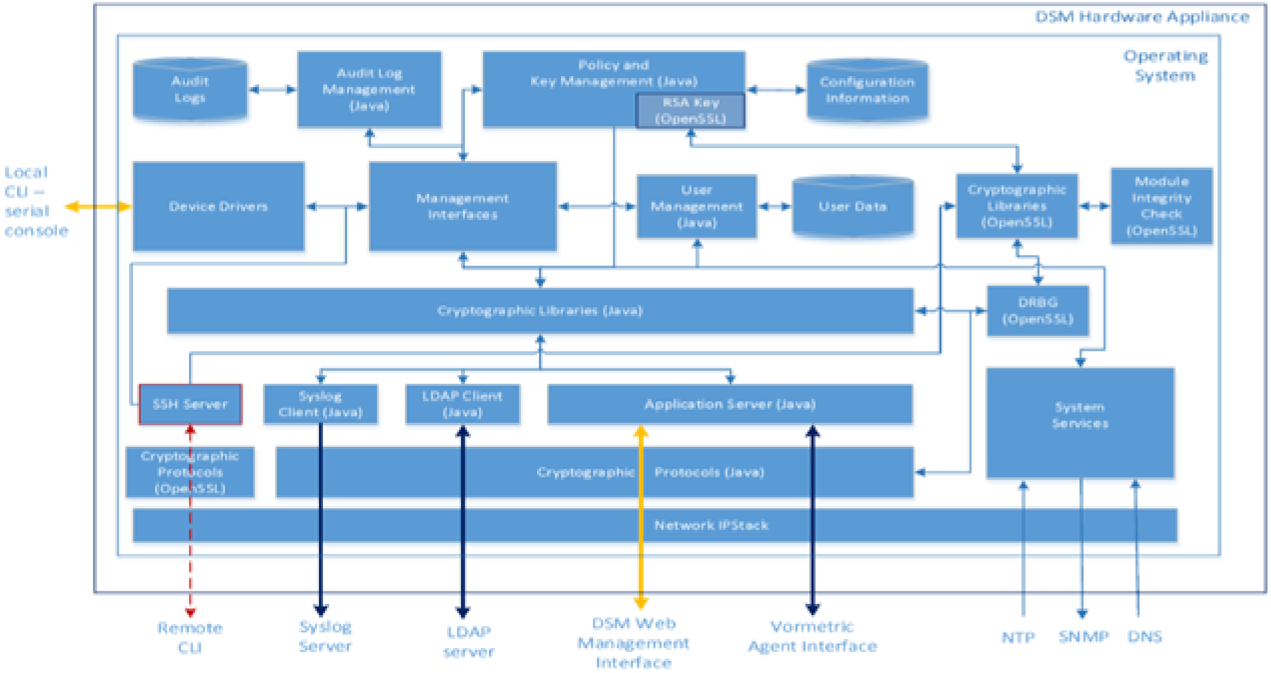
DSM Hardware Appliance
Operating System
Audit Logs
Audit Log Management (Java)
Policy and Key Management (Java)
RSA Key (OpenSSL)
Configuration Information
Local CLI – serial console
Device Drivers
Management Interfaces
User Management (Java)
User Data
Cryptographic Libraries (OpenSSL)
Module Integrity Check (OpenSSL)
Cryptographic Libraries (Java)
DRBG (OpenSSL)
SSH Server
Syslog Client (Java)
LDAP Client (Java)
Application Server (Java)
System Services
Cryptographic Protocols (OpenSSL)
Cryptographic Protocols (Java)
Network IPStack
Remote CLI
Syslog Server
LDAP server
DSM Web Management Interface
Vormetric Agent Interface
NTP
SNMP
DNS

Figure 4: DSM Functional Block Diagram

(FCS_COP.1 (1), FCS_COP.1 (2), FCS_COP.1 (3), FCS_COP.1 (4))

8 Security Problem Definition Rationale

This section identifies the mappings between the threats and objectives defined in the Security Problem Definition as well as the mappings between the assumptions and environmental objectives. In addition, rationale is provided based on the SFRs that are used to satisfy the listed objectives so that it can be seen that the mappings are appropriate.

Note: The Rationale text is from the [ESM PM PP].

Table 8-1: Assumptions, Environmental Objectives, and Rationale

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

Assumptions	Objectives	Rationale
A.SYSTIME – The TOE will receive reliable time data from the Operational Environment.	OE. SYSTIME – The Operational Environment will provide reliable time data to the TOE.	The TSF is expected to use reliable time data in the creation of its audit records. If the TOE is a software-based product, then it is expected that the TSF will receive this time data from a source within the Operational Environment such as a system clock or NTP server.
A.USERID – The TOE will receive identity data from the Operational Environment.	OE.USERID – The Operational Environment shall be able to identify a user requesting access to the TOE.	The expectation of an ESM product is that it is able to use organizationally-maintained identity data that resides in the Operational Environment.

Table 8-2: Policies, Threats, Objectives, and Rationale

Policies and Threats	Objectives	Rationale
P.BANNER – The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	O.BANNER – The TOE will display an advisory warning regarding use of the TOE.	FTA_TAB.1 The requirement for the TOE to display a banner is sufficient to ensure that this policy is implemented.
T.ADMIN_ERROR – An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.MANAGE – The TOE will provide Authentication Managers with the capability to manage the TSF.	FAU_SEL_EXT.1 FMT_MOF.1 FMT_MOF_EXT.1 FMT_MTD.1 FMT_SMF.1 By requiring authenticated users to have certain privileges in order to perform different management functions, the TSF can enforce separation of duties and limit the consequences of improper administrative behavior.
	OE.ADMIN – There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.	This objective requires the TOE to have designated administrators for the operation of the TOE. This provides some assurance that the TOE will be managed and configured consistently.
	OE.INSTALL – Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	This objective reduces the threat of administrative error by ensuring that the TOE is installed in a manner that is consistent with the evaluated configuration.
	OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	This objective reduces the threat of administrative error by ensuring that administrators have been properly vetted and trained prior to having access to the TOE.
T.CONTRADICT – A careless administrator may create a policy that contains contradictory rules for access control enforcement resulting in a security policy that does not have unambiguous enforcement rules.	O.CONSISTENT – The TSF will provide a mechanism to identify and rectify contradictory policy data.	FMT_MSA_EXT.5 The ability of the TSF to detect inconsistent data and to provide the ability to correct any detected inconsistencies will ensure that only consistent policies are transmitted to Access Control products for consumption.

Policies and Threats	Objectives	Rationale
T.EAVES – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	O.CRYPTO – The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	FCS_CKM.1 FCS_CKM_EXT.4 FCS_COP.1 (1) FCS_COP.1 (2) FCS_COP.1 (3) FCS_COP.1 (4) FCS_RBG_EXT.1 By providing cryptographic primitives, the TOE is able to establish and maintain trusted channels and paths.
	O.DISTRIB – The TOE will provide the ability to distribute policies to trusted IT products using secure channels.	ESM_ACT.1 FTP_ITC.1 The TOE will leverage cryptographic tools to generate CSPs for usage within the product and its sensitive connections. The TOE will be expected to use appropriate CSPs for the encryption, hashing, and authentication of data sent over trusted channels to remote trusted IT entities.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	FCS_HTTPS_EXT.1 FCS_TLS_EXT.1 (1-3) FPT_SKP_EXT.1 FTP_ITC.1 FTP_TRP.1 Implementation of trusted channels and paths ensures that communications are protected from eavesdropping.
T.FORGE – A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.	O.ACCESSID – The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.	FTP_ITC.1 Requiring an Access Control product to provide proof of its identity prior to the establishment of a trusted channel from the TOE will reduce the risk that the TOE will disclose authentic policies to illegitimate sources. This reduces the risk of policies being examined for reconnaissance purposes.

Policies and Threats	Objectives	Rationale
	O.CRYPTO – The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	FCS_CKM.1 FCS_CKM_EXT.4 FCS_COP.1 (1) FCS_COP.1 (2) FCS_COP.1 (3) FCS_COP.1 (4) FCS_RBG_EXT.1 By providing cryptographic primitives, the TOE is able to establish and maintain trusted channels and paths.
	O.INTEGRITY – The TOE will contain the ability to assert the integrity of policy data.	FTP_ITC.1 Providing assurance of integrity of policy data sent to the Access Control product allows for assurance that the policy the Access Control product receives is the policy that was intended for it.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	FCS_HTTPS_EXT.1 FCS_TLS_EXT.1(1-3) FPT_SKP_EXT.1 FTP_ITC.1 FTP_TRP.1 Implementation of a trusted channel between the TOE and an Access Control product ensures that the TOE will securely assert its identity when transmitting data over this channel.
	O.SELFID – The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.	FTP_ITC.1 Requiring the TOE to provide proof of its identity prior to the establishment of a trusted channel with an Access Control product will help mitigate the risk of the Access Control product consuming a forged policy.

Policies and Threats	Objectives	Rationale
T.MASK – A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.	O.AUDIT – The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.	FAU_GEN.1 FAU_SEL.1 FAU_STG_EXT.1 FPT_STM.1 If security relevant events are logged and backed up, an attacker will have difficulty performing actions for which they are not accountable. This allows an appropriate authority to be able to review the recorded data and acquire information about attacks on the TOE.
	OE.SYSTIME – The TOE will receive reliable time data from the Operational Environment.	This objective helps ensure the accuracy of audit data by providing an accurate record of the timing and sequence of activities, which were performed against the TOE.
T.UNAUTH – A malicious user could bypass the TOE's identification, authentication, and authorization mechanisms in order to use the TOE's management functions.	O.AUTH – The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.	ESM_EAU.2 (1) ESM_EID.2 (1) ESM_EAU.2 (2) ESM_EID.2 (2) ESM_EAU.2 (3) ESM_EID.2 (3) FIA_USB.1 FMT_MOF.1 FMT_SMR.1 FPT_APW_EXT.1 FTP_TRP.1 The Policy Management product is required to have its own access control policy defined to allow authorized users and disallow unauthorized users specific management functionality within the product. Doing so requires the user to be successfully identified and authenticated and to have an established session such that the user is appropriately bound to their assigned role(s).

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

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

9 Acronyms and Terminology

9.1 *CC Acronyms*

The following table defines CC specific acronyms used within this Security Target.

Table 9-1: CC Acronyms

Acronym	Definition
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standards Publication
NIST	National Institute of Standards and Technology
PM	Policy Manager
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

9.2 *CC Terminology*

The following table defines CC-specific terminology used within this Security Target.

Table 9-2: CC Terminology from [ESM PP PM]

Terminology	Definition
Access Control	A mechanism put in place to allow or deny the execution of defined operations requested by defined subjects to be performed against defined objects or the result achieved by employing such a mechanism.
Attribute-Based Access Control	A means of access control that is based upon the attributes of a user rather than the rights of a user. An example would be a system that grants access to specific resources if a user is an engineer and denies access to the same resources if the user is a contractor.
Authorized Administrator	A term synonymous with “Administrator”, used because some Common Criteria SFRs use the specific terminology.
Consume	The act of an Access Control product receiving a policy, parsing it, and storing it in a manner such that it can be used to enforce access control
Discretionary Access Control	A means of access control based on authorizations issued to a subject by virtue of their identity or group membership.
Enterprise Security Management	Systems and personnel required to order, create, disseminate, modify, suspend, and terminate security management controls

Terminology	Definition
Identity and Credential Management Product	An ESM product that contains the primary functionality to store and manage identities and credentials within an ESM deployment for the purposes of identification and authentication.
Mandatory Access Control	A means of access control based on the notion that all subjects and objects within an enterprise are associated with one or more hierarchical labels. The dominance relationship assigned to these labels determines if access is permitted.
Operational Environment	The collection of hardware and software resources in an enterprise that are not within the TOE boundary. This may include but is not limited to third-party software components the TOE requires to operate, resources protected by the TOE, and the hardware upon which the TOE is installed.
Policy	A collection of rules that determine how the Access Control SFP is instantiated. These rules define the conditions under which defined subjects are allowed to perform defined operations against defined objects.
Policy Administrator	Within the context of the PP, this refers to one or more individuals who are responsible for using the TOE to generate and distribute policies.
Policy Enforcement Point	A component of an Enterprise Security Management that is responsible for applying the Access Control SFP to all relevant behavior in an enterprise. Synonymous with the Access Control product referred to within this PP.
Policy Management product	An application that is responsible for creating policies that are consumed by the Policy Enforcement Point. These policies may be created through automated mechanisms, by manual administrative input, or by some combination of the two. This is the TOE as defined within this PP.
Role-Based Access Control	A means of access control that authorizes subject requests based on the roles to which they are assigned and the authorizations that are associated with those roles.
Secure Configuration Management Product	A product with the capability to alter the configuration of an ESM component and/or the ability to provision systems that reside in the Operational Environment
TOE Administrator	Within the context of the PP, this refers to the one or more individuals who are responsible for setting up the TOE, using the Policy Management product to define policies the TOE consumes, and reviewing audit data the TOE generates.
User	A blanket term for a generic user of the TOE; any entity that is identified and authenticated to the Policy Management product.
Access Control	A mechanism put in place to allow or deny the execution of defined operations requested by defined subjects to be performed against defined objects or the result achieved by employing such a mechanism.
Attribute-Based Access Control	A means of access control that is based upon the attributes of a user rather than the rights of a user. An example would be a system that grants access to specific resources if a user is an engineer and denies access to the same resources if the user is a contractor.
Authorized Administrator	A term synonymous with “Administrator”, used because some Common Criteria SFRs use the specific terminology.

Terminology	Definition
Consume	The act of an Access Control product receiving a policy, parsing it, and storing it in a manner such that it can be used to enforce access control
Discretionary Access Control	A means of access control based on authorizations issued to a subject by virtue of their identity or group membership.
Enterprise Security Management	Systems and personnel required to order, create, disseminate, modify, suspend, and terminate security management controls
Identity and Credential Management Product	An ESM product that contains the primary functionality to store and manage identities and credentials within an ESM deployment for the purposes of identification and authentication.
Mandatory Access Control	A means of access control based on the notion that all subjects and objects within an enterprise are associated with one or more hierarchical labels. The dominance relationship assigned to these labels determines if access is permitted.
Operational Environment	The collection of hardware and software resources in an enterprise that are not within the TOE boundary. This may include but is not limited to third-party software components the TOE requires to operate, resources protected by the TOE, and the hardware upon which the TOE is installed.
Policy	A collection of rules that determine how the Access Control SFP is instantiated. These rules define the conditions under which defined subjects are allowed to perform defined operations against defined objects.
Policy Administrator	Within the context of the PP, this refers to one or more individuals who are responsible for using the TOE to generate and distribute policies.
Policy Enforcement Point	A component of an Enterprise Security Management that is responsible for applying the Access Control SFP to all relevant behavior in an enterprise. Synonymous with the Access Control product referred to within this PP.
Policy Management product	An application that is responsible for creating policies that are consumed by the Policy Enforcement Point. These policies may be created through automated mechanisms, by manual administrative input, or by some combination of the two. This is the TOE as defined within this PP.
Role-Based Access Control	A means of access control that authorizes subject requests based on the roles to which they are assigned and the authorizations that are associated with those roles.
Secure Configuration Management Product	A product with the capability to alter the configuration of an ESM component and/or the ability to provision systems that reside in the Operational Environment
TOE Administrator	Within the context of the PP, this refers to the one or more individuals who are responsible for setting up the TOE, using the Policy Management product to define policies the TOE consumes, and reviewing audit data the TOE generates.
User	A blanket term for a generic user of the TOE; any entity that is identified and authenticated to the Policy Management product.
Access Control	A mechanism put in place to allow or deny the execution of defined operations requested by defined subjects to be performed against defined objects or the result achieved by employing such a mechanism.

Terminology	Definition
Attribute-Based Access Control	A means of access control that is based upon the attributes of a user rather than the rights of a user. An example would be a system that grants access to specific resources if a user is an engineer and denies access to the same resources if the user is a contractor.
Authorized Administrator	A term synonymous with "Administrator", used because some Common Criteria SFRs use the specific terminology.
Consume	The act of an Access Control product receiving a policy, parsing it, and storing it in a manner such that it can be used to enforce access control
Discretionary Access Control	A means of access control based on authorizations issued to a subject by virtue of their identity or group membership.
Enterprise Security Management	Systems and personnel required to order, create, disseminate, modify, suspend, and terminate security management controls
Identity and Credential Management Product	An ESM product that contains the primary functionality to store and manage identities and credentials within an ESM deployment for the purposes of identification and authentication.

9.3 *Product Acronyms and Terminology*

The following table defines Product-specific acronyms and terminology used within this Security Target.

Table 9-3: Product-specific Acronyms and Terminology

Terminology	Definition
admin Administrator	The default administrator created when you install the DSM or Security Server.
Administrative Domain (Domains)	A logical entity that is used to separate Remote Administrative Management administrators, and the data they access, from other Remote Administrative Management Administrators. Administrative tasks are performed in each domain based upon each administrator's assigned type. Administrative tasks in each domain can only be performed by administrators in that domain.
Administrator	A user with access to the DSM Remote Administrative Management. There are five types of administrators: System, Domain, Security, Domain and Security, and All.
Agent	A Vormetric software program that is loaded onto the host machine containing the data to be secured. Vormetric Agents implement the security policies that are defined and stored in the DSM. Vormetric Agents include the Transparent Encryption Agent, and Key Agents for Oracle Database TDE and Microsoft SQL Server, and Application Encryption Agent. Only Transparent Encryption Agents are applicable to the TOE

Terminology	Definition
Agent Keys	Encryption keys used by the Vormetric agents. There are two categories of Agent Keys, Vormetric Transparent Encryption Agent keys and Key Agent keys. Transparent Encryption Agent keys consist of keys for the Transparent Encryption Agent. Key Agent keys consist of keys for the Application Encryption Agent, Oracle Database TDE agent and Microsoft SQL TDE agent. Not applicable to TOE. Only Transparent Encryption Agent keys are applicable to the TOE
Application Encryption Agent	Vormetric agent that supports PKCS#11 API calls. Not applicable to TOE.
Asymmetric Key Cryptography	*See public key cryptographic algorithm.*
Asymmetric Key Pair	A public key and its corresponding private key used with a public key algorithm. Also simply called a key pair.
Authentication	A process that establishes the origin of information, or determines the legitimacy of an entity's identity.
Authorization	Access privileges granted to an entity that convey an "official" sanction to perform a security function or activity.
Block Devices	Devices that move data in and out by buffering in the form of blocks for each input/output operation.
Certification Authority (CA)	A trusted third party that issues digital certificates that certify the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. The trusted third party must be trusted by both the subject (owner) of the certificate and the party relying upon the certificate.
Challenge-response	The cryptographic algorithm used to limit access to the Remote Administrative Management. The host user enters a new password each time a host password is required. When a host is configured with a dynamic password, the host user runs a utility that displays a seemingly random string (the challenge), which he or she then gives to a DSM administrator. The DSM administrator returns a counter-string (the response) that the host user must enter to decrypt guarded data. The host user has 15 minutes to enter the counter-string.
Character device	*See Raw device*
Ciphertext	Data in its encrypted form. Ciphertext is the result of encryption performed on plaintext using an algorithm, called a cipher.
Cryptographic Algorithm	A computational procedure that takes variable inputs, including a cryptographic key, and produces ciphertext output. Also called a cipher. Examples of cryptographic algorithms include AES, ARIA, and DES.
Cryptographic Key	*See encryption key.*
Cryptographic Signature	*See signing files.*
Data Security Manager (DSM) & Data Security Appliance	*See Security Server.*
Decryption	The process of changing ciphertext into plaintext using a cryptographic algorithm and key.

Terminology	Definition
Digital signature	A cryptographic transformation of data that provides the services of origin authentication, data integrity, and signer non-repudiation.
Domains	*See administrative domains.*
Encryption	The process of changing plaintext into ciphertext using a cryptographic algorithm and key.
Encryption Agents	Vormetric agents consisting of the Transparent Encryption Agent, Application Encryption Agent, and Key Agents for Oracle Database TDE and Microsoft SQL Server. Only Transparent Encryption Agents are applicable to the TOE
Encryption Key	A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. Also called an encryption key.
Transparent Encryption Agent	A Vormetric software agent that resides on a host machine and allows administrators to control access to the files, directories and executables on that host system. For example, administrators can restrict access to specific files and directories to specific users at specific times using specific executables. Files and directories can be fully encrypted, while the file metadata (for example, the file names) remain in unchanged clear text.
FQDN	Fully qualified domain name. A domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS).
GPFS	General Parallel File System is a high-performance shared-disk clustered file system developed by IBM.
GuardPoint	A GuardPoint is a location in the file system hierarchy where everything underneath has the policy applied to it. It can be thought of as a UNIX mount point. The Transparent Encryption Agent intercepts any attempt to access anything in the GuardPoint and uses policies obtained from the DSM to grant or deny the access attempt.
Host	Typically refers to the system on which a Vormetric agent resides.
Host Locks	Two options, FS Agent Locked and System Locked, which are used to protect the Transparent Encryption Agent and certain system files. Transparent Encryption Agent protection includes preventing some changes to the Transparent Encryption Agent installation directory and preventing the unauthorized termination of Transparent Encryption Agent processes
Key Group	A key group is a collection of asymmetric keys that are applied as a single unit to a policy.
Key Management	The management of cryptographic keys and other related security parameters (for example, passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.
Key Template	A template that lets you quickly add agent keys by specifying a template with pre-defined attributes. You can define specific attributes in a template, and then you can call up the template to add a key with those attributes.
Remote Administrative Management	The user interface to the DSM.

Terminology	Definition
Multi-factor Authentication	An authentication algorithm that requires at least two of the three following authentication factors: 1) Something the user knows (for example, password); 2) Something the user has (example: RSA SecurID); and 3) Something the user is (example: fingerprint). The Vormetric implements an optional form of multi-factor authentication for Remote Administrative Management users by requiring DSM administrators to enter the token code displayed on an RSA SecurID, along with the administrator name each time the administrator logs into the Remote Administrative Management
Policies	A set of security access rules for protected data. These rules are specified by security administrators, stored in the DSM, and implemented on hosts by Transparent Encryption Agents.
Public Key Cryptographic Algorithm	A cryptographic system requiring two keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the ciphertext. Neither key will do both functions. One keys is published (public key) and the other is kept private (private key). If the lock/encryption key is the one published then the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published, then the system serves as a signature verifier of documents locked by the owner of the private key. Also called asymmetric key cryptography.
Raw Device	A type of Block device that performs input/output operations without caching or buffering resulting in access that is more direct.
Roles	A set of Remote Administrative Management permissions assigned to Security Administrators by administrators of type Security, Domain and Security Administrator, or All. There are five roles conferring permissions to perform specific types of tasks: Audit, Key, Policy, Host and Challenge & Response
RSA SecurID	A hardware authentication token which is assigned to a computer user and which generates an authentication code at fixed intervals (usually 60 seconds). In addition to entering a static password, Remote Administrative Management administrators can be required to input an 8-digit number that is provided by an external electronic device or software.
SECFS	An acronym for Vormetric Secure File System. It generally refers to the kernel module that handles policies (locks, host settings, logging preferences) and keys, and enforces data security protection. This also may refer to the Transparent Encryption Agent initialization script.
Security Server	A Vormetric server that acts as the central repository and manager of encryption keys and security policies. Receives instructions and configuration from administrators through a GUI-based interface called the Remote Administrative Management. Passes information to and from the Vormetric agents. Available as a complete hardened hardware system (Security Server Appliance) or as software solution to be installed on a UNIX box (software-only Security Server). Sometimes called the Data Security Manager (DSM) and the Vormetric Data Security Server.
Separation of Duties	A method of increasing data security by creating customized administrator roles for individual users such that no one user has complete access to all encryption keys in all domains of all files.

Terminology	Definition
Signing Files	File signing is a method that VDS uses to check the integrity of executables and applications before they are allowed to access GuardPoint data. If file signing is initiated in the Remote Administrative Management, the Transparent Encryption Agent calculates the cryptographic signatures of the executables that are eligible to access GuardPoint data. A tampered executable, such as a Trojan application, malicious code, or rogue process, with a missing or mismatched signature, is denied access. Also called cryptographic signatures.
Symmetric-key Algorithm	A class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.
System Administrator Reports	Reports available to System Administrators. For example Administrators, DSM Servers, Security Domains, and Executive Summary reports.
VMD	Acronym for Vormetric Daemon, VMD is a process that supports communication between the DSM and kernel module.
Vormetric Data Security (VDS)	The overall name of the product.