Senforce™ Endpoint Security Suite
Version 3.1.175
Security Target

Version 1.0
06/19/07

Prepared for:
Senforce™ Technologies, Inc.

147 W Election Rd Ste 110
Draper UT 84020

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

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 Endpoint Security Suite (ESS) provided by Senforce Technologies, Inc..

ESS is designed to protect computing resources and data assets stored on mobile clients, such as notebook computers and tablet PCs, using centrally managed servers to create and distribute security policies to enforcement components installed on each mobile client. Furthermore, it is designed to protect those resources and assets regardless of the mobility of the mobile client by enforcing an appropriate security policy based on the location (or inability to determine the location) of the client.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Senforce Endpoint Security Suite Security Target

ST Version – Version 1.0

ST Date – 06/19/07

TOE Identification – Senforce Endpoint Security Suite Version 3.1.175

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
    - Part 2 Extended (with FAU_GEN_EX.1)
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.
    - Part 3 Conformant
    - EAL 4 augmented with ALC_FLR.2

1.3 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 placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b 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 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: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

The Target of Evaluation (TOE) is Senforce Endpoint Security Suite Version 3.1.175.

ESS protects computing resources and data assets stored on mobile clients, such as notebook computers and tablet PCs, using centrally managed servers to create and distribute security policies to enforcement components installed on each mobile client.

ESS is designed to protect mobile clients moving from location to location inside or outside of a defined (such as for a corporation) security perimeter. It addresses specific mobile and wireless connectivity-related security concerns by adapting security protections as the mobile client moves from one network environment to another. This is accomplished by configuring the enforcement components within each mobile client to detect when the network environment changes and then to attempt to obtain specific policy information for the current environment or, if specific policy settings cannot be obtained, to use a default policy for the unknown environment.

The mobile client enforcement component intermediates between external connections, from which it receives secure requests, and internal resources, to which it makes requests on behalf of users. The mobile client enforcement component also intermediates between network-based storage, where data resides, and controls writing data to locally-attached storage.

2.1 TOE Overview

The TOE is comprised of the ESS components created by Senforce. The TOE architecture consists of five subsystems that are also functional components, which are placed at key points within the Enterprise architecture: Distribution Server, Management Server, Client Location Assurance Service, Policy Editor, and Senforce Security Client (SSC). The figure below shows these components, their location, and interaction in the architecture:

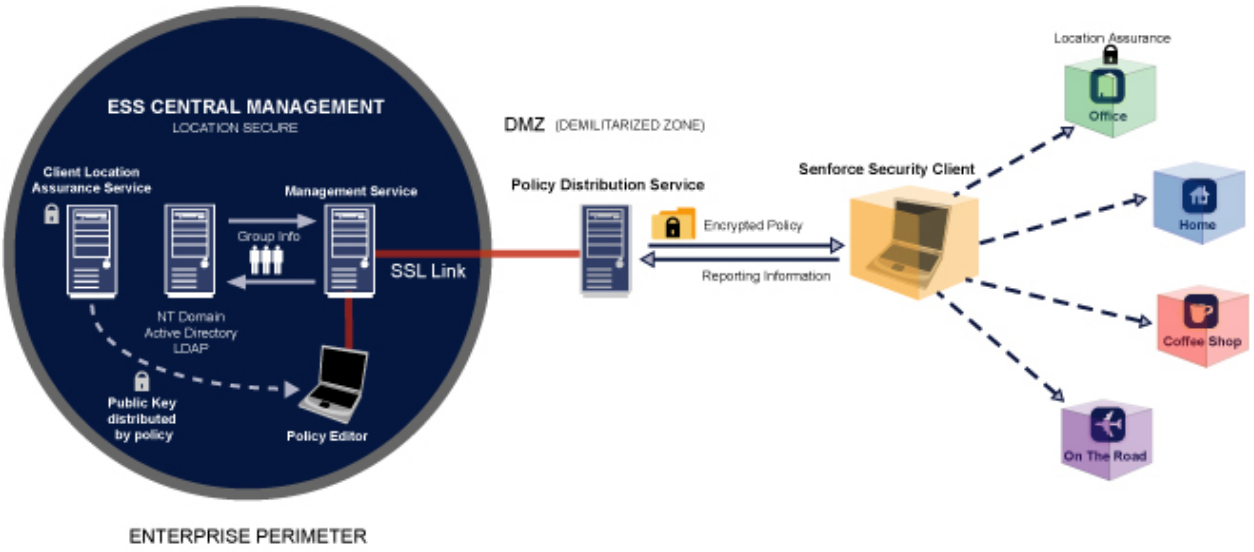

Figure 1 ESS Architecture

2.2 TOE Architecture

Four of the five components that are provided by the TOE, run in a specific environments and work together to enforce the overall security policies. The fifth component, the Senforce Security Client, assumes the client device moves from network environment to network environment, including known and new or unknown networks.

2.2.1 Physical Boundaries

Each of the TOE components is a software application designed to execute within an operating system context provided by the environment. The two “server” components (i.e., Distribution and Management) are designed to operate on a Windows 2000 (w/Service Pack 4) Server or Advanced Server or Windows 2003 Server, and the Client Location Assurance Service is designed to co-exist with either of the server components or alternately in its own server. The Policy Editor and SSC components are designed to operate on Windows XP (w/Service Pack 1-2), or any Windows 2000 (w/Service Pack 4) system. In addition to basic operating system services, including process, memory, and file management, the TOE also requires access to a database (Microsoft SQL Server 2000, SQL Server Standard, or SQL Server Enterprise), web server (Microsoft Internet Information Server), web browser (Microsoft Internet Explorer), and secure socket layer (SSL) capabilities. 'Note that the SSL capabilities provided by the IT environment are not tested as part of the evaluation.

2.2.1.1 The Distribution Server

2.2.1.1.1 Policy Distribution

The Distribution Server is a web service application that distributes security policies to clients based on user ID. The user-policy assignments are received from the ESS Management Server, which supplies the policies, along with opaque user credentials, to the Distribution Server. The Distribution Server stores and distributes XML-based security policies which are compressed, encrypted (using AES-256), and signed (using SHA-1 and 2048-bit RSA). The security policies are created and edited with the ESS Policy Editor. The Distribution Server authenticates SSCs based on the credentials obtained from the Management Server, and supplies each client with the designated security policy.

The Distribution Server utilizes Microsoft’s .NET architecture. The Distribution Server can reside outside the corporate firewall, providing increased convenience by allowing IT managers to distribute updates to clients regardless of where or how the clients are connected to the Internet or Intranet. It can also be deployed inside the

firewall, providing increased security by requiring users to only receive updates when they are inside the corporate firewall (either directly or via a VPN connection).

The Distribution Server creates a credential to be used by the Management Server. This credential is distributed out-of-band. All communications from the Management Server to the Distribution Server use 128-bit SSL to protect the confidentiality and integrity of the data, and certificates are used to authenticate the communications from the Management Server to prevent unauthorized Management Servers from tampering with the Distribution Server's data.

2.2.1.1.2 Reporting

The Distribution Server collects reporting data from the SSCs on behalf of the Management Server. Reporting data is retrieved from the SSCs upon "check-in." Check-in frequency is configured by policy and location. The Management Server periodically downloads the reporting data and deletes it from the Distribution Server.

2.2.1.2 The Management Server

2.2.1.2.1 User-Policy Assignment

The Management Server provides security policies and user information to the Distribution Server, as well as providing opaque credentials[1] to the clients. The client connects to the Management Server via SSLv3 and then authenticates to the Management Server using Microsoft authentication, and the Management Server sends back the credentials. After providing client credentials, the Management Server transmits the credentials to the Distribution Server, over an authenticated 128-bit SSL session, to be used in authenticating users requesting future policy updates.

All communications between the Management Server and the Distribution Server are initiated by the Management Server and are sent over 128-bit SSL to protect the confidentiality and integrity of the data.

The Management Server monitors user and group changes within the customer's existing directory (NT Domain, Active Directory, or LDAP) and sends updates to the Distribution Server when user-policy assignments change. If required, one Management Server can manage users from multiple directories.

The Management Server uses a local or remote Microsoft SQL database to store user-policy assignment data. Each Management Server currently requires its own user-policy assignment database instance (i.e., multiple Management Servers cannot share a single user-policy assignment database). Multiple Management Servers can keep their user-policy assignment databases on the same remote servers, if required.

Upon initial installation of the SSC on an end-user's mobile computer, the Management Server sends a unique set of credentials to the client and to the Distribution Server. This information is used for future authentication and to assure the correct policy is distributed to the client. Changes in the enterprise directory are monitored so that corresponding changes in user-policy assignments can be detected by the Management Server and sent to the Distribution Server.

2.2.1.2.2 Reporting

The Management Server provides adherence and status reports for the Enterprise. The Management Server reporting database may reside on the same server as its user-assignment database, or on a separate server (this decision may depend on the amount and age of reporting data to be collected and analyzed). Reporting data is retrieved from the Distribution Server.

The Management Server gathers and stores policy adherence and client compliance data to a Microsoft SQL Server database back end, and provides reporting views to this information through a web based user interface. No proprietary interfaces are required. Reporting information may be viewed through a web-based interface, with standard reports for adherence and individual user status; or with third party, ODBC-compliant reporting tools such

[1] The user is provided a credential that is formatted in a manner that is not expected to be interpretable by the user (i.e., they are not expected to understand or manipulate the contents).

as Crystal Reports, Brio, or Actuate. These reporting tools can view and query the reporting information from a common data warehouse, star format[2]. Data views to the information are made available to end-users for convenience.

The Management Server standard reports are accessed through a URL that is accessible to authenticated users, inside the corporate firewall, who have been assigned the appropriate ESS permission. Users not granted the appropriate permissions will not be allowed to view the web-based standard reports. This permission-based access control is not enforced on users creating custom reports with third-party tools that directly access the Management Server's SQL database. These custom reports can be created by any user with an account that has been granted access to the views of the Management Reporting Server's database.

2.2.1.2.3 Adherence Reports

Adherence Reports provide compliance information regarding the distribution and administration of Senforce™ managed users. A score of 100% adherence indicates that all Senforce™ managed users have "checked in" and received the current policy.

2.2.1.2.4 User Status Reports

In addition to adherence reports, the Management Server provides a number of status reports for disparate entities within the Senforce™ managed Enterprise. Status Reports provide views of system activity that affect managed directories or domains, groups, users and policies. Managed entities, such as users, may have greater levels of data granularity. This detail is useful for identifying activities and environmental conditions that may require policy modifications or enhancements.

2.2.1.3 The Client Location Assurance Service

The Client Location Assurance Service can be installed on any server in any Enterprise-owned network environment to provide a cryptographic guarantee to SSCs that they are indeed in the location that the other existing network environment parameters would indicate. The SSC detects the location, and if the policy indicates that this location has a Client Location Assurance Service (at IP address A with public key certificate C), then the SSC sends a random challenge (consisting of a 128-bit pseudo-random bit string (nonce) generated via the Crypto++ FIPS-140 certified cryptographic library[3]) to the Client Location Assurance Service, encrypted with the Client Location Assurance Server's public key. The Client Location Assurance Service decrypts the challenge and sends back a SHA-1 hash of the challenge, proving that it possesses the corresponding private key.

The Client Location Assurance Service can be optionally installed directly on the Management Server, but it also can be installed separately, if, for example, the Enterprise has a highly secured, isolated network where no Management Server is present.

2.2.1.4 The Policy Editor

The Policy Editor is a tool, which can run on a workstation that resides inside the corporate firewall or directly on the Management Server. By default, any authenticated user who is a local administrator on the Management Server is allowed to use the Policy Editor. Additionally, other users and/or groups can be granted the ESS Administrator role. An ESS Administrator uses the Policy Editor to manage user and group security policies. Policies can be created, copied, edited, or deleted using the editor.

[2] A star schema is a specialized database design consisting of multiple dimension tables, which describe aspects of an enterprise, and one fact table, which contains the facts or measurements about the enterprise.

[3] The nonce is also concatenated with itself to make a 256 nonce with a highly artificial structure. Checking for this structure prevents the presentation of chosen ciphertext to the Client Location Assurance Server from providing an attacker with any cryptographic insight into the Client Location Assurance Service.

2.2.1.5 The Senforce Security Client (SSC)

The SSC resides on the mobile client computer. It connects one time to the Management Server to authenticate the user and retrieve credentials that are used from then on to authenticate the SSC to the Distribution Server. It receives and authenticates the policy from the Distribution Server and then enforces the security policy on the mobile client. All SSC security functionality is controlled by the security policy. However, prior to receiving a policy the SSC permits full access to all devices and the firewall setting is 'All Adaptive', whereby client-generated packets are allowed out but unsolicited packets from the network are blocked. The user interface options displayed and available to SSC end users are dependent upon the permissions set in the security policy. Note that the evaluated configuration of the SSC requires that a policy is being enforced and hence an installed SSC is not in the evaluated configuration until its first policy is received.

When a mobile user enters a known network environment, the security policy for that environment is applied and enforced. If it's an unknown (or unrecognized) environment the SSC sets the location to a 'catch all' labeled as *Unknown*, and applies the *Unknown* security policy (it disables any access to the network unless the user takes an overt action to request access, and then allows only limited access, such as web-browsing, or VPN with no split-tunneling, or whatever other policy the ESS Administrator has specified for the *Unknown* location). These security policies are completely configurable by the ESS Administrator.

SSCs can be Managed or Unmanaged. A primary difference is that Managed SSCs are expected to normally be able to communicate with the Distribution Server and Management Server, while Unmanaged SSCs are expected to have only infrequent communication with the Servers. As such, Unmanaged SSCs do not generate audit records since the SSC itself would be required to manage the storage of that data indefinitely.

2.2.2 Logical Boundaries

The logical boundaries of the TOE are based in the security functions as they are realized and ultimately represented at the interfaces of the TOE. From a user perspective, the TOE offers primarily user data protection in the form of access control and information flow policies. From an administrative and internal operation perspective, the TOE offers security audit, security management, cryptographic operations, and TSF protection security functions.

2.2.2.1 Security audit

Auditing is performed by and initially stays on the SSC until the client "checks-in" with the Distribution Service. Audit data for a specific SSC is retrieved from the client upon 'check-in' and check-in frequency is configured by policy and location. Note that audit data is not collected by Unmanaged clients.

When the SSC checks-in with the Distribution Server, the adherence and client compliance audit data is collected and stored in a Microsoft SQL database. Subsequently, the Management Server downloads the audit data from the Distribution Server and provides reporting views to this information through a web based user interface. Reporting information may be viewed through a web-based interface, with standard reports for adherence and individual user status.

2.2.2.2 Cryptographic support

The Distribution Server and Management Servers are each configured with a private/public key pair so they can communicate using mutually authenticated SSL. Additionally, SSCs get cryptographic credentials (i.e., the public key) from the Management Server so that the SSC can establish an SSL connection with the Management Server to obtain a key used to encrypt policy keys (each policy is encrypted with its own encryption key which is encrypted and distributed with the policy). Once the keys are configured, policies are signed and encrypted by the Management Server so the SSC can verify them before enforcing them and audit records generated by managed SSC are encrypted so that they can be decrypted only by the Management Server.

2.2.2.3 User data protection

The SSC is installed in each mobile host at various points in the network protocol and file driver layers of the host operating system. The SSC enforces policies retrieved from the Distribution Server to ensure that only appropriate network operations can occur relative to the current environment of the mobile host, whether the traffic is incoming

or outgoing, where the traffic is coming from or going to, and also various additional attributes of the network traffic such as transport protocol, network application, etc.

The SSC also enforces access policies for a number of devices and resources. In particular, it can restrict access to specific removable media devices and files and directories to read, read/write, or no access. It can restrict execution access to application programs. It can also restrict the use of specific network communication devices (e.g., adapters) and network access points.

2.2.2.4 Security management

Security management is primarily performed using a Policy Editor that is used to manage policies stored on the Management Server and subsequently distributed to SSCs via the Distribution server. Note that the Policy Editor could be used on essentially any enterprise host, but is often used directly on the Management Server. Regardless, the Management Server stores the security policies and, hence, controls access to them.

The following list summarizes some aspects of the security policy that can be defined and enforced on SSCs relative to the current SSC environment:

- Manage which wired/wireless/analog network communication devices can be used;
- Manage which network access points (APs) users can use;
- Manage the access to network applications;
- Manage the use of network protocols (e.g., HTTP MIME types);
- Manage communication with specific network hosts;
- Manage user communication to corporate LANs enforcing Virtual Private Networking (VPN);
- Manage access to removable storage devices (e.g., CD/RW, DVD/RW, floppy disk drives, firewire disk drives, USB thumb drives, etc.);
- Manage access to specific files and directories;
- Manage endpoint integrity of third-party solutions (such as Antivirus solutions);
- Manage the use and distribution of wireless security encryption keys; and,
- Manage which application programs users may invoke.

2.2.2.5 Protection of the TSF

The cryptographic operations, summarized above, are used primarily to protect the security policies when they are being transmitted between the various TOE components to ensure that the SSCs ultimately enforce the appropriate security policies.

The solution contains various Client Self Defense (CSD) mechanisms, intended to protect the SSC component of the TSF from unauthorized manipulation or disabling. See section 6.1.5 for more details.

2.3 TOE Documentation

Senforce offers a series of documents that describe the installation process for Endpoint Security Suite as well as guidance for subsequent use and administration of the applicable security features. Refer to Section 6 for information about these and other documents associated with Endpoint Security Suite.

3. Security Environment

The security environment for the functions addressed by this specification includes threats and usage assumptions, as discussed below.

3.1 Threats

Note that in each case below the 'attacker' is assumed to be anyone who is not authorized to control the applicable security policies or to access the applicable resources (computational or data). The attacker would generally be on the same network as the protected hosts, regardless of whether that is inside or outside an enterprise boundary.

T.BAD_POLICY	An attacker may be able to cause a mobile host to enforce an inappropriate or insecure security policy.
T.ENV_CHANGE	An attacker may be able to exploit a change in the environment of a mobile host to gain unauthorized access to data or computing resources.
T.NET_ACCESS	An attacker may be able to gain unauthorized access to data or computing resources by directly accessing a mobile host or by exploiting improper network accesses made by a mobile host user.
T.BAD_RESOURCE	An attacker may be able to gain unauthorized access to data or computing resources when a user uses inappropriate storage or network devices or file or program resources.
T.NO_FAULT	An attacker's attempts to violate network or file restrictions may go undetected.

3.2 Assumptions

A.CONNECTION	Each TOE component will be located in the environment such that it can reliably communicate with the other applicable TOE components when necessary.
A.GOOD_ADMIN	Administrators will adhere to applicable administrator guidance.
A.GOOD_USER	Users will adhere to applicable user guidance.
A.PHYSICAL	The TOE is physically protected commensurate with the data and resources it protects. Note that in the case of mobile components, users are expected to protect the components to the degree necessary to ensure that the TOE software cannot be uninstalled or otherwise disabled.
A.ITENVIRON	The environment will include the IT components required to support the proper operation of the TOE; specifically, suitable operating system, database, web server, and SSL capabilities (as identified in the TOE Description, section 2).

4. Security Objectives

This section defines the security objectives for the TOE and its environment. These objectives are suitable to counter all identified threats and cover all identified assumptions. The TOE security objectives are identified with 'O.' inserted at the beginning of the name and the environment objectives are identified with 'OE.' inserted at the beginning of the name.

4.1 Security Objectives for the TOE

O.AUDIT	The TOE must be able to audit application of the security policy and make that information available to administrators.
O.ENV_CHANGE	The TOE must allow security policies to be defined individually for different operational environments.
O.NET_ACCESS	The TOE must enforce an information flow policy that can control network access attempts originating internal or external to a mobile host.
O.RESOURCES	The TOE must enforce an access control policy that can control access to removable media devices, network access devices, individual files and directories, and executable programs available to a mobile host.
O.SECURE_POLICY	The TOE must allow security policies to be defined and distributed securely throughout the TOE components for enforcement on mobile hosts.

4.2 Security Objectives for the IT Environment

OIE.AUDIT	The IT environment must be able to protect the audit records and provide reliable time information for use in the audit records.
OIE.NET_ACCESS	The IT environment must ensure that the network information flow policy implemented by the TOE is not bypassed.
OIE.RESOURCES	The IT environment must ensure that the access control policy implemented by the TOE is not bypassed.
OIE.SECURE_POLICY	The IT environment must ensure that only appropriately identified and authenticated administrators can manage the security policies supported by the TOE and also that the TOE is protected from tampering

4.3 Security Objectives for the Environment

OE.CONNECTION	Each TOE component will be located in the environment such that it can reliably communicate with the other applicable TOE components.
OE.GOOD_ADMIN	Administrators will adhere to applicable administrator guidance.

OE.GOOD_USER	Users will adhere to applicable user guidance.
OE.PHYSICAL	The TOE is physically protected commensurate with the data and resources it protects. Note that in the case of mobile components, users are expected to protect the components to the degree necessary to ensure that the TOE software cannot be uninstalled or otherwise disabled.
OE.ITENVIRON	The environment will include the IT components required to support the proper operation of the TOE; specifically, suitable operating system, database, web server, and SSL capabilities (as identified in the TOE Description, section 2).

5. IT Security Requirements

This section defines the security functional and security assurance requirements for the TOE and associated IT environment components.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by Endpoint Security Suite.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN_EX.1: Audit data generation
	FAU_SAR.1: Audit review
	FAU_SAR.3: Selectable audit review
FCS: Cryptographic support	FCS_COP.1: Cryptographic operation
FDP: User data protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
	FDP_IFC.2: Complete information flow control
	FDP_IFF.1: Simple security attributes
FMT: Security management	FMT_SMF.1: Specification of Management Functions
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN_EX.1)

FAU_GEN_EX.1.1 The Managed client component of the TSF shall be able to generate an audit record of the following auditable events: mobile host security policy updates; mobile host location changes.

FAU_GEN_EX.1.2 The Managed client component of the TSF shall record within each audit record at least the following information: Date and time of the event; type of event; subject identity; and outcome of the event.

5.1.1.2 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**an authorized administrator**] with the capability to read [**all audit data**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches***] of audit data based on [**subject identity and date**].

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1a The TSF shall perform [**encryption and decryption of security policies**] in accordance with a specified cryptographic algorithm [**Advanced Encryption Standard (AES-256)**] and cryptographic key sizes [**256 bits**] that meet the following: [**FIPS PUB 197**].

FCS_COP.1.1b The TSF shall perform [**signature generation and validation of security policies**] in accordance with a specified cryptographic algorithm [**RSA-2048 with Secure Hash Standard (SHA-1)**] and cryptographic key sizes [**2048 bits**] that meet the following: [**RSASSA-PKCS1-v1_5, FIPS PUB 180-1**].

5.1.3 User data protection (FDP)

5.1.3.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the [**Device Control SFP**] on [
a) subjects: mobile host;
b) objects: removable media devices, network communication devices, network access points, files and directories, and executable programs; and,
c) operations: removable media device read and write operations, network communication device use operations, network access point use operations, file read/write/execution operations].

5.1.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**Device Control SFP**] to objects based on the following:[
a) subject security attributes: mobile host security policies and mobile host environment;
b) object security attributes: device type and device identification].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
a) for removable media device access, the mobile host security policy associated with the current mobile host environment must allow the requested read or write operation (either by including the requested access for the specified device on a 'white list' or by not having a 'white list' at all) for successful access;
b) for network communication devices, the mobile host security policy associated with the current mobile host environment must allow use of a given network communication device (either by including it on a 'white list' , excluding it from a 'black list', or by having neither list) for successful use;
c) for network access points, the mobile host security policy associated with the current mobile host environment must allow use of a given network access point (either by including it on a 'white list', excluding it from a 'black list', or by having neither list) for successful use;
d) for file access (including executables), the mobile host security policy associated with the current mobile host environment must allow the requested read or write operation (either by excluding it from a 'black list', or by having no such list) for successful access; and,

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no explicit authorization rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**no explicit denial rules**].

5.1.3.3 Complete information flow control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the [**Network Information Flow SFP**] on [
a) subjects: mobile host and network hosts;
b) information: network packets] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

5.1.3.4 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**Network Information Flow SFP**] based on the following types of subject and information security attributes: [

a) subject security attributes: mobile host security policies, mobile host environment, network host address;
b) information attributes: presumed source address, destination addressed, point of origin (i.e., mobile host or network), network transport layer protocol, network application identifier, encryption state].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [
a) when sending data from the mobile host, the mobile host security policy associated with the current mobile host environment allows the applicable combination of security attributes to be sent to the network host address specified in the destination address; and
b) when receiving data, the mobile host security policy associated with the current mobile host environment allows the applicable combination of security attributes to be received from the network host address specified in the presumed source address].

FDP_IFF.1.3 The TSF shall enforce the [**no additional rules**].

FDP_IFF.1.4 The TSF shall provide the following [**no additional capabilities**].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [**no explicit authorization rules**].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [**no explicit denial rules**].

5.1.4 Security management (FMT)

5.1.4.1 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**creation, modification, and deletion of Network Information Flow SFP, Device Control SFP]**

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Basic internal TSF data transfer protection (FPT_ITT.1)

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure* and *modification***] when it is transmitted between separate parts of the TOE.

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by the IT environment of Endpoint Security Suite.

Requirement Class	Requirement Component
FAU: Security audit	FAU_STG.1: Protected audit trail storage
FIA: Identification and authentication	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MTD.1: Management of TSF data
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps

Table 2 IT Environment Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The IT Environment shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The IT Environment shall be able to [***prevent***] unauthorized modifications to the audit records in the audit trail.

5.2.2 Identification and authentication (FIA)

5.2.2.1 User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1 The IT Environment shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.2.2 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The IT Environment shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.3 Security management (FMT)

5.2.3.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The IT Environment shall restrict the ability to [***modify the behavior of***] the functions [**security audit, Network Information Flow SFP, Device Control SFP, cryptographic operation**] to [**the authorized administrator**].

5.2.3.2 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The IT Environment shall restrict the ability to [***change defaults, query, modify*** **and** ***delete***] the [**Network Information Flow SFP and Device Control SFP mobile host security policies**] to [**the authorized administrator**].

5.2.3.3 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The IT Environment shall maintain the roles [**authorized administrator**].

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

5.2.4 Protection of the TSF (FPT)

5.2.4.1 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The IT Environment shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.4.2 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The IT Environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The IT Environment shall enforce separation between the security domains of subjects in the TSC.

5.2.4.3 Reliable time stamps (FPT_STM.1)

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

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 4 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_AUT.1: Partial CM automation
	ACM_CAP.4: Generation support and acceptance procedures
	ACM_SCP.2: Problem tracking CM coverage
ADO: Delivery and operation	ADO_DEL.2: Detection of modification
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.2: Fully defined external interfaces
	ADV_HLD.2: Security enforcing high-level design
	ADV_IMP.1: Subset of the implementation of the TSF
	ADV_LLD.1: Descriptive low-level design
	ADV_RCR.1: Informal correspondence demonstration
	ADV_SPM.1: Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.2: Validation of analysis
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.2: Independent vulnerability analysis

Table 3 EAL 4 augmented with ALC_FLR.2 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1d The developer shall use a CM system.
ACM_AUT.1.2d The developer shall provide a CM plan.
ACM_AUT.1.1c The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.
ACM_AUT.1.2c The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.1.3c The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.1.4c The CM plan shall describe how the automated tools are used in the CM system.
ACM_AUT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1d The developer shall provide a reference for the TOE.
ACM_CAP.4.2d The developer shall use a CM system.
ACM_CAP.4.3d The developer shall provide CM documentation.
ACM_CAP.4.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2c The TOE shall be labelled with its reference.

ACM_CAP.4.3c The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
ACM_CAP.4.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.4.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.4.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.4.8c The CM plan shall describe how the CM system is used.
ACM_CAP.4.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.11c The CM system shall provide measures such that only authorized changes are made to the configuration items.
ACM_CAP.4.12c The CM system shall support the generation of the TOE.
ACM_CAP.4.13c The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ACM_CAP.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.3 Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.2.1c The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Detection of modification (ADO_DEL.2)

ADO_DEL.2.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.2.2d The developer shall use the delivery procedures.
ADO_DEL.2.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.2.2c The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.
ADO_DEL.2.3c The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.
ADO_DEL.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1d The developer shall provide a functional specification.
ADV_FSP.2.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.2.2c The functional specification shall be internally consistent.
ADV_FSP.2.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.
ADV_FSP.2.4c The functional specification shall completely represent the TSF.
ADV_FSP.2.5c The functional specification shall include rationale that the TSF is completely represented.
ADV_FSP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.2.1c The presentation of the high-level design shall be informal.
ADV_HLD.2.2c The high-level design shall be internally consistent.
ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.
ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Subset of the implementation of the TSF (ADV_IMP.1)

ADV_IMP.1.1d The developer shall provide the implementation representation for a selected subset of the TSF.
ADV_IMP.1.1c The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.1.2c The implementation representation shall be internally consistent.
ADV_IMP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_IMP.1.2e The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.4 Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1d The developer shall provide the low-level design of the TSF.
ADV_LLD.1.1c The presentation of the low-level design shall be informal.
ADV_LLD.1.2c The low-level design shall be internally consistent.
ADV_LLD.1.3c The low-level design shall describe the TSF in terms of modules.
ADV_LLD.1.4c The low-level design shall describe the purpose of each module.

ADV_LLD.1.5c The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.
ADV_LLD.1.6c The low-level design shall describe how each TSP-enforcing function is provided.
ADV_LLD.1.7c The low-level design shall identify all interfaces to the modules of the TSF.
ADV_LLD.1.8c The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.
ADV_LLD.1.9c The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_LLD.1.10c The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.
ADV_LLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_LLD.1.2e The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.5 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.6 Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1d The developer shall provide a TSP model.
ADV_SPM.1.2d The developer shall demonstrate correspondence between the functional specification and the TSP model.
ADV_SPM.1.1c The TSP model shall be informal.
ADV_SPM.1.2c The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.
ADV_SPM.1.3c The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.
ADV_SPM.1.4c The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.
ADV_SPM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life cycle support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.

ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.5.2 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3d The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5c The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ALC_FLR.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1d The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2d The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1c The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2c The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.4 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1d The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2d The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.1c All development tools used for implementation shall be well-defined.

ALC_TAT.1.2c The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3c The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.

ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Validation of analysis (AVA_MSU.2)

AVA_MSU.2.1d The developer shall provide guidance documentation.
AVA_MSU.2.2d The developer shall document an analysis of the guidance documentation.
AVA_MSU.2.1c The guidance documentation 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.
AVA_MSU.2.2c The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.2.3c The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.2.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.2.5c The analysis documentation shall demonstrate that the guidance documentation is complete.
AVA_MSU.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.2.2e The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.2.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.
AVA_MSU.2.4e The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Independent vulnerability analysis (AVA_VLA.2)

AVA_VLA.2.1d The developer shall perform a vulnerability analysis.

AVA_VLA.2.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.2.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.2.2c The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.2.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.4c The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.2.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3e The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4e The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5e The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The majority of audit information relates to the immediate enforcement of security measures and is created by the appropriate Senforce Security Client (SSC), when configured in Managed mode, and passed back (via the Distribution Server) to the Management Server's Reporting Database for collation and synthesis. Some security management data is generated on the Distribution Server and passed up to the Management Server. Each audit record includes a time stamp obtained from the mobile host operating system, the nature of the audit event, identification of the mobile host, applicable result of the event (e.g., success or failure), and other details specific to the event (e.g., source and destination addresses).

The audit records are stored on the SSC until the SSC checks-in with the Distribution Server. The check-in is a regularly scheduled event dictated by the specific security policy being enforced by the SSC. When the check-in occurs, the audit records will be sent to the Distribution Server where they will be stored until they are downloaded, per another schedule, to the Management Server. Once on the Management Server, the audit data is available from the Management Server via a web server interface for standard views and via review tools included in the TOE that facilitate searching audit data based on any content within the audit records. The 'Endpoint Check-in Adherence' and 'Location Usage Data' reports, in particular, provide information on mobile host security policy updates.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN_EX.1: Audit records are generated 'by the SSC (when configured in Managed mode) for the appropriate security-relevant events and include the date/time, nature of the event (i.e., event type), subject identity, and applicable results (i.e., outcome).
- FAU_SAR.1: The Management Server provides access to all audit records.
- FAU_SAR.3: The Management Server provides tools to search the audit data based on subject identity and date.

6.1.2 Cryptographic support

When the Management Server and Distribution Server are installed, public/private key pairs are generated and configured and each is also configured with the public key of the other so that subsequently mutually authenticated SSL connections can be established for all communication between those servers. In addition, when a SSC is installed, it is configured with the public key of the Management Server so that it can establish an SSL connection with the Management Server where the Management Server will provide the SSC with a policy key encryption key so that it can later decrypt policies that it will enforce.

Network Information Flow SFP and Device Control SFP security policies are always encrypted and signed (and subsequently decrypted and the signature validated) to ensure both confidentiality and integrity when they are sent from the Management Server to the Distribution Server and on to the SSCs. The signatures are based on the private key of the Management Server and can be verified using the public key and the encryption is based on AES with a 256-bit key generated for each policy. That policy encryption key is encrypted with the policy key encryption key and distributed with the policy so that properly configured clients can decrypt the policy key and subsequently the policy itself before enforcing it. Note that when passing data between the Management Server and SSCs, the Distribution Server is a passive conduit of previously-encrypted content.

When a Managed SSC sends audit data back to the Management Server (via a Distribution Server), the audit data will be encrypted using the public key of the Management Server so that it is protected until the Management Server decrypts it using its corresponding private key.

The 'Crypto++' library is installed on each of the TOE components performing the required cryptographic operation using the SHA-1, AES-256, and RSA-2048 [**RSASSA-PKCS1-v1_5, FIPS PUB 180-1**] algorithms in accordance with FIPS PUB 180-1 and FIPS PUB 197. Note that the Crypto++ library has been subject to FIPS 140-2 certification, and the certified libraries have been incorporated into the TOE.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_COP.1: The encryption, decryption, signature generation, and signature verification operations are applied whenever security policies are transmitted between distributed TOE components. This operation is based on SHA-1, AES-256, and RSA-2048 in accordance with the applicable FIPS publications.

6.1.3 User data protection

Each Senforce Security Client (SSC) is installed in the network protocol stack and file system stack of its host operating system. As such, it enforces its Network Information Flow SFP security policy at multiple points within that stack; specifically at the NDIS, TDI, and application layers. SSC enforces its policies on all network traffic incoming and outgoing and bases its decisions on the security policy settings currently in place depending on the specific environment of the mobile host. The specific environment is determined based on available network information (e.g., gateways, address ranges) and optionally on a Client Location Assurance Server which can provide positive confirmation of the mobile host's environment. If the environment cannot be determined, the SSC will default to the policy corresponding with an 'unknown' environment.

A security policy for a given environment can specify which combinations of direction, transport protocols, source and destination addresses, network applications, and state of encryption of the traffic (e.g., when requiring a VPN) are allowed in order to effectively control the flow of information in and out of the mobile host.

In addition to information flow, the Device Control SFP security policy enforced by the SSC can limit access to specific devices. Removable media devices can be identified as being read-only, read-write, or not accessible. Removable individual files can be identified as being not accessible via a 'black list'. A 'black list' defines the set of resources that are not allowed to be used. Similarly, network communication devices (e.g., network adapters), and network access points can be restricted by either defining a 'white list' which defines the set of network devices or executable programs that can be used or alternately a 'black list' which defines the set of network devices or executable programs that cannot be used. Note that where no black list is defined, then no restrictions are indicated. In each case, the policy is relative to the current SSC environment so that device access can vary and yet remain controlled from environment to environment.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1: Operations on removable storage, network communication, and network access point devices are controlled.
- FDP_ACF.1: The device control policy allows the specification of network communication devices and network access points that can be used as well as specification of read-only, read-write, or 'no access' restrictions to be placed on specific removable media devices.
- FDP_IFC.2: All network information flow (i.e., packets), regardless of operation, between mobile hosts and other network hosts is subject to the Network Information Flow SFP security policy.
- FDP_IFF.1: The information flow policy allows combinations of network traffic attributes (presumed source address, destination addressed, point of origin (i.e., mobile host or network), network transport layer protocol, network application identifier, encryption state) to be used to dictate allowable information flows between mobile hosts and other network hosts respective of the current operational environment.

6.1.4 Security management

The Policy Editor provides the ability to create, edit, and delete Network Information Flow SFP and Device Control SFP security policies that are stored on the Management Server.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_SMF.1: See above.

6.1.5 Protection of the TSF

Network Information Flow SFP and Device Control SFP security policies are developed on the Management Server. The Crypto++ library is used to encrypt the security policies when they are transmitted to the SSCs via the Distribution Server. The encryption mechanism is used both to ensure the secrecy and integrity of security polices while they are outside the direct control of the TOE.

The Protection of the TSF function is designed to satisfy FPT_ITT.1 in the following ways:

- The Network Information Flow SFP and Device Control SFP security policy is always encrypted to ensure secrecy and integrity when distributed among distributed TOE components. Digital Signatures are used to authenticate the identity of those parties involved in policy distribution.
- All users must present an opaque credential to authenticate themselves before receiving a policy update.
- The STEngine module protects the TSF via a collection of mechanisms called 'Client Self Defense'. These measures include:
  - **STEngine & STUser Task Manager terminate protection**. STEngine hooks Windows Task Manager and denies requests to terminate STEngine.exe and STUser.exe (the two critical Senforce Security Client user space processes);
  - **Password Protection**. STEngine requires a password defined by policy to stop or pause the service and to uninstall the client;
  - **Registry Entry Protection**. STEngine validates and monitors the registry entries for the STEngine Service, the NDIS driver, the File System Filter driver, and the Storage driver. If a change is made to any of the keys or values that is not valid, the value is immediately changed back to valid values.
  - **NSID driver binding protection**. An Administrative user can unbind the NDIS filter driver from a network card to disable the firewall on that card. STEngine checks to make sure that the NDIS driver is bound to each adapter. If it is not bound, STEngine will rebind the NDIS driver.
  - **File Protection.** A backup copy of critical Senforce Security Client files is kept in the protected store. When these Senforce Security Client files are needed (for example, on boot), these files are verified against the known-good copies to ensure integrity, and are restored from the protected store if needed.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Senforce ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Senforce ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated configuration item modifications are properly controlled. Senforce performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, configuration management documentation, security flaws, and also this Security Target.

These activities, including the list of configuration items, are documented in:

- Endpoint Security Suite version 3 Configuration Management Plan, version 5.0, 13 March 2007

The Configuration management assurance measure satisfies the following EAL 4 augmented with ALC_FLR.2 assurance requirements:

- ACM_AUT.1
- ACM_CAP.4
- ACM_SCP.2

6.2.2 Delivery and operation

Senforce provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Senforce's delivery procedures describe all applicable procedures to be used to detect modification to the TOE. Senforce also provides documentation that describes the steps necessary to install Endpoint Security Suite in accordance with the evaluated configuration.

These activities are documented in:

Enterprise Mobile Security Suite Delivery and Operation Procedures, version 4.1, 21 March 2007

Endpoint Security Suite Version 3.1 Installation and Quick-Start Guide, version 4.3

The Delivery and operation assurance measure satisfies the following EAL 4 augmented with ALC_FLR.2 assurance requirements:

- ADO_DEL.2
- ADO_IGS.1

6.2.3 Development

Senforce has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; a low-level design that further decomposes the TOE architecture into modules and describes each module and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the actual implementation of the TOE. Furthermore, Senforce has a security model that describes each of the security policies implemented by Endpoint Security Suite. Of course, the implementation of the TOE itself is also available as necessary.

These activities are documented in:

- Endpoint Security Suite Version 3.1 Design Documentation, version 6.4, 16 February 2007

The Development assurance measure satisfies the following EAL 4 augmented with ALC_FLR.2 assurance requirements:

- ADV_FSP.2
- ADV_HLD.2
- ADV_IMP.1
- ADV_LLD.1

- ADV_RCR.1
- ADV_SPM.1

6.2.4 Guidance documents

Senforce provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- Endpoint Security Suite Version 3.1 Administrator's Manual, version 4.2
- Endpoint Security Suite Version 3.1 User's Manual, version 4.3

The Guidance documents assurance measure satisfies the following EAL 4 augmented with ALC_FLR.2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

Senforce ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. Senforce includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. Senforce achieves this through the use of a documented model of the TOE life cycle and well-defined development tools that yield consistent and predictable results. In addition, Senforce identifies and tracks reported flaws, ensuring that they are addressed and corrections and corrective measures are made available as applicable.

These activities are documented in:

- Endpoint Security Suite version 3 Life Cycle Document, version 3.2, 27 September 2006

The Life cycle support assurance measure satisfies the following EAL 4 augmented with ALC_FLR.2 assurance requirements:

- ALC_DVS.1
- ALC_FLR.2
- ALC_LCD.1
- ALC_TAT.1

6.2.6 Tests

Senforce has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. Senforce has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- Endpoint Security Suite version 3 Testing Plan, version 5.1, 26 March 2007
- Security Test Cases

- 3.1.175 Test Case Reports, 23 March 2007

The Tests assurance measure satisfies the following EAL 4 augmented with ALC_FLR.2 assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of Endpoint Security Suite and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references. Furthermore, Senforce has conducted a misuse analysis demonstrating that the provided guidance is complete.

Senforce has conducted a search for non-cryptographic probabilistic and permutational mechanisms that implement the security functions of the TOE. No such mechanisms have been identified, and as such, a SOF claim for the TOE is not applicable.

Senforce performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- Endpoint Security Suite Version 3.1 Vulnerability Assessment, version 1.3, 8 May 2007
- Enterprise Endpoint Security Suite Vulnerability Assessment – Misuse, version 1.0, 22 Aug 2006

The Vulnerability assessment assurance measure satisfies the following EAL 4 augmented with ALC_FLR.2 assurance requirements:

- AVA_MSU.2
- AVA_SOF.1
- AVA_VLA.2

7. Protection Profile Claims

This Security Target does not claim conformance with any Protection Profile.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	T.BAD_POLICY	T.ENV_CHANGE	T.NET_ACCESS	T.BAD_RESOURCE	T.NO_FAULT	A.CONNECTION	A.GOOD_ADMIN	A.GOOD_USER	A.PHYSICAL	A.ITENVIRON
O.AUDIT					X					
O.ENV_CHANGE		X								
O.NET_ACCESS			X							
O.RESOURCES				X						
O.SECURE_POLICY	X									
OIE.AUDIT					X					
OIE.NET_ACCESS			X							
OIE.RESOURCES				X						
OIE.SECURE_POLICY	X									
OE.CONNECTION						X				
OE.GOOD_ADMIN							X			
OE.GOOD_USER								X		
OE.PHYSICAL									X	
OE.ITENVIRON										X

Table 4 Environment to Objective Correspondence

8.1.1.1 T.BAD_POLICY

An attacker may be able to cause a mobile host to enforce an inappropriate or insecure security policy.

This Threat is satisfied by ensuring that:

- O.SECURE_POLICY: The TOE allows policies to be defined and then protects the policies during distribution to mobile clients.
- OIE.SECURE_POLICY: The IT environment ensures that only appropriately authorized administrators can manage the policies supported by the TOE and also ensures that the TOE is appropriately protected from tampering.

8.1.1.2 T.ENV_CHANGE

An attacker may be able to exploit a change in the environment of a mobile host to gain unauthorized access to data or computing resources.

This Threat is satisfied by ensuring that:

- O.ENV_CHANGE: The TOE allows policies to be defined for enforcement within specific environments.

8.1.1.3 T.NET_ACCESS

An attacker may be able to gain unauthorized access to data or computing resources by directly accessing a mobile host or by exploiting improper network accesses made by a mobile host user.

This Threat is satisfied by ensuring that:

- O.NET_ACCESS: The TOE controls network access attempts both outbound and inbound relative to the mobile host.
- OIE.NET_ACCESS: The IT environment ensures that the information flow policies provided by the TOE cannot be bypassed.

8.1.1.4 T.BAD_RESOURCE

An attacker may be able to gain unauthorized access to data or computing resources when a user uses inappropriate storage or network devices or file or program resources.

This Threat is satisfied by ensuring that:

- O.RESOURCES: The TOE controls access to removable media and network devices as well as file and executable programs relative to the mobile host.
- OIE.RESOURCES: The IT environment ensures that the access control policies provided by the TOE cannot be bypassed.

8.1.1.5 T.NO_FAULT

An attacker's attempts to violate network or file restrictions may go undetected.

This Threat is satisfied by ensuring that:

- O.AUDIT: The TOE audits the enforcement of the security policy and allows the audit data to be reviewed.
- OIE.AUDIT: The IT environment provides reliable time stamps for the audit records and protects the audit records.

8.1.1.6 A.CONNECTION

Each TOE component will be located in the environment such that it can reliably communicate with the other applicable TOE components when necessary.

This Assumption is satisfied by ensuring that:

- OE.CONNECTION: The distributed TOE components can communicate appropriately.

8.1.1.7 A.GOOD_ADMIN

Administrators will adhere to applicable administrator guidance.

This Assumption is satisfied by ensuring that:

- OE.GOOD_ADMIN: The administrators follow applicable guidance.

8.1.1.8 A.GOOD_USER

Users will adhere to applicable user guidance.

This Assumption is satisfied by ensuring that:

- OE.GOOD_USER: The users follow applicable guidance.

8.1.1.9 A.PHYSICAL

The TOE is physically protected commensurate with the data and resources it protects. Note that in the case of mobile components, users are expected to protect the components to the degree necessary to ensure that the TOE software cannot be uninstalled or otherwise disabled.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: Those responsible for various TOE components protect them appropriately.

8.1.1.10 A.ITENVIRON

The environment will include the IT components required to support the proper operation of the TOE; specifically, suitable operating system, database, web server, and SSL capabilities (as identified in the TOE Description, section 2).

This Assumption is satisfied by ensuring that:

- OE.ITENVIRON: The environment will provide the necessary IT capabilities for the proper operation of the TOE.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 5** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.AUDIT	OIE.AUDIT	O.ENV_CHANGE	O.NET_ACCESS	OIE.NET_ACCESS	O.RESOURCES	OIE.RESOURCES	O.SECURE_POLICY	OIE.SECURE_POLICY
FAU_GEN_EX.1	X								
FAU_SAR.1	X								
FAU_SAR.3	X								
FCS_COP.1								X	

	O.AUDIT	OIE.AUDIT	O.ENV_CHANGE	O.NET_ACCESS	OIE.NET_ACCESS	O.RESOURCES	OIE.RESOURCES	O.SECURE_POLICY	OIE.SECURE_POLICY
FDP_ACF.2						X			
FDP_ACC.1						X			
FDP_IFC.2				X					
FDP_IFF.1			X	X					
FMT_SMF.1								X	
FPT_ITT.1								X	
FAU_STG.1		X							
FIA_UAU.2									X
FIA_UID.2									X
FMT_MOF.1									X
FMT_MTD.1									X
FMT_SMR.1									X
FPT_RVM.1					X		X		
FPT_SEP.1									X
FPT_STM.1		X							

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.AUDIT

The TOE must be able to audit application of the security policy and make that information available to administrators.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN_EX.1: Audit data is generated for important security-relevant events.
- FAU_SAR.1: Audit data is available for review.
- FAU_SAR.3: Audit data can be searched to improve review effectiveness.

8.2.1.2 OIE.AUDIT

The IT environment must be able to protect the audit records and provide reliable time information for use in the audit records.

This IT environment Security Objective is satisfied by ensuring that:

- FAU_STG.1: The IT environment protects audit data.
- FPT_STM.1: The IT environment provides reliable timestamps to audit data.

8.2.1.3 O.ENV_CHANGE

The TOE must allow security policies to be defined individually for different operational environments.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFF.1: Security policies are enforced relative to specific operational environments.

8.2.1.4 O.NET_ACCESS

The TOE must enforce an information flow policy that can control network access attempts originating internal or external to a mobile host.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.2: Network access operations are controlled.
- FDP_IFF.1: Network information flow operations are controlled.

8.2.1.5 OIE.NET_ACCESS

The IT environment must ensure that the network information flow policy implemented by the TOE is not bypassed.

This IT environment Security Objective is satisfied by ensuring that:

- FPT_RVM.1: The IT environment ensures that the TOE security mechanisms cannot be bypassed.

8.2.1.6 O.RESOURCES

The TOE must enforce an access control policy that can control access to removable media devices, network access devices, individual files and directories, and executable programs available to a mobile host.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACF.2: Removable media and network access device, file, and program operations are controlled.
- FDP_ACC.1: Removable media and network access device, file, and program operations are controlled.

8.2.1.7 OIE.RESOURCES

The IT environment must ensure that the access control policy implemented by the TOE is not bypassed.

This IT environment Security Objective is satisfied by ensuring that:

- FPT_RVM.1: The IT environment ensures that the TOE security mechanisms cannot be bypassed.

8.2.1.8 O.SECURE_POLICY

The TOE must allow security policies to be defined and distributed securely throughout the TOE components for enforcement on mobile hosts.

This TOE Security Objective is satisfied by ensuring that:

- FCS_COP.1: Security policies are encrypted when outside the direct control of the TOE.
- FMT_SMF.1: Security policies can be comprehensively managed.
- FPT_ITT.1: Security policies are protected from modification and disclosure between distributed TOE components.

8.2.1.9 OIE.SECURE_POLICY

The IT environment must ensure that only appropriately identified and authenticated administrators can manage the security policies supported by the TOE and also that the TOE is protected from tampering.

This IT environment Security Objective is satisfied by ensuring that:

- FIA_UAU.2: The IT environment ensures only authenticated users can access protected TOE resources.
- FIA_UID.2: The IT environment ensures only identified users can access protected TOE resources.
- FMT_MOF.1: The IT environment restricts review and modification of the TOE security policy and other security-relevant behavior to an authorized administrator.
- FMT_MTD.1: The IT environment restricts access to the security policy-related attributes to an authorized administrator.
- FMT_SMR.1: The IT environment provides an administrator role to support control of other security features.

- FPT_SEP.1: The IT environment ensures that the TOE security mechanisms cannot be tampered with.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL 4 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a low to medium level of risk to the applicable assets. As such, EAL 4 (augmented with ALC_FLR.2) is appropriate to provide the assurance necessary to counter the potential for attack.

8.4 Strength of Functions Rationale

The Endpoint Security Suite TOE does not implement any non-cryptographic permutational or probabilistic mechanisms. As such, a Strength Of Function (SOF) claim is not applicable to this TOE.

8.5 Requirement Dependency Rationale

The following table represents an analysis of the dependencies of the security requirements (SRs), both functional and assurance, in this security target. The first column identifies all of the SRs in this security target. The TOE SRs are highlighted in bold, unlike the IT environment SRs. The second column identifies the minimum dependencies defined in the Common Criteria v2.2. The third column identifies the actual requirements in this security target that correspond to the identified dependencies. The corresponding TOE SFRs are highlighted in bold, SARs are underlined, and IT environment SFRs are italicized. Notice that this table demonstrates that all of the identified dependencies are satisfied with the exception of FCS_CKM.1, FCS_CKM.4, FMT_MSA.2, and FMT_MSA.3 (all identified in brackets and bold red text and rationalized below). Note also that FAU_GEN_EX.1 is used to fulfill the FAU_GEN.1 dependencies – the primary difference between these requirements is that FAU_GEN_EX.1 does not record events associated with starting and stopping the audit function, but otherwise it fulfills the FAU_GEN.1 dependency by generating audit events.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN_EX.1	FPT_STM.1	*FPT_STM.1*
FAU_SAR.1	FAU_GEN.1	FAU_GEN_EX.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FCS_COP.1	(FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	**[FCS_CKM.1]** and **[FCS_CKM.4]** and **[FMT_MSA.2]**
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1 and **[FMT_MSA.3]**
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.2 and **[FMT_MSA.3]**
FMT_SMF.1	none	none
FPT_ITT.1	none	none
FAU_STG.1	FAU_GEN.1	FAU_GEN_EX.1
FIA_UAU.2	FIA_UID.1	*FIA_UID.2*
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	*FMT_SMR.1* and FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	*FMT_SMR.1* and FMT_SMF.1
FMT_SMR.1	FIA_UID.1	*FIA_UID.2*
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
ACM_AUT.1	ACM_CAP.3	ACM_CAP.4
ACM_CAP.4	ALC_DVS.1	ALC_DVS.1
ACM_SCP.2	ACM_CAP.3	ACM_CAP.4

ST Requirement	CC Dependencies	ST Dependencies
ADO_DEL.2	ACM_CAP.3	ACM_CAP.4
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.2	ADV_RCR.1	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.2 and ADV_RCR.1
ADV_IMP.1	ADV_LLD.1 and ADV_RCR.1 and ALC_TAT.1	ADV_LLD.1 and ADV_RCR.1 and ALC_TAT.1
ADV_LLD.1	ADV_HLD.2 and ADV_RCR.1	ADV_HLD.2 and ADV_RCR.1
ADV_RCR.1	none	none
ADV_SPM.1	ADV_FSP.1	ADV_FSP.2
AGD_ADM.1	ADV_FSP.1	ADV_FSP.2
AGD_USR.1	ADV_FSP.1	ADV_FSP.2
ALC_DVS.1	none	none
ALC_FLR.2	none	none
ALC_LCD.1	none	none
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.2 and ATE_FUN.1
ATE_DPT.1	ADV_HLD.1 and ATE_FUN.1	ADV_HLD.2 and ATE_FUN.1
ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.2 and AGD_ADM.1 and AGD_USR.1
ATE_IND.2	none	none
AVA_MSU.2	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1	ADO_IGS.1 and ADV_FSP.2 and AGD_ADM.1 and AGD_USR.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.2 and ADV_HLD.2
AVA_VLA.2	ADV_FSP.1 and ADV_HLD.2 and ADV_IMP.1 and ADV_LLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.2 and ADV_HLD.2 and ADV_IMP.1 and ADV_LLD.1 and AGD_ADM.1 and AGD_USR.1

Table 6 Requirement Dependencies

FCS_COP.1 has dependencies on FCS_CKM.1 (key generation), FCS_CKM.4, (key destruction), and FMT_MSA.2 (secure data). The FCS_COP.1 claim is included in this ST to support the use of cryptography in protecting security policies as they are distributed among TOE components. This requirement is supported by using a commercially available, FIPS-140 certified cryptographic library – 'Crypto++'. Since this library was FIPS-140 certified it is assumed that it addresses the issues related to key generation, key destruction, and secure data since the TOE was not developed with any mechanisms to support any of these functions, other than adopting the identified library. It is not the intent of this ST to make or substantiate claims about third-party components that seem already to have been verified.

FDP_ACF.1 and FDP_IFF.1 both have a dependency on FMT_MSA.3 which requires specification of initial security attribute values and identification of who can change them. The TOE allow definition of security policies as specified in FMT_SMF.1 and restricts who can modified those policies via the IT environment as specified in FMT_MOF.1 and FMT_MTD.1. Given that the policy must always be defined and is enforced specifically as defined, the notion of 'default' initial values isn't obviously applicable and while an administrator can change the policy, there is no notion of changing any default initial value. Note also that the security attributes not defined within a security policy are identification attributes that are inherent properties of mobile hosts and various controlled devices. Hence, it seems these dependencies are not necessary as they seem to be satisfied by the other requirements identified above.

8.6 Explicitly Stated Requirements Rationale

This Security Target defines the explicit functional requirement FAU_GEN_EX.1, which is based on the CC version of FAU_GEN.1. This is necessary because only Senforce Security Clients configured in Managed mode are able to generate audit records and pass them back (via the Distribution server) to the Management Server's Reporting Database for collation and synthesis.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	**Cryptographic support**	**User data protection**	**Security management**	**Protection of the TSF**
FAU_GEN_EX.1	X				
FAU_SAR.1	X				
FAU_SAR.3	X				
FCS_COP.1		X			
FDP_ACC.1			X		
FDP_ACF.1			X		
FDP_IFC.2			X		
FDP_IFF.1			X		
FMT_SMF.1				X	
FPT_ITT.1					X

Table 7 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.