National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Senforce Endpoint Security Suite v3.1.175

Report Number: CCEVS-VR-07-0045
Dated: 7 June 2007
Version: 0.4

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Ralph Broom
Noblis

Robin Medlock
The MITRE Corporation

Common Criteria Testing Laboratory

SAIC
Columbia, Maryland

Table of Contents

List of Tables

1 Executive Summary

This document is intended to assist end-users of this product with determining the suitability of the product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, and this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of Senforce Endpoint Security Suite v3.1.175. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS). The criteria against which the Senforce Endpoint Security Suite TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.2 and International Interpretations effective on 21 May 2004. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2. A validation team on behalf of the CCEVS Validation Body monitored the evaluation carried out by SAIC. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. The evaluation was completed in May 2007.

The SAIC evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 4 augmented with ALC_FLR.2 family of assurance requirements.

Senforce Endpoint Security Suite v3.1.175 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 software TOE comprises three server components, a management console component, and a client component that together provide centralized management of computing resources and data assets on mobile clients. The three server components are supported on any of the following in the IT environment: Microsoft Windows 2000 Server SP4; Microsoft Windows 2000 Advanced Server SP4; and Windows 2003 Server. The client component is supported on any of the following: Windows XP SP1; Windows XP SP2; and Windows 2000 SP4. The management console component can be installed on the same server as the Management Service (recommended) or on a separate computer, in which case it is supported on Windows XP SP1, Windows XP SP2, and Windows 2000 SP4.

The product, when installed and configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the Senforce Endpoint Security Suite Security Target Version 3.1.175.

The validation team agrees that the CCTL presented appropriate rationales to support the Results of Evaluation presented in Section 5, and the Conclusions presented in Section 6 of the ETR. The

validation team therefore concludes that the evaluation and the Pass results for the Senforce Endpoint Security Suite v3.1.175 is complete and correct.

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Senforce Endpoint Security Suite v3.1.175
Sponsor:	Senforce Technologies, Inc 147 W Election Rd Ste 110 Draper, UT 84020
Developer:	Senforce Technologies, Inc 147 W Election Rd Ste 110 Draper, UT 84020
CCTL:	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Kickoff Date:	21 May 2004
Completion Date:	30 April 2007
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.2
Interpretations:	RI-137
CEM:	Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, Version 0.6, January 1997; Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.2, August 1999.
Evaluation Class:	EAL 4, augmented with ALC_FLR.2
Description:	The TOE, Senforce Endpoint Security Suite v3.1.175, 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.

Disclaimer:	The information contained in this Validation Report is not an endorsement of the Senforce Endpoint Security Suite v3.1.175 product by any agency of the U.S. Government and no warranty of the Endpoint Security Suite product is either expressed or implied.
PP:	None
Evaluation Personnel:	Science Applications International Corporation: Anthony J. Apted Dawn Campbell J. David Thompson Lisa Vincent
Validation Team:	Ralph Broom, Noblis Robin Medlock, The MITRE Corporation

1.2 Interpretations

Interpretation ID	Impact on CC Requirements	Impact on CEM Work Units	Comment
RI-137	FIA_USB.1 changed	None	Not applicable

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 2 – Threats

Threat Identifier	Threat Description
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.

2 Identification

The product being evaluated is Senforce Endpoint Security Suite v3.1.175.

3 Security Policy

The TOE enforces the following security policies as described in the Security Target.

3.1 Information Flow

The client component of the TOE is installed on mobile hosts, at various points in the network protocol and file driver layers of the host operating system. The TOE enforces information flow (firewall) policies retrieved from the central management service 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.

3.2 Access Control

The client component of the TOE 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.

3.3 Cryptographic Support

The TOE protects the policies it distributes to mobile clients from disclosure and undetected modification by encrypting critical parts of the policy and digitally signing the policy. The TOE uses 256-bit AES for encryption and 2048-bit RSA in conjunction with SHA-1 for generating digital signatures. The TOE incorporates the FIPS 140-2 validated Crypto++ cryptomodule, which is used for these cryptographic operations.

3.4 Auditing

The TOE generates audit records of security relevant events as they occur on the mobile client computers. They are stored by the underlying operating system and, hence, the TOE is dependent upon that OS for proper protection of the audit trail. The clients periodically upload stored audit records to the central management servers, based on the client's current policy settings. At the central management servers, the audit records are stored in a SQL Server database in the IT environment. Hence, the central management components are also dependent upon the underlying IT environment for proper protection of the audit trail.

4 Assumptions

4.1 Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 3 – Physical Assumptions

Assumption Identifier	Assumption Description
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.

4.2 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 4 – Personnel Assumptions

Assumption Identifier	Assumption Description
A.GOOD_ADMIN	Administrators will adhere to applicable administrator guidance.
A.GOOD_USER	Users will adhere to applicable user guidance

4.3 Operational Assumptions

The following operational assumptions are identified in the Security Target:

Table 5 – Operational Assumptions

Assumption Identifier	Assumption Description
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.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)

4.4 Clarification of Scope

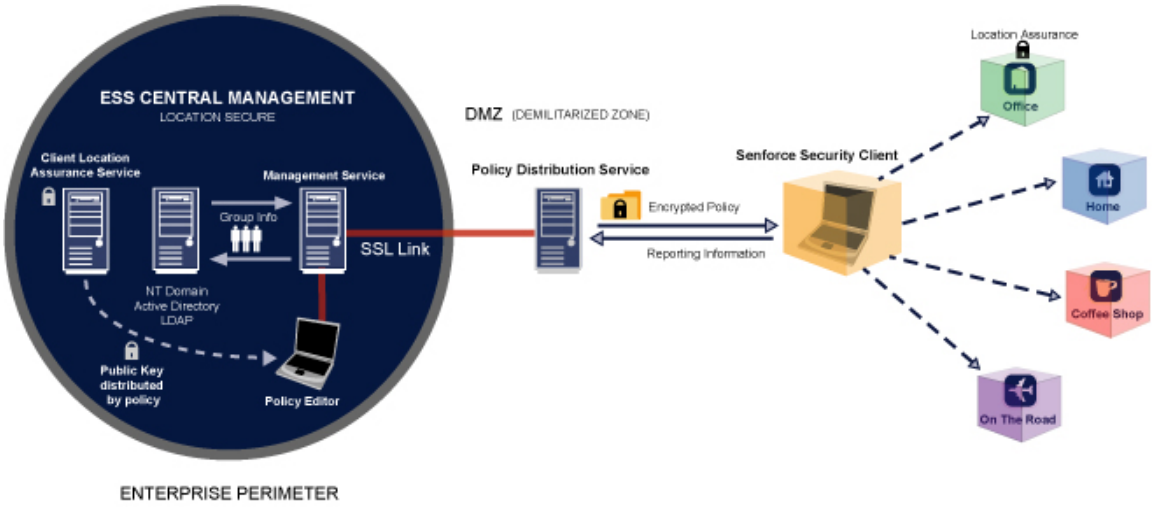
The product being evaluated and consequently the TOE is entirely software. The client component of the TOE is installed as a number of kernel drivers along with a user mode application and implements a variety of self-protection mechanisms. Nevertheless, it is also reliant on the underlying operating system to provide protection from bypass and tampering.

Similarly, the central management components are reliant on the underlying operating system for protection of policies and audit data.

It should also be noted that while the client component applies some controls on the client computer when it is first installed, the client is not considered to be in its evaluated configuration until it has received a policy from the Management Server.

5 Architectural Information

The TOE architecture comprises four main components that are placed at key points within the enterprise architecture: Distribution Server, Management Server, Client Location Assurance Service (CLAS), and Senforce Security Client (SSC). In addition, the TOE includes the Policy Editor, an application that provides the interface for administrators to configure and manage the TOE and to create, edit and publish the security policies that are distributed to endpoint clients.



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 Distribution Server authenticates Senforce Security Clients based on the credentials obtained from the Management Server, and supplies each client with the designated security policy.

The Management Server provides security policies and user information to the Distribution Server, as well as providing opaque credentials 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.

The Client Location Assurance Service can be installed on any server in any Enterprise-owned network environment to provide a cryptographic guarantee to Senforce Security Clients that they

are indeed in the location that the other existing network environment parameters would indicate. The Senforce Security Client 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 Senforce Security Client sends a random challenge (consisting of a 128-bit pseudo-random bit string (nonce) generated via the Crypto++ FIPS-140 certified cryptographic library[1]) 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 Policy Editor is a tool that 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.

The Senforce Security Client (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. The user interface options displayed and available to SSC end users are dependent upon the permissions set in the security policy.

6 Documentation

The following documents are available to customers and are pertinent to the installation, configuration, and operation of the TOE.

- Senforce Endpoint Security Suite v3.1 Installation and Quick-Start Guide, version 4.3
- Senforce Endpoint Security Suite v3.1 Administrator's Guide, version 4.2
- Senforce Endpoint Security Suite v3.1 User's Guide, version 4.3

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

The evaluated configuration of the TOE is the Senforce Endpoint Security Suite, version 3.1, build 175. The TOE comprises three server components, a management console component, and a client component that together provide centralized management of computing resources and data assets on mobile clients. The server components are the Management Service, Policy Distribution Service, and Client Location Assurance Service. The management console component is the Policy Editor (also identified as the Management Console). The client component is the Senforce Security Client.

The three server components are supported on any of the following: Microsoft Windows 2000 Server SP4; Microsoft Windows 2000 Advanced Server SP4; and Windows 2003 Server. The client component is supported on any of the following: Windows XP SP1; Windows XP SP2; and

[1] 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.

Windows 2000 SP4. The management console component can be installed on the same server as the Management Service (recommended) or on a separate computer, in which case it is supported on Windows XP SP1, Windows XP SP2, and Windows 2000 SP4.

In a typical deployment, the Management Service and Client Location Assurance Service (CLAS) are installed on servers within the secure boundary of the enterprise—the CLAS can but need not be installed on the same server as the Management Service. The Policy Distribution Service is typically installed on a separate server, which can be inside or outside the enterprise firewall—the main criterion is that it be reachable by mobile clients so that they can receive policy updates.

Testing took place at the SAIC CCTL facility in Columbia, MD, during the week of 16-20 April, 2007.

The evaluation team used the following configuration for testing:

- Management Service and CLAS installed on one server (Windows 2000 Server SP4)
- Policy Distribution Service installed on second server (Windows 2003 Server SP2)
- Management Console installed on same server as Management Service (the recommended configuration)
- Senforce Security Client installed on two laptops (Windows XP SP2; Windows 2000 SP4).

The following additional components are required in the IT environment:

- RDBMS (Microsoft SQL Server Enterprise SP4)
- Microsoft Internet Information Services (configured for SSL)
- Supported Directory Service (Active Directory).

Once all team testing was completed, the evaluation team uninstalled the TOE and reinstalled it with the Management Service, CLAS, and Management Console installed on the Windows 2003 Server system, and the Policy Distribution Service installed on the Windows 2000 Server system, in order to broaden the coverage of possible configurations. A selection of vendor and evaluation team tests was re-run on this configuration.

7.1 Developer Testing

The vendor ran the entire test suite on the test configuration described in the Test Documentation and gave the evaluation team the actual results. The actual results comprise information exported from TestLog and provide test case reports for all test cases. The test case reports identify that all tests passed. The evaluation team examined the test cases and determined that the expected behavior described at each test step would demonstrate the correct behavior of the TOE.

The evaluation team ran each of the test cases in the vendor's test suite to validate that the test cases correctly represent the behavior of the TOE and that the actual results match the expected results described in the test cases.

7.2 Evaluation Team Independent Testing

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The vendor test system was used with team generated test procedures and team analysis to determine the expected results. All actual results matched the expected results.

The evaluation team performed the following additional functional tests:

- Audit Generation and Review: The evaluation team expanded on the developer's testing to confirm that the TOE provided the audit capabilities described in the ST. As a result of the evaluation team's testing, the audit claims and description of audit functionality were updated in the ST to correctly represent the TOE capabilities
- Information Flow Attribute Combinations: The TOE enforces network information flow decisions based on combinations of the following traffic attributes: source and destination addresses; point of origin (mobile host or network); transport layer protocol; application identifier; and encryption state. The evaluation team extended the developer's testing of this capability with various combinations of Access Control Lists, TCP/UDP ports, and application controls
- Default Client Behavior: The evaluation team performed the following tests related to the behavior of the Senforce client when it is first installed and before it obtains a Senforce policy: test client behavior prior to initial check-in; check for the existence of a default policy; test what happens when a client is deployed without a policy. The test results demonstrated that the Senforce Security Client applies default behavior to the client computer in both Unmanaged and Managed modes. It should be noted, however, that prior to installing its initial policy, the client is applying default protection rather than a default policy created by the Policy Editor workstation. Therefore, until such time as the first policy is installed, the client is not in the evaluated configuration. An explanation of this behavior was added to the Security Target.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. No relevant results were found. The evaluation team developed team penetration tests building on the developer's vulnerability analysis and on their own independent analysis based on a flaw hypothesis methodology. The evaluation team devised and executed test procedures to determine that the TOE, in its intended environment, is resistant to an attacker possessing a low attack potential.

The evaluation team performed the following vulnerability tests and analyses:

- Integrity of SSC Audit Records: The evaluation team examined the storage of audit records on the mobile client prior to their being uploaded to the Distribution server, in order to determine if they were adequately protected by default. The evaluation team found that the audit records are protected by the IT environment from modification or deletion by non-administrative users of the mobile host. However, a user on the mobile host with administrative privileges would be able to modify or delete the audit records. An appropriate warning about this was added to the guidance documentation
- Client Self Defense: The TOE implements a number of mechanisms in the Senforce Security Client in order to protect it from bypass and tampering. The vendor tests include tests of the claimed self-protection capabilities. Any successful disabling, deletion, or bypass can only be achieved by violating assumptions about the method or environment of use of the TOE (in particular, A.GOOD_USER and A.PHYSICAL). Access to media and devices otherwise blocked by Senforce could be achieved by booting the system from a CD-resident OS. However, the intended use of the TOE is to protect the resources of the mobile client from possible network attacks or accidental misuse. The user of the

mobile client is assumed to adhere to user guidance, not to attempt to disable or otherwise bypass the TOE, and to physically protect the mobile host

- SSL Exposure: The TOE relies on the IT environment to provide secure communications over SSL. The evaluation team investigated if any vulnerabilities in the SSL implementation could expose the TOE (e.g., man-in-the-middle attack). SSL is used in two ways: to protect communications between the Management Server and the Distribution Server; to protect communications between the client and the Management Server when the client initializes itself to the Management Server (a one-time occurrence). The Distribution Server and the Management Server each has its own public-private key pair (which can be obtained from an external certificate authority, or generated and self-signed during installation of each server). Each server is provided with the other's public key and these are used to establish mutually-authenticated SSL communications. Prior to installing the Senforce Security Client component on a mobile host, the Management Server public key is installed on the client. Once the Senforce Security Client is installed, it communicates with the Management Server in order to initialize itself. It uses the Management Server public key to establish an SSL session, and then provides the Management Server with the client user's username and password. The Management Server authenticates the user against the Enterprise Identity Repository (e.g., Active Directory) and generates a client credential which it passes back to the client. This is the only communication between the Management Server and client. The client subsequently obtains encrypted and signed policies from the Distribution Server and uploads audit records (encrypted using the Management Server public key) to the Distribution Server. The evaluation team did not identify any exposure of the TOE to potential SSL vulnerabilities that would be exploitable in the intended environment of the TOE.

8 Evaluated Configuration

The evaluated version of the TOE is Endpoint Security Suite v3.1.175.

The three server components (i.e., Distribution, Management, and CLAS) are designed to operate on a Windows 2000 Server SP4 or Advanced Server SP4 or Windows 2003 Server. The CLAS component is designed to co-exist with either of the other server components, or alternately in its own server. The Policy Editor and SSC components are designed to operate on Windows XP SP1, Windows XP SP2, or any Windows 2000 SP4 system. Alternatively, the Policy Editor can be installed on the same server as the Management Service, or on its own workstation. 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 SP4, SQL Server Standard, or SQL Server Enterprise), web server (Microsoft Internet Information Server), web browser (Microsoft Internet Explorer), and secure socket layer (SSL) capabilities.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.2 and CEM version 2.2. The evaluation determined the Senforce Endpoint Security Suite TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level 4 (EAL 4) requirements augmented with ALC_FLR.1. The rationale supporting each CEM work unit verdict is recorded

in the **Evaluation Technical Report for Senforce Endpoint Security Suite v3.1.175 Part 2** which is considered proprietary.

10 Validator Comments/Recommendations

The validator would like to restate the following from the Security Target for clarity.

- "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."
- "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."
- "The 'Endpoint Check-in Adherence' and 'Location Usage Data' reports, in particular, provide information on mobile host security policy updates." These reports contain the relevant audit information to meet the audit generation security functional requirement. The Senforce Endpoint Security Suite also provides other reports that may provide useful information

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is **Senforce Endpoint Security Suite v3.1.175 Security Target**, Version 1.0, dated June 19, 2007.

13 Glossary

No definitions beyond those in the CC or CEM are supplied.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.2, January 2004, CCIMB-2004-01-001.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.2, January 2004, CCIMB-2004-01-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.2, January 2004, CCIMB-2004-01-003.

[4] Common Methodology for Information Technology Security: Evaluation Methodology, Version 2.2, January 2004, CCIMB-2004-01-004.

[5] Evaluation Technical Report for Senforce Endpoint Security Suite v3.1.175 Part 1, Version 1.0, 19 June 2007.

[6] Evaluation Technical Report for Senforce Endpoint Security Suite v3.1.175 Part 2, Version 1.0, 19 June 2007.

[7] Evaluation Team Test Report for Senforce Endpoint Security Suite v3.1.175 Part 2 ETR Supplement, Version 1.0, 19 June 2007.

[8] Senforce Endpoint Security Suite Security Target, Version 1.0, 19 June 2007.

[9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.