National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

StillSecure
StillSecure Safe Access V5.0

Report Number: CCEVS-VR-VID10270-2007
Dated: October 4, 2007
Version: Version 1.0

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

Table of Contents

1. Executive Summary 3
2. Identification 4
3. Security Policy 5
4. Assumptions and Clarification of Scope 7
4.1 Usage Assumptions 7
4.2 Environmental Assumptions 7
4.3 Clarification of Scope 7
5. Architectural Information 8
6. Documentation 9
7. IT Product Testing 9
7.1 Developer Testing 10
7.2 Evaluator Independent Testing 10
7.3 Strength of Function 11
8. Evaluated Configuration 11
9. Results of Evaluation 12
10. Validator Comments/Recommendations 12
11. Security Target 13
12. Glossary 13
13. Bibliography 14

Table of figures

Figure 1 TOE Components 9

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product StillSecure Safe Access V5.0, a product of StillSecure, Superior, CO 80027.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

StillSecure Safe Access is a flexible Network Access Control Solution that fits into existing network architecture and covers a range of endpoint devices and users. Safe Access protects the network by ensuring that endpoint devices are in compliance with the organization's IT security standards before they are granted access to the protected network

Safe Access administrators create Network Access Control (NAC) policies that define which applications and services are permitted (or not permitted) on the endpoint device before it is granted access to the protected network and specifies the actions to be taken when the endpoint devices do not comply. With support from the IT environment, Safe Access automatically applies the NAC policies to endpoint devices as they connect to the network. Depending on the endpoint device testing method chosen, Safe Access can periodically test devices that have been granted access to ensure that real-time system changes do not violate the network access security policy. Safe Access provides three NAC enforcement methods for quarantining non-compliant endpoints. Physical deployment of the Safe Access is dependent on the enforcement method used. The three enforcement methods are: Inline for VPN and RAS connections, DHCP, and 802.1X.

Based on the test results, endpoint devices are either permitted access to the protected network or quarantined to a specific part of the network, thus enforcing the NAC policy. Safe Access audits all testing and connection activity and produces a range of reports for auditors.

StillSecure Safe Access also supports authenticating users, allows management of user privileges, and reports the result of enforcing the NAC security policy on endpoints connecting to the protected network.

StillSecure Safe Access V5.0 consists of following software components:

- Management Server (MS)
- Enforcement Server (ES)
- StillSecure Safe Access Agent
- StillSecure ActiveX Control

Aspects of the following security functions are controlled / provided by the TOE in conjunction with its information technology (IT) environment:

- Security audit
- Network Access Control
- Identification and authentication
- Security management
- Protection of TSF
- StillSecure Safe Access Reporting
- Trusted Path/Channel usage

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during July 2007. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.3 [CC] Part 2 and Part 3 conformant, and meets the assurance requirements of EAL2 from the Common Methodology for Information Technology Security Evaluation, Version 2.3, [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The Security Target (ST) is contained within the document Security Target for StillSecure Safe Access V5.0 [ST].

2. Identification

Target of Evaluation:	StillSecure Safe Access V5.0.
Evaluated Software:	StillSecure Safe Access V5.0, Build 5.0-3146 Agents have the same version as Safe Access software.
Developer:	StillSecure 100 Superior Plaza Way Suite 200 Superior, CO 80027
CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive

	McLean, VA 22102-3305
Evaluator	Mossadeq Zia, Cygnacom Solutions
Validation Scheme:	National Information Assurance Partnership CCEVS
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements. A description of the principle security policies is as follows:

- **Security Audit**

StillSecure Safe Access provides its own internal auditing capabilities separate from those of the Operating System. StillSecure Safe Access provides the ability to search and view its own audit records.

- **Network Access Control**

StillSecure Safe Access provides user data protection by enforcing default or administrator defined NAC policy on endpoints accessing the protected network. StillSecure Safe Access tests all endpoints for compliance and grants or denies access to the protected network based on test results.

- **Identification and Authentication**

StillSecure Safe Access provides TOE user identification and authentication through the use of user accounts and passwords.

- **Security Management**

StillSecure Safe Access provides security management through the Management Server's Web-based console and by reporting the endpoint compliance and access activity. Also, the TOE provides two administrative roles as Cluster Administrator and System Administrator.

- **Protection of the TSF**

StillSecure Safe Access partially protects its programs and data from unauthorized access through its own interfaces.

- **StillSecure Safe Access Reporting**

Safe Access provides Safe Access users with the necessary privileges to generate and view reports providing security status information on endpoint compliance and access activity. System administrators can operate on the reports pertaining to all clusters. Cluster administrator, Help desk technician, and User defined role with explicitly assigned privilege can operate on the reports pertaining to their own clusters.

- **Trusted Path/Channel Usage**

The TOE makes use of trusted paths and channel supported in the IT environment.

A summary of the SFRs for the TOE and IT environment are included in the following tables.

TOE Security Functional Requirements

Item	SFR ID	SFR Title
1.	FAU_GEN.1	Audit data generation
2.	FAU_GEN.2	User identity association
3.	FAU_SAR.1	Audit review
4.	FAU_SAR.3	Selectable audit review
5.	FAU_STG_EXP.1-1	Protected audit trail storage
6.	FDP_ACC.1	Subset access control
7.	FDP_ACF.1	Security attribute based access control
8.	FDP_ACC_8021X_EXP.1-1	Partial subset access control
9.	FDP_ACF_8021X_EXP.1-1	Partial security attribute based access control
10.	FDP_ACC_BRIDGE_EXP.1-1	Partial subset access control
11.	FDP_ACF_BRIDGE_EXP.1-1	Partial security attribute based access control
12.	FIA_ATD.1	User attribute definition
13.	FIA_UAU.2	User authentication before any action
14.	FIA_UAU.7	Protected authentication feedback
15.	FIA_UID.2	User identification before any action
16.	FMT_MSA.3	Static attribute initialization
17.	FMT_MTD.1	Management of TSF data
18.	FMT_SMR.1	Security roles
19.	FMT_SMF.1	Specification of management functions
20.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP
21.	FPT_SEP_EXP.1-1	TSF domain separation
22.	FSR_SRG_EXP.1	StillSecure report generation
23.	FSR_SRR_EXP.1	StillSecure report review
24.	FTP_TRP_EXP.1-1	Partial trusted channel

IT Environment Security Functional Requirements

No.	SFR ID	SFR Title
1.	FAU_STG_EXP.1-2	Protected audit trail storage
2.	FDP_ACC_8021X_EXP.1-2	Partial Subset access control
3.	FDP_ACF_8021X_EXP.1-2	Partial security attribute based access control

No.	SFR ID	SFR Title
4.	FDP_ACC_BRIDGE_EXP.1-2	Partial Subset access control
5.	FDP_ACF_BRIDGE_EXP.1-2	Partial Security attribute based access control
6.	FIA_UAU_8021X_EXP.1	Timing of authentication
7.	FIA_UID_8021X_EXP.1	Timing of identification
8.	FPT_IDSCAN_EXP.1	Endpoint scan
9.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
10.	FPT_SEP_EXP.1-2	TSF domain separation
11.	FPT_STM.1	Reliable time stamps
12.	FTP_TRP_EXP.1-2	Partial trusted channel

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

- Administrators and operators are non-hostile, appropriately trained and follow all administrative guidance, including guidance on setting passwords.
- Administrators will ensure that the environment has adequate facility to provide disk storage and other capabilities for the TOE's protection.
- The attack potential on the TOE is assumed to be low.
- It is assumed that there will be no untrusted users and no untrusted software on the StillSecure Safe Access Server host which hosts the Management Server and the Enforcement Servers.
- Physical protection is assumed to be provided by the environment. The TOE hardware and software is assumed to be protected from unauthorized physical access.
- Those responsible for the TOE will ensure the communications between the Administrator PC and StillSecure Safe Access Server host are secure.
- It is assumed that authorized users will protect their authentication data.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL2 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. StillSecure Safe Access, the product that a customer would purchase, includes more than the evaluated TOE. The evaluated TOE does not include the product components that are optionally installed on client platform.
5. TOE depends on IT environment for the following:
    a. to provide the capability to protect audit information.
    b. to provide assured client identification and authentication of users prior to allowing access to IT environment functions and data.
    c. to ensure that the IT environment's security functional policy is invoked and succeeds before allowing another IT environment function to proceed.
    d. to maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
    e. to protect TSF data when transferred between TOE Components by providing SSL communication channels.
    f. to provide reliable time stamps.

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

The TOE consists of the following components:

- StillSecure Safe Access V5.0 Management Server (MS)
- StillSecure Safe Access V5.0 Enforcement Server (ES)
- StillSecure Safe Access Agent
- StillSecure ActiveX Control

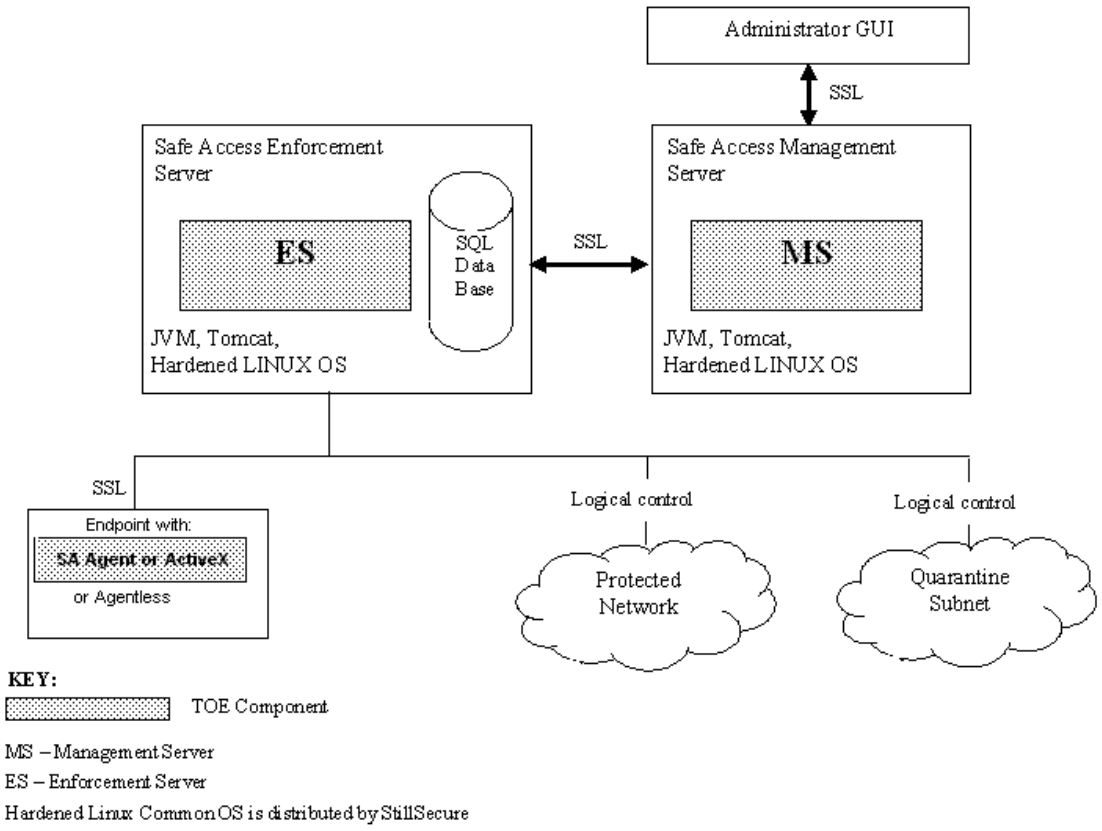

Figure 1 TOE Components

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- StillSecure Safe Access V5.0 Security Target (ST) V1.0; September 4, 2007
- StillSecure Safe Access V5.0 Common Criteria Supplement to the Guidance Documentation V1.0; September 4, 2007
- StillSecure Safe Access V5.0 Release Notes (rev-s); July 20, 2007
- StillSecure Safe Access v5.0 Installation Guide (rev-j); July 13, 2007
- StillSecure Safe Access v5.0 User's Guide (rev-n); July 13, 2007

7. IT Product Testing

At EAL2, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 2, the developer's test evidence must only "demonstrate a correspondence between the tests and the functional specification" (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings are considered by the evaluator during the independent testing sub-activity." (6.8.2.2 [CEM]).

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests" (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset and states that the "evaluators should exercise most of the security functional requirements identified in the ST using at least one test" (6.8.4.4 [CEM]). While, the evaluators build on the developer's testing and use the developer's correspondence evidence to identify shortcomings in the developer's test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

7.1 Developer Testing

The vendor testing covered the security functions identified in Section 6.1 of the ST. These security functions were: Security audit, Network Access Control (NAC), Identification and Authentication, Security Management, Protection of the TSF, Security Status Reporting and Trusted Channel.

The vendor test procedures consisted primarily of manually invoking functions described in the product's user and administrative guides and verifying the function's behavior. The evaluator determined that the developer's approach to testing the TSFs was appropriate for this EAL2 evaluation.

7.2 Evaluator Independent Testing

The environment and configuration for the Team-Defined testing was the same as that for the Developer Functional testing. No general test setup procedures were performed prior to the Team-Defined testing. The following test configuration was used:

- ES and MS Servers
  - StillSecure Safe Access V5.0, Build 5.0-3146
- 1 workstation with windows OS XP SP2
  - Browser: IE 6.0
- 1 workstation with MAC OS 10
  - Agent-based testing only
- 1 CISCO 2950 or HP ProCurve Switch

The evaluator tested the TOE at the developer's facility using both vendor and team developed test cases. The evaluator repeated a subset of the developer's tests (approximately 60%) and verified the actual results against the expected results. A test failure was reported to StillSecure who upgraded the software with an appropriate fix. This software fix was incorporated in the final build 3146.

7.3 Strength of Function

The TOE depends on the strength of the passwords used to authenticate access by administrative users. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. The overall strength of function (SOF) requirements claim for the TOE is SOF-Basic, which effectively requires resistance to password guessing attacks of greater than one day.

The TOE's SOF analysis assumed that each user selects a password meeting the following criteria: a minimum of 8 characters and at least one each of a lower case, an upper case, a special character, and a numeric character. The SOF analysis assumed a worst case password guessing rate of 1000 guesses per second. To effectively resist password guessing attacks for 24 hours, the users must ensure that the passwords are sufficiently random (i.e., requiring more than 100 million guesses).

8. Evaluated Configuration

The StillSecure SafeAccess V5.0 evaluated configuration consists of the following:

Safe Access Software V5.0 Build 5.0-3146

The following components of the IT environment are included as part of StillSecure SafeAccess install CD:

- Java Virtual Machine (JVM): version 1.5.0-b10
- Apache/Tomcat: version 5.5.7
- PostgreSQL: version 8.1.8

- Linux OS: StillSecure customized version

Install CD can be created from an image file downloaded from the StillSecure Web site, or can be requested from StillSecure.

9. Results of 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 version 2.3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_CAP.2	CM Documentation
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.1	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

10. Validator Comments/Recommendations

The following comments and recommendations are offered:

1. Windows Vista is listed as an unsupported OS in the release notes.
2. The high availability and load balancing functions of Safe Access are not claimed or tested as part of the evaluation.

3. The StillSecure product is bundled with several significant third party components that are not directly maintained by StillSecure. When new vulnerabilities are discovered, end-users should not independently install publicly available patches to or newer versions of these components. StillSecure should be contacted to obtain security critical patches related to the following components: Java Virtual Machine, Apache/Tomcat, PostgreSQL, and Linux OS.

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team, and an EAL2 certificate rating is issued for the StillSecure Safe Access V5.0.

11. Security Target

The Security Target for StillSecure Safe Access V5.0 is contained within the document Security Target for Security Target for StillSecure Safe Access V5.0, ST Version 1.1 [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Criteria Evaluation Methodology
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ES	Enforcement Server
ETR	Evaluation Technical Report
IT	Information Technology
MS	Management Server
NAC	Network Access Control
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OS	Operating System
PP	Protection Profile
SFR	Security Functional Requirement
SOF	Strength of Function

ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- StillSecure (http://www.stillsecure.com/).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.

Other Documents

- [ST] Security Target for StillSecure Safe Access V5.0, ST Version 1.1, September 17, 2007.