National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

SecureWave

Sanctuary Application Control Custom Edition

Version 2.8

Report Number: CCEVS-VR-06-0036

Dated: 11 September 2006

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

ACKNOWLEDGEMENTS

Validation Team

The Aerospace Corporation
Columbia, MD

Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300

Columbia, MD 21046

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the evaluation of SecureWave Sanctuary Application Control Custom Edition (SACCE) Version 2.8. It presents the evaluation results, their justifications, and the conformance results. This validation report 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.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL), and was completed during June 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by the CCTL. The evaluation determined the product to be **Common Criteria Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL2.**

Sanctuary Application Control Custom Edition (SACCE) is a three-tiered client/server application that provides the capability to control what users are able to execute on their client computers. The TOE centrally controls authorization of applications and executable files by maintaining a database of hashes of approved executables and associating the hashes with users or user groups. When a user logs on to a client that is protected by the TOE, the TOE client driver contacts the server and downloads the list of authorized hashes for the user. Whenever the user attempts to execute a file on the client, the TOE client driver intercepts the execution request at the operating system level, calculates the hash value of the file and searches for a match in the list of authorized hashes. If a match is found, execution of the file proceeds; otherwise, execution is blocked.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the evaluation technical report (ETR) and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST) for an EAL2 evaluation. Therefore, the validation team concludes that the CCTL findings are accurate, and the conclusions justified.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

2. IDENTIFICATION

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing

Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Sanctuary Application Control Custom Edition Version 2.8
Protection Profile	n/a
Security Target	*SecureWave Sanctuary Application Control Custom Edition Security Target* Version 1.0, 12 July 2006
Evaluation Technical Report	*Evaluation Technical Report for SecureWave Sanctuary Application Control Custom Edition version 2.8.* Version 1.0, 12 July 2006
Conformance Result	CC V2.1, Part 2 conformant, Part 3 conformant, EAL 2
Sponsor	SecureWave
Developer	SecureWave
Evaluators	Science Applications International Corporation
Validators	The Aerospace Corporation

3. SECURITY POLICY

3.1. Audit Function

The TOE records the actions that occur at the administrator and the client driver components. Administrative actions performed by the SecureWave Management Console (SMC) are audited by the TOE. The Sanctuary Application Control Client Driver (SXD) logs the allowed or denied program executions of the client on the client computer. These logs are stored and protected by the operating environment of the client computer.

3.2. Cryptographic Function

The TOE utilizes a public-private key to sign the listings retrieved from the Database and sent to the client computers.

The TOE utilizes the SHA-1 Hash to create the digital signatures that are assigned to each executable file and that are created from the contents of the file. On the client computers, SHA-1 Hash is utilized to create digital signatures from the files the user attempts to execute. The resulting signatures are used for comparison against the authorized file signatures.

3.3. User Data Protection

Sanctuary™ Application Control provides two methods for granting access to authorized executable files. One is based on matching the SXD-generated file signature to the authorized file signature assigned to an executable file. The files are associated to file groups and users are assigned to file groups.

The second method is the use of Path Rules that grant access to executable files and/or file directories based on a set of rules.

3.4. Security Management

The TOE provides the tool sets that are utilized by the administrator to manage and configure the security and administrative functions. These functions include the management of the file groups, the ability to manage the audit and log records, and the management of the access to the executable files.

The tool set consists of the following:

- **SecureWave Management Console (SMC)** - The SMC provides the administrative interface to SecureWave Application Server. It is used to configure Sanctuary™ Application Control and carry out a range of day-to-day administrative tasks.

- **Authorization Wizard** - The Authorization Wizard can be used to identify the files that are present in the file directory, and to incorporate these files into the Database.

- **Key Pair Generator** - The Key Pair Generator is used to create an encryption key pair. The SXS uses an asymmetric encryption system to communicate with the SXD.

- **SXDomain command-line tool** - The SXDomain command-line tool provides an alternative method (other than using the SMC) for updating the Database with changes to the domains, users, groups and workstations within the network.

3.5. Protection of the TSF

The TOE implements security mechanisms to detect any tampering of the listing of file signatures and path rules that may have occurred during transmission of the listing from the SecureWave Application Server (SXS) to the client's computer and the enforcement of the access control policy.

3.6. Resource Utilization

The TOE ensures that the access control policy is always enforced even if the client computer loses communication with the SXS. The TOE stores the listing of the file signatures on the client computer, which is utilized to enforce the access control policy when a user attempts to access an executable file.

4. ASSUMPTIONS

4.1. Usage Assumptions

Although there are several assumptions stated in the Security Target[1], the primary conditions are that:

- The server and database TOE components are located within controlled facilities and are protected from unauthorized physical access;
- Communications paths between TOE components are protected from unauthorized access;
- The operating environment provides administrative identification and authentication;
- TOE is protected from unauthorized modification;
- The operating environment provides reliable system time.

4.2. Clarification of Scope

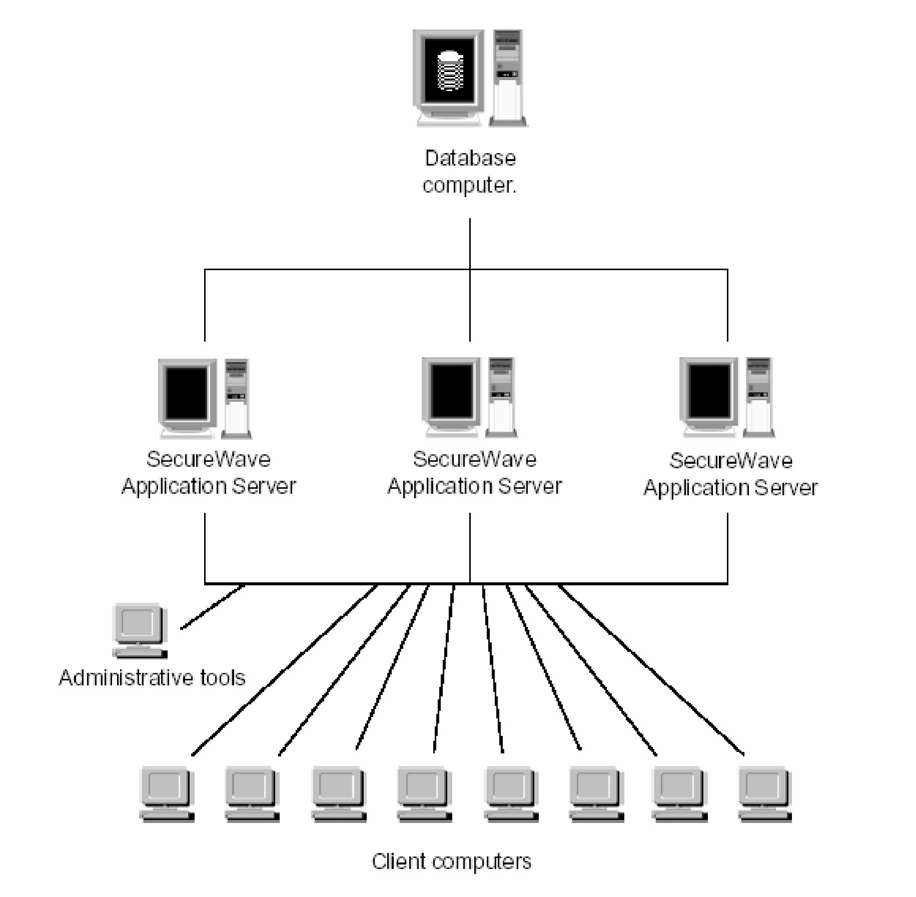
The TOE is an application running on top of, and kernel driver running inside of, multiple versions of the Microsoft Windows operating system. The TOE relies on the underlying operating system's security features, such as identification & authentication and file permissions, for secure operation. However, the operating system is outside the TOE boundary and as such was not part of this evaluation. Likewise, the database is outside the TOE boundary and was not included in the evaluation.

5. ARCHITECTURAL INFORMATION

Sanctuary™ Application Control is a three-tiered client/server application designed to allow or prevent execution of specific types of executable files depending on the executable contents. The tiers are: a backend database (SQL Server); application server(s); and a client front end. The client front end comprises the administrative client, which is software used to control and direct the operation of the system, and the client drivers, which reside on the computers that the Sanctuary™ Application Control protects. The administrative client software resides in a main program and some smaller utility programs; the client drivers consist of one kernel driver each for NT 4.0, Windows 2000 and XP. The fundamental rule used within the product is to allow only the use and/or execution of known and authorized executables and deny all else. In other words, the TOE does not

[1] See Section 3.2 of the ST.

use a “black list” of what is to be prevented. It only uses a “white list” of what is allowed; everything else is denied by default. The product also authenticates, at every attempt to launch and/or use, that the “allowed” is valid.



The Sanctuary™ Application Control uses a ‘white list’ of executable files that are allowed to run. The Sanctuary™ Application Control also lets a system administrator decide which applications are allowed to run on the client computer systems. A SHA-1 hash of each authorized application and executable is recorded in a database from which a positive list is then derived. Every time a user decides to run an application, a local agent (kernel driver) will compare the application with the positive list. The positive list can be defined either in terms of a specific user or group of users. The Sanctuary™ Application Control calculates a unique hash signature (based on SHA-1) for every binary executable file of the authorized applications. The Sanctuary™ Application Control eliminates a wide range of threats and management problems including Trojan horses, viruses, games, suspicious downloads, and unlicensed software regardless of the source.

To achieve the desired protection, the server component of the TOE maintains a list of known and allowed executables, together with information on which user or user-group is allowed to run which executables. Also present in the database is information on the users and computers to be protected, as well as ancillary items.

Sanctuary™ Application Control is composed of four components which are described as follows:

- **Sanctuary™ Database -** This is the main storage point for the authorization information and is managed through the SecureWave Management Console. The database is hosted by Microsoft SQL Server 7/2000, MSDE or MSDE2000 and the underlying operating system. The TOE relies on the environment to provide Microsoft SQL Server 7/2000, MSDE or MSDE 2000 database for its use.

- **SecureWave Application Server -** SecureWave Application Server (SXS) communicates with the client computers and obtains from the Database the lists of files that the clients are permitted to run. SXS runs as a Windows service under any domain user account.

- **Sanctuary™ Application Control Client Driver -** The Sanctuary™ Application Control Client Driver (SXD) ensures that only the executable files that the user has been authorized to use can run on the computer. Any attempt to run an unauthorized file is barred and logged. The logs can be viewed using the SecureWave Management Console. The SXD provides interfaces that allow a user to authorize or deny the execution of a file and receive notification that access to a file has been denied. The SXD is installed on each client computer that will be controlled by the TOE.

- **Administrative Tools -** The Administration tools are utilized by the administrators to perform various administrative functions. The tools are SecureWave Management Console (SMC), Authorization Wizard, Key Pair Generator, and SXDomain command-line tool.

6. DOCUMENTATION

The TOE is delivered with the following user documentation:

- SecureWave Sanctuary Application Control Custom Edition Administrator’s Guide, Version 2.8, January 2006;
- SecureWave Sanctuary Application Control Custom Edition Setup Guide, Version 2.8, January 2006.

7. IT PRODUCT TESTING

7.1. Sponsor Testing

SecureWave tests Sanctuary Application Control to uncover limitations and measure the full capabilities. The sponsor provided mappings of each test case to the relevant TSF interface (TSFI), interface specification (i.e., FSP), and high-level design description (i.e., HLD). The Evaluation Team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the Evaluation Team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.2. Evaluator Testing

As an integral component of testing, the evaluator installed and configured the TOE on a sample of the platforms supported in the evaluated configuration, and verified that the test configuration was consistent with the ST. The configuration used for evaluator testing is documented in the Evaluation Team Test Report supplement to the Final ETR.

Component	***Operating System***	***Additional Software***
Database Server	*Windows Server 2003 Enterprise Edition, SP1*	*SQL Server 2000, V.8.00.761*
SXS Server	*Windows Server 2003 Enterprise Edition, SP1*	*Microsoft Data Access Components (MDAC), v2.7*
Admin Console (SMC)	*Windows Server 2003 Enterprise Edition, SP1*	
SXD Client	*Windows XP Professional, Version 2002, SP2*	

The Evaluation Team exercised a substantial subset of the vendor test suite for Windows Server 2003 and Windows XP clients, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The sponsor's test suite was judged to be quite complete and comprehensive, and thus the evaluator needed to design relatively few additional tests. However, additional and variant test cases were developed and executed to broaden test coverage of Security Audit, User Data Protection, Security Management, and Protection of the TSF.

8. EVALUATED CONFIGURATION[2]

The evaluated configuration is as follows:

	Application Server	***Database***	***Admin Tools***	***Client***

[2] For more complete information on the evaluated configurations, see Section 3.2.3 of the Security Target.

Operating System	*Windows NT4 SP5 Server or Workstation, Windows 2000 Server or Professional, Windows Server 2003.*	*Windows NT4 SP5 Server or Workstation, Windows 2000 Server or Professional, Windows XP, Windows Server 2003.*	*Windows NT4 SP6a Server or Workstation, Windows 2000 Server or Professional, Windows XP, Windows Server 2003.*	*Windows NT4 SP4 Server or Workstation, Windows 2000 Server or Professional, Windows XP, Windows Server 2003.*
Hard disk space	*Program files: 1Mb* *Free disk space needed to install: 10Mb.*	*Program files: 5MB* *Free disk space needed to install: 40 MB* *Disk space for data: 20Mb+ (Depends on number of users)*	*Program files: 10Mb.* *Free disk space needed to install: 10Mb.*	*Program files: 5Mb* *Free disk space needed to install: 10Mb.* *Disk space for data: approx 10Mb*
Memory	*128Mb (256Mb recommended)*	*128Mb (256Mb recommended)*	*128Mb (256Mb recommended)*	*128Mb (256Mb recommended)*
Deployment	*Running setup.exe will install MSI 2.0 if not yet present. Using the MSI setup directly requires MSI 2.0 installed.*			*Using the MSI setup requires MSI 1.1.*
Display Resolution	*N/A*	*N/A*	*1024x768*	*N/A*
File System	*NTFS*	*NTFS*	*NTFS*	*NTFS*
Other	*MDAC V2.6 SP1* *IE 4.01 SP2 or later.* *Setup will install MSI2.0 if not yet present.*	*Microsoft SQL Server (version 7.0 or above) or MSDE2000 (requires IE 5.0 or later* *MDAC V2.6 SP1 Setup will install MSI2.0 if not yet present.*	*Internet Explorer 5.0 or later* *Setup will install MSI2.0 if not yet present.*	*Using the MSI setup requires MSI 1.1, IE 4.01 SP2 or later.*

9. RESULTS OF THE EVALUATION[3]

The evaluation team determined the product to be **CC Part 2 conformant, CC Part 3 conformant,** and to meet the requirements of **EAL 2**. In short, the product satisfies the security technical requirements specified in *SecureWave Sanctuary Application Control Custom Edition Security Target* Version 1.0, 12 July 2006.

10. VALIDATOR COMMENTS

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

11. SECURITY TARGET

The ST, *SecureWave Sanctuary Application Control Custom Edition Security Target* Version 1.0, 12 July 2006 is included here by reference.

[3] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

12. LIST OF ACRYONYMS

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] SecureWave Sanctuary Application Control Custom Edition Security Target Version 1.0, 12 July 2006.

[8] Evaluation Technical Report for SecureWave Sanctuary Application Control Custom Edition version 2.8. Version 1.0, 12 July 2006.

[9] Evaluator Team Test Plan for SecureWave Sanctuary 2.8 Version 0.1, April 10 2006 (SecureWave and SAIC Proprietary).