National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

SecureWave
Sanctuary Device Control
Version 3.2

Report Number: CCEVS-VR-06-0057

Dated: 16 March 2007

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 Device Control (SDC) Version 3.2. 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 October 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 Device Control is a three-tiered client/server application that provides the capability to control what devices users are able to access on their client computers. The TOE centrally controls authorization of I/O devices by maintaining a database of device permissions for computers, computer groups, users and 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 permissions for the user. Whenever the user attempts to access a protected I/O device on the client, the TOE client driver intercepts the operating system request and determines if the user has been granted the requested access to the requested I/O device. If permission is granted, the I/O request proceeds; otherwise, it 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 Device Control Version 3.2
Protection Profile	n/a
Security Target	*SecureWave Sanctuary Device Control Security Target* Version 1.0, 15 March 2007
Evaluation Technical Report	*Evaluation Technical Report for SecureWave Sanctuary Device Control version 3.2.* Version 1.0, 15 March 2007
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. Security Audit

Sanctuary Device Control v3.2 audits the actions that occur at the SecureWave Application Servers and the Sanctuary Device Control v3.2 Client workstation. All administrative actions performed on the Sanctuary Device Console are audited and stored by the TOE. The Sanctuary Device Control v3.2 Client logs the actions of the client on the client workstation. These logs are stored and protected by the operating system of the client computer.

3.2. Cryptographic Support

The TOE implements cryptographic functionality to protect communication between its client and server components. The TOE also implements cryptographic functionality to protect removable media.

3.3. Identification and Authentication

The Database stores the user identity, user groups, and I/O Device access control list (ACL).

3.4. User Data Protection

The Sanctuary Device Control v3.2 stores the user identity, user groups, and I/O Device access control list (ACL), and the associated access rights. When a user logs onto a client computer, the access control list of the permissions and I/O Devices are transmitted, first to SecureWave Application Server, and then the Sanctuary Device Control v3.2 Client workstation. When a user attempts to access an I/O Device, the access permission will be verified to determine if access is allowed as well as the access right that was granted.

3.5. Security Management

The Sanctuary Device Console provides the administrator with graphical user interfaces that can be used to configure and modify the options of the TOE. There are several modules available to the authorized administrator, such as the Device Explorer, which is used to grant access rights to I/O Devices for specific user and user groups and the audit viewers that are used to view the audit records of administrative activities.

3.6. Protection of the TSF

Sanctuary Device Control v3.2 controls access to devices by applying an Access Control List (ACL) to each device type. Based on the Least Privilege Principle, device access for all users is not allowed by default. Therefore, to grant access, the administrator only needs to associate those users or user groups to the devices to which they should have access.

3.7. Resource Utilization

When the Sanctuary Device Control v3.2 Client workstation cannot communicate with the SecureWave Application Server, it will be operated in a standalone mode, utilizing the copy of the access control listing that was placed in a secure area on the hard disk of the workstation. The Sanctuary Device Control v3.2 Client workstation will utilize this listing until a new logon is performed.

4. ASSUMPTIONS

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

- Any network resources used for communication between TOE components will be adequately protected from unauthorized access;
- The database and server components must be located within controlled access facilities that will be protected from unauthorized physical access and modification;
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains;
- The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance.

5. ARCHITECTURAL INFORMATION

Sanctuary Device Control v3.2 is a three-tiered client/server system designed to allow system administrators to implement strict security policies by controlling end-user access to I/O Devices. The three tiers are: A backend database (SQL Server); a middle tier of SecureWave Application Servers; and a client tier. The clients fall into administrative clients, software used to control and direct the operation of the system, and client drivers, residing on the computers that Sanctuary Device Control v3.2 protects. The administrative client software resides in a main program Management Console (Administrative Tools) and some smaller utility programs; the client drivers for Sanctuary Device Control v3.2 Client, consist of one driver each for Microsoft Windows NT 4.0, Microsoft Windows 2000, and Microsoft Windows XP.

A Sanctuary Device Control v3.2 solution includes four components. These are the Database, SecureWave Application Server, Sanctuary Device Control v3.2 Client Driver, and the Administrative Tools. These components are described below:

- **Database:** This is the main storage point for the information. Each Sanctuary Device Control v3.2 site must have at least one database. This is the master storage point for the user policies and permissions. The database is hosted by Microsoft SQL Server 7/2000, MSDE or MSDE 2000 and the underlying operating system. The Sanctuary Device Control v3.2 relies on the environment to provide Microsoft SQL Server 7/2000, MSDE or MSDE 2000 database for its use.

- **SecureWave Application Server:** Each Sanctuary Device Control v3.2 installation can also have one or more SecureWave Application Servers. The purpose of SecureWave Application Server is to communicate with the Sanctuary Device Control v3.2 Client computers and obtain from the Database, the lists of devices and permissions.

[1] See Section 3.2 of the ST.

- **Sanctuary Device Control v3.2 Client Driver**: The purpose of the Sanctuary Device Control v3.2 Client is to enforce the policies and permissions for each user. The client is installed on each computer that is to be included in the Sanctuary Device Control v3.2 solution. Each Sanctuary Device Control client system contains a client component that runs as a kernel driver (sk.sys (SK)). The SK driver enforces the policy management (and permissions) for each user, provides device shadowing capability that tracks the data written to any Sanctuary Device Control protected device, and enforces a device white list that blocks access to unknown (i.e., not managed by the SK driver) devices. When the client is first installed, the SK places a default ACL (access control list) on all of the devices (block all devices by default, as SDC applies the "least privilege principle" which requires deny access to any device that is not expressly permitted). Following placement of the default ACL, it hooks each of the device entry points to their respective drivers. When a user logs on to the client, the SK sends a message to the SecureWave Application Server to retrieve the list of the permissions for known devices for the user. The Sanctuary Client, installed on the client machines, ensures that only those I/O devices that the user has been authorized to use can be accessed on the client computer. Any attempt to access an unauthorized device is denied, regardless of the computer from which a user attempts access. The setup also installs an application (RTNotify) that provides to the end user information about the status of each device (denied, changed/updated and permitted).

- **Administrative Tools**

  - **Sanctuary Device Console (a.k.a. Management Console)**: The Sanctuary Device Console is used to configure Sanctuary Device Control v3.2 and to perform day-to-day administrative functions. If required, the Sanctuary Device Console may be installed on several computers.

  - **Key Pair Generator** - The Key Pair Generator is used to create an encryption key pair. The SecureWave Application Server uses an asymmetric encryption system to communicate with the Sanctuary Device Control v3.2 Client Driver.

  - **SXDomain command-line tool** - The SXDomain command-line tool is used to inform the Database of changes to the users, user groups, and client workstations within the network.

6. DOCUMENTATION

The TOE is delivered with the following user documentation:

- SecureWave Sanctuary Device Control Administrator’s Guide, Version 3.2.0, May 2006;
- SecureWave Sanctuary Device Control Setup Guide, Version 3.2.0, April 2006.

7. IT PRODUCT TESTING

7.1. Sponsor Testing

SecureWave tests Sanctuary Device 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.

Purpose	***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*	
SDC 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, Security Management, and Protection of the TSF.

8. EVALUATED CONFIGURATION[2]

The evaluated configuration is as follows:

	Application Server	***Database***	***Admin Tools***	***Client***
Operating System	*Windows 2000 (Service Pack 4 or later) Server or Windows Server 2003.*	*Windows 2000 (Service Pack 3 or later) Server or Professional, Windows XP Professional, Windows Server 2003.*	*Windows 2000 (Service Pack 3 or later) Server or Professional, Windows XP Professional, Windows Server 2003.*	*Windows 2000 (Service Pack 3 or later) Server or Professional (not for Sanctuary Server Edition), Windows XP Professional (not for Sanctuary Server Edition), Windows Server 2003.*
Hard disk space	*5 Mb free disk space for program files and 15 Mb for the installation.*	*5 Mb free disk space for program files, 40 Mb for the installation, and 20Mb+ for data (depends on number of users)*	*10 Mb free disk space for program files and 15 Mb for the installation.*	*2 Mb free disk space for program files and 15 Mb for the installation.*
Memory	*128Mb (256Mb recommended)*	*128Mb (256Mb recommended)*	*128Mb (256Mb recommended)*	*128Mb (256Mb recommended)*
Display Resolution	*N/A*	*N/A*	*1024x768*	*N/A*
File System	*NTFS*	*NTFS*	*NTFS*	*NTFS*
Other	*MDAC V2.6 SP1*	*Microsoft SQL Server 2000/2005 or MSDE2000 (requires IE 5.0 or later) MDAC V2.6 SP1*	*Internet Explorer 5.0 or later. Adobe PDF Reader v5.0 or later to consult the on-line manuals.*	

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

Novell		*LDAP and NDAP (for workstation objects synchronization)*		*Novell – and optionally ZENworks - client*

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 Device Control Security Target* Version 1.0, 15 March 2007.

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 Device Control Security Target* Version 1.0, 15 March 2007 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
I/O	Input/Output
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 Device Control Security Target Version 1.0, 15 March 2007.

[8] Evaluation Technical Report for SecureWave Sanctuary Device Control version 3.2. Version 1.0, 15 March 2007.

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