National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

SupportSoft, Inc. Knowledge Center Suite Version 6.5 Service Pack 4

Report Number: CCEVS-VR-VID10099-2007
Dated: 21 December 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

James Dondelinger
Deborah Downs
Aerospace Corporation
Columbia, MD

Maureen Cheheyl
Victoria A. Ashby
The MITRE Corporation
McLean, VA

Common Criteria Testing Laboratory

DIAL
(DSD Information Assurance Laboratory)
White Hall, WV

Table of Contents

1.0 Executive Summary

The evaluation of SupportSoft, Inc. Knowledge Center Suite Version 6.5 was performed by DIAL (DSD Information Assurance Laboratory) in the United States and was completed on xx November 2007. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.2, January 2004 and the Common Methodology for IT Security Evaluation (CEM), Version 2.2, January 2004.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.2) for conformance to the Common Criteria for IT Security Evaluation (Version 2.2). The TOE is a web-based application that allows organizations to create, approve, and publish all types of content and make that content available to a large set of end-users and Support Analysts. The TOE is intended to be used as a knowledge base and end-user technical support solution.

The SupportSoft Platform and SupportSoft Knowledge Center (KC) are both included in the SupportSoft Intelligent Assistance Suite. The Intelligent Assistance Suite allows users to develop, share, research, and resolve end-user technical support issues throughout an organization. It enables Administrators and Analysts to support technical issues surrounding end-point management. The TOE includes a management capability that allows authorized administrators to configure and maintain the web server, application interfaces, components and product features. These features include creating users and groups, setting permissions for applications and tools, configuring content filtering, and creating, editing and publishing content reports.

The TOE provides Web interfaces via virtual directories to administrator systems (Support Administrator), analyst systems (Support Center), knowledge author systems (Author Center), and end user systems (User Center).

- **Support Administrator (SA):** A virtual directory, browser-based application utilized by administrators to configure and maintain the web server, application interfaces, components and product features. The Support Administrator can create SupportSoft users and groups, set Platform permissions for SupportSoft applications and tools, configure content filtering, and create, edit and publish content reports.

- **Support Center (SC):** Support Center is provided as both a Win32-based container application and as a virtual directory browser-based application. Support Center is used by Support Analysts to search and browse content in order to provide solutions for end users. Support Analysts can also use this application to contribute content ideas. Support Center container application is a 32-bit container used in place of a browser to provide the tabbed interface for tools. The Win32 Support Center container application utilizes the SSL handling in Internet Explorer to perform all communication with the TOE.

- **Author Center (AC):** A browser-based application used to author content when Knowledge Center is installed. The virtual directory associated to Author Center provides the interface for a knowledge author to create and manage content as well as view audit trail information on any selected content item the author developed. Both simple and complex content is managed in the same interface and organized in a hierarchical taxonomy.

- **User Center (UC):** A browser-based application used by end-users to obtain self-service. The associated virtual directory provides an online interface for the user subscriber to search for frequently asked questions (FAQs), automated solutions, tutorials and other self-service tools.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) (proprietary) produced by DIAL.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the SupportSoft Knowledge Center Suite product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The DIAL evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2) have been met.

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.2, January 2004. The evaluation started in June 2005, and all international and NIAP interpretations issues between January 2004 and June 2005 have been considered and applied when applicable.

2.0 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 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
TOE:	SupportSoft, Inc. Knowledge Center Suite Version 6.5 Service Pack 4
Protection Profile	Not applicable.
ST:	*SupportSoft, Inc. Knowledge Center Suite Version 6.5 Security Target*, Version 1.0, 11 January 2008
Evaluation Technical Report	*Evaluation Technical Report for SupportSoft Knowledge Center Suite Version 6.5*, Version 1.3, 17 October 2007
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2, Version 256, January 2004
Conformance	CC Part 2 Extended and Part 3 conformant

Item	Identifier
Result	
Sponsor	SupportSoft, Inc
Developer	SupportSoft, Inc
Common Criteria Testing Lab (CCTL)	DIAL (DSD Information Assurance Laboratory), White Hall, WV
CCEVS Validators	James Donndelinger, Aerospace Corporation Deborah Downs, Aerospace Corporation Maureen Cheheyl, The MITRE Corporation Vicky Ashby, The MITRE Corporation

3.0 Security Policy

The security services provided by the TOE are summarized below:

3.1 Access Control

Access controls are enforced at the interface level. Content is accessible via the UC and SC interfaces only after it is published. KC access levels are enforced when the Author Center interface is used. The KC access levels do not apply to the other TOE security function interfaces. The TOE develops the logic required to enforce the access levels and sends that logic in the retrieval request to the DB. Using the logic provided by the TOE, the DB retrieves only the requested content items to which the requesting user has access. The TSF shall create and send queries to the DB in the IT environment in order to retrieve data to which the user has access.

For each folder, KC assigns access levels to groups. Different access levels can be assigned to a folder for each content item type. Access levels are a defined set of KC permissions. KC is responsible for maintaining all access levels and KC permissions.
Access levels can also be assigned to the Contribution Content Type. Access to Contribution content items is controlled by the access levels assigned to the contribution content type.

3.2 Audit

The TOE provides two different types of auditing. One is the ability to audit the following login events: successful logins, user resets, and failed login attempts due to supplying an incorrect password. (A user reset is performed when an administrator enables a disabled account.) The other is the ability to audit every state change to a content item. The possible states for all content types are Under Construction, Pending Approval, Published, Approved, Rejected, Expired, Delisted, or Superseded.

The generation of login audit records is provided by Platform. The generation of content item state change audit records is provided by KC. All audit events are time stamped by the database as they are stored in the DB. Therefore, the TOE relies on the IT environment (DB, OS, and hardware) to provide a reliable timestamp.

To view login audit records, the Administrator can run a report. This functionality is provided by Platform. Generated reports are stored in the DB and can be deleted by the users with the appropriate permission or role.

To view content item records, the Administrator, Author, Approver, and users with the appropriate permission can view the audit trail page for the content item. This functionality is provided by KC.

3.3 Identification and Authentication

Users log into the TOE via one of the TOE interfaces. The SupportSoft Platform requires that all users except anonymous users provide a user ID and password in order to access the TOE. In the evaluated configuration, anonymous users only have access to perform the functions available from the KC Home page, which allows searching and subsequent viewing of content items, but does not allow browsing the database for content items.

The user account information is stored in the database in the IT environment. The SupportSoft Platform makes the identification and authentication decisions based on the information input by the user and the information received from the database.

3.4 Security Management

Platform provides the ability to perform general management functions, such as:

- Create users and groups
- Configure and assign roles (defined by a set of Platform permissions)
- Create and review reports
- Configure the password policy

KC provides the ability to perform functions specific to content management, such as:

- Create and configure workflows and content types
- Configure access controls to content items by assigning access levels to folders and the Contribution content type

The TOE implements roles by assigning Platform permissions to groups in order to determine access to specific components. Platform permissions are assigned to groups using SupportSoft Platform. Platform is also responsible for enforcing roles.

3.5 Protection of TOE functions

Logical protection of the TOE is required to ensure the TOE security services are not bypassed or tampered with. The TOE and the operating system, which is in the IT environment, work together to protect the TOE.

4.0 Assumptions and Clarification of Scope

This section described the security aspects of the environment and configuration in which the product is expected to be used.

4.1 Usage Assumptions

In order to provide a baseline for the product during the evaluation effort certain assumptions about the usage of the IT product are often made. Items such as proper installation and configuration, minimum hardware requirements being satisfied, etc., all have to be assumed. This section documents any usage assumptions made about the IT product during the evaluation.

The following assumptions have been made about how the product will be used:

- The SupportSoft web server and database systems are dedicated to the TOE functions and do not provide any general purpose or non-TOE user data storage capabilities.
- The TOE is installed and configured so that it is consistent with the installation guidance.

The following product capabilities that are included in the product, but which are outside of the evaluated configuration:

- **Knowledge Center SDK**

The Knowledge Center SDK is outside the scope of the evaluation. This component was not tested in the evaluation and no claims are made about it in the Security Target, but it can be used in conjunction with the TOE.

- **AnalystAssist**

The Analyst Assist products (LiveAssist, AnalystAssist, RemoteAssist, and VoiceAssist) are outside the scope of the evaluation. These products will not be tested in the evaluation and there are no claims made about them, but they can be used in conjunction with the TOE.

- **External Authentication**

The SupportSoft Platform can be configured to use external authentication methods to replace the default SupportSoft user login authentication. SupportSoft Platform supports Windows NT authentication, LDAP authentication, or any other third party or custom type of user authentication. The use of external authentication to the TOE is not allowed in the evaluated configuration.

- **Caching**

Caching on the SupportSoft web server and database are not allowed in the evaluated configuration due to the fact that the use of caching may delay the effects of administrative changes to security parameters.

- **SmartResults Filters by Audience**

SmartResults filters are dynamically applied to folders and/or content items when a user searches or browses for content in UC or SC (this is also called personalization). The filters are used to determine whether data is made available to the user based on criteria of the user and the user's system. Filters can be created based on active browser, active browser language, group membership (audience), browser, HTTP request method, HTTP server port, mail client, operating system, remote host/IP address, content requirements, and tenancy qualification. The group membership criteria are based on Windows domain group membership, not SupportSoft group membership. All filters, except filters based on group membership, are enforced by the TOE itself. The group membership (audience) criteria of the filters are performed by the TOE creating and sending the logic to the DB and then the DB enforcing it. SmartResults filtering is not considered security-relevant. However, the group membership (audience) filtering requires external authentication which is excluded from the TSF, therefore it cannot be used in the evaluated configuration.

4.2 Environmental Assumptions

The following assumptions about the environment in which the product operates have been made:

- The network connecting the SupportSoft web servers to the DB(s) is a private, separate physical network that is not globally routable and that is protected from attacks and from unauthorized physical access.
- The processing resources of the SupportSoft web servers and database servers are located within controlled access facilities, which provide physical security commensurate with the value of the TOE and the data it contains.

4.3 Clarification of Scope

The product does not counter the following threats:

- Authorized users may not be accountable for their actions within the TOE because their actions were not audited (thus if the user violates the access controls, then the user can escape detection) or because the audit trail was not reviewed.
- A user or process may gain unauthorized access to the audit trails and cause records to be lost or modified.
- A user or process may gain unauthorized access to content items and delete or modify the content items.
- A user or process may bypass TOE security to gain access to TOE security functions and data.
- A user or process may masquerade as another entity in order to gain access to TOE security functions and data.
- A user or process may cause through an unsophisticated attack, TSF data to be inappropriately accessed (viewed, modified, or deleted). This includes TSF data transmitted between the TOE and the IT environment.

- Audit data may be lost if the database administrator does not preserve it. The product cannot protect the audit data, but depends on the database to do that.

5.0 Architectural Information

The TOE allows organizations to create, approve, and publish all types of content and make that content available to a large set of end-users and Support Analysts. The TOE is intended to be used as a knowledge base and end-user technical support solution. From a Common Criteria Evaluation and Validation Scheme (CCEVS) standpoint, this TOE falls under the "Miscellaneous" category.

The SupportSoft Platform and SupportSoft Knowledge Center (KC) are both included in the SupportSoft Intelligent Assistance Suite. The Intelligent Assistance Suite allows users to develop, share, research, and resolve end-user technical support issues throughout an organization. It enables Administrators and Analysts to support technical issues surrounding endpoint management. The Intelligent Assistance Suite includes the AnalystAssist application(s) which is a web based support automation system providing issue resolution and remote end user assistance. The TOE includes only the Platform and KC components. The other components of the Intelligent Assistance Suite are not in the scope of the TOE. (See section 4.1 below for more information about what is excluded.)

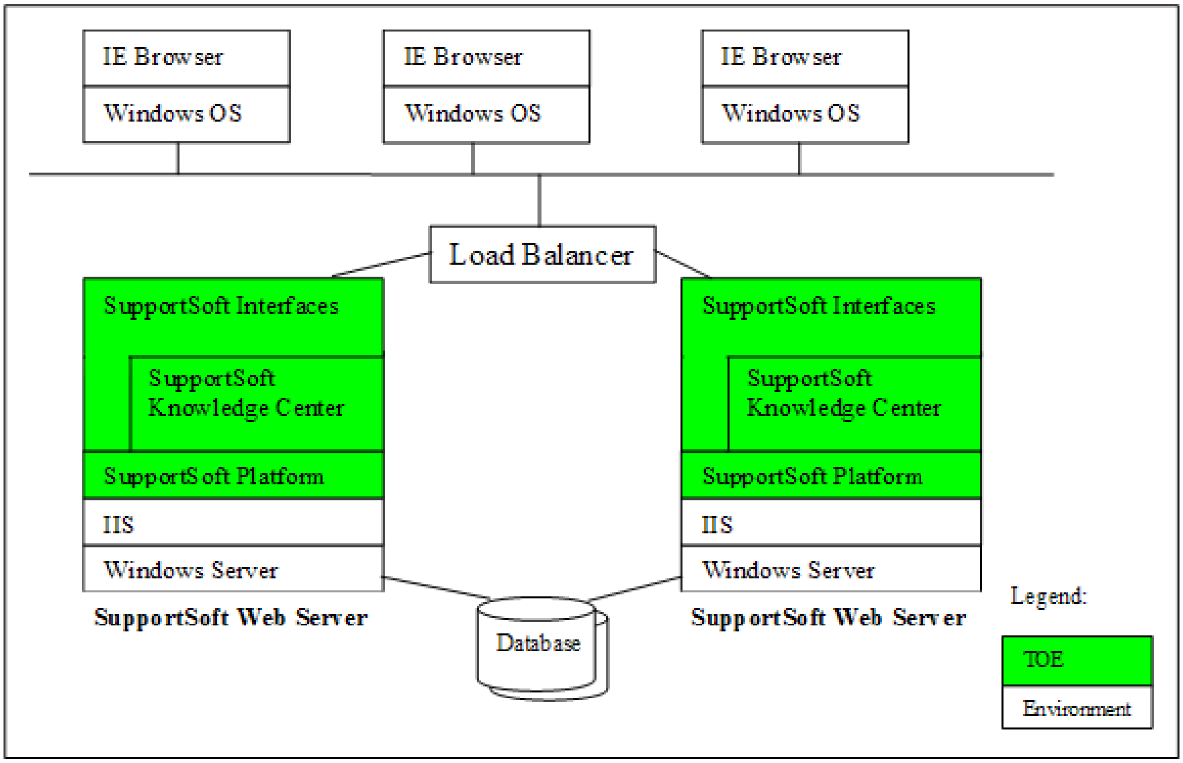

Figure 1: The TOE in a Sample Environment

The TOE (Platform and KC) is installed on a SupportSoft web server. The TOE includes multiple web-based interfaces available to users to interact with the TOE. These interfaces rely on Microsoft Internet Information Server (IIS) to provide the HTTPS protocol and to process the requests to and from the TOE. (The product also supports using the HTTP protocol, but that is not included in the evaluated configuration.) Users can interact with the TOE from any system using one of the approved web browsers. The browser is used to display information from the TSF for the user and to input information from the user for the TSF. The browser does not perform any security relevant functionality needed to implement the TSF. All human interactions with the TOE are performed via the browser or the Support Center Win32 client.

The TOE depends upon the underlying Microsoft Windows 2000 Server operating system (OS) and IIS to provide basic functionality, including secure communications (HTTPS). For small scale deployments, it is possible to deploy in a single system configuration (one SupportSoft web server). For medium to large scale deployments, a multiple system configuration is needed (two or more SupportSoft web servers). For multiple system configurations, a load balancer (in the IT environment) is required.

The TOE depends upon a database (in the IT environment) to store and retrieve the content items and TOE system data, including user account information. The database (DB) can be installed on a single machine or in a database cluster. The TOE depends upon the DB to require identification and authentication prior to granting access to the DB. The TOE logs into the DB under an administrative account created for the TOE to perform its operations. In order to protect the content items and TOE system data, the TOE depends upon the database requiring identification and authentication prior to allowing users to indirectly access the database via the TOE. Only the TOE and TOE administrative users are allowed to have user accounts on the database.

The TOE provides web interfaces via virtual directories to administrator systems (Support Administrator), analyst systems (Support Center), knowledge author systems (Author Center), and end user systems (User Center). The following gives more detail about each of these web interfaces:

- **Support Administrator (SA):** A virtual directory, browser-based application utilized by administrators to configure and maintain the web server, application interfaces, components and product features. The Support Administrator can create SupportSoft users and groups, set Platform permissions for SupportSoft applications and tools, configure content filtering, and create, edit and publish content reports.
- **Support Center (SC):** Support Center is provided as both a Win32-based container application and as a virtual directory browser-based application. Support Center is used by Support Analysts to search and browse content in order to provide solutions for end users. Support Analysts can also use this application to contribute content ideas. Support Center container application is a 32-bit container used in place of a browser to provide the tabbed interface for tools. The Win32 Support Center container application utilizes the SSL handling in Internet Explorer to perform all communication with the TOE.

- **Author Center (AC):** A browser-based application used to author content when Knowledge Center is installed. The virtual directory associated to Author Center provides the interface for a knowledge author to create and manage content as well as view audit trail information on any selected content item the author developed. Both simple and complex content is managed in the same interface and organized in a hierarchical taxonomy.
- **User Center (UC):** A browser-based application used by end-users to obtain self-service. The associated virtual directory provides an online interface for the user subscriber to search for frequently asked questions (FAQs), automated solutions, tutorials and other self-service tools.

These web interfaces and SC Win32 can be used either locally or remotely. There is no console and no distinction between local and remote users.

6.0 Documentation

SupportSoft offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features. Following is the list of documentation that was evaluated and is provided to the end user.

Guidance Documentation

Document	Version	Date
SupportSoft Installation and Administration Supplemental CC Guidance	1.0	October 12, 2007
SupportSoft Platform Version 6.5 Service Pack 4 Administrator's Guide	--	October 20, 2005
SupportSoft Platform v6.5 SP4 and Product Installation Guide	(web page)	September 23, 2005
SupportSoft Platform Version 6.5 Service Pack 04 Release Notes	--	July 8, 2005
SupportSoft Content Administration Guide (Applies to All v6.5 SP1 or Higher products that include Content)	--	September 29, 2005
SupportSoft Knowledge Center Version 6.5 Service Pack 1 Release Notes	--	--
SupportSoft User Supplemental CC Guidance	1.0	October 12, 2007

Security Target

Document	Version	Date
SupportSoft, Inc. Knowledge Center Suite Version 6.5 Security Target	1.0	11 January 2008

7.0 IT Product Testing

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

7.1 Developer Testing

SupportSoft's approach to security testing for SupportSoft, Inc. Knowledge Center Suite Version 6.5 is interface based. Essentially, SupportSoft developed a set of test suites that correspond to a security function enforced by a particular subsystem interface. Each test suite targets the specific security behavior associated with that interface and security function. The developer tested interfaces for the audit mechanism, the access control policy and attributes, the SSL invocation and the administrative permissions and restrictions. The test procedures are designed to be run manually.

Depth analysis is based on an understanding of the high-level design and is intended to show that the TOE as presented in the high-level design has been adequately tested. The team analyzed each test suite, determined which SFRs were addressed by that test suite, and compared the analysis results to the ST description of that security function. Each SFR maps to one or more test suites, and the rationale for each test suite demonstrates why that test suite covers that particular SFR

Prior to independent testing, the evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected. The Evaluation Team added tests to the team test plan in cases where additional tests were indicated to ensure complete test coverage.

Before testing, the vendor provided a complete set of expected and actual test results for analysis. The evaluation team examined the vendor's actual test results for the TOE configuration. During this examination, and during preliminary run-throughs of the vendor tests, the evaluation team found two areas of concern which were addressed by the vendor. During analysis of the vendor test suite prior to actual testing, the vendor test suite, expanded by the team tests, was shown to adequately address all security functions claimed in the ST for the TOE.

7.2 Evaluation Team Independent Testing

The Evaluation Team installed the product in the evaluated configuration in its test lab. The tests were executed on a workstation connected to an isolated lab network and then to the evaluated configuration.

The evaluation team followed the download instructions as documented in the Delivery document to download and verify the TOE for testing. The TOE was installed as indicated in the *SupportSoft Installation and Administration Supplemental CC Guidance*, Version

1.0. A few issues with the installation documentation were noted during the set up and testing, and these have been corrected in the Version 1.0 document.

The evaluation team ran the vendor's entire test suite on the evaluated configuration during testing. All tests were manual and run from the keyboard of a workstation. All results were as expected.

In addition to rerunning the vendor's tests, the Evaluation Team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests. These independent team tests included confirmation of the following:

- No TSFI allows unauthorized access, even when the user knows the URL for the interface. The vendor tests were from the GUI interface; this independent team test repeated the vendor test suite using the URL instead of a button click.
- Passwords expire as claimed.
- The change password page does not allow an unauthorized user to change another user's password.
- Access to all components of the product is consistent and requires login.
- SQL injection and cross-site scripting is rejected from the login screen.
- The database server is not accessible to end users.
- Data passed between the database server and the product server is encrypted.

The evaluation team has determined the TOE behaves as expected and all test suites have been successfully executed on all identified platforms.

The following hardware and software is necessary to create the test configurations used during independent testing:

Operating System:	Microsoft Windows 2000 – SP4
2 CPU(s):	Intel Pentium 4 @ 2.80Ghz x1 (connected by a crossover cable)
Memory:	1,030,888KB RAM
HDD:	Hitachi 76.69GB HDD
C:	4.40GB Used of 20.40GB
D:	5.98MB Used of 26.90GB
E:	1.52GB Used of 29.26GB
Alternate Media Drives:	CDROM
	1.44 MB Floppy Drive
Network Adapters:	Intel 10/100 NIC
Sound Card:	SoundMAX Integrated Digital Audio
Video Card:	Intel 82865G
Monitor	None
Input Peripherals:	None
Software:	

MS SQL Server Version 8.00.760
Symantec Anti-Virus Corporate Version 8.1.0.825
Internet Explorer Version 6.0.2800.1106 (6.0 with SP1)

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of open-source vulnerability documentation and a set of test procedures proposed by the Evaluation Team to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used their test configuration to successfully perform its penetration tests. The open-source vulnerability search produced no vulnerabilities not already included in the vendor's vulnerability analysis. An Active X vulnerability for a previous version of the product was tested and shown to have been mitigated. An independent team test had already tested that communication between the database server and the product server was in fact encrypted and therefore protected from modification and disclosure.

The Evaluation Team's Test Plan and Test Results document (proprietary) provides a detailed description of the tests and the results. No effects were found on the information presented in the ST or other evaluation evidence.

8. Evaluated Configuration

The product must be configured according to the SupportSoft Installation and Administration Supplemental CC Guidance, Version 1.0. This guidance includes instructions on how to configure the IT environment, which includes two servers. The server supporting the product must run Microsoft Windows 2000 Server operating system (OS) and IIS. The database server runs an operating system to support the database management system chosen from either Microsoft SQL Sever 2000 Service Pack 3 or later, or Oracle 9.i or higher. The two servers are connected by a crossover cable. In addition, workstations to support client browsers are in assumed. The client browsers are part of the TOE. Allowed browsers are Internet Explorer 5.5 with XML parser update (Microsoft XML 3.0 Service Pack), or Internet Explorer 6.0 or higher.

8.1 Product Configuration

Configuration settings are chosen during the installation process using a GUI. The installation process includes the application of a bug fix to repair a problem found during the evaluation. This bug fix requires copying a file and complete instructions are provided in the installation guide referenced above.

8.2 Ports/Protocols/Services

N/A

9. Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.2 and the Common Evaluation Methodology (CEM) Version 2.2 and all applicable National and International Interpretations in effect since the evaluation start on June 10, 2005.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. Verdicts were not assigned to assurance classes.

Section 2, Conclusions, in the Evaluation Team's Evaluation Technical Report, examines each work unit and gives a verdict of Pass for that work unit, along with a summary of rationale for the verdict and the issues resolved to achieve that Pass verdict.

The SupportSoft, Inc. Knowledge Center Suite Version 6.5 product in the evaluated configuration satisfies the SupportSoft, Inc. Knowledge Center Suite Version 6.5 Security Target, Version 1.0, dated 11 January 2008.

The validation team followed the procedures outlined in the *Common Criteria Evaluation and Validation Scheme (CCEVS) Publication # 3* for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor test suites, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10. Validator Comments/Recommendations

The product retrieves data from the database by formatting SQL queries and sending them to the database. The database executed the query and returns the data requested, which is then displayed to the user by the product. The product looks to the database like one user with access to all of the data in the database. The access control decision is made by the product when it formulates the query. This can be done in one of two ways: the product can ask for the stored permission for the user, and then use those stored permissions to formulate the query for data, or the product can formulate a complex query for both the stored permissions and the data. In either case, the product is making the access control decision.

Access control is implemented by access control lists (ACLs) but the location of the ACL differs depending on the storage location for the object type. The content types that matter for the ACL location are contribution and non-contribution, not the list of "content" types provided on the selection list by the product. It is important to keep the concepts of content item and contribution/non-contribution separate. Contributions are comments on documents (like a suggestion for a suggestion box). Non-contributions are resources, FAQs, URLs, documents, etc.

- Non-contributions (documents and other resources) are stored in folders and are controlled for access by the folder ACL. Each folder can have multiple ACLs, one per each resource type (that is, one per each of item listed on the selection list provided by the product).
- Non-contribution content at the root level (that is, not in a folder) is publicly available.
- Contributions have ACLs based on group permissions only, and do not use the folder ACL because they are not stored in folders.
- Reports created by the product using the Report feature are treated like contributions.

Independent team testing showed that reports are created at the root level with an ACL. This testing also showed that the default parameter for group membership forces "inheritance" of the new parameter created to control access to the new report. That is, when a new report is created, a new permission is created to allow access to it. This new permission is given to each group of which the creating user is a member when the new report is created, as long as the default parameter is checked. If the default parameter is not checked, then the permission is not added to the permissions for the group.

Timestamps are provided by both the product and the database for different purposes. Audit records are timestamped with the database's timestamp. Counters such as the session timeout counter use a timestamp obtained from the IT environment.

The product provides auditing, but the audit trail is kept in the database. The database is in the environment, and was not examined during the evaluation. The database administrator is responsible for preserving the audit trail. This includes checking for audit trail overflow, cycling the audit trail storage space, and notifying the product administrator when there is an audit trail problem.

The audit record for a user session contains a timestamp from the last successful login and last failed login. The product will not know the history of logins for a user, but the audit trail contains this information. In addition to the audit of logins and logouts, the audit trail also contains the audit of access control decisions for content items.

11. Annexes

Not applicable.

12. Security Target

The Security Target is identified as *SupportSoft, Inc. Knowledge Center Suite 6.5 Security Target Version 1.0, January 11, 2008.* The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

13. Glossary

The following definitions are used throughout this document:

Hardware: the physical equipment used to process programs.

Software: the programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

14. Bibliography

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

- *Common Criteria for Information Technology Security Evaluation* Part 1: Introduction and general model, Version 2.2, Revision 256, January 2004
- *Common Criteria for Information Technology Security Evaluation* Part 2: Security Functional Requirements, Version 2. 2, Revision 256, January 2004
- *Common Criteria for Information Technology Security Evaluation* Part 3: Security Assurance Requirements, Version 2. 2, Revision 256, January 2004
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.2, January 2004
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- SupportSoft, Inc. Knowledge Center Suite 6.5 Security Target Version 1.0, January 11, 2008
- Evaluation Technical Report for SupportSoft, Inc. Knowledge Center Suite 6.5, Version 1.3, October 17, 2007
- SupportSoft Installation and Administration Supplemental CC Guidance, Version 1.0, October 12, 2007