SupportSoft, Inc.
Knowledge Center Suite Version 6.5
Security Target

Release Date:	January 11, 2008
Version:	1.0

Prepared By:	Saffire Systems P.O. Box 11154 Champaign, IL 61826
Prepared For:	SupportSoft, Inc. 575 Broadway Redwood City, CA 94063

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the Knowledge Center Suite Version 6.5.

1.1 Identification

TOE Identification:	SupportSoft Platform Version 6.5 SP4 and SupportSoft Knowledge Center Suite Version 6.5 SP1
ST Identification:	SupportSoft, Inc. Knowledge Center Suite Version 6.5 Security Target.
ST Version:	1.0
ST Publish Date:	January 11, 2008
ST Authors[1]:	Michelle Ruppel, Saffire Systems
	Ward Rosenberry
PP Identification:	None.

1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.2[2] Part 2 extended.

The TOE is Common Criteria (CC) Version 2.2 Part 3 conformant at EAL2.

The TOE is also compliant with all International interpretations with effective dates on or before June 10, 2005.

The TOE is compliant with selected NIAP Interpretations. The selected NIAP Interpretations are identified as they are applied to the security requirements in Section 5.

This TOE is not conformant to any Protection Profiles (PPs).

1.3 Overview

The Knowledge Center (KC) application 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. KC provides support content creation, delivery, and management services. KC integrates with existing call tracking systems (CTS) to help resolve service desk incidents more efficiently through readily available knowledge based solutions. KC automatically correlates real-time diagnostic data with the problem description to suggest likely solutions from a rich content repository. KC is intended to be utilized as a knowledge base and end-user technical support solution.

KC is installed atop SupportSoft's Platform (Platform) application. Platform is the "backbone"

[1] Previous ST author was William Godwin DSD Laboratories, Security Systems Division

[2] Common Criteria (CC) for Information Technology Security Evaluation – January 2004, Version 2.2.

and "foundation" all SupportSoft products are built upon. Platform provides Administrators with management tools to administer the operating environment of KC. The Platform can automatically link computing endpoints, network devices, end-users, and service professionals in-context -- and in real-time.

KC is part of the Intelligent Assistance Suite. The Intelligent Assistance Suite also includes AnalystAssist. However, the scope of this evaluation is limited to the Knowledge Center along with the underlying Platform application.

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides.
7	PP Claims	Protection Profile Conformance Claims
8	Rationale	Contains pointers to the rationales contained throughout the document.
9	Appendix A: KC Access Levels and Functions	Contains the list of access levels and functions (operations).

Table 1 – ST Organization and Description

1.5 Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations. When NIAP Interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Refinement: ***additions and replacements indicated with bold text and italics***

deletions without replacing text indicated with strike-through ~~bold text and italics~~

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

The explicitly stated requirements claimed in this ST are denoted by the "_EXP" extension in the unique short name for the explicit security requirement.

1.6 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

1.6.1 ST Specific Terminology

AC	Author Center
CTS	Call Tracking System
FG	Filter Group permissions
KC	Knowledge Center
RP	Report permissions
SA	Support Administrator
SC	Support Center
UC	User Center

1.6.2 Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
DB	Database
EAL2	Evaluation Assurance Level 2
FAQ	Frequently asked question
IIS	Internet Information Server
MAC	Message authentication code
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function

ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

2 TOE Description

2.1 Overview

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 end-point 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. The SupportSoft Knowledge Center product can be purchased separately without the Intelligent Assistance Suite. The SupportSoft Platform is included with the purchase of the KC.

2.2 Architecture Description

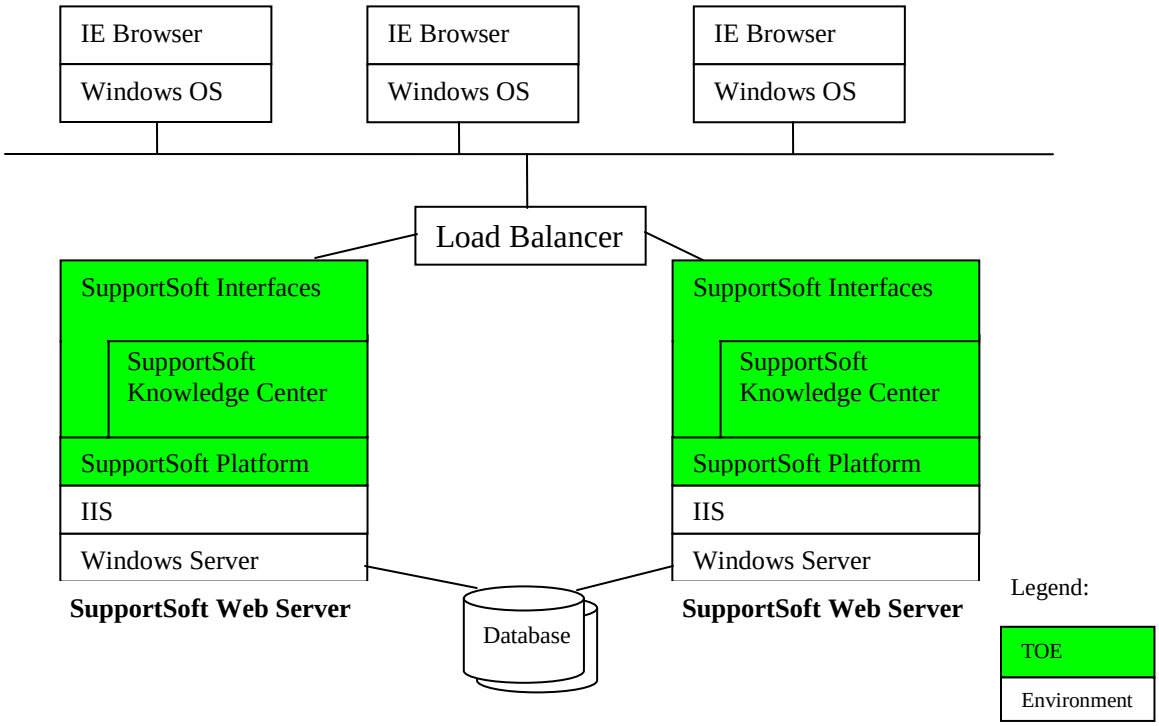

Figure 1: The TOE in a Sample Environment

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, as defined in Section 2.3.2. 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[3] 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).

- **Support Administrator (SA):** A virtual directory[4], 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

[3] A content item is a knowledge base entry that contains information (content) made available for access by the users of the TOE. There are multiple types of content items. Platform provides the Folder content type. Knowledge Center provides the following content types: Resource, Script SupportAction, SupportArticle – FAQ, SupportArticle - Document, SupportArticle – Inline Document, SupportArticle – Problem Resolution, SupportArticle – URL, , Shortcut, Web document, and Contribution.

[4] A virtual directory represents a namespace, often seen as a URL. For example, the namespace http://www.supportsoft.com could contain a tree of documents. Virtual directories can be created below a root URL, so a typical virtual directory might be http://www.supportsoft.com/sdcxuser, where sdcxuser is the virtual directory.

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.

2.3 Physical Scope and Boundaries

This section lists the hardware and software components of the product and denotes which are in the TOE and which are in the environment.

2.3.1 Hardware Components

This table identifies hardware components in the IT environment. There are no hardware components in the TOE. The following hardware components are required for the IT environment:

Database Server Hardware	Any hardware with at least one network adapter that will run the OS required by the DB described in Section 2.3.2. It is recommended that the computer have 100 GB disk space, but the amount needed is dependent upon the number and size of the content items.
Web Server Hardware	Any hardware that will run Windows 2000 Server with Service Pack 2 or higher. At least two network adapters are required; one to connect to the DB (physically protected network) and one to connect to the network. The recommended minimum disk space is 20 GB.
Client/Browser Workstation	Any hardware that will run the Windows OS that supports the client browser described in Section 2.3.2. The client/browser workstation must have at least one network adapter and have network connectivity to the SupportSoft web server.

Load Balancer	A separate device used to balance network traffic across a number of servers in order to enhance scalability and availability. It also can detect server failures and redistribute traffic to operating servers. This component of the IT environment is provided by a third party. A load balancer is only needed if the deployment requires load balancing and there is more than one SupportSoft web server deployed to service requests from external entities. When a load balancer is used, the load balancer receives all network traffic to the TOE and it determines which SupportSoft web server to route the traffic to for processing.

2.3.2 Software Components

This table identifies software components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	SupportSoft Platform v6.5 Service Pack 4 (SP4)	Backbone providing comprehensive support infrastructure
TOE	SupportSoft Knowledge Center v6.5 Service Pack 1 (SP1)	Allows organizations to create, approve, and publish content
Environment	Database software: Microsoft SQL Sever 2000 Service Pack 3 or later Or Oracle 9.i or higher	Database host server
Environment	Database Server OS For Microsoft SQL Server – Any OS that Microsoft SQL Server 2000 SP 3 or later is approved by Microsoft to execute on For Oracle – Any OS that Oracle 9.i or higher is approved by Oracle to execute on	Operating System for the Database host server

Environment	SupportSoft web server OS Windows 2000 Server with Service Pack 2 or higher with Microsoft Windows Scripting Host 5.6[5] or higher and the DB client software required by the SQL or Oracle	Internet Explorer 5.5 with XML parser update (Microsoft XML 3.0 Service Pack)[6] Or Internet Explorer 6.0 or higher Note: Windows 2000 Server includes Internet Information Services (IIS). The TOE supports IIS version 5.0.
Environment	Client Browser	Internet Explorer 5.5 with XML parser update (Microsoft XML 3.0 Service Pack) Or Internet Explorer 6.0 or higher

2.3.3 Guidance

The TOE includes the following guidance documentation:

SupportSoft Platform Version 6.5 Service Pack 4 Administrator's Guide

SupportSoft Platform Version 6.5 Service Pack 04 Release Notes

SupportSoft Content Administration Guide (Applies to All v6.5 SP1 or Higher products that include Content)

SupportSoft Knowledge Center Version 6.5 Service Pack 1 Release Notes

SupportSoft Platform v6.5 SP4 and Product Installation Guide

SupportSoft Installation and Administration Supplemental CC Guidance

SupportSoft User Supplemental CC Guidance

2.4 Logical Boundaries

This section contains the product features and denotes which are in the TOE.

2.4.1 Access Control

Access controls are enforced at the interface level. 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

[5] Microsoft Windows Scripting Host 5.6 is required to install and configure the TOE.

[6] The XML parsing is required for client side processing and formatting.

to which the user has access.

SmartResults can be used to determine what data is available to users of the User Center and Support Center interfaces based upon their session parameters. These sessions parameters are not considered security-relevant and as such are not part of the TSF, but they can be used in the TOE.

2.4.1.1 KC Access Levels

For each folder[7], 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[8]. Access to Contribution content items is controlled by the access levels assigned to the contribution content type.

2.4.1.2 SmartResults

Content is accessible via the UC and SC interfaces only after it is published.

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 is 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. (Note: The group membership (audience) filtering requires external authentication which is excluded from the TSF, therefore it cannot be used in the evaluated configuration.).

2.4.2 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,

[7] The term "folder" in the ST refers to all folders except the three pre-defined folders under the "Review Contributions".

[8] The Contribution content type is a type of content item used to contribute ideas for content while using Support Center. By comparison to Contribution content types, non-contribution content types include Resources, FAQs, URLs, Documents, etc.

Expired, Delisted, 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.

2.4.3 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. By default, 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.

2.4.4 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[9] 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[10] to groups in order to determine access to specific components[11]. Platform permissions are assigned to groups using SupportSoft

[9] A workflow defines an approval scheme for publishing newly created or updated content. If a workflow is not defined for the content, the approval process is skipped and the content is published when it is submitted.

[10] Note these permissions are different than the access control permissions.

[11] Components are the SupportSoft interfaces and the tools and features within the interfaces.

Platform. Platform is also responsible for enforcing roles.

2.4.5 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.

2.5 Items Excluded from the TOE/TSF

This section identifies any items that are included in the product, but specifically excluded from the TOE and TSF.

2.5.1 Knowledge Center SDK

The Knowledge Center SDK is outside the scope of the evaluation.

2.5.2 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.

2.5.3 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.

2.5.4 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.

3 TOE Security Environment

The TOE is intended to be used in environments in which, at most, sensitive but unclassified information is processed.

This section contains assumptions regarding the security environment and the intended usage of the TOE, threats on the TOE and the IT environment, and organizational security policies.

3.1 Assumptions

The assumptions are ordered into three categories: personnel assumptions, physical environment assumptions, and operational assumptions.

3.1.1 Personnel Assumptions

A.MANAGE Two or more individuals are assigned to manage and operate the TOE as administrators.

A.NOEVIL The administrative users of the TOE, web server, database, and corresponding OSs, in their assigned role, are appropriately trained, not careless, not willfully negligent, non-hostile and follow and abide by the instructions provided in the guidance documentation.

3.1.2 Physical Environment Assumptions

A.DBNET 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.

A.PHYSICAL 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.

3.1.3 Operational Assumptions

A.DEDICATED 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.

A.TOE_CONFIG The TOE is installed and configured so that it is consistent with the installation guidance.

3.2 Threats

The TOE or IT environment addresses the threats identified in this section. The threat agents are

authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent has a low attack potential who possesses an average expertise, few resources, and low to moderate motivation.

T.ACCOUN	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.
T.AUD_COMP	A user or process may gain unauthorized access to the audit trails and cause records to be lost or modified.
T.ACCESS	A user or process may gain unauthorized access to content items and delete or modify the content items.
T.BYPASS	A user or process may bypass TOE security to gain access to TOE security functions and data.
T.MASQ	A user or process may masquerade as another entity in order to gain access to TOE security functions and data.
T.TSF_COMP	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.

3.3 Organizational Security Policies

This ST has no Organizational Security Policies.

4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

The following are the IT security objectives that are to be addressed by the TOE.

O.AUD_GEN	The TOE will provide the capability to detect and create records of login events and of content item status changes.
O.AUD_PROT	The TOE will provide the capability to protect audit information from unauthorized disclosure through its own interfaces.
O.AUD_REV	The TOE will provide the capability to review audit information.
O.CONTENT_AC	The TOE will provide the capability to determine the logic required to protect the content items from unauthorized access through its own interfaces. In addition the TOE will provide this logic to the DB to be enforced prior to returning the content items to which the user has access.
O.MANAGE	The TOE will provide the functions and facilities necessary to support authorized users in the management of the content items and the TOE.
O.PART_SELF_PROT	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosures through its own interfaces.
O.TOE_ACCESS	The TSF will provide features that control a user's logical access to the TOE.

4.2 Security Objectives For The Environment

4.2.1 IT Security Objectives For The Environment

The following IT security objectives for the environment are to be addressed by the IT environment by technical means.

OE.AUD_STOR	The IT environment will provide a means for secure storage of the TOE audit trails, protecting the audit trails from unauthorized access.

OE.AUD_TIME	The IT environment will provide the capability to timestamp all audit records prior to storage.
OE.CONTENT_AC	The IT environment will provide the capability to protect content items, which are stored in the IT environment, from unauthorized modification and disclosure.
OE.DOMAIN_SEP	The IT environment will provide an isolated domain for the execution of the TOE.
OE.QUERY	The IT environment will provide the capability to correctly resolve queries meeting the logic provided by the TOE to support the TOE's enforcement of content access control.
OE.NO_BYPASS	The IT environment will ensure that the TOE security mechanisms cannot be bypassed in order to gain access to TOE security functions and data.
OE.SEC_COMM	The IT environment will provide secure communications that prevent unauthorized disclosure and unauthorized modification of transmissions between the web server and web browser.
OE.TIME_STAMP	The IT environment will provide reliable time stamps.
OE.TSF_DATA_PROT	The IT environment will provide a means to protect the TSF data from unauthorized access.

4.2.2 Non-IT Security Objectives For The Environment

The non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

OE.DBNET	The network connecting the SupportSoft web server(s) to the DB(s) will be a private, separate physical network that is not globally routable and that is protected from attacks and from unauthorized physical access.
OE.DEDICATED	Administrators will ensure that the systems executing the SupportSoft web server(s) and DB system(s) are dedicated to those functions and do not provide any general purpose or non-TOE user data storage capabilities.
OE.MANAGE	Organizations using the TOE will ensure that two or more individuals are assigned to manage and operate the TOE as administrators.
OE.NOEVIL	Organizations using the TOE will ensure that administrative users of the TOE, web server, database, and corresponding OSs are appropriately

trained, not careless, not willfully negligent, non-hostile and follow and abide by all instructions provided in the guidance documentation.

OE.PHYSICAL The processing resources of the SupportSoft web servers and database servers will be located within controlled access facilities, which limit unauthorized physical access and provide physical security commensurate with the value of the TOE and the data it contains.

OE.TOE_CONFIG The TOE will be installed and configured so that it is consistent with the installation guidance.

4.3 Security Objectives Tracing

The following table represents a mapping of the threats and assumptions to the security objectives defined in this ST.

	A.DBNET	A.DEDICATED	A.MANAGE	A.NOEVIL	A.PHYSICAL	A.TOE_CONFIG	T.ACCOUN	T.AUD_COMP	T.ACCESS	T.BYPASS	T.MASQ	T.TSF_COMP
O.AUD_GEN							X					
O.AUD_PROT								X				
O.AUD_REV							X					
O.CONTENT_AC									X			
O.MANAGE												X
O.PART_SELF_PROT								X		X		X
O.TOE_ACCESS							X			X	X	

	A.DBNET	A.DEDICATED	A.MANAGE	A.NOEVIL	A.PHYSICAL	A.TOE_CONFIG	T.ACCOUN	T.AUD_COMP	T.ACCESS	T.BYPASS	T.MASQ	T.TSF_COMP
OE.AUD_STOR								X				
OE.AUD_TIME							X					
OE.CONTENT_AC									X			
OE.DOMAIN_SEP								X				X
OE.QUERY									X			
OE.NO_BYPASS								X		X		X
OE.SEC_COMM									X		X	X
OE.TIME_STAMP							X					
OE.TSF_DATA_PROT											X	X
OE.DBNET	X							X	X			X
OE.DEDICATED		X										
OE.MANAGE			X									
OE.NOEVIL				X			X					
OE.PHYSICAL					X							
OE.TOE_CONFIG						X						

Table 2 – Threats & IT Security Objectives Mappings

4.4 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

T.ACCOUN — O.AUD_GEN helps to mitigate this threat by ensuring that security-relevant actions are detected and recorded for review. The audit records are time stamped, stored and protected in the IT environment. O.AUD_REV helps to mitigate this threat by providing interfaces for viewing the audit trails. O.TOE_ACCESS contributes to mitigating this threat by requiring the TOE to identify and authenticate all authorized users prior to allowing administrative TOE access. OE.AUD_TIME assists in mitigating this threat by requiring the IT environment to time stamp (include the current date and time within) all audit records as they are stored. OE.TIME_STAMP assists in mitigating this threat by requiring the IT environment to provide a reliable time stamp. OE.NOEVIL assists in mitigating this threat by requiring administrative users to follow the instructions provided in the guidance documentation which will include guidance on reviewing audit data.

T.AUD_COMP — O.AUD_PROT contributes to mitigating this threat by controlling access to the audit trail. None of the TSF interfaces support modifying or deleting

	information in the audit record. O.PART_SELF_PROT contributes to countering this threat by ensuring that the TSF can protect itself from users via its own interfaces. This limits access to the audit information to the functions defined for the specified roles. OE.AUD_STOR contributes to mitigating this threat by providing storage for the audit trail and by restricting the ability of users in the IT environment to access the audit log file. OE.DOMAIN_SEP contributes to countering this threat by ensuring that the TSF is protected from users through mechanisms other than its own interfaces. If the operating system could not maintain and control a domain of execution for the TSF separate from other processes, the TSF could not be trusted to control access to the resources under its control, which includes the audit trail. OE.NO_BYPASS ensures audit compromise cannot occur simply by bypassing the TSF. OE.DBNET ensures that the network connecting the SupportSoft web server(s) 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.
T.ACCESS	O.CONTENT_AC contributes to mitigating this threat by determining the logic required to protect the content items from unauthorized access through its own interfaces and by providing this logic to the DB for enforcement prior to the DB returning the requested information. OE.CONTENT_AC contributes to mitigating this threat by ensuring that the database where the content items are stored is capable of protecting the content items from unauthorized modification and disclosure. OE.SEC_COMM provides secure communications that prevent unauthorized disclosure of transmissions between the web server and web browser. OE.DBNET contributes to mitigating this threat by requiring a private, separate physical network connecting the SupportSoft web server(s) to DB(s). OE.QUERY contributes to mitigating this threat by correctly resolving the DB queries that meet the logic provided by the TOE to support content access control.
T.BYPASS	O.PART_SELF_PROT contributes to countering this threat by ensuring that the TSF can protect itself from users via its own interfaces. O.TOE_ACCESS contributes to mitigating this threat by requiring the TOE to identify and authenticate all authorized users prior to allowing TOE access, except for anonymous access configured by the administrator. OE.NO_BYPASS ensures TSF compromise cannot occur simply by bypassing the TSF.
T.MASQ	O.TOE_ACCESS mitigates this threat by requiring authorized administrators and users (represented by processes) to be identified and authenticated prior to accessing TSF-mediated functions, except for

anonymous access configured by the administrator. OE.SEC_COMM provides secure communications that prevent unauthorized disclosure of transmissions, including authentication data, between the web server and web browser. OE.TSF_DATA_PROT is necessary to control who is able to access TSF data stored in the IT environment using non-TSF interfaces by requiring all DB users to be identified and authenticated.

T.TSF_COMP O.MANAGE contributes to mitigating this threat by providing an access control policy which control access to TSF data. This objective is used to dictate who is able to view and modify TSF data via the TOE interfaces, as well as the behavior of TSF functions. O.PART_SELF_PROT is necessary so that the TSF protects itself and its resources from inappropriate access through its own interfaces. OE.DBNET ensures that the network connecting the SupportSoft web server(s) 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. OE.DOMAIN_SEP is necessary so that the TSF is protected from other processes executing on the workstation. OE.NO_BYPASS ensures TSF compromise cannot occur simply by bypassing the TSF. OE.SEC_COMM provides secure communications that prevent unauthorized disclosure of transmissions between the web server and web browser. OE.TSF_DATA_PROT is necessary to control who is able to view and modify TSF data stored in the IT environment using non-TSF interfaces.

4.5 Rationale For Organizational Policy Coverage

This ST has no Organizational Security Policies.

4.6 Rationale For Assumption Coverage

The non-IT security objectives for the environment listed below are, in part, a re-statement of the corresponding security assumptions. Therefore, the security objectives for the environment listed below obviously cover the corresponding assumption.

Assumption (Section 3.1)	**Non-IT Security Obejctive for the Environment (Section 4.2.2)**
A.DBNET	OE.DBNET
A.DEDICATED	OE.DEDICATED
A.MANAGE	OE.MANAGE
A.NOEVIL	OE.NOEVIL

Assumption (Section 3.1)	**Non-IT Security Obejctive for the Environment (Section 4.2.2)**
A.PHYSICAL	OE.PHYSICAL
A.TOE_CONFIG	OE.TOE_CONFIG

5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST. These security requirements are defined in Sections 5.1 - 5.3.4.

TOE Security Functional Requirements (from CC Part 2)	
FAU_GEN.2	User identity association
FAU_SAR.1a	Audit review – Login
FAU_SAR.1b	Audit review – Content Items
FAU_SAR.2	Restricted audit review
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes – AC
FMT_MSA.3	Static attribute initialization - AC
FMT_MTD.1a	Management of TSF data – Query
FMT_MTD.1b	Management of TSF data – Modify
FMT_MTD.1c	Management of TSF data – Create, Delete
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Explicitly Stated TOE Security Functional Requirements	
FAU_GEN_EXP.1	Explicit audit data generation
FDP_ACC_EXP.1	Subset access control logic – AC
FDP_ACF_EXP.1	Security attribute based access control logic - AC
FIA_UAU_EXP.2	User authentication with anonymous
FIA_UID_EXP.2	User identification with anonymous
FPT_RVM_EXP.1	Partial Non-bypassability of the TSP
FPT_SEP_EXP.1	Partial TSF domain separation

Table 3 – TOE Security Functional Requirements

IT Environment Security Functional Requirements (from CC Part 2)	
FAU_STG.1	Protected audit trail storage
FIA_UAU.2	User authentication before any action - Database
FIA_UID.2	User identification before any action - Database
FPT_ITC.1	Partial Inter-TSF confidentiality during transmission (web server to browser)
FPT_ITI.1	Inter-TSF detection of modification (web server to browser)
FPT_STM.1	Reliable time stamps
FTA_SSL.3	TSF-initiated termination

Explicitly Stated IT Environment Security Functional Requirements	
FAU_TIM_EXP.1	Audit data time stamp
FDP_QRY_EXP.1	Query Resolution
FPT_RVM_ENV_EXP.1	Environment Non-bypassability of the TSP
FPT_SEP_ENV_EXP.1	Environment TSF domain separation

Table 4 – IT Environment Security Functional Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 ***For audit events resulting from actions of identified users, the ~~The~~*** TSF shall be able to associate each auditable event with the identity of the user that caused the event. ***(NIAP Interpretation 0410)***

5.1.1.2 FAU_SAR.1a Audit Review – Login

FAU_SAR.1.1a The TSF shall provide **Administrators and users with the SA: Support Administrator Interface, SA: List Reports and corresponding Platform "RP: User XXX Report" permissions** with the capability to read **all login audit trail data** from the audit records.

FAU_SAR.1.2a The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 FAU_SAR.1b Audit Review – Content Items

FAU_SAR.1.1b The TSF shall provide **Administrators, Authors, and users with the AC: Author Center Interface and AC: Manage Content permissions** with the capability to read **audit trail data for a content item** from the audit records.

FAU_SAR.1.2b The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.2 Identification and Authentication (FIA)

5.1.2.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within **the range of 3 to 10** unsuccessful authentication attempts occur related to **login events**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **lock out the user account**.

5.1.2.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) identity;

b) password;

c) group(s);

5.1.2.3 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the following password complexity rules:**

a) minimum password length: 8 characters

b) maximum password length: 20 characters

c) contain at least one upper case character

d) contain at least one lower case character

e) contain at least one digit

f) contain at least one punctuation character

g) password expires in an administrator configurable value of 30-90 days

h) new password must be different than the old password

5.1.3 Security Management (FMT)

5.1.3.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of the functions **listed in Table 5** to **the identified roles listed in Table 5**.

Function	Role
Password Policy, including Login auditing	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Password Policy permissions**
Anonymous Logins (Access)	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: User Center Design permissions**

Function	Role
Workflow Schemes	**Administrator** **Users assigned to a group with the AC: Author Center Interface and AC: Workflow Administration permissions**

Table 5 – Security Management Functions

5.1.3.2 FMT_MSA.1 Management of security attributes - AC

FMT_MSA.1.1 The TSF shall enforce the **AC Access Control Policy** to restrict the ability to modify, delete the security attributes **group/KC access level pairs** to **Administrators or subjects with the AC: Author Center Interface and AC: Manage Content permissions.**

5.1.3.3 FMT_MSA.3 Static attribute initialization - AC

FMT_MSA.3.1 The TSF shall enforce the **AC Access Control Policy** to provide permissive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **Administrators and subjects with the AC: Author Center Interface and AC: Manage Content permissions** to specify alternative initial values to override the default values when an object or information is created.

5.1.3.4 FMT_MTD.1a Management of TSF data - Query

FMT_MTD.1.1a The TSF shall restrict the ability to query the **TSF data listed in Table 6** to **the associated role listed in Table 6**.

TSF Data	Role
Password policy	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Password Policy permissions**
Login Audit records	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface, SA: List Reports and corresponding RP: permissions (RP: User Failed Login Report, RP: User Login Report, or RP: User Reset Report)**
Session Timeout Period	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Platform Registry permissions**

TSF Data	Role
Content Item Audit records (view content item audit trail)	**Administrator, Author** **Users assigned to a group with the AC: Author Center Interface and AC: Manage Content permissions**
Workflows	**Administrator** **Users assigned to a group with the AC: Author Center Interface and AC: Workflow Administration permissions**
User accounts	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Users permissions**
Groups	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Groups permissions**
Platform permissions (roles)	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Permissions permissions**
Reports	**Administrator** **Users assigned to the SA: Support Administrator Interface, SA: List Reports and corresponding RP permissions**
Access Levels	**Administrator** **Users assigned to the AC: Author Center Interface and AC: Role Administration permissions**

Table 6 – Query TSF Data

5.1.3.5 FMT_MTD.1b Management of TSF data – Modify

FMT_MTD.1.1b The TSF shall restrict the ability to modify the **TSF data listed in Table 7** to **the associated role listed in Table 7**.

TSF Data	Role
Password policy	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Password Policy permissions**

TSF Data	Role
Session Timeout Period	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Platform Registry permissions**
Workflows	**Administrator** **Users assigned to a group with the AC: Author Center Interface and AC: Workflow Administration permissions**
User accounts	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Users permissions**
Groups	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Groups permissions**
Platform permissions (roles)	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Permissions permissions**
Reports	**Users assigned to a group with the SA: Support Administrator Interface and RF: Report Editing permissions. To edit read-only (predefined) reports, the user must also be assigned to a group with the RF: Edit Read-Only Reports**
Access Levels	**Administrator** **Users assigned to the AC: Author Center Interface and AC: Role Administration permissions**

Table 7 – Modify TSF Data

5.1.3.6 FMT_MTD.1c Management of TSF data – Create, Delete

FMT_MTD.1.1c The TSF shall restrict the ability to create, delete the **TSF data listed in Table 8** to **the associated role listed in Table 8**.

TSF Data	Role
Password policy	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Password Policy permissions**

TSF Data	Role
Session Timeout Period	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Platform Registry permissions**
Workflows	**Administrator** **Users assigned to a group with the AC: Author Center Interface and AC: Workflow Administration permissions**
User accounts	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Users permissions**
Groups	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Groups permissions**
Platform permissions (roles)	**Administrator** **Users assigned to a group with the SA: Support Administrator Interface and SA: Permissions permissions**
Reports	**Administrator** **Users assigned to the corresponding SA: Support Administrator Interface and RP permissions**
Access Levels	**Administrator** **Users assigned to the AC: Author Center Interface and AC: Role Administration permissions**

Table 8 – Create. Delete TSF Data

5.1.3.7 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a. **Create and manage SupportSoft users and groups**
b. **Assign Platform permissions to groups (e.g., manage roles)**
c. **Create and manage access levels**
d. **Create and view reports**
e. **Configure the password policy**
f. **Change user passwords**
g. **Change session timeout periods**

h. Create and configure workflows and content types

i. Assign access controls to folders and the Contribution content type

j. Configure to allow or deny anonymous access.

k. Edit reports

5.1.3.8 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles **Administrator, Author, Approver, Support Analyst, users assigned Platform permissions[12] via group membership**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2 Explicitly Stated TOE Security Functional Requirements

The SFRs defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN_EXP.1 Explicit Audit Data Generation

FAU_GEN_EXP.1.1 The TSF shall be able to generate an audit record of the auditable events identified in Table 9 and Table 10.

FAU_GEN_EXP.1.2 The TSF shall record within each content item audit record at least the following information:

a) Type of event, subject identity, and the outcome (success or failure) of the event

Functional Component	Auditable Event
FDP_ACF_EXP.1	Changes to the content items resulting in state changes. See Section 2.4.2 for a list of possible states.

Table 9 – FAU_GEN_EXP.1.2 Content Item Auditable Events

FAU_GEN_EXP.1.3 The TSF shall record within each logon audit record at least the following information:

a) Type of event, user identity, number of times for this event type for that user

Functional Component	Auditable Event
FIA_AFL.1	Admnistrator re-enables (resets) a user account because the threshold for unsuccessful authentication attempts was reached.
FIA_UAU_EXP.2	Successful logins.
FIA_UAU_EXP.2	Failed logins due to supplying an incorrect password.

[12] Refer to Appendix B – SupportSoft Platform Permissions for a complete list of Platform permissions.

Table 10 – FAU_GEN_EXP.1.3 Logon Auditable Events

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_ACC_EXP.1 Subset access control logic - AC

FDP_ACC_EXP.1.1 The TSF shall enforce the **AC Access Control Policy,** by creating and sending queries to the DB in the IT environment, on:

- **Subjects: ASP session acting on the behalf of users**
- **Objects: Content items (Folder, Resource, script SupportAction, SupportArticle - Document, SupportArticle – FAQ, SupportArticle – Inline Document, SupportArticle – Problem Resolution, SupportArticle – URL, Shortcut, web document, Contribution)**
- **Operations: All operations provided from Author Center (AC)[13].**

5.2.2.2 FDP_ACF_EXP.1 Security attribute based access control logic - AC

FDP_ACF_EXP.1.1 The TSF shall enforce the **AC Access Control Policy** to objects, by creating and sending queries to the DB in the IT environment, based on the following:

Subject Security Attributes:

a) The user identity and group memberships

Object Security Attributes:

b) The permission associated with the groups whom the user is a member of

c) The following access control attributes associated with the content item, except Contributions:

- **Access control list (ACL) on the folder in which the content item resides consisting of pairs of group identifiers and access levels or KC permissions.**

d) ACL on the Contribution content type consisting of pairs of group identifiers and access levels or KC permissions

FDP_ACF_EXP.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) For non-Contribution content items, access is allowed in AC if there is no ACL on the folder in which the non-Contribution content item resides.

b) For non-Contribution content items, access to a content item is allowed in AC if the access control attributes on the folder in which the content item resides explicitly grant access to a group of which the requesting subject is a member.

c) For non-Contribution content items, access is denied in AC if there is an

[13] Refer to Appendix A: KC Access Levels and Functions for a complete list of operations available within AC.

ACL on the folder in which the content item resides and the access control attributes do not explicitly grant access to a group of which the requesting subject is a member.

d) For Contribution content items, access is allowed in AC if there is no ACL on the Contribution content type.

e) Access to a Contribution Content item is allowed in AC if the Contribution content type ACL explicitly grant access to a group of which the requesting subject is a member.

f) Access is denied in AC if there is an ACL on the Contribution content type and the access control attributes do not explicitly grant access to a group of which the requesting subject is a member.

FDP_ACF_EXP.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **None**.

FDP_ACF_EXP.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules: **None**.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_UAU_EXP.2 User Authentication with anonymous

FIA_UAU_EXP.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user, unless the TSF is configured to allow anonymous access.

FIA_UAU_EXP.2.2 If the TSF is configured to allow anonymous access, the TSF will perform mediated actions on behalf of anonymous user without authenticating the user.

5.2.3.2 FIA_UID_EXP.2 User Identification with anonymous

FIA_UID_EXP.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user, unless the TSF is configured to allow anonymous access.

FIA_UID_EXP.2.2 The TSF shall use the account selected as the anonymous user account to identify all users that login without accessing the login page.

5.2.4 Protection of TSF (FPT)

5.2.4.1 FPT_RVM_EXP.1 Partial Non-bypassability of the TSP

FPT_RVM_EXP.1.1 The TSF, when invoked shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.4.2 FPT_SEP_EXP.1 Partial TSF Domain Separation

FPT_SEP_EXP.1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.2 The TSF shall enforce separation between the security domains of subjects in the

TSC.

5.3 IT Environment Security Requirements

The SFRs on the IT environment defined in this section are taken from Part 2 of the CC.

5.3.1 Security Audit (FAU)

5.3.1.1 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The ***IT Environment*** shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The ***IT Environment*** shall be able to prevent unauthorised modifications to the audit records in the audit trail.

5.3.2 Identification and Authentication (FIA)

5.3.2.1 FIA_UAU.2 User Authentication before any action –Database

FIA_UAU.2.1 The ***Database of the IT Environment*** shall require each user to be successfully authenticated before allowing any other ***database-mediated*** actions on behalf of that user.

5.3.2.2 FIA_UID.2 User Identification before any action – Database

FIA_UID.2.1 The ***Database of the IT Environment*** shall require each user to identify itself before allowing any other ***database-mediated*** actions on behalf of that user.

5.3.3 Protection of the TSF (FPT)

5.3.3.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The ***IT environment*** shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

5.3.3.2 FPT_ITI.1 Inter-TSF Detection of Modification

FPT_ITI.1.1 The ***IT environment*** shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **at least one MAC error in SSL transmissions.**

FPT_ITI.1.2 The ***IT environment*** shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform **a re-send of network packet(s) that caused the error** if modifications are detected.

5.3.3.3 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The ***IT environment*** shall be able to provide reliable time stamps for ***the TOE's*** use.

5.3.4 TOE Access (FTA)

5.3.4.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The ***IT environment*** shall terminate an interactive session after a **TOE administrative user configurable number of minutes of user inactivity**.

5.4 Explicitly Stated IT Environment Security Functional Requirements

The SFRs on the IT environment defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

5.4.1 Security Audit (FAU)

5.4.1.1 FAU_TIM_EXP.1 Audit Data Time Stamp

FAU_TIM_EXP.1.1 The ***IT environment*** shall record within each TOE content item audit record the date and time of the event.

FAU_TIM_EXP.1.2 The ***IT environment*** shall record within each TOE logon audit record the date and time of the last occurrence of this event type for that user.

5.4.2 User Data Protection (FDP)

5.4.2.1 FDP_QRY_EXP.1 –Query Resolution

FDP_QRY_EXP.1.1 The IT environment shall support the TOE's enforcement of the **AC Access Control Policy** by correctly resolving queries received from the TOE.

5.4.3 Protection of the TSF (FPT)

5.4.3.1 FPT_RVM_ENV_EXP.1 Environment Non-bypassability of the TSP

FPT_RVM_ENV_EXP.1.1 The ***IT Environment*** shall ensure that ***IT Environment security policy*** enforcement functions are invoked and succeed before each function within the ***IT environment scope of control*** is allowed to proceed.

5.4.3.2 FPT_SEP_ENV_EXP.1 Environment TSF Domain Separation

FPT_SEP_ENV_EXP.1.1 The ***IT Environment*** shall maintain a security domain for ***the TOE's*** execution that protects ***the TOE*** from interference and tampering by untrusted subjects.

FPT_SEP_ENV_EXP.1.2 The ***IT Environment*** shall enforce separation between the security domains of subjects in the TSC.

5.5 TOE Strength of Function Claim

The only probabilistic or permutational mechanisms in the product are the password mechanism used to authenticate users and the cryptographic mechanisms used for secure communications.

Strength of cryptographic algorithms is outside the scope of the Common Criteria.

The claimed minimum strength of function is SOF-basic. FIA_SOS.1 and FIA_UAU_EXP.2 are the only non-cryptographic TOE security functional requirements that contain a permutational function.

5.6 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) as defined by the CC. The assurance components are summarized in the following table.

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.2	Configuration items
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 11 – Assurance Requirements: EAL2

5.6.1 ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.2 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.3 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.6.4 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using

an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.6.5 ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.6.6 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.7 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.8 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.9 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.10 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.11 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.6.12 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.6.13 AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.7 Rationale For TOE Security Requirements

5.7.1 TOE Security Functional Requirements

	O.AUD_GEN	O.AUD_PROT	O.AUD_REV	O.CONTENT_AC	O.MANAGE	O.PART_SELF_PROT	O.TOE_ACCESS
FAU_GEN_EXP.1	X						
FAU_GEN.2	X						
FAU_SAR.1a			X				
FAU_SAR.1b			X				
FAU_SAR.2		X					
FDP_ACC_EXP.1				X			
FDP_ACF_EXP.1				X			
FIA_AFL.1							X
FIA_ATD.1							X
FIA_SOS.1							X
FIA_UAU_EXP.2							X
FIA_UID_EXP.2							X
FMT_MOF.1					X		
FMT_MSA.1					X		
FMT_MSA.3				X			
FMT_MTD.1a					X		

	O.AUD_GEN	O.AUD_PROT	O.AUD_REV	O.CONTENT_AC	O.MANAGE	O.PART_SELF_PROT	O.TOE_ACCESS
FMT_MTD.1b					X		
FMT_MTD.1c					X		
FMT_SMF.1					X		
FMT_SMR.1					X		
FPT_SEP_EXP.1						X	
FPT_RVM_EXP.1						X	

Table 12 – TOE SFR and Security Objectives Mapping

O.AUD_GEN The TOE will provide the capability to detect and create records of login events and of content item status changes.

FAU_GEN_EXP.1 defines the set of security-relevant events that the TOE must be capable of recording. This requirement also defines the information that the TOE must include in the audit record for each auditable event. FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event.

O.AUD_PROT The TOE will provide the capability to protect audit information from unauthorized disclosure through its own interfaces.

FAU_SAR.2 restricts the ability to read the logon audit events to the Administrator and users with the SA: Support Administrator Interface, SA: List Reports and corresponding Platform "RP: User XXX Report" permissions. It also restricts the ability to read content item audit events to the Administrator, Author, Approver, and users with the AC: Author Center Interface and AC: Manage Content permissions thus preventing the disclosure of the audit data to any other users.

O.AUD_REV The TOE will provide the capability to review audit information.

FAU_SAR.1a and FAU_SAR.1b provide the ability to review the audit records in a user-friendly manner

O.CONTENT_AC	The TOE will provide the capability to protect the content items from unauthorized access through its own interfaces. FDP_ACC_EXP.1 identifies the entities involved in content access control logic created by the TOE when AC is used. FDP_ACF_EXP.1 identifies the security attributes of the subjects and objects involved in the access request and then the policy defines under what conditions the access control logic created by the TOE permits access when AC is used. FMT_MSA.3 requires that the TOE have a default allow policy for requests to access content information. This default policy applies in AC when there are no ACLs on the folder in which the content item resides or on the Contribution content type. Due to the type of product, no ACLs is assumed to be global access.
O.MANAGE	The TOE will provide the functions and facilities necessary to support authorized users in the management of the content items and the TOE. FMT_MOF.1 defines particular TOE management capabilities that can be used only by select users. FMT_MSA.1 defines which roles are allowed to modify the group/KC access level pairs. FMT_MTD.1a, FMT_MTD.1b, and FMT_MTD.1c define TSF data that may be queried, created, and altered only by users with select roles. FMT_SMF.1 defines the administrative functions provided by the TOE. FMT_SMR.1 defines the roles provided by the TOE.
O.PART_SELF_PROT	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosures through its own interfaces. FPT_SEP_EXP.1 ensures that the TSF maintains a domain that protects itself from untrusted users and from interference that would prevent it from performing its functions. FPT_RVM_EXP.1 ensures that the functions are invoked and succeed before each function may proceed.
O.TOE_ACCESS	The TSF will provide features that control a user's logical access to the TOE. FIA_AFL.1 detects all unsuccessful authentication attempts and locks the targeted account after an administrator configured number of consecutive unsuccessful attempts. This feature assists in preventing unauthorized users from gaining access to authorized user's account by guessing authentication data. FIA_ATD.1 ensures that for each user the TOE maintains a set of security attributes, which are used to make

logical TOE access decisions. FIA_SOS.1 ensures that the strength of the user password meets a configured set of requirements. FIA_UID_EXP.2 requires that a user be identified to the TOE in order to access the TOE. FIA_UAU_EXP.2 requires that a user be authenticated to the TOE before accessing the TOE, unless anonymous access is allowed. If anonymous access is allowed, only anonymous users do not need to login; other users still need to login

5.7.2 TOE Security Assurance Requirements

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

5.8 Rationale For IT Environment Security Requirements

	OE.AUD_STOR	OE.AUD_TIME	OE.CONTENT_AC	OE.DOMAIN_SEP	OE.QUERY	OE.NO_BYPASS	OE.SEC_COMM	OE.TIME_STAMP	OE.TSF_DATA_PROT
FAU_STG.1	X								
FIA_UAU.2	X		X						X
FIA_UID.2	X		X						X
FPT_STM.1								X	
FPT_ITC.1							X		
FPT_ITI.1							X		
FTA_SSL.3									X
FAU_TIM_EXP.1		X							
FDP_QRY_EXP.1					X				
FPT_RVM_ENV_EXP.1						X			
FPT_SEP_ENV_EXP.1				X					

Table 13 – IT Environment SFR and Security Objectives Mapping

OE.AUD_STOR The IT environment will provide a means for secure storage of the TOE audit trails, protecting the audit trails from unauthorized access.

FAU_STG.1 requires that the OS and database protect the audit trail from unauthorized deletion and modification. FIA_UAU.2 and FIA_UID.2 protect the content items stored in the database by requiring all users to identify and authenticate themselves to the database prior to accessing the database and subsequently viewing the

	audit trails.
OE.AUD_TIME	The IT environment will provide the capability to timestamp all audit records prior to storage. FAU_TIM_EXP.1 provides the timestamp in each audit record as it is placed in the database.
OE.CONTENT_AC	The IT environment will provide the capability to protect content items, which are stored in the IT environment, from unauthorized modification and disclosure. FIA_UAU.2 and FIA_UID.2 protect the content items stored in the database by requiring all users to identify and authenticate themselves to the database prior to accessing the database. Since all database users are authorized users, the content items are protected from unauthorized modification and disclosure.
OE.DOMAIN_SEP	The IT environment will provide an isolated domain for the execution of the TOE. FPT_SEP_ENV_EXP.1 requires the operating system to provide an isolated domain for the TOE to execute within
OE.QUERY	The IT environment will provide the capability to correctly resolve queries meeting the logic provided by the TOE to support the TOE's enforcement of content access control. FDP_QRY_EXP.1 requires that the database correctly resolve queries sent to it by the TOE in order for the TOE to enforce content access control.
OE.NO_BYPASS	The IT environment will ensure that the TOE security mechanisms cannot be bypassed in order to gain access to TOE security functions and data. FPT_RVM_ENV_EXP.1 requires the IT environment to ensure that the TOE will not be bypassed.
OE.SEC_COMM	The IT environment will provide secure communications that prevent unauthorized disclosure and unauthorized modification of transmissions between the web server and web browser. FPT_ITC.1 requires that the IT environment protect the data from unauthorized disclosure when the data is transmitted to another remote trusted IT product. FPT_ITI.1 requires that the IT environment protect the data from modification and ensure its integrity when the data is

transmitted to another remote trusted IT product. The approved web browsers defined in Section 2.3.2 are considered the remote trusted IT products.

OE.TIME_STAMP The IT environment will provide reliable time stamps.

FPT_STM.1 requires that the IT environment provide time stamps for the TOE's use.

OE.TSF_DATA_PROT The IT environment will provide a means to protect the TSF data from unauthorized access.

FIA_UAU.2 and FIA_UID.2 protect the content items stored in the database by requiring all users to identify and authenticate themselves to the database prior to accessing the database. Since all database users are authorized users, the content items are protected from unauthorized modification and disclosure. FTA_SSL.3 ensures that the TSF terminates interactive sessions after a TOE administrative user configurable number of minutes of user inactivity, which limits attackers from using an unattended session.

5.9 Rationale for Explicitly Stated Security Requirements

Table 14 presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
FAU_GEN_EXP.1	Explicit audit data generation	The TOE does not timestamp the audit records it generates, as required by FAU_GEN.1. The audit records are timestamped by the IT environment (database) when stored in the database.
FDP_ACC_EXP.1	Subset access control logic	CC Part 2 does not include an SFR that requires the TOE to create and send the access control logic for an identified access control policy to be enforced by the DB in the IT environment..
FDP_ACF_EXP.1	Security attribute based access control logic	CC Part 2 does not include an SFR that requires the TOE to create and send the access control logic based on security attributes to be enforced by the DB in the IT environment..
FIA_UAU_EXP.2	User authentication with anonymous	CC Part 2 does not include an identification and authentication SFR that allows anonymous users to interact with the TOE without providing authentication data, while requiring authentication for all other users.

Explicit Requirement	Identifier	Rationale
FIA_UID_EXP.2	User identification with anonymous	CC Part 2 does not include an identification and authentication SFR that allows anonymous users to interact with the TOE without providing identification data, while requiring identification for all other users.
FPT_SEP_EXP.1	Partial TSF domain separation	The FPT_SEP SFR from CC Part 2 cannot be completely satisfied by an application TOE. This component defines the separation that can be performed by the TOE (applications).
FPT_RVM_EXP.1	Partial Non-bypassability of the TSP	The FPT_RVM SFR from CC Part 2 is not completely satisfied by the TOE. This component defines the non-bypassability that is performed by the TOE.
FAU_TIM_EXP.1	Audit data time stamp	This requirement was explicitly defined to require that the IT environment (database) timestamp the audit records before storing them in the database.
FDP_QRY_EXP.1	Query Resolution	CC Part 2 does not include an SFR that requires the IT environment to correctly resolve DB queries to support the TOE's enforcement of an access control policy..
FPT_SEP_ENV_EXP.1	Environment TSF domain separation	The FPT_SEP SFR from CC Part 2 cannot be completely satisfied by an application TOE. This component defines the separation that is performed by the IT environment.
FPT_RVM_ENV_EXP.1	Environment Non-bypassability of the TSP	The FPT_RVM SFR from CC Part 2 is not completely satisfied by the TOE. This component defines the non-bypassability that is performed by the IT environment.

Table 14 – Explicitly Stated SFR Rationale

5.10 Rationale For Security Requirement Dependencies

This section includes a table of all the TOE security functional requirements and their associated dependencies with a rationale for any dependencies that are not satisfied.

SFR	Dependencies	Included
FAU_GEN_EXP.1	None	N/A
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	YES, via FAU_GEN_EXP.1 The dependency on FIA_UID.1 is met by FIA_UID_EXP.2 since FIA_UID.2 is hierarchical to FIA_UID.1.
FAU_SAR.1a FAU_SAR.1b	FAU_GEN.1	YES, via FAU_GEN_EXP.1
FAU_SAR.2	FAU_SAR.1	YES
FDP_ACC_EXP.1	FDP_ACF_EXP.1	YES
FDP_ACF_EXP.1	FDP_ACC_EXP.1 FMT_MSA.3	YES
FIA_AFL.1	FIA_UAU.1	YES, via FIA_UAU_EXP.2 since FIA_UAU.2 is hierarchical to FIA_UAU.1
FIA_ATD.1	None	N/A
FIA_SOS.1	None	N/A
FIA_UAU_EXP.2	FIA_UID.1	YES, via FIA_UID_EXP.2 since FIA_UID.2 is hierarchical to FIA_UID.1.
FIA_UID_EXP.2a	None	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	YES
FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	YES. FDP_ACC.1 is met via FDP_ACC_EXP.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	YES
FMT_MTD.1a FMT_MTD.1b FMT_MTD.1c	FMT_SMF.1 FMT_SMR.1	YES
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	YES, via FIA_UID_EXP.2 since FIA_UID.2 is hierarchical to FIA_UID.1.

SFR	Dependencies	Included
FPT_SEP_EXP.1	None	N/A
FPT_RVM_EXP.1	None	N/A

Table 15 – SFR Dependencies

5.11 Rationale For Internal Consistency and Mutually Supportive

The selected requirements are internally consistent. The ST includes all the SFRs provided by the TSF. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in Table 15 – SFR Dependencies
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.7.1
- including the SFRs FPT_SEP_EXP.1, FPT_RVM_EXP.1, FPT_SEP_ENV_EXP.1, and FPT_RVM_ENV_EXP.1 to protect the TSF
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely.

5.12 Rationale For Strength of Function Claim

The rationale for choosing SOF-basic is based on the low to moderate attack potential of the threats identified in this ST. The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the password management features provided by the TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Access Control

The TSF mediates access between subjects and content items. The access controls are enforced by the AC, UC, and SC interfaces. Subjects are the ASP sessions running on behalf of users. The TOE keeps track of both the user ID and list of groups for the ASP session.

The TOE retrieves only the content items from the DB that for which the user has the requested access. 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. This applies to both the AC Access Control Policy and the User Access Control Policy. To retrieve the requested information, the TOE accesses the database on behalf of the user using the TOE's database account.

AC Access Control Policy: FDP_ACC_EXP.1, FDP_ACF_EXP.1

The TSF create the logic required for the DB to enforce the AC Access Control Policy and mediate access requests to content items made through the AC interfaces.

For each folder, KC assigns access levels to groups. (Access levels are defined sets of KC permissions.) Different access levels can be assigned to a folder for each content item type.

Access to content items is enforced based on the user's group membership, access levels (KC permissions) associated with the group, and content item security attributes. The content item security attributes consist of the access control list which contains pairs of group identifiers and access levels. The TOE retrieves the user's group membership, access levels associated with the group(s), content types of the requested content items, and content item security attributes from the DB. The TOE uses this information to create the specific logic used to enforce the access controls on the requested data. That logic is then sent to the DB to retrieve the requested data that is allowed by the logic.

Access levels are assigned to groups on folders and are inherited by the content items contained within that folder, including subfolders. Access to a content item is allowed from the AC interface if the associated access control list explicitly grants access to the group of which the requesting user is a member. If there are no matching KC permissions in the ACL for the user, access is denied. (So, if an ACL is present, users are denied access unless they are explicitly granted access.) Absence of an ACL on the folder is treated as explicitly granting permission to all content items within the folder (global access).

Access levels can also be assigned to the Contribution Content Type. Contributions are contained within three predefined "Review Contributions folders". These do not have access levels. Access to a Contribution content item is allowed only if the Contribution content type ACL explicitly grants access to the group of which the requesting user is a member. If there are no matching KC permissions in the ACL for the user, access is denied. (So, if an ACL is present, users are denied access unless they are explicitly granted access within the ACL.) Absence of an ACL on the Contribution content type is treated as explicitly granting permission to all Contributions.

There are many KC permissions that can be assigned to folders and the Contribution content type. Each content type has its own set of possible permissions (called functions in the product documentation). A permission/function defines the operation to be performed on the content item from the AC interface. Examples of KC permissions include View Article, Save Article, Submit for Approval, Audit Trail, Personalize, etc. The complete list of KC permissions can be found in Appendix A: KC Access Levels and Functions.

6.1.2 Audit

The TOE provides the ability to generate audit records for login events and content item state changes. Audit records are generated by the TOE and immediately sent to the database in the IT environment for timestamping and storage. (The audit records are not buffered.)

The database provides the date/time stamp for the audit events. The audit events are timestamped immediate upon receipt by the database. Each of the content item state changes are timestamped. The most recent successful login, failed login attempt, and user reset is timestamped and stored in the DB.

The TOE also provides interfaces to allow users the ability to review the audit records. Platform provides the functionality necessary to view the login audit records. KC provides the functionality necessary to view the audit trail page for content items.

Security audit generation: FAU_GEN_EXP.1, FAU_GEN.2

Audit data is generated by Platform. The audit data includes audit records for successful logins and failed login attempts due to supplying an incorrect password as well as changes to content items resulting in a state change. The audit records generated by the TSF include the type of the event (e.g., user logins, user resets, content item state changes), user identity that performed the action, and a success/failure indicator. The user resets event is a type of login event which indicates every time the administrator had to enable a user account that was disabled by the system due to reaching the maximum number of failed logins.

Login event audit review: FAU_SAR.1a

The SA interface allows administrators and users with the corresponding Platform "RP: User XXX Report" the ability to review Login Reports. There are 3 Login reports available:

- User Failed Login Report: Displays the number of invalid attempts to log into the TOE due to providing an invalid password.
- User Login Report: Displays the number of times each user logged into the TOE.
- User Reset Report: Displays the number of times an Administrator had to enable a user account that was disabled by the system due to reaching the maximum number of failed logins.

Each of these reports also displays the date/time of the most recent corresponding event.

Content item audit review: FAU_SAR.1b

The AC interface allows Administrators, Authors, Approvers, and users with the AC: Manage Content permission to review the list of actions performed on a selected content item. The TOE does not provide an interface for viewing all content item records simultaneously. Users must

view the records for each content item separately.

Restricted audit review: FAU_SAR.2

The TSF allows only Administrators and users with the SA: Support Administrator Interface, SA: List Reports and corresponding Platform "RP: User XXX Report" permissions to view the Login Reports and only Administrators, Authors, Approvers, and users with the AC: Author Center Interface and AC: Manage Content permissions to view the content item audit trails.

6.1.3 Identification and Authentication

Identification and authentication is performed by the SupportSoft Platform. The identification and authentication TSF requires users to identify and authenticate themselves, except when accessing the TOE anonymously and the TOE has been configured to allow anonymous access. The TOE provides the ability to lockout accounts after an administrator configurable number of unsuccessful consecutive login attempts. The TOE manages user account attributes and enforces an administrator configurable password policy which ensures that passwords meet the policy when they are set or changed.

Authentication failure handling: FIA_AFL.1

The password policy provides the ability to configure the account lockout parameter. The account lockout parameter defines the number of unsuccessful consecutive login attempts allowed before the account is disabled. This feature detects the unsuccessful consecutive login attempts and disables the account after an administrator-configured number of unsuccessful consecutive login attempts have occurred. This feature applies to all logins from any of the 4 interfaces. Administrators must reset the account in order for the user to log in again. The administrator guidance instructs the Administrator to set the account lockout parameter to a value between 3 and 10.

The TSF will disable users in the Administrators group after the configured number of unsuccessful consecutive attempts is reached, so the administrator guidance instructs the Administrators to ensure that there are at least 2 individuals with the Administrator role at any given time.

User attribute definition: FIA_ATD.1

The TOE manages the user attributes that are stored in the database in the IT environment. The user security attributes managed by the TOE are the user identity, group memberships, and authentication data. Permission and access levels are assigned to groups, not users.

Verification of Secrets: FIA_SOS.1

The password policy provides the ability to configure the password rules (password length and password composition) and password access control (password age, and password reuse). The password length parameters include defining the minimum and maximum length of a password. The password composition parameters include defining the minimum number of upper case characters, lower case characters, digits, and punctuation characters. The password age parameter defines the maximum age for a password. The password reuse parameters allow the administrator to require that the new password must be different than the previous password.

The administrator guidance instructs the Administrator to set the password policy parameters as

follows:

- minimum password length: 8 characters
- maximum password length: 20 characters
- contain at least one upper case character
- contain at least one lower case character
- contain at least one digit
- contain at least one punctuation character
- password expires in an administrator configurable value of 30-90 days
- new password must be different than the old password

The verification of secrets is realized by a probabilistic or permutational security mechanism within SupportSoft Platform.

Identification and Authentication: FIA_UAU_EXP.2, FIA_UID_EXP.2

Users log into the TOE via one of the interfaces identified in Section 2.2. If the TOE is configured to not allow anonymous users, user identification and authentication must take place before the user can perform any other actions. The user enters their username and password to login. The SupportSoft Platform computes a hash of the password, retrieves the hashed password associated with the username from the database and compares the two hashed values. If the values match, the user login succeeds. Otherwise, the user login fails.

If the TOE is configured to allow anonymous access, users are allowed to interact with the TSF anonymously, without accessing the login page. Anonymous users are assigned the identity of the anonymous user account (guest) which is a member of the Guests group. Anonymous users obtain their Platform permissions from the Guests Group. The identification and authentication mechanism for non-anonymous users is the same as when the TOE is configured to not allow anonymous users.

The password authentication mechanism is realized by a probabilistic or permutational security mechanism.

6.1.4 Security Management

The TOE provides security management functions and tools to manage the security features it provides. In addition, the TOE supports roles, implemented using groups and Platform permissions, to determine what security management functions the TOE administrative interfaces (SA, AC, and SC,) make available to the administrative user and therefore determine what security management functions a particular user can perform.

All TSF data is stored in the database and the TOE provides interfaces for accessing and managing the TSF data. TOE administrators do not need to login to the database to manage the TOE.

Security Management: FMT_MOF.1, FMT_SMF.1

The TOE provides functions via SA, AC, and SC to manage the TOE security features. It also restricts who can use these security functions. The ability to perform a specific job function is

determined by the permissions and access level(s) of the groups to which the user is a member. Table 5 – Security Management Functions identifies which management function behaviours can be configured and what roles can perform those actions.

Additional security management tools provided by the TOE allow users to manage security attributes, manage TSF data, and maintain roles. Which users can perform these functions is defined below.

The SA interface provides management tools to perform the following functions:

- Configure the password policy (rules), including the ability to audit login events
- Configure the TOE to allow anonymous users
- Create and manage users and groups
- Assign Platform permissions to groups
- Create, view, and edit reports (including Login audit records)
- Change user passwords
- Change session timeout periods

The SA interface prevents the deletion of the Administrators group and prevents the deletion of the last user in the Administrators group.

The AC interface provides management tools to perform the following functions:

- Create and modify workflow schemes
- Create and manage access levels
- Create and configure content types
- Assign access levels to folders and the Contribution content type

Security Attribute Management: FMT_MSA.1, FMT_MSA.3

The AC interface provides functions to modify and delete the security attributes (ACLs) for content items. Only Administrators and users that are members of a group with the AC: Author Center Interface and AC: Manage Content permissions can modify or the delete the ACL of a content item.

The TSF provides permissive default values for the security attributes. By default, users are allowed access to content items in folders which have no ACLs set and to the Contribution content type items if there is no ACL set.

TSF Data Management: FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c

The TOE provides functions and interfaces for the administrator to query, modify, delete, and create TSF data and restrict who can manage the TSF data. Refer to Table 6 – Query TSF Data for the TSF data that can be queried and what permissions or access levels are needed to perform the query. Refer to Table 7 – Modify TSF Data for the TSF data that can be modified and what permissions or access levels are needed to perform the modification. Refer to Table 8 – Create. Delete TSF Data for the TSF data that can be created or deleted and what permissions are needed to perform the creation/deletion.

Security Roles: FMT_SMR.1

The TOE implements roles by assigning Platform permissions to groups and then assigning users as members of the group(s). Groups are assigned Platform permissions to specific SupportSoft web interfaces and components, which allow different components to be available to different groups of users.

The TOE includes predefined groups which already have Platform permissions set. The TOE includes the following predefined example groups which implement roles. (This is not the complete set of predefined groups.)

Administrators	This group has the permissions necessary to fully administer the TOE, which includes creating and editing users and groups, configuring permissions, importing and exporting content, and scheduling and distributing reports. This group is used to implement the Administrator role.
Approvers	This group has the permissions necessary to approve content using the Author Center application content approval process and publish content. This group is used to implement the Approver role.
Authors	This group has the permissions necessary to create support content in the Author Center application. This group is used to implement the Author role.
Supervisors	This group has the permissions needed to manage support analyst message boards within Support Center. This group is one of the groups that implement the Support Analyst role.
Tier 1 Analysts	This is a sample Tier 1 support analyst group with permissions to find solutions using Support Center. This group is one of the groups that implement the Support Analyst role.
Tier 2 Analysts	This is a sample Tier 2 support analyst group with permissions to find and contribute solutions using Support Center. This group is one of the groups that implement the Support Analyst role.
Guests	Anonymous users are assigned the guest user id which is a member of the Guests group by default. By default, the Guests group only has access to perform the functions available on the User Center home page, which provides the ability to search, but not browse. Users in this group are a type of end user and are considered to be in the “users assigned permissions via group membership” role.

The Support Analyst role represents users with the permission to use the Support Center interface who cannot author content, approve content, manage content or use the SA interface to administer the TOE.

Users in the Administrators group can configure their own groups with different Platform permissions. Users in these custom groups are considered to be in the "users assigned permissions via group membership" role.

An administrator could change the Platform permissions assigned to any of the groups. Administrator guidance instructs the administrator to not delete permissions from the Administrator and to not modify the permissions associated with the Approver, Author, and Guests groups.

6.1.5 Protection of TOE functions

The TOE provides protection for itself from untrusted subjects and from subjects attempting to bypass the TSF. In addition, it provides the ability to terminate interactive sessions which have been inactive for an administrator defined period of time. The protections are described in more detail below.

Non-bypassability of the TSP: FPT_RVM_EXP.1

The TOE protects its management functions by isolating them through identification and authentication of administrative users. In addition, the role enforcement and Platform permissions enforced by the TOE ensure that administrative users are only allowed access to the management functions for which they are authorized Administration guidance instructs the administrator to limit the Platform permissions assigned to the Guests group when the TOE is configured to allow anonymous users.

The IT environment also supports non-bypassability by ensuring that its security functions cannot be bypassed.

TSF Domain Separation: FPT_SEP_EXP.1

The external interfaces to the TOE ensure that users must login prior to accessing administrative TOE functions and resources. In addition, the external interfaces to the TOE ensure that users must login prior to accessing other TOE resources, unless the TOE is configured to allow anonymous access. Anonymous users interact with the TSF using the anonymous user account which is a member of the Guests group. Administration guidance instructs the administrative users to limit the Platform permissions assigned to the Guests group when the TOE is configured to allow anonymous users. The TOE maintains a separate session for each interaction with the TOE. Protection of the TOE from physical and logical tampering from other methods is ensured by the physical security assumptions and by the domain separation requirements on the hardware and operating system in the environment.

6.2 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 6.1.

	Access Control	Identification & Authentication	Audit	Security Management	Protection of TOE functions
FAU_GEN_EXP.1			X		
FAU_GEN.2			X		
FAU_SAR.1a			X		
FAU_SAR.1b			X		
FAU_SAR.2			X		
FIA_AFL.1		X			
FIA_ATD.1		X			
FIA_SOS.1		X			
FIA_UAU_EXP.2		X			
FIA_UID_EXP.2		X			
FMT_MOF.1				X	
FMT_MSA.1				X	
FMT_MSA.3				X	
FMT_MTD.1a FMT_MTD.1b FMT_MTD.1c				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FDP_ACC_EXP.1	X				
FDP_ACF_EXP.1	X				
FPT_SEP_EXP.1					X
FPT_RVM_EXP.1					X

Table 16 – TOE Security Function to SFR Mapping

6.3 Appropriate Strength of Function Claim

The claim of SOF-basic for the Identification and Authentication security function is consistent with the claim of SOF-basic for the FIA_UAU_EXP.2 and FIA_SOS.1 SFRs that map to that security function.

6.4 Security Assurance Measures and Rationale

The assurance measure documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

The documentation titles in the table below will be updated with new titles and version numbers

during the course of the evaluation.

Assurance Requirement	Assurance Measures	Assurance Rationale
ACM_CAP.2	*SupportSoft EAL2 Configuration Management Document*	The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.
ADO_DEL.1	*SupportSoft EAL2 Delivery Procedures*	The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer.
ADO_IGS.1	*SupportSoft Installation and Administration Supplemental CC Guidance* *SupportSoft Platform v6.5 SP4 and Product Installation Guide (Updated September 23, 2005)* *SupportSoft Platform Version 6.5 Service Pack 04 Release Notes (Updated July 8, 2005)* *SupportSoft Knowledge Center Version 6.5 Service Pack 1 Release Notes*	The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.1	*SupportSoft, Inc. KC Suite Version 6.5 EAL 2 Design Documentation*	This document includes the informal functional specification which identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.
ADV_HLD.1	*SupportSoft, Inc. KC Suite Version 6.5 EAL 2 Design Documentation*	This document includes the descriptive high-level design which describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
ADV_RCR.1	*SupportSoft, Inc. KC Suite Version 6.5 EAL 2 Design Documentation*	This document includes the informal correspondence document which maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.

Assurance Requirement	Assurance Measures	Assurance Rationale
AGD_ADM.1	*SupportSoft Installation and Administration Supplemental CC Guidance* *SupportSoft Platform Version 6.5 Service Pack 4 Administrator's Guide (Updated October 20, 2005)* *SupportSoft Platform Version 6.5 Service Pack 04 Release Notes (Updated July 8, 2005)* *SupportSoft Content Administration Guide (Applies to All v6.5 SP1 or Higher products that include Content) (Updated September 29, 2005)* *SupportSoft Knowledge Center Version 6.5 Service Pack 1 Release Notes* *Support Administrator Help System, installed with the product* *Support Center Help System, installed with the product* *Author Center Help System, installed with the product*	The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	*SupportSoft User Supplemental CC Guidance* *SupportSoft Content Administration Guide (Applies to All v6.5 or Higher Products that include Content) (Updated September 29, 2005)*	The user guidance describes the security functions and interfaces in a way that allows a user to interact with the TOE securely.
ATE_COV.1	*SupportSoft EAL2 Test Plan and Procedures*	The test coverage document provides a mapping of the test cases performed against the TSF.
ATE_FUN.1	*SupportSoft EAL2 Test Plan and Procedures*	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	*SupportSoft Platform Version 6.5 SP4 and SupportSoft Knowledge Center Suite Version 6.5 SP1* All documents listed above as satisfying AGD_ADM.1, AGD_USR.1, and ATE_FUN.1.	The TOE software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.

Assurance Requirement	Assurance Measures	Assurance Rationale
AVA_SOF.1	*SupportSoft Strength of Function Analysis*	The strength of function analysis document provides the SOF argument for the password mechanism.
AVA_VLA.1	*SupportSoft Vulnerability Analysis*	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Table 17 – Assurance Requirements: EAL2

7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

8 Rationale

This Security Target does not claim conformance to any Protection Profiles.

8.1 Security Objectives Rationale

Sections 4.4 - 4.6 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.7 - 5.12 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.2 - 6.4 provide the TOE summary specification rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles.

9 Appendix A: KC Access Levels and Functions

This appendix lists all of the KC access levels (defined sets of KC permissions) that administrators may assign to folders and contribution content types within Knowledge Center. These access levels only apply to access attempts made from the AC interface. As is shown below, each content type has its own set of possible permissions (also called functions). A permission/function defines the operation to be performed on the content item from the AC interface.

KC_AccessLevel	KC_ContentType	KC_Functions
Full-Control	Contribution	Implement
Full-Control	Contribution	Notify
Full-Control	Contribution	Reject
Full-Control	Folder	Associate Workflow
Full-Control	Folder	Copy Content
Full-Control	Folder	Cut Content
Full-Control	Folder	Delete Content
Full-Control	Folder	Delete Folder
Full-Control	Folder	Expire Content
Full-Control	Folder	Export
Full-Control	Folder	Folder Info
Full-Control	Folder	New
Full-Control	Folder	New Folder
Full-Control	Folder	Paste Content
Full-Control	Folder	Paste Shortcut
Full-Control	Folder	Personalize
Full-Control	Folder	Rename Folder
Full-Control	Folder	Restore Content
Full-Control	Folder	Restore Folder
Full-Control	Folder	Security
Full-Control	Folder	Set Attributes
Full-Control	Folder	Unlock Content
Full-Control	Folder	Unpublish Content
Full-Control	Resource	Approve Resource
Full-Control	Resource	Audit Trail
Full-Control	Resource	Delete Latest Version
Full-Control	Resource	Edit Properties
Full-Control	Resource	Edit Resource
Full-Control	Resource	New Resource

KC_AccessLevel	KC_ContentType	KC_Functions
Full-Control	Resource	Notify
Full-Control	Resource	Personalize
Full-Control	Resource	Preview Resource
Full-Control	Resource	Read Only Mode
Full-Control	Resource	Recall
Full-Control	Resource	Reject Resource
Full-Control	Resource	Resource Info
Full-Control	Resource	Save Resource
Full-Control	Resource	Statistics
Full-Control	Resource	Submit for Approval
Full-Control	Resource	View Feedback
Full-Control	Resource	View Resource
Full-Control	Resource	Workflow Status
Full-Control	Script SupportAction	Admin Weight
Full-Control	Script SupportAction	Approve Action
Full-Control	Script SupportAction	Audit Trail
Full-Control	Script SupportAction	Content Info
Full-Control	Script SupportAction	Delete Latest Version
Full-Control	Script SupportAction	Edit Action
Full-Control	Script SupportAction	Edit Properties
Full-Control	Script SupportAction	New Action
Full-Control	Script SupportAction	Notify
Full-Control	Script SupportAction	Personalize
Full-Control	Script SupportAction	Preview Action
Full-Control	Script SupportAction	Read Only Mode
Full-Control	Script SupportAction	Recall
Full-Control	Script SupportAction	Reject Action
Full-Control	Script SupportAction	Save Action
Full-Control	Script SupportAction	Statistics
Full-Control	Script SupportAction	Submit for Approval
Full-Control	Script SupportAction	View Action
Full-Control	Script SupportAction	View Feedback
Full-Control	Script SupportAction	Workflow Status
Full-Control	Shortcut	Admin Weight
Full-Control	Shortcut	Approve Shortcut

KC_AccessLevel	KC_ContentType	KC_Functions
Full-Control	Shortcut	Audit Trail
Full-Control	Shortcut	Content Info
Full-Control	Shortcut	Delete Latest Version
Full-Control	Shortcut	Edit Properties
Full-Control	Shortcut	Edit Shortcut
Full-Control	Shortcut	New Shortcut
Full-Control	Shortcut	Notify
Full-Control	Shortcut	Personalize
Full-Control	Shortcut	Preview Shortcut
Full-Control	Shortcut	Read Only Mode
Full-Control	Shortcut	Recall
Full-Control	Shortcut	Reject Shortcut
Full-Control	Shortcut	Save Shortcut
Full-Control	Shortcut	Statistics
Full-Control	Shortcut	Submit for Approval
Full-Control	Shortcut	View Feedback
Full-Control	Shortcut	View Shortcut
Full-Control	Shortcut	Workflow Status
Full-Control	SupportArticle - Document	Admin Weight
Full-Control	SupportArticle - Document	Approve Article
Full-Control	SupportArticle - Document	Audit Trail
Full-Control	SupportArticle - Document	Content Info
Full-Control	SupportArticle - Document	Delete Latest Version
Full-Control	SupportArticle - Document	Edit Article
Full-Control	SupportArticle - Document	Edit Properties
Full-Control	SupportArticle - Document	New Article
Full-Control	SupportArticle - Document	Notify
Full-Control	SupportArticle - Document	Personalize
Full-Control	SupportArticle - Document	Preview Article
Full-Control	SupportArticle - Document	Read Only Mode
Full-Control	SupportArticle - Document	Recall
Full-Control	SupportArticle - Document	Reject Article
Full-Control	SupportArticle - Document	Save Article
Full-Control	SupportArticle - Document	Statistics
Full-Control	SupportArticle - Document	Submit for Approval

KC_AccessLevel	KC_ContentType	KC_Functions
Full-Control	SupportArticle - Document	View Article
Full-Control	SupportArticle - Document	View Feedback
Full-Control	SupportArticle - Document	Workflow Status
Full-Control	SupportArticle - FAQ	Admin Weight
Full-Control	SupportArticle - FAQ	Approve Article
Full-Control	SupportArticle - FAQ	Audit Trail
Full-Control	SupportArticle - FAQ	Content Info
Full-Control	SupportArticle - FAQ	Delete Latest Version
Full-Control	SupportArticle - FAQ	Edit Article
Full-Control	SupportArticle - FAQ	Edit Properties
Full-Control	SupportArticle - FAQ	New Article
Full-Control	SupportArticle - FAQ	Notify
Full-Control	SupportArticle - FAQ	Personalize
Full-Control	SupportArticle - FAQ	Preview Article
Full-Control	SupportArticle - FAQ	Read Only Mode
Full-Control	SupportArticle - FAQ	Recall
Full-Control	SupportArticle - FAQ	Reject Article
Full-Control	SupportArticle - FAQ	Save Article
Full-Control	SupportArticle - FAQ	Statistics
Full-Control	SupportArticle - FAQ	Submit for Approval
Full-Control	SupportArticle - FAQ	View Article
Full-Control	SupportArticle - FAQ	View Feedback
Full-Control	SupportArticle - FAQ	Workflow Status
Full-Control	SupportArticle - Inline Document	Admin Weight
Full-Control	SupportArticle - Inline Document	Approve Article
Full-Control	SupportArticle - Inline Document	Audit Trail
Full-Control	SupportArticle - Inline Document	Content Info
Full-Control	SupportArticle - Inline Document	Delete Latest Version
Full-Control	SupportArticle - Inline Document	Edit Article
Full-Control	SupportArticle - Inline Document	Edit Properties
Full-Control	SupportArticle - Inline Document	New Article
Full-Control	SupportArticle - Inline Document	Notify
Full-Control	SupportArticle - Inline Document	Personalize
Full-Control	SupportArticle - Inline Document	Preview Article
Full-Control	SupportArticle - Inline Document	Read Only Mode

KC_AccessLevel	KC_ContentType	KC_Functions
Full-Control	SupportArticle - Inline Document	Recall
Full-Control	SupportArticle - Inline Document	Reject Article
Full-Control	SupportArticle - Inline Document	Save Article
Full-Control	SupportArticle - Inline Document	Statistics
Full-Control	SupportArticle - Inline Document	Submit for Approval
Full-Control	SupportArticle - Inline Document	View Article
Full-Control	SupportArticle - Inline Document	View Feedback
Full-Control	SupportArticle - Inline Document	Workflow Status
Full-Control	SupportArticle - Problem Resolution	Admin Weight
Full-Control	SupportArticle - Problem Resolution	Approve Article
Full-Control	SupportArticle - Problem Resolution	Audit Trail
Full-Control	SupportArticle - Problem Resolution	Content Info
Full-Control	SupportArticle - Problem Resolution	Delete Latest Version
Full-Control	SupportArticle - Problem Resolution	Edit Article
Full-Control	SupportArticle - Problem Resolution	Edit Properties
Full-Control	SupportArticle - Problem Resolution	New Article
Full-Control	SupportArticle - Problem Resolution	Notify
Full-Control	SupportArticle - Problem Resolution	Personalize
Full-Control	SupportArticle - Problem Resolution	Preview Article
Full-Control	SupportArticle - Problem Resolution	Read Only Mode
Full-Control	SupportArticle - Problem Resolution	Recall
Full-Control	SupportArticle - Problem Resolution	Reject Article
Full-Control	SupportArticle - Problem Resolution	Save Article
Full-Control	SupportArticle - Problem Resolution	Statistics
Full-Control	SupportArticle - Problem Resolution	Submit for Approval
Full-Control	SupportArticle - Problem Resolution	View Article
Full-Control	SupportArticle - Problem Resolution	View Feedback
Full-Control	SupportArticle - Problem Resolution	Workflow Status
Full-Control	SupportArticle - URL	Admin Weight
Full-Control	SupportArticle - URL	Approve Article
Full-Control	SupportArticle - URL	Audit Trail
Full-Control	SupportArticle - URL	Content Info
Full-Control	SupportArticle - URL	Delete Latest Version
Full-Control	SupportArticle - URL	Edit Article
Full-Control	SupportArticle - URL	Edit Properties

KC_AccessLevel	KC_ContentType	KC_Functions
Full-Control	SupportArticle - URL	New Article
Full-Control	SupportArticle - URL	Notify
Full-Control	SupportArticle - URL	Personalize
Full-Control	SupportArticle - URL	Preview Article
Full-Control	SupportArticle - URL	Read Only Mode
Full-Control	SupportArticle - URL	Recall
Full-Control	SupportArticle - URL	Reject Article
Full-Control	SupportArticle - URL	Save Article
Full-Control	SupportArticle - URL	Statistics
Full-Control	SupportArticle - URL	Submit for Approval
Full-Control	SupportArticle - URL	View Article
Full-Control	SupportArticle - URL	View Feedback
Full-Control	SupportArticle - URL	Workflow Status
Full-Control	Web Document	Admin Weight
Full-Control	Web Document	Content Info
Full-Control	Web Document	Delete Latest Version
Full-Control	Web Document	Edit Properties
Full-Control	Web Document	Notify
Full-Control	Web Document	Personalize
Full-Control	Web Document	Preview Content
Full-Control	Web Document	Read Only Mode
Full-Control	Web Document	Statistics
Full-Control	Web Document	View Article
Full-Control	Web Document	View Feedback
Manage	Contribution	Implement
Manage	Contribution	Notify
Manage	Contribution	Reject
Manage	Folder	Associate Workflow
Manage	Folder	Copy Content
Manage	Folder	Cut Content
Manage	Folder	Delete Content
Manage	Folder	Delete Folder
Manage	Folder	Folder Info
Manage	Folder	New
Manage	Folder	New Folder

KC_AccessLevel	KC_ContentType	KC_Functions
Manage	Folder	Paste Content
Manage	Folder	Personalize
Manage	Folder	Rename Folder
Manage	Folder	Unlock Content
Manage	Resource	Approve Resource
Manage	Resource	Audit Trail
Manage	Resource	Edit Properties
Manage	Resource	Edit Resource
Manage	Resource	New Resource
Manage	Resource	Notify
Manage	Resource	Personalize
Manage	Resource	Preview Resource
Manage	Resource	Read Only Mode
Manage	Resource	Reject Resource
Manage	Resource	Resource Info
Manage	Resource	Save Resource
Manage	Resource	Statistics
Manage	Resource	Submit for Approval
Manage	Resource	View Feedback
Manage	Resource	View Resource
Manage	Resource	Workflow Status
Manage	Script SupportAction	Approve Action
Manage	Script SupportAction	Audit Trail
Manage	Script SupportAction	Content Info
Manage	Script SupportAction	Edit Action
Manage	Script SupportAction	Edit Properties
Manage	Script SupportAction	New Action
Manage	Script SupportAction	Notify
Manage	Script SupportAction	Personalize
Manage	Script SupportAction	Preview Action
Manage	Script SupportAction	Read Only Mode
Manage	Script SupportAction	Reject Action
Manage	Script SupportAction	Save Action
Manage	Script SupportAction	Statistics
Manage	Script SupportAction	Submit for Approval

KC_AccessLevel	KC_ContentType	KC_Functions
Manage	Script SupportAction	View Action
Manage	Script SupportAction	View Feedback
Manage	Script SupportAction	Workflow Status
Manage	Shortcut	Approve Shortcut
Manage	Shortcut	Audit Trail
Manage	Shortcut	Content Info
Manage	Shortcut	Edit Properties
Manage	Shortcut	Edit Shortcut
Manage	Shortcut	New Shortcut
Manage	Shortcut	Notify
Manage	Shortcut	Personalize
Manage	Shortcut	Preview Shortcut
Manage	Shortcut	Read Only Mode
Manage	Shortcut	Reject Shortcut
Manage	Shortcut	Save Shortcut
Manage	Shortcut	Statistics
Manage	Shortcut	Submit for Approval
Manage	Shortcut	View Feedback
Manage	Shortcut	View Shortcut
Manage	Shortcut	Workflow Status
Manage	SupportArticle - Document	Approve Article
Manage	SupportArticle - Document	Audit Trail
Manage	SupportArticle - Document	Content Info
Manage	SupportArticle - Document	Edit Article
Manage	SupportArticle - Document	Edit Properties
Manage	SupportArticle - Document	New Article
Manage	SupportArticle - Document	Notify
Manage	SupportArticle - Document	Personalize
Manage	SupportArticle - Document	Preview Article
Manage	SupportArticle - Document	Read Only Mode
Manage	SupportArticle - Document	Reject Article
Manage	SupportArticle - Document	Save Article
Manage	SupportArticle - Document	Statistics
Manage	SupportArticle - Document	Submit for Approval
Manage	SupportArticle - Document	View Article

KC_AccessLevel	KC_ContentType	KC_Functions
Manage	SupportArticle - Document	View Feedback
Manage	SupportArticle - Document	Workflow Status
Manage	SupportArticle - FAQ	Approve Article
Manage	SupportArticle - FAQ	Audit Trail
Manage	SupportArticle - FAQ	Content Info
Manage	SupportArticle - FAQ	Edit Article
Manage	SupportArticle - FAQ	Edit Properties
Manage	SupportArticle - FAQ	New Article
Manage	SupportArticle - FAQ	Notify
Manage	SupportArticle - FAQ	Personalize
Manage	SupportArticle - FAQ	Preview Article
Manage	SupportArticle - FAQ	Read Only Mode
Manage	SupportArticle - FAQ	Reject Article
Manage	SupportArticle - FAQ	Save Article
Manage	SupportArticle - FAQ	Statistics
Manage	SupportArticle - FAQ	Submit for Approval
Manage	SupportArticle - FAQ	View Article
Manage	SupportArticle - FAQ	View Feedback
Manage	SupportArticle - FAQ	Workflow Status
Manage	SupportArticle - Inline Document	Approve Article
Manage	SupportArticle - Inline Document	Audit Trail
Manage	SupportArticle - Inline Document	Content Info
Manage	SupportArticle - Inline Document	Edit Article
Manage	SupportArticle - Inline Document	Edit Properties
Manage	SupportArticle - Inline Document	New Article
Manage	SupportArticle - Inline Document	Notify
Manage	SupportArticle - Inline Document	Personalize
Manage	SupportArticle - Inline Document	Preview Article
Manage	SupportArticle - Inline Document	Read Only Mode
Manage	SupportArticle - Inline Document	Reject Article
Manage	SupportArticle - Inline Document	Save Article
Manage	SupportArticle - Inline Document	Statistics
Manage	SupportArticle - Inline Document	Submit for Approval
Manage	SupportArticle - Inline Document	View Article
Manage	SupportArticle - Inline Document	View Feedback

KC_AccessLevel	KC_ContentType	KC_Functions
Manage	SupportArticle - Inline Document	Workflow Status
Manage	SupportArticle - Problem Resolution	Approve Article
Manage	SupportArticle - Problem Resolution	Audit Trail
Manage	SupportArticle - Problem Resolution	Content Info
Manage	SupportArticle - Problem Resolution	Edit Article
Manage	SupportArticle - Problem Resolution	Edit Properties
Manage	SupportArticle - Problem Resolution	New Article
Manage	SupportArticle - Problem Resolution	Notify
Manage	SupportArticle - Problem Resolution	Personalize
Manage	SupportArticle - Problem Resolution	Preview Article
Manage	SupportArticle - Problem Resolution	Read Only Mode
Manage	SupportArticle - Problem Resolution	Reject Article
Manage	SupportArticle - Problem Resolution	Save Article
Manage	SupportArticle - Problem Resolution	Statistics
Manage	SupportArticle - Problem Resolution	Submit for Approval
Manage	SupportArticle - Problem Resolution	View Article
Manage	SupportArticle - Problem Resolution	View Feedback
Manage	SupportArticle - Problem Resolution	Workflow Status
Manage	SupportArticle - URL	Approve Article
Manage	SupportArticle - URL	Audit Trail
Manage	SupportArticle - URL	Content Info
Manage	SupportArticle - URL	Edit Article
Manage	SupportArticle - URL	Edit Properties
Manage	SupportArticle - URL	New Article
Manage	SupportArticle - URL	Notify
Manage	SupportArticle - URL	Personalize
Manage	SupportArticle - URL	Preview Article
Manage	SupportArticle - URL	Read Only Mode
Manage	SupportArticle - URL	Reject Article
Manage	SupportArticle - URL	Save Article
Manage	SupportArticle - URL	Statistics
Manage	SupportArticle - URL	Submit for Approval
Manage	SupportArticle - URL	View Article
Manage	SupportArticle - URL	View Feedback
Manage	SupportArticle - URL	Workflow Status

KC_AccessLevel	KC_ContentType	KC_Functions
Manage	Web Document	Content Info
Manage	Web Document	Edit Properties
Manage	Web Document	Notify
Manage	Web Document	Personalize
Manage	Web Document	Preview Content
Manage	Web Document	Read Only Mode
Manage	Web Document	Statistics
Manage	Web Document	View Article
Manage	Web Document	View Feedback
Read	Folder	Folder Info
Read	Resource	Preview Resource
Read	Resource	Read Only Mode
Read	Resource	Resource Info
Read	Resource	View Resource
Read	Script SupportAction	Content Info
Read	Script SupportAction	Preview Action
Read	Script SupportAction	Read Only Mode
Read	Script SupportAction	View Action
Read	Shortcut	Content Info
Read	Shortcut	Preview Shortcut
Read	Shortcut	Read Only Mode
Read	Shortcut	View Shortcut
Read	SupportArticle - Document	Content Info
Read	SupportArticle - Document	Preview Article
Read	SupportArticle - Document	Read Only Mode
Read	SupportArticle - Document	View Article
Read	SupportArticle - FAQ	Content Info
Read	SupportArticle - FAQ	Preview Article
Read	SupportArticle - FAQ	Read Only Mode
Read	SupportArticle - FAQ	View Article
Read	SupportArticle - Inline Document	Content Info
Read	SupportArticle - Inline Document	Preview Article
Read	SupportArticle - Inline Document	Read Only Mode
Read	SupportArticle - Inline Document	View Article
Read	SupportArticle - Problem Resolution	Content Info

KC_AccessLevel	KC_ContentType	KC_Functions
Read	SupportArticle - Problem Resolution	Preview Article
Read	SupportArticle - Problem Resolution	Read Only Mode
Read	SupportArticle - Problem Resolution	View Article
Read	SupportArticle - URL	Content Info
Read	SupportArticle - URL	Preview Article
Read	SupportArticle - URL	Read Only Mode
Read	SupportArticle - URL	View Article
Read	Web Document	Content Info
Read	Web Document	Preview Content
Read	Web Document	Read Only Mode
Read	Web Document	View Article
Read/Review	Contribution	Reject
Read/Review	Folder	Copy Content
Read/Review	Folder	Folder Info
Read/Review	Folder	Paste Content
Read/Review	Resource	Approve Resource
Read/Review	Resource	Audit Trail
Read/Review	Resource	Edit Properties
Read/Review	Resource	Edit Resource
Read/Review	Resource	Personalize
Read/Review	Resource	Preview Resource
Read/Review	Resource	Read Only Mode
Read/Review	Resource	Reject Resource
Read/Review	Resource	Resource Info
Read/Review	Resource	Submit for Approval
Read/Review	Resource	View Resource
Read/Review	Resource	Workflow Status
Read/Review	Script SupportAction	Approve Action
Read/Review	Script SupportAction	Audit Trail
Read/Review	Script SupportAction	Content Info
Read/Review	Script SupportAction	Edit Action
Read/Review	Script SupportAction	Edit Properties
Read/Review	Script SupportAction	Personalize
Read/Review	Script SupportAction	Preview Action
Read/Review	Script SupportAction	Read Only Mode

KC_AccessLevel	KC_ContentType	KC_Functions
Read/Review	Script SupportAction	Reject Action
Read/Review	Script SupportAction	Submit for Approval
Read/Review	Script SupportAction	View Action
Read/Review	Script SupportAction	Workflow Status
Read/Review	Shortcut	Approve Shortcut
Read/Review	Shortcut	Audit Trail
Read/Review	Shortcut	Content Info
Read/Review	Shortcut	Edit Properties
Read/Review	Shortcut	Edit Shortcut
Read/Review	Shortcut	Personalize
Read/Review	Shortcut	Preview Shortcut
Read/Review	Shortcut	Read Only Mode
Read/Review	Shortcut	Reject Shortcut
Read/Review	Shortcut	Submit for Approval
Read/Review	Shortcut	View Shortcut
Read/Review	Shortcut	Workflow Status
Read/Review	SupportArticle - Document	Approve Article
Read/Review	SupportArticle - Document	Audit Trail
Read/Review	SupportArticle - Document	Content Info
Read/Review	SupportArticle - Document	Edit Article
Read/Review	SupportArticle - Document	Edit Properties
Read/Review	SupportArticle - Document	Personalize
Read/Review	SupportArticle - Document	Preview Article
Read/Review	SupportArticle - Document	Read Only Mode
Read/Review	SupportArticle - Document	Reject Article
Read/Review	SupportArticle - Document	Submit for Approval
Read/Review	SupportArticle - Document	View Article
Read/Review	SupportArticle - Document	Workflow Status
Read/Review	SupportArticle - FAQ	Approve Article
Read/Review	SupportArticle - FAQ	Audit Trail
Read/Review	SupportArticle - FAQ	Content Info
Read/Review	SupportArticle - FAQ	Edit Article
Read/Review	SupportArticle - FAQ	Edit Properties
Read/Review	SupportArticle - FAQ	Personalize
Read/Review	SupportArticle - FAQ	Preview Article

KC_AccessLevel	KC_ContentType	KC_Functions
Read/Review	SupportArticle - FAQ	Read Only Mode
Read/Review	SupportArticle - FAQ	Reject Article
Read/Review	SupportArticle - FAQ	Submit for Approval
Read/Review	SupportArticle - FAQ	View Article
Read/Review	SupportArticle - FAQ	Workflow Status
Read/Review	SupportArticle - Inline Document	Approve Article
Read/Review	SupportArticle - Inline Document	Audit Trail
Read/Review	SupportArticle - Inline Document	Content Info
Read/Review	SupportArticle - Inline Document	Edit Article
Read/Review	SupportArticle - Inline Document	Edit Properties
Read/Review	SupportArticle - Inline Document	Personalize
Read/Review	SupportArticle - Inline Document	Preview Article
Read/Review	SupportArticle - Inline Document	Read Only Mode
Read/Review	SupportArticle - Inline Document	Reject Article
Read/Review	SupportArticle - Inline Document	Submit for Approval
Read/Review	SupportArticle - Inline Document	View Article
Read/Review	SupportArticle - Inline Document	Workflow Status
Read/Review	SupportArticle - Problem Resolution	Approve Article
Read/Review	SupportArticle - Problem Resolution	Audit Trail
Read/Review	SupportArticle - Problem Resolution	Content Info
Read/Review	SupportArticle - Problem Resolution	Edit Article
Read/Review	SupportArticle - Problem Resolution	Edit Properties
Read/Review	SupportArticle - Problem Resolution	Personalize
Read/Review	SupportArticle - Problem Resolution	Preview Article
Read/Review	SupportArticle - Problem Resolution	Read Only Mode
Read/Review	SupportArticle - Problem Resolution	Reject Article
Read/Review	SupportArticle - Problem Resolution	Submit for Approval
Read/Review	SupportArticle - Problem Resolution	View Article
Read/Review	SupportArticle - Problem Resolution	Workflow Status
Read/Review	SupportArticle - URL	Approve Article
Read/Review	SupportArticle - URL	Audit Trail
Read/Review	SupportArticle - URL	Content Info
Read/Review	SupportArticle - URL	Edit Article
Read/Review	SupportArticle - URL	Edit Properties
Read/Review	SupportArticle - URL	Personalize

KC_AccessLevel	KC_ContentType	KC_Functions
Read/Review	SupportArticle - URL	Preview Article
Read/Review	SupportArticle - URL	Read Only Mode
Read/Review	SupportArticle - URL	Reject Article
Read/Review	SupportArticle - URL	Submit for Approval
Read/Review	SupportArticle - URL	View Article
Read/Review	SupportArticle - URL	Workflow Status
Read/Review	Web Document	Content Info
Read/Review	Web Document	Edit Properties
Read/Review	Web Document	Personalize
Read/Review	Web Document	Preview Content
Read/Review	Web Document	Read Only Mode
Read/Review	Web Document	View Article
Read/Write	Contribution	Implement
Read/Write	Contribution	Notify
Read/Write	Contribution	Reject
Read/Write	Folder	Associate Workflow
Read/Write	Folder	Copy Content
Read/Write	Folder	Folder Info
Read/Write	Folder	New
Read/Write	Folder	New Folder
Read/Write	Folder	Paste Content
Read/Write	Folder	Personalize
Read/Write	Folder	Rename Folder
Read/Write	Resource	Approve Resource
Read/Write	Resource	Audit Trail
Read/Write	Resource	Edit Properties
Read/Write	Resource	Edit Resource
Read/Write	Resource	New Resource
Read/Write	Resource	Notify
Read/Write	Resource	Personalize
Read/Write	Resource	Preview Resource
Read/Write	Resource	Read Only Mode
Read/Write	Resource	Reject Resource
Read/Write	Resource	Resource Info
Read/Write	Resource	Save Resource

KC_AccessLevel	KC_ContentType	KC_Functions
Read/Write	Resource	Statistics
Read/Write	Resource	Submit for Approval
Read/Write	Resource	View Feedback
Read/Write	Resource	View Resource
Read/Write	Script SupportAction	Approve Action
Read/Write	Script SupportAction	Audit Trail
Read/Write	Script SupportAction	Content Info
Read/Write	Script SupportAction	Edit Action
Read/Write	Script SupportAction	Edit Properties
Read/Write	Script SupportAction	New Action
Read/Write	Script SupportAction	Notify
Read/Write	Script SupportAction	Personalize
Read/Write	Script SupportAction	Preview Action
Read/Write	Script SupportAction	Read Only Mode
Read/Write	Script SupportAction	Reject Action
Read/Write	Script SupportAction	Save Action
Read/Write	Script SupportAction	Statistics
Read/Write	Script SupportAction	Submit for Approval
Read/Write	Script SupportAction	View Action
Read/Write	Script SupportAction	View Feedback
Read/Write	Shortcut	Approve Shortcut
Read/Write	Shortcut	Audit Trail
Read/Write	Shortcut	Content Info
Read/Write	Shortcut	Edit Properties
Read/Write	Shortcut	Edit Shortcut
Read/Write	Shortcut	New Shortcut
Read/Write	Shortcut	Notify
Read/Write	Shortcut	Personalize
Read/Write	Shortcut	Preview Shortcut
Read/Write	Shortcut	Read Only Mode
Read/Write	Shortcut	Reject Shortcut
Read/Write	Shortcut	Save Shortcut
Read/Write	Shortcut	Statistics
Read/Write	Shortcut	Submit for Approval
Read/Write	Shortcut	View Feedback

KC_AccessLevel	KC_ContentType	KC_Functions
Read/Write	Shortcut	View Shortcut
Read/Write	SupportArticle - Document	Approve Article
Read/Write	SupportArticle - Document	Audit Trail
Read/Write	SupportArticle - Document	Content Info
Read/Write	SupportArticle - Document	Edit Article
Read/Write	SupportArticle - Document	Edit Properties
Read/Write	SupportArticle - Document	New Article
Read/Write	SupportArticle - Document	Notify
Read/Write	SupportArticle - Document	Personalize
Read/Write	SupportArticle - Document	Preview Article
Read/Write	SupportArticle - Document	Read Only Mode
Read/Write	SupportArticle - Document	Reject Article
Read/Write	SupportArticle - Document	Save Article
Read/Write	SupportArticle - Document	Statistics
Read/Write	SupportArticle - Document	Submit for Approval
Read/Write	SupportArticle - Document	View Article
Read/Write	SupportArticle - Document	View Feedback
Read/Write	SupportArticle - FAQ	Approve Article
Read/Write	SupportArticle - FAQ	Audit Trail
Read/Write	SupportArticle - FAQ	Content Info
Read/Write	SupportArticle - FAQ	Edit Article
Read/Write	SupportArticle - FAQ	Edit Properties
Read/Write	SupportArticle - FAQ	New Article
Read/Write	SupportArticle - FAQ	Notify
Read/Write	SupportArticle - FAQ	Personalize
Read/Write	SupportArticle - FAQ	Preview Article
Read/Write	SupportArticle - FAQ	Read Only Mode
Read/Write	SupportArticle - FAQ	Reject Article
Read/Write	SupportArticle - FAQ	Save Article
Read/Write	SupportArticle - FAQ	Statistics
Read/Write	SupportArticle - FAQ	Submit for Approval
Read/Write	SupportArticle - FAQ	View Article
Read/Write	SupportArticle - FAQ	View Feedback
Read/Write	SupportArticle - Inline Document	Approve Article
Read/Write	SupportArticle - Inline Document	Audit Trail

KC_AccessLevel	KC_ContentType	KC_Functions
Read/Write	SupportArticle - Inline Document	Content Info
Read/Write	SupportArticle - Inline Document	Edit Article
Read/Write	SupportArticle - Inline Document	Edit Properties
Read/Write	SupportArticle - Inline Document	New Article
Read/Write	SupportArticle - Inline Document	Notify
Read/Write	SupportArticle - Inline Document	Personalize
Read/Write	SupportArticle - Inline Document	Preview Article
Read/Write	SupportArticle - Inline Document	Read Only Mode
Read/Write	SupportArticle - Inline Document	Reject Article
Read/Write	SupportArticle - Inline Document	Save Article
Read/Write	SupportArticle - Inline Document	Statistics
Read/Write	SupportArticle - Inline Document	Submit for Approval
Read/Write	SupportArticle - Inline Document	View Article
Read/Write	SupportArticle - Inline Document	View Feedback
Read/Write	SupportArticle - Problem Resolution	Approve Article
Read/Write	SupportArticle - Problem Resolution	Audit Trail
Read/Write	SupportArticle - Problem Resolution	Content Info
Read/Write	SupportArticle - Problem Resolution	Edit Article
Read/Write	SupportArticle - Problem Resolution	Edit Properties
Read/Write	SupportArticle - Problem Resolution	New Article
Read/Write	SupportArticle - Problem Resolution	Notify
Read/Write	SupportArticle - Problem Resolution	Personalize
Read/Write	SupportArticle - Problem Resolution	Preview Article
Read/Write	SupportArticle - Problem Resolution	Read Only Mode
Read/Write	SupportArticle - Problem Resolution	Reject Article
Read/Write	SupportArticle - Problem Resolution	Save Article
Read/Write	SupportArticle - Problem Resolution	Statistics
Read/Write	SupportArticle - Problem Resolution	Submit for Approval
Read/Write	SupportArticle - Problem Resolution	View Article
Read/Write	SupportArticle - Problem Resolution	View Feedback
Read/Write	SupportArticle - URL	Approve Article
Read/Write	SupportArticle - URL	Audit Trail
Read/Write	SupportArticle - URL	Content Info
Read/Write	SupportArticle - URL	Edit Article
Read/Write	SupportArticle - URL	Edit Properties

KC_AccessLevel	KC_ContentType	KC_Functions
Read/Write	SupportArticle - URL	New Article
Read/Write	SupportArticle - URL	Notify
Read/Write	SupportArticle - URL	Personalize
Read/Write	SupportArticle - URL	Preview Article
Read/Write	SupportArticle - URL	Read Only Mode
Read/Write	SupportArticle - URL	Reject Article
Read/Write	SupportArticle - URL	Save Article
Read/Write	SupportArticle - URL	Statistics
Read/Write	SupportArticle - URL	Submit for Approval
Read/Write	SupportArticle - URL	View Article
Read/Write	SupportArticle - URL	View Feedback
Read/Write	Web Document	Content Info
Read/Write	Web Document	Edit Properties
Read/Write	Web Document	Notify
Read/Write	Web Document	Personalize
Read/Write	Web Document	Preview Content
Read/Write	Web Document	Read Only Mode
Read/Write	Web Document	Statistics
Read/Write	Web Document	View Article
Read/Write	Web Document	View Feedback

10 Appendix B – SupportSoft Platform Permissions

This section describes the SupportSoft platform permissions that administrators may assign to groups to allow access to specific interfaces. This controls what user interface you can log into and what web pages (components) and options you have once you do log in.

Permissions are grouped by their component category which refers to the component (Author Center, Filter Groups, and so forth) to which a permission applies. The components are designated by the following acronyms that precede permission names.

AC Author Center application - Tool and features.

FG Filter Group - Filter groups that appear on content targeting pages.

RF Report Function - Functions, such as add and edit, within the reports management interface.

RP Report - Individual reports that appear in the report tree view.

SA Support Administrator application - Tool and features.

SC Support Center Win32 container based application - Tool and features.

SC-Web Support Center Web based application - Tool and features.

UC User Center application - Tool and features.

Permission	Description
AC: Author Center Interface	This permission allows the KC application to be used.
AC: Content Type Administration	Provides ability to define and edit content types.
AC: Import Content	This permission allows you to import content
AC: Manage Content	Provides permission for ability to browse Content Directory.
AC: Review Content	Provides permission for ability to view Content Queue.
AC: Review Contributions	Provides permission for review analyst suggestions for new content.
AC: Role Administration	Permission to administer the verbs that are allowed for each role. That is, this controls the permission to administer access levels in the Author Center. Also known as Access Level Administration.
AC: Workflow Administration	Provides permission for ability to edit Workflow Schemes.
FG: Active Browser	Provides permission for Active Browser for use in SmartResults
FG: Active Browser Language	Provides permission for Active Browser Language for use in SmartResults

Permission	Description
FG: Audience	Provides permission for audience that contains filters that can be used to target specific user groups through Windows Active Directory for use in SmartResults. Note: These are Windows groups, not SupportSoft groups.
FG: Browser	Provides permission for browsers that contain filters related to the user's Default Browser for use in SmartResults.
FG: Http Request Method	Provides permission for Http Request Method for use in SmartResults.
FG: Http Server Port	Provides permission for Http Server Port for use in SmartResults.
FG: Mail Client	Provides permission for Mail Clients that contains filters related to the user's Mail Client for use in SmartResults.
FG: Operating System	Provides permission for OS that contains filters related to the user's Operating System for use in SmartResults.
FG: Page Referer	Provides permission for Page Referer for use in SmartResults.
FG: Remote Host/IP	Provides permission for Remote Host/IP for use in SmartResults.
FG: Samples	Provides permission for Sample group containing sample filters for use in SmartResults.
FG: SPRT External Authentication	Provides permission for Ext Auth that contains filters used to authenticate users via External Authentication for use in SmartResults.
FG: Tenant	Provides permission for Tenant usage for use in SmartResults.
RF: Edit Read-Only Reports	Allows permissions for editing, copying, and deleting standard reports. Read-only reports are standard reports provided with the delivered product. Read only reports are not intended to be changed (edited).
RF: Report Editing	Provides permissions for the ability to edit, copy, and delete reports. To edit a read-only report, you also need the permission RF: Edit Read-Only Reports.
RP: All available content	Permission to run a report or manage existing runs of the report for: All available content
RP: Content activating in the future	Permission to run a report or manage existing runs of the report for: Content activating in the future
RP: Content expiring in the future	Permission to run a report or manage existing runs of the report for: Content expiring in the future
RP: Content in workflow process	Permission to run a report or manage existing runs of the report for: Content in workflow process
RP: Content pending review	Permission to run a report or manage existing runs of the report for: Content pending review
RP: Deleted content	Permission to run a report or manage existing runs of the report for: Deleted content
RP: Detailed Content Usage Report	Permission to run a report or manage existing runs of the report for: A report of how often different types of search have been used, grouped by folder and ranked by usage

Permission	Description
RP: Lowest rated content	Permission to run a report or manage existing runs of the report for: Lowest rated content
RP: Most visited content	Permission to run a report or manage existing runs of the report for: Most visited content
RP: Published content expiring in the future	Permission to run a report or manage existing runs of the report for: Published content expiring in the future
RP: Ratings of content	Permission to run a report or manage existing runs of the report for: Ratings of content
RP: Results of Queries	Permission to run a report or manage existing runs of the report for: Results of Queries
RP: Solution effectiveness	Permission to run a report or manage existing runs of the report for: Solution effectiveness
RP: Summary Usage by Access	Permission to run a report or manage existing runs of the report for: This report ranks the number of times content was viewed by type of access method
RP: SupportSoft Product Metrics Summary	Permission to run a report or manage existing runs of the report for: This report shows the summary of SupportSoft Product Metrics result within the specified time period.
RP: Top rated content	Permission to run a report or manage existing runs of the report for: Top rated content
RP: Totals of all content by type	Permission to run a report or manage existing runs of the report for: Totals of all content by type
RP: Usage by folder	Permission to run a report or manage existing runs of the report for: Summary usage by folder
RP: Usage by type	Permission to run a report or manage existing runs of the report for: Summary usage by type
RP: User Failed Login Report	Permission to run a report or manage existing runs of the report for: User Failed Login Report
RP: User Login Report	Permission to run a report or manage existing runs of the report for: User Login Report
RP: User Reset Report	Permission to run a report or manage existing runs of the report for: User Reset Report
SA: Activator States	Provides permission to control submitter activator states
SA: Activators	Provides permission to modify Activators
SA: Add New Email Template	Provides permission to add new email templates.
SA: Autonomy Server	Provides permission for Management of Autonomy Server list.
SA: Build Packages	Provides permission to Create new MSI packages from SupportSoft DNA

Permission	Description
SA: Cache Configuration	Provides permission to Configure Content Cache on the Database as well as the Application Servers
SA: Configure Support Center Client	Provides permission to Configure Support Center Client
SA: Default Settings	Provides permission to Edit the Reporting Default Profile
SA: Email Templates	Provides permission to manage Email Templates
SA: Export Content	Provides permission to Export content in large numbers
SA: External Authentication	Provides permission to Set External Authentication Options
SA: Get External Packages	Provides permission to Upload a new MSI package or pull SupportSoft DNA from another server
SA: Getting Support	Provides permission for Viewlet describing how to get support from SupportSoft.
SA: Groups	Provides permission to manage Groups
SA: Import Content	Provides permission to Import content in large numbers
SA: LDAP Server Configuration	Provides permission to configure the LDAP Service
SA: List Reports	Provides permission to Render Reports inside of the admin tree
SA: Manage Constants	Provides permission to Manage the SupportSoft Constants used on all your SupportSoft Servers.
SA: Manage Email Server Configuration	Provides permission to configure email
SA: Manage Packages	Provides permission to Create MSI package from DNA
SA: Manage Services	Provides permission to Manage the SupportSoft Services installed on all your SupportSoft Servers.
SA: Manage Slivers	Provides permission to configure slivers
SA: Manage Sync Servers List.	Provides permission to Configure the list of Sync Servers used in an environment with multiple Sync Servers.
SA: Manage Web-Control Plugins	Provides permission to configure controls
SA: New Report	Provides permission to Create a new SupportSoft Report
SA: Online Assistance	Provides permission to display links to helpful information on Expert Exchange.
SA: Password Policy	Provides permission to Allows for the setting of password policy
SA: Permissions	Provides permission to manage Permissions
SA: Platform Registry	Provides permission to manage Platform Registry
SA: Platform Version Information	Provides permission to View database, web server, plugin, and application server installed version information.

Permission	Description
SA: Scheduled Tasks	Provides permission to Scheduled Tasks
SA: Scheduler Report	Provides permission to manage Scheduler Report
SA: Scheduler Server Configuration	Provides permission to manage configuration of the scheduler
SA: Servlet Config	Provides permission to manage submitter servlet configuration
SA: Servlet Status	Provides permission to manage submitter servlet stats
SA: Set Certificate Paths	Provides permission to manage configuration certificate paths
SA: Signing Server Configuration	Provides permission to manage configuration signing
SA: SmartResults	Provides permission to manage SmartResults
SA: Snapin Containers	Provides permission to manage Snapin Containers
SA: Snapins	Provides permission to manage Snapins
SA: Submission Timing	Provides permission to manage Submission Timing
SA: Support Administrator Interface	This permission allows the admin application to be used.
SA: Task Parameters	Provides permission to manage Task Parameters
SA: Time Zone And Date Format Preferences	Provides permission to manage Server Time Zone And Date Format Preferences
SA: Tools	Provides permission to Manage the Support Center tools that are available to your support analysts
SA: Top Problems Ranking	Provides permission to manage the Top Problems Ranking
SA: User Center Design	Provides permission to manage User Center Design
SA: Users	Provides permission to manage Users
SA: View Email Outbox	Provides permission to View and manage email outbox
SA: View Sent Emails	Provides permission to View and manage sending email items.
SC: Contribute Content	Permission provides ability to contribute solution.
SC: Find Solutions	Permission provides ability to search for solutions.
SC-Web: Contribute Content	Provides permission for Contribute solutions for Author Center
SC-Web: Find Solutions	Provides permission for KC find solutions
SC-Web: Support Center Client	Provides permission to Install and Launch the Support Center Win32 Client
SC-Web: Support Center Web Interface	This permission allows the SC Win32 container based application and the SC Web based application to be used (healtop for the Web based application).
SC-Web: Time Zone And Date Format Preferences	Provides permission for Time Zone And Date Format Preferences

Permission	Description
UC: Browse	Provides permission for User Center browse
UC: Home	Provides permission for Home Page for the User Center, which allows searching and subsequent viewing of content items, but does not allow browsing the database for content items.
UC: Search	Provides permission for User Center search