AquaLogic Interaction Collaboration 4.2 MP1 Security Target

Version 1.0
03/17/2008

Prepared for:
BEA Systems, Inc

475 Sansome Street
San Francisco, California 94111

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is AquaLogic Interaction Collaboration 4.2 MP1 provided by BEA Systems, Inc.

The Security Target contains the following additional sections:

- TOE Description (Section 2): This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Security Environment (Section 3): This section details the intended environment: describing the security organizational policies enforced by the TOE and its environment, and the assumptions that the TOE and its environment must adhere to.
- Security Objectives (Section 4): This section details the security objectives of the TOE and its environment.
- IT Security Requirements (Section 5): The section presents the security functional requirements (SFR) for TOE and IT Environment that supports the TOE, and details the requirements for EAL 2 augmented with ALC_FLR.2.
- TOE Summary Specification (Section 6): The section describes the security functions represented in the TOE that satisfies the security requirements.
- Protection Profile Claims (Section 7): This section identifies the Protection Profile Claim made in the ST.
- Rationale (Section 8): This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – AquaLogic Interaction Collaboration 4.2 MP1 Security Target

ST Version – Version 1.0

ST Date – 03/17/2008

TOE Identification – AquaLogic Interaction Collaboration 4.2 MP1

TOE Developer – BEA Systems, Inc

Evaluation Sponsor – BEA Systems, Inc

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

1.2 Conformance Claims

This ST is conformant to the following CC specifications:

- Common Criteria (CC) for Information Technology (IT) Security Evaluation Part 2: Security functional requirements, Version 2.3, August 2005.
    - Part 2 Conformant
- Common Criteria (CC) for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August 2005.
    - Part 3 Conformant

- Assurance Level: EAL 2 augmented with ALC_FLR.2

1.3 Conventions

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.
- Explicitly stated requirements – Security Functional Requirements not defined in Part 2 of the CC are annotated with EX.

The terminology and acronyms are listed in the appendices.

2. TOE Description

The Target of Evaluation (TOE) is AquaLogic Interaction Collaboration 4.2 MP1 henceforth referred to as TOE or Collaboration. Collaboration is part of the BEA AquaLogic User Interaction (ALUI) suite of products and is designed to work with AquaLogic Interaction 6.1 with AquaLogic Interaction Development Kit 6.0[1], hereafter referred to as ALI.

Collaboration is not a stand-alone product; rather it integrates directly with ALI and depends on ALI portal pages and security functions. Collaboration functions as a remote server of ALI by providing Collaboration data and application functions in portlets and application views to ALI users. A collection of Collaboration web services provide the communication mechanism for this exchange of portlet data between ALI and Collaboration.

2.1 TOE Overview

Collaboration is a web application featuring a collection of collaboration tools that help users organize, share, and manage information. Collaboration facilitates teamwork among members of a project team by providing a unified online workspace for project members to share information. Collaboration can have many projects and project information can be accessed from any ALI community page or My Page that contains a Collaboration portlet.

Collaboration also provides several features that enable desktop, groupware, and AquaLogic BPM integration as follows:

- Map a Web Folder - Map a Web Folder uses the Web-Based Document Authoring and Versioning (WebDAV) protocol to enable users to manage Collaboration documents directly from their desktop using Microsoft Windows Explorer. The Map a Web Folder feature enables a user to map a Network Place on their desktop computer (running Microsoft Windows) to the document hierarchy in Collaboration. This enables the user to view the project document and file hierarchy using Windows Explorer. Folders and files on Collaboration appear as directories and files in Explorer. Documents opened through Windows Explorer are then automatically opened in edit mode and checked out in Collaboration. This helps users to work more efficiently by removing the need to check out and download the document. All security and version control operations are performed by Collaboration.
- WebEdit - WebEdit lets Collaboration users edit Microsoft Office documents directly on their desktop without having to explicitly check-out and download the document to their machine.
- Office Tools Add-in - Office Tools Add-In enables end users choose from several check-in options and type additional check-in comments.
- Calendar synchronization with Microsoft Exchange and Lotus Notes - Calendar synchronization uses the Groupware Service to enable users to synchronize My Calendar portlet information with Microsoft Exchange and Lotus Notes groupware calendars.
- Instant messaging feature - The Instant Messaging feature enables users to see which project members are currently logged in to their Yahoo! Instant Messaging client.
- AquaLogic BPM integration - AquaLogic BPM integration enables users to attach a Collaboration document to an AquaLogic BPM WorkSpace process instance, and then initiate the process from the document in the Collaboration UI.
- Microsoft Project Import - Microsoft Project Import enables users to import Microsoft Project files into a Collaboration calendar.
- E-mail a Project - E-mail a Project feature enables users to do the following:
    - E-mail a message to a discussion within a project,
    - E-mail a document to a folder within a project, and
    - Reply to a message post notification.

The basic unit of organization for Collaboration is the project. Collaboration uses portlets, the Collaboration application view, and the Project Explorer to display project information and provide access to the Collaboration functions. Collaboration portlets can be added to and viewed in ALI community pages and ALI personal pages

[1] Note: ALI 6.1 MPI was evaluated separate and is used by Collaboration in ALI's evaluated configuration.

(called My Pages). The Collaboration application view and Project Explorer are accessed from the Collaboration portlets displayed on the ALI pages.

Users can participate in more than one project. Using the Collaboration portlet, My Projects, users can select the projects for which to view information. Access to project information and permissions to perform various actions on project objects are determined by Collaboration's access control mechanism. The mechanism determines what actions a user may perform on a project and on the objects within the project. The access control mechanism defines a set of access levels for the objects in the project for each role and associates users to the roles. The roles are Project Leader, Project Member, and Project Guest.

A Collaboration Project Leader can configure Collaboration portlets to display the following:

- Project calendars with milestones, events, and tasks
- Documents (and files) for project members to view or check-out (check-in and check-out are functions of the Collaboration document and file version control)
- Discussion messages to which members can reply
- Task lists with progress indicators in an ALI community page
- Project-related announcements

For example, an engineering project manager might embed Collaboration portlets in an engineering ALI community page to display product milestones and release dates in a group calendar, threaded discussion messages about feature requests, or technical specification documents and feature lists.

Individual users can use a collection of portlets to track their involvement across multiple projects. Using these portlets, an employee can see from her My Page all the tasks for which she is responsible, all the documents that pertain to the project, all the events and milestones she needs to keep track of, and all the threaded discussions she is participating in—across all the projects in which she is involved.

2.2 TOE Architecture

Collaboration consists of the following components:

- Web application: This application runs on an Tomcat web server and includes the following functionality:
  - Project application view,
  - Collaboration Portlets,
  - Project Explorer,
  - Collaboration web services, and
  - Collaboration Administrative utility: This utility is accessed via the ALI Administrative Portal, however the functionality is provided and controlled by Collaboration and affects Collaboration global settings.
- Notification Service: The Notification Service generates and sends e-mail notifications from projects to project users, and functions as a job server for ALI Collaboration. These jobs are distinct from portal jobs, which run using the ALI Automation Service.
- Groupware Service: This optional service enables integration with the following groupware servers:
  - Microsoft Exchange 2000 SP3 and above
  - Microsoft Exchange 2003
  - Lotus Domino 5.0.11
- WebDAV Service: This optional service enables desktop integration with Collaboration project documents and files.

- Image Service Files: Files that provide the necessary static images, styles, user interface controls, Java applets, and online help for Collaboration. These files are installed on the same system as ALI's Image Service.

The Notification, Groupware, and WebDAV Services run as Microsoft Windows services or Unix daemon processes depending on the deployment platform.

2.2.1 Physical Boundaries

The TOE is a web application functioning as a remote server to an *owning* ALI instance within the ALI deployment. Collaboration is installed into an ALI deployment network and depends on components of the ALI installation as depicted in Figure 1. Collaboration is installed on a Tomcat web server. ALI and Collaboration share the same database server with each TOE having its own set of database tables.

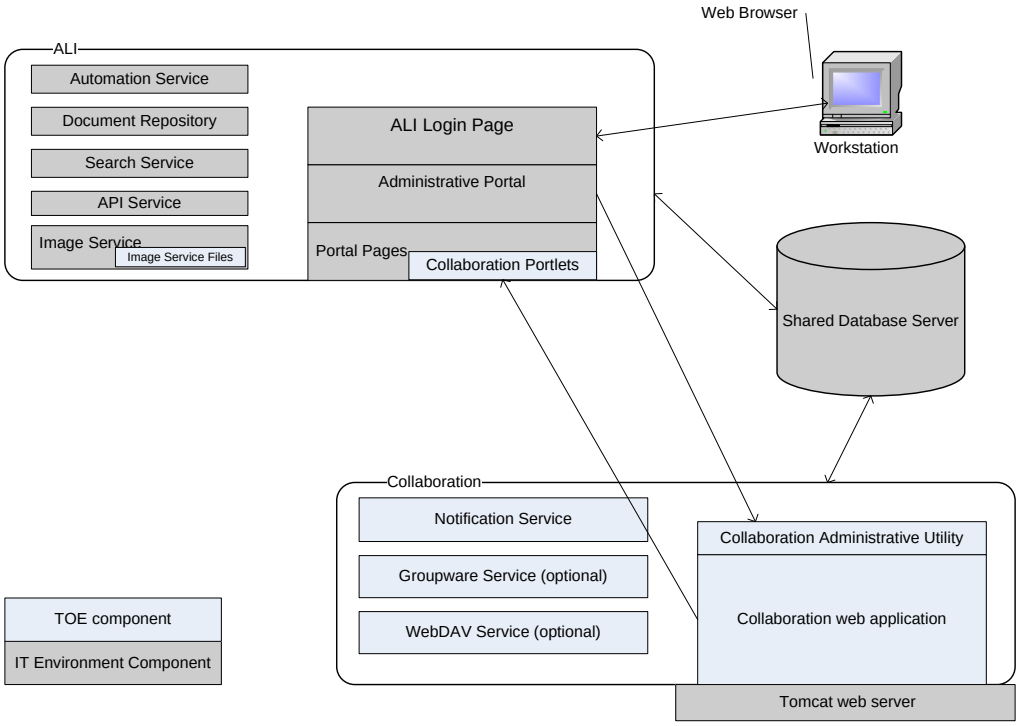

Figure 1: Collaboration with its IT Environment

Collaboration's supporting services run as Windows services or as UNIX daemon processes.

Collaboration relies on the Collaboration database, which must reside on the same server as the ALI database. The Collaboration database stores the project data and the related project objects. Collaboration can reside on a system separate from the ALI and the database server. The IT environment for Collaboration includes the deployment environment of the owning ALI instance, as well as the Tomcat server.

The following table lists the elements of the IT environment for the evaluated configurations.

Table 2-1: TOE Security Functional Components

IT Environment Components	Supported Versions/Descriptions
Operating systems	Microsoft Windows Server 2003 SP1 Solaris 10 (on SPARC) Red Hat Enterprise Linux 4 Update 3 (x86) *Operating systems host all of the components identified below.*
Tomcat web server (application server)	Tomcat Server 5.0.28 *Collaboration is deployed on the Tomcat web server, which is a separate web application server and is not part of the TOE. The Tomcat web server is not a product produced by BEA. Tomcat is part of the IT environment for the TOE and is packaged and installed with Collaboration as a convenience to the user.*
AquaLogic Interaction (ALI)	6.1 MP1 *ALI Includes the following components:* • ***Administrative Portal**. Handles portal setup, configuration, other administrative functions, such as creating and managing portlets and web services. The Collaboration Administrative utility is accessed via the Administrative Portal's utility drop-down menu.* • ***ALI Login Page**. This web page is part of the ALI user interface and is used by both administrators and non-administrative users. The **Log In** page enables users to log into their ALI portal.* • ***API Service**. A component of ALI, the API Service enables remote client applications to call into ALI from other machines on the network. Collaboration is one such remote client and makes calls to ALI to synchronize community users in ALI with the users of community projects that exist in Collaboration and with other projects that are accessible to ALI community members.* • ***Automation Service**. Runs jobs and other automated ALI tasks. The Automation Service runs jobs that perform tasks such as crawling documents into the Knowledge Directory, synchronizing groups and users with external authentication sources, and maintaining the search collection.* • ***Document Repository**. Stores documents and files uploaded by ALUI components. This is where the Collaboration documents and files are stored.* • ***Image Service**. Serves images and other static content for ALI and its component ALUI products, such as Collaboration.* • ***ALI Portal Pages**. Web pages that are part of the ALI portal. These pages include the Login page, users' personal My Page, community pages, and the Knowledge Directory.* • ***Search Service**. A component of ALI that returns indexed content stored in the ALI portal. The Search Service returns content that is indexed in the AquaLogic User Interaction system from the portal, Collaboration, and Publisher. Content that is indexed in the ALUI system includes documents, portlets, communities, and users as well as many other ALUI objects.*
Shared Database Server – provided as part of the ALI installation.	Microsoft SQL Server 2005 (with SQL Server 2000 compatibility level) Oracle 10g R2 (10.2.0.1 and above) in default or Oracle RAC configuration

IT Environment Components	Supported Versions/Descriptions
	The Shared Database Server contains the ALI database tables and the Collaboration database tables. The ALI database stores portal objects, such as user and group configurations, document records, and administrative objects. The ALI database does not store the documents available through the portal. Source documents are left in their original locations. Collaboration database stores Collaboration data such as calendar, task, discussion, and subscription information. It also stores information about the documents (and files) uploaded to Collaboration projects. The Collaboration database does not store these files; they are stored in the Document Repository.
Web browsers	Internet Explorer 6.0 SP2 Mozilla Firefox 1.5 *Web browsers are used by clients to access functions of the product.*

2.2.2 Logical Boundaries

The logical boundary consists of the security functionality of TOE is summarized below.

2.2.2.1 User data protection

The TOE defines an access control mechanism to control the users that can access the TOE defined objects. The users of the TOE are defined, managed and maintained by BEA ALI.

2.2.2.2 Security management

The TOE provides the ability for an authorized administrator to manage and define access control attributes and TOE security functions data.

2.2.2.3 Protection of the TSF

The TOE enforces the access control mechanisms to ensure that the security functions can not be by-passed. The TOE depends on its operating environment to store, protect, and ensure that the TOE functions are not tampered with or bypassed.

The TOE leverages the security functions offered by ALI to ensure that users of the TOE are identified and authenticated before access to the TOE is granted. The TOE depends upon ALI to define, maintain, and manage the administrator groups of the TOE, and the users, user groups, and community groups that can be assigned to the roles in the TOE. The TOE also depends upon ALI to define, maintain, and manage administrative objects that implement the Collaboration integration with ALI.

2.3 TOE Documentation

The TOE has a number of administrative, user and installation guides for the TOE. These documents and others are described in section 6.2.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

- Assumptions made on the operational environment and the method of use intended for the TOE
- Organizational security policies to which the TOE is designed to comply

3.1 Organizational Policies

P.ACCESS Protected objects must be controlled so that they are accessible only to authorized users.

P.MANAGE Authorized administrators must have the utilities necessary to effectively manage the security-related functions of the system.

3.2 Assumptions

A.AUTH_USERS Only the users authorized to access the information within the TOE may access the TOE.

A.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner to maintain to the IT security objectives.

A.NOEVIL The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance.

A.PHYSICAL The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

A.OPE_ENV The TOE operating environment shall provide the mechanism to isolate the TOE components and resources, ensure the TOE cannot be tampered with or bypassed and the TOE data is protected from unauthorized deletions.

A.TRANSMIT The operating environment will protect the data transmitted to and from the TOE.

A.USER The authorized users will not be negligent or malicious and will follow the guidance provided.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to satisfy identified assumptions and/or comply with any organizational security policies identified. All of the identified assumptions and organizational policies are addressed under one of the categories below.

4.1 Security Objectives for the TOE

O.ACCESS	The TSF shall restrict access of the TOE defined objects to authorized users. The TSF must allow authorized administrators to specify which users may access the objects and the actions performed on the objects.
O.MANAGE	The TOE shall allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized users with the administrative privileges are able to access the security functions.

4.2 Security Objectives for the IT Environment

OE.ACCESS	The IT Environment shall restrict access to objects to identified users and groups. The IT Environment must allow authorized administrator to specify which users and groups may access the objects and the operations that may be performed.
OE.AUTH	The IT environment shall ensure that all users have been identified and authenticated before access to the TOE is permitted.
OE.MANAGE	The IT environment shall allow environment administrators to effectively manage the environment and its security functions.
OE.OPE_ENV	The TOE operating environment shall provide the mechanism to isolate the TOE components and resources, ensure the TOE cannot be tampered with or bypassed and the TOE data is protected from unauthorized deletions.

4.3 Security Objectives for the Environment

OE.ADMIN	The TOE administrators shall be competent, trustworthy, trained in the proper operation of the TOE and will follow the guidance provided.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner consistent with the IT security objectives.
OE.PHYSICAL	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.
OE.TRANSMIT	The operating environment shall protect the data transmitted by the TOE from disclosure.
OE.USER	The authorized users will not be negligent or malicious and will follow the guidance provided.

5. IT Security Requirements

This section defines the security functional requirements satisfied by the TOE and security assurance requirements levying against the TOE in an evaluation. The security functional requirements are drawn from the CC Part 2.

5.1 TOE Security Functional Requirements

The following table describes the SFRs satisfied by TOE.

Table 5-1: TOE Security Functional Components

Requirement Class	Requirement Component
FDP: User data protection	FDP_ACC.1a: Subset access control
	FDP_ACF.1a: Security attribute based access control
FMT: Security management	FMT_MSA.1a: Management of security attributes
	FMT_MSA.1b: Management of security attributes
	FMT_MSA.3a: Static attribute initialization
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_SMF.1a: Specification of Management Functions
	FMT_SMR.1a: Security roles
FPT: Protection of the TSF	FPT_RVM.1a: Non-bypassability of the TSP

5.1.1 User data protection (FDP)

5.1.1.1 Subset access control (FDP_ACC.1a)

FDP_ACC.1a.1 The TSF shall enforce the [**Collaboration role-based Access Control Policy**] on [

- **subjects: Users, Crawler Definers, and Crawlers;**
- **objects: projects, events, task lists, document folders, documents and files, and discussions;**
- **operations: the actions listed in table 6-2**].

Application Note: The primary distinction between Users, Crawler Definers and Crawlers is the interface used to access protected objects. The interfaces applicable to each type of subject are protected by the underlying ALI product. The User interface is intended for general purpose users of the TOE that will use the provided object management mechanisms to share information in controlled ways. The Crawler Definer interface is used to browse available document folders in order to select those that should be 'crawled' by a Crawler. The Crawler interface is for special purpose content crawlers that serve to catalog available information for subsequent use (via the other interface). In the context of these requirements, Crawlers and Crawler Definers are identified as security roles that are not available to Users as identified here.

5.1.1.2 Security attribute based access control (FDP_ACF.1a)

FDP_ACF.1a.1 The TSF shall enforce the [**Collaboration role-based Access Control Policy**] to objects based on the following: [

- **subjects:**
  - **(non-Crawler and Crawler Definer) Users: identity and groups;**
  - **Crawlers: role;**
  - **Crawler Definer: identity, groups, and role;**
- **objects:**

- **projects: access control list and roles;**
- **events and task lists: access control list;**
- **discussions: access control list, moderator, and moderator approval (of contents);**
- **document folders: access control list, crawler, moderator, and moderator approval (of contents);**
- **documents and files: access control list and owner**].

Application Note: Technically roles are defined in the context of each project where users are assigned to the specific roles. Regardless, they are treated as user attributes for the purpose of defining the access rules here. A user is associated with a given role if their user identity or a group to which they are assigned is assigned to the role.

Application Note: Moderator approval applies to the contents of moderated objects. For document folders, it applies to files and documents within the folders and for discussions it applies to specific messages that form the discussion. This property is unlike other object properties in that it can be viewed only indirectly by moderators.

FDP_ACF.1a.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

i. **Users are assigned to a role within a given project if their user identity or an assigned group is assigned to the role;**

ii. **Users can only perform operations as defined in table 6-2 on identified objects within a specific project based on the highest access level assigned to their role(s) by the applicable project and/or object access control lists:**
   - **if the identified object has an explicit access control list and the user is not a member of the Project Leader role, the object access control list is used to determine the access level associated with the user's role; or**
   - **if the identified object doesn't have an explicit access control list or the user is a member of the Project Leader role, the project access control list is used to determine the access level associated with the user's role;**

iii. **in addition, Users attempting to access (see Table 6-2) the contents of discussion or document folders that have been assigned a moderator, can only access those contents:**
   - **if they are an Authorized Project or Object Administrator for the applicable discussion or document folder or the target contents (e.g., file);**
   - **if they are the assigned moderator of the applicable discussion or document folder by virtue of their user identity or membership in a group assigned as moderator; or**
   - **if the target contents have been approved for access by an Authorized Project or Object Administrator or an assigned moderator**

iv. **Crawlers can:**
   - **only access the contents of document folders;**
   - **only when the crawler property is set; and**
   - **IF a document folder has been assigned a moderator, the contents are accessible only if they have been approved**

v. **Crawler Definers are subject to rules i and ii above except that**
   - **User is treated as Crawler Definer;**
   - **the only applicable operation is to view document folders; and**
   - **at least the Read access level is required in order to view each document folder**].

Application Note: Note that a User can potentially belong to more than one role. When that occurs, they will effectively have a superset of the access associated with the applicable roles for all applicable objects.

FDP_ACF.1a.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**the owner (based on identity) of an identified document or file is granted all operations**].

FDP_ACF.1a.4 The TSF shall explicitly deny access of subjects to objects based on the [**no explicitly deny access rules**].

5.1.2 Security management (FMT)

5.1.2.1 Management of security attributes (FMT_MSA.1a)

FMT_MSA.1a.1 The TSF shall enforce the [**Collaboration role-based Access Control Policy**] to restrict the ability to [***change_default, modify***] the security attributes [**project access control list and role assignments**] to [**Authorized Project Administrators**].

5.1.2.2 Management of security attributes (FMT_MSA.1b)

FMT_MSA.1b.1 The TSF shall enforce the [**Collaboration role-based Access Control Policy**] to restrict the ability to [***modify***] the security attributes [**object access control lists, owner, moderator, and crawler**] to [**Authorized Project Administrators, Authorized Object Administrators, and the object owner (when applicable)**].

5.1.2.3 Static attribute initialization (FMT_MSA.3a)

FMT_MSA.3a.1 The TSF shall enforce the [**Collaboration role-based Access Control Policy**] to provide [***[inherited]***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3a.2 The TSF shall allow the [**no role**] to specify alternative initial values to override the default values when an object or information is created.

Application Note: Default permissions are defined per object type and the default can only be overridden, in accordance with FMT_MSA.1a, after a given object has been created. The defaults cannot be overridden *during* creation.

5.1.2.4 Management of TSF data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to [***modify, delete***, ***[move]***] the [**project**] to [**Collaboration Administrators**].

5.1.2.5 Management of TSF data (FMT_MTD.1b)

FMT_MTD.1b.1 The TSF shall restrict the ability to [***[create]***, ***[archive], [restore]***] the [**project**] to [**Collaboration Project Administrators and, in the case of project creation, Collaboration Administrators**].

5.1.2.6 Specification of Management Functions (FMT_SMF.1a)

FMT_SMF.1a.1 The TSF shall be capable of performing the following security management functions: [**management of access control lists and role assignments as specified in FMT_MSA.1a; management of the access control lists and moderator and owner attributes as specified in FMT_MSA.1b; and the management of projects as specified in FMT_MTD.1a and FMT_MTD.1b**].

5.1.2.7 Security roles (FMT_SMR.1a)

FMT_SMR.1a.1 The TSF shall maintain the roles [**Authorized Project Administrators, Authorized Object Administrators, Collaboration Administrators, Collaboration Project Administrators, Crawler Definers, and Crawlers**].

FMT_SMR.1a.2 The TSF shall be able to associate users with roles.

Application Note: Note that while there are specific roles defined within the product, security management is enabled via the possession of specific rights. As such, Authorized Project Administrators are limited to a given project and are users either in the Project Leader role or alternately in the Project Member or Project Guest role where that role has been granted administrator access to that project. Similarly, Authorized Object Administrators are limited to the specific object types within a specific project and are users in the Project Member or Project Guest role where that role has been granted administrator access to that object type. Collaboration Administrators and Collaboration Project Administrators are implemented in the underlying ALI product, but are realized in the TOE via specific rights just like the other roles. As such, they are identified here and referenced in the applicable security management requirements above.

5.1.3 Protection of the TSF (FPT)

5.1.3.1 Non-bypassability of the TSP (FPT_RVM.1a)

FPT_RVM.1a.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs satisfied by the IT environment of TOE.

Table 5-2: IT Environment Security Functional Components

Requirement Class	Requirement Component
FDP: User data protection	FDP_ACC.1b: Subset access control
	FDP_ACF.1b: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1c: Management of security attributes
	FMT_MSA.3b: Static attribute initialization
	FMT_SMF.1b: Specification of Management Functions
	FMT_SMR.1b: Security roles
FPT: Protection of the TSF	FPT_RVM.1b: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation

5.2.1 User Data Protection

5.2.1.1 Subset access control (FDP_ACC.1b)

FDP_ACC.1b.1 The ~~TSF~~ **IT Environment** shall enforce the [**ALI Access Control Policy**] on [

- **subjects: users;**
- **objects: Administrative folders, authentication sources, communities, community templates, content crawlers, content sources, content types, experience definitions, external operations, federated searches, filters, groups, invitations, jobs, pages, page templates, portlets, portlet bundles, portlet templates, profile sources, properties, remote servers, snapshot queries, Web services;**
- **operations: view, modify, create, copy, move, delete**].

5.2.1.2 Security attribute based access control (FDP_ACF.1b)

FDP_ACF.1b.1 The ~~TSF~~ **IT Environment** shall enforce the [**ALI Access Control Policy**] to objects based on the following: [

- **subjects (Users): user name and group name (object creation activity rights are conferred via the group membership);**
- **objects: ACL**].

FDP_ACF.1b.2 The ~~TSF~~ **IT Environment** shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- **The move operation is granted if the ACL associated to the parent folder, destination folder, and the object grants the user name/group name permission.**
- **The create operation is granted if the user name via the user's group name has the appropriate object creation activity right.**
- **The copy operation is granted if user name via the user's group name has the appropriate object creation activity right and the ACL associated to the parent folder, destination folder, and the object grants the user name/group name permission.**
- **The other requested operations are granted if the ACL associated to the parent folder and the object grants the user name/group name permission**].

FDP_ACF.1b.3 The ~~TSF~~ **IT Environment** shall explicitly authorize access of subjects to objects based on the following additional rules: [

- **Read access to authentication source, content types, filters, invitations, and properties is explicitly granted to all authorized users,**
- **The authorized administrator (built-in administrator or user in the Administrator group) is granted all access to the object**].

FDP_ACF.1b.4 The ~~TSF~~ **IT Environment** shall explicitly deny access of subjects to objects based on the [**no explicitly deny access rules**].

5.2.2 Identification and authentication (FIA)

5.2.2.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The ~~TSF~~ **IT Environment** shall maintain the following list of security attributes belonging to individual users: [**user name, password, communities, and groups**].

5.2.2.2 User authentication before any action (FIA_UAU.2)

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

5.2.2.3 User identification before any action (FIA_UID.2)

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

5.2.3 Security management (FMT)

5.2.3.1 Management of security attributes (FMT_MSA.1c)

FMT_MSA.1c.1 The ~~TSF~~ **IT Environment** shall enforce the [**ALI Access Control Policy**] to restrict the ability to [**assign to communities and groups**] the security attributes [**activity rights**] to [**authorized administrator**].

5.2.3.2 Static attribute initialization (FMT_MSA.3b)

FMT_MSA.3b.1 The ~~TSF~~ **IT Environment** shall enforce the [**ALI Access Control Policy**] to provide [***[inherited]***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3b.2 The ~~TSF~~ **IT Environment** shall allow the [**authorized administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.2.3.3 Specification of Management Functions (FMT_SMF.1b)

FMT_SMF.1b.1 The ~~TSF~~ **IT Environment** shall be capable of performing the following security management functions: [**management of communities and groups as specified in FMT_MSA.1c**].

5.2.3.4 Security roles (FMT_SMR.1b)

FMT_SMR.1b.1 The ~~TSF~~ **IT Environment** shall maintain the roles [**Collaboration Project Administrator, Collaboration Administrators**, **and authorized administrators**].

FMT_SMR.1b.2 The ~~TSF~~ **IT Environment** shall be able to associate users with roles.

5.2.4 Protection of the TSF (FPT)

5.2.4.1 Non-bypassability of the TSP (FPT_RVM.1b)

FPT_RVM.1b.1 The ~~TSF~~ **IT Environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.4.2 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The ~~TSF~~ **IT Environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

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

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 5-3: EAL 2 augmented with ALC_FLR.2 Assurance Components

Requirement Class	Requirement Component
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
ALC: Life cycle support	ALC_FLR.2: Flaw reporting procedures
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

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

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.
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 that comprise the TOE.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

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

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

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

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

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

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

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

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.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

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

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.

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

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

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

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 behaviour 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.

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

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

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

5.3.5 Life cycle support (ALC)

5.3.5.1 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3d The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5c The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Tests (ATE)

5.3.6.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
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.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
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.

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

5.3.6.3 Independent testing - sample (ATE_IND.2)

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

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.

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.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Strength of TOE security function evaluation (AVA_SOF.1)

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.

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.

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.

5.3.7.2 Developer vulnerability analysis (AVA_VLA.1)

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

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

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.

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.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 User data protection

Projects provide a common workspace for online collaboration for project teams. Projects contain and provide a structure for the Collaboration objects that are subject to Collaboration's security model.

In the Collaboration application view, objects in a project are organized into functional areas where users can perform actions to manage and track their projects. The functional areas are the following:

- Overview (displays project summary, announcements, and recently updated documents)
- Calendar (displays events and tasks)
- Documents (displays document folders, documents and other files)
- Discussions (displays discussions and messages)
- Tasks (displays task lists, tasks, and sub-tasks)

Collaboration implements application level data protection security for Collaboration projects and their contents by assigning an access level for each type of Collaboration object to each project role. Users, groups, and communities are then assigned to roles in the project.

- When users are assigned to roles, the associated users have access to that role.
- When groups are assigned to roles, users that are members of that group have access to that role. Group membership is managed by the underlying ALI[2] component and ALI is queried when group membership needs to be determined.
- When specific communities (defined within ALI) are assigned to roles, Collaboration queries ALI for the current community membership and in effect adds the associated users to the applicable role. As such, for access control purposes only users and groups are applicable when determining role assignments. Collaboration queries ALI once a day for current community membership information in order to update the role assignments accordingly.

The combination of a user's assigned roles[3] within a project and the access levels assigned to the object types (categories) for those roles determines what actions can be taken on the objects in the project.

Collaboration has the following types of objects:

- Project (the primary container for the Collaboration objects)
- Events
- Task Lists (tasks and subtasks comprise the task lists)
- Document Folders (a container for all types of files)
- Document files (can actually be documents or any type of file)

[2] ALI is used in this section to refer to the AquaLogic Interaction 6.1 MP1 portal TOE which has been evaluated independently and is a component of the Collaboration TOE environment in the context of this Security Target.
[3] Note that a user can effectively be assigned to multiple roles.

- Discussions

The Collaboration project role, along with the access level assigned to each object type for that role controls the permitted actions for Collaboration objects. A user can access a Collaboration project only when assigned to a role in that project.

Collaboration defines the following project roles and default object access levels for access to new projects.

Table 6-1: Project Roles and Default Access Level

Collaboration Project Role	Default Access Level
Project Leader	Admin
Project Member	Write
Project Guest	Read

Each role has an associated access level for each object type in a Collaboration project. The term *permissions* is defined as the complete set of access levels assigned to a project role for the six object types. Role assignments are project-specific, and the same user can have different roles in different projects. Alternately, under the same role, a user can have different permissions in different projects because the access level associated with roles can vary from project to project. Furthermore, a given user can have multiple roles (assigned via user identity, groups, and/or communities) in a single project and the result would be access to a superset of the available permissions for those roles.

Note that the Project Leader role is assigned the Admin access level for all objects and these permissions cannot be modified.

Collaboration has five access levels that can be assigned to the Project Member and Project Guest roles. These access levels are:

- Admin
- Edit
- Write
- Read
- No Access

Each access level above No Access includes the rights of all lower access levels. A user's access level for each type of Collaboration object depends on the role they have been granted in the project. When a project is created, each role has a default access level for each type of object as shown in Table 6-1: Project Roles and Default Access Level.

Note that the role and access level information is stored at the project level. The permissions assigned to the roles in the project apply to all objects in the project unless object-level security has been set for an individual object – see Overriding Project Security to Set Object-Level Security, below.

Using the Roles and Permissions page of the Project Editor, Project Leaders can change the default access level assigned to different types of objects for the Project Member or Project Guest roles. Because the role and object access level settings are stored at the project level, changes take effect immediately for all objects that are configured to inherit the default permissions.

Project Leaders can add users, groups, and communities to each project role.

Table 6-2 shows the actions permitted by each access level for each object. Note that designating an access level of 'No Access' entirely prevents users from viewing a project or the contents of a functional area.

Table 6-2: Collaboration Access Levels and Allowed Actions

Access Level / Object	Allowed Actions with Read Access	Allowed Actions with Write Access	Allowed Actions with Edit Access	Allowed Actions with Admin Access
Projects	*View announcements*	*View announcements*	• View announcements	• Create, edit and delete announcements • Subscribe Others
Events	• View Calendars • Notify other users about an event	• Create events	• Modify event properties • Attach files, task lists, and discussions	• Delete events • Configure events security
Task Lists	• View • Notify other users about tasks or task lists	• Create tasks • Claim tasks • Update task status for assigned tasks • Order tasks	• Modify task list and task properties • Create task lists • Assign owners to tasks • Copy task lists • Import and export task lists • Attach files and discussions	• Delete task lists and tasks • Move task lists • Configure task list security • Subscribe Others • Generate overdue task Alerts
Document Folders (can contain any file type)	• View • Notify other users about changes to folder contents • Function as moderator of a folder	• Upload documents and files to the folders • Create new MS Office documents directly in the project	• Modify folder properties • Rename folders • Copy folders • Create folders	• Delete folders • Move folders with the project • Configure folder security • Assign a moderator to a folder • Subscribe Others
Documents and Files	• View files • Notify other users about the file • View versions	• Check files in and out (pertains to Collaboration version control function) • Undo Check-out • WebEdit	• Modify file properties • Create shortcuts • Publish to ALI Knowledge Directory • Revert files to previous versions • Copy files • Attach task lists and discussions	• Delete files • Move files • Configure file security • Delete previous versions of the file • Remove owner security settings from a file • Subscribe Others
Discussions	• View • Notify other users about discussions • Function as moderator of a discussion	• Post messages • Reply to messages	• Modify discussion properties • Create new discussions • Export discussions • Copy discussions • Attach task lists and files	• Delete discussions and messages • Configure discussion security • Edit messages • Approve or reject messages • Assign a moderator to a discussion • Subscribe Others

Overriding Project Security to Set Object-Level Security

Project Leaders and Users with Admin access to a type of object can assign object-level security settings to the individual instances of that object type. The object-level security that can be changed is the access level associated with the Project Member or Project Guest roles. The Admin access level of the Project Leader cannot be changed nor can users or groups be added at the object level.

To assign object-level security and exempt an object from current and future project security settings, the Inherit Default Security Settings option of the individual object must be disabled. With Inherit Default Security Settings disabled, an object retains its individual security setting for a role regardless of the security settings of the project. The access levels that can be assigned to roles for individual Collaboration objects are the same as for objects at the project level. Object-level security can be set for events, task lists, document folders, documents, and discussions using the Security page of the appropriate object editor.

Note that the tasks and sub-tasks of a task list are governed by the security that applies to the task list (either the project security setting for all task lists or the specific task-list security when object-level security has been set for the specific task list).

Table 6-3: Collaboration Object Security Access Levels

Access Level	Description
No Access	Cannot view the object.
Read	Can view the object in the project.
Write	Can view and create objects in the project.
Edit	Can view, create, copy, and modify objects in the project.
Admin	Can view, create, copy, modify, and delete objects in a project and set permissions for other roles.

Additional Security Properties

Three object-level properties provide additional security settings for files, folders, and discussions as described below.

Table 6-4: Object Properties

Object	Property	Description	Collaboration Interface Used
Document (and file) Folder	Moderator	Files uploaded to a *moderated* folder cannot be viewed in the folder until they are approved by a folder moderator.	Properties page of the Folder Properties Editor
Discussion	Moderator	Messages posted to a *moderated* discussion cannot be viewed in the discussion until they are approved by a discussion moderator.	Properties page of the Discussion Editor
File (document or other type of file uploaded to a project document folder)	Owner	The user who uploads a file to a Collaboration document folder is the owner of the file and has owner security permissions on the file. Owner security can be removed by a Project Leader or other project user with Admin access in the project.	Security page of the Document Properties Editor

Object	Property	Description	Collaboration Interface Used
Document (and file) Folder	Accessible to content crawler	This property controls whether the contents of the folder can be accessed by a Collaboration content crawler and *published* to the ALI Knowledge Directory.	Properties page of the Folder Properties Editor

Moderator Property for Discussions

Project Leaders or users with Admin access to discussions can assign a group or a single user to moderate a discussion. Discussion moderators approve or reject messages posted in the discussion. Messages posted in moderated discussions do not appear to users (except moderators) in discussions unless approved by the moderator. Having a moderator is a property of the discussion object. To be a moderator, the user must have at least Read access level to discussions.

Moderator Property for Folders

Project Leaders or users with Admin access to folders can assign a group or a single user to moderate a folder. Folder moderators approve files in the folder. A file in a moderated folder does not appear in searches or become publicly available (i.e., to users other than, the owner or the moderators) until a moderator approves it. Having a moderator is a property of the folder object. To be a moderator, the role must have at least Read access level to folders.

Moderated Discussion or Folder

The assignment of a moderator changes the object (discussions and folders) to a moderated object. This is a property of the discussion or the folder object. Once a folder or discussion becomes moderated, anyone with Admin access to the discussion or folder can also act as a moderator.

The moderator function is not different between the “assigned” moderator and the user with Admin access. A user with Admin access to discussions (or folders) can approve or reject messages. When no moderator is assigned to a discussion or folder, the Admin user cannot moderate it either. Rejecting a message or file is not the same as deleting it. If a message is rejected, it is not posted in a discussion, which means it cannot be seen by other users when they view the discussion. When a message is approved, it is posted in the discussion and can be seen by any users who can view the discussion. Similarly, a file uploaded to a moderated folder is not visible to all users of the project until a moderator approves it.

Owner Property

Documents and files also have an owner property. The user who uploads a document or file to a document folder in a project is the owner of the file and has owner security settings on that file. Owner security settings include all actions for the file in the document folder. The Admin access level, typically assigned to Project Leaders, confers the capability to remove owner security settings on documents from a user. This is useful when the user is no longer participating in the project and, consequently, should not have high-level access privileges to the file.

Accessible to Crawlers Property

Project Leaders or users with Admin access to folders can enable or disable a folder property called “Accessible to crawlers”. This property controls whether the files in the folder can be “crawled” into the ALI Knowledge Directory by a content crawler. This property is enabled by default. Note that the contents of moderated folders can be crawled only when approved by a moderator.

Crawlers use a special purpose interface in order to “crawl” the applicable folders. This interface, like those used by normal users, is instantiated and controlled by the underlying ALI product. Any user that can access the crawler interface is in effect a crawler and can only access the limited crawler functions (collect descriptive information, properties, and link/location) which do not include any of the operations identified above.

Note that there is a special purpose interface made available to support the definition of crawlers. Users of this interface (i.e., known as Crawler Definers in this Security Target) are able select document folders, to which they have at least the read access level, to be subsequently crawled by the resulting crawler.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1: The TOE defines an access control policy for the access to the TOE objects as explained above.
- FDP_ACF.1: The TOE defines an access control policy based on the roles as explained above.
- FMT_MSA.3a: Each project has a role definitions and access levels associated with each role that serve to restricts access to objects within projects upon their creation. While the access settings can be changed on the project or the object once an object is created, they cannot be changed while the object is being created, hence there is no means to override default access in this sense. Note that when projects are created, they either have the default settings identified above or inherit the settings defined within an identified project template.

6.1.2 Security management

The TOE provides web-based administrative interfaces to manage the security functions of the TOE. Some administrative interfaces are accessed via the ALI Administrative Portal. The Collaboration project-level security interfaces are accessed via the Collaboration application view.

Collaboration has four different types of authorized administrators, each with a different scope of permissible action on Collaboration security.

- **Collaboration Administrators** - Any user with the Manage Collaboration activity right[4]. A Collaboration Administrators group is created in ALI during installation and initially does not contain any users or groups. This group is maintained and managed by ALI. The group is assigned two Collaboration activity rights: Manage Collaboration and Manage Collaboration Projects. As such, in effect many Collaboration Administrators will also be Collaboration Project Administrators (see below). Note that the activity right could be assigned to other users and/or groups at the discretion of the ALI authorized administrator. The Manage Collaboration activity right allows management of project folders including the abilities to create, delete, move, and edit (e.g., rename) projects as abstract objects.
- **Collaboration Project Administrators** - Any user with the Manage Collaboration Projects activity right. A Collaboration Project Administrators group is created in ALI during installation and initially contains the ALI Administrators group. The Collaboration Project Administrators group is an ALI group, which is maintained and managed by ALI. This group has the Manage Collaboration Projects activity right and can create projects and project templates and also archive and restore projects. Note that the activity right could be assigned to other users and/or groups at the discretion of the ALI authorized administrator. This activity right does not grant administrative permissions in projects, however when a project is created the creator is added to the Project Leader role by default and as such Collaboration Project Administrators have the ability to manage the projects they create by default.
- **Authorized Project Administrators** - Users with Admin access to the project. By default, this includes the users assigned the Project Leader role for a given project. If the Project Member or Project Guest role for a project has been assigned Admin access, then users assigned to those roles are also Authorized Project Administrators for that project. When a project is created, the default Project Leaders are the user who created the project and the users in the ALI Administrators group. Authorized Project Administrator can manage essentially every aspect of the project and its objects, including security settings (e.g., role assignments, access levels associated with roles at the project and object level, and other object attributes).

[4] Activity rights are ALI permissions that confer system-wide privileges maintained in ALI. Users who do not have permission to perform a particular activity do not see the corresponding user interface elements in ALI. Activity rights are not assigned directly to individual users, rather activity rights are assigned to groups. Then users are assigned to groups and the users acquire the associated group activity rights conferred by their specific group membership.

- **Authorized Object Administrators** – Users with Admin access to the object. Users assigned to the Project Member or Project Guest role within a project where Admin access has been assigned to a specific type of object in the project for the Project Member or Project Guest role are Authorized Object Administrators. When Admin access is assigned to objects for the Project Member or Guest roles, users assigned to that role can change the security for that specific category of object and not the entire project. Note that object owners can perform any operation on the objects they own, including modification of security attributes.

The Collaboration interfaces used to maintain project security settings, including object-level properties, are part of the Collaboration application views.

Collaboration Administrators and Collaboration Project Administrators use the Project Explorer to manage projects at large.

Authorized Project Administrators use the Project Editor to configure project-level security.

Authorized Project Administrators and Authorized Object Administrators use the object editors to manage the object-level attributes as follows:

- Enable the moderator attribute for discussions and folder objects.
- Enable or disable the Accessible to Content Crawler file attribute.
- Remove the owner file attribute.

In addition to normal users and their roles as described above, a special purpose crawler interface is available for the purpose of crawling specially marked folders to catalog and index the contents. Users of this interface have access only to the limited crawler functions and are not specifically or individually identified, unlike other users. As such, '**Crawlers**' is treated as a distinct role for the purpose of differentiating those users in the context of this Security Target. Similarly, a special purposed interface is available for the purpose of defining crawlers. Users of this interfaces are identified as '**Crawler Definers'** in the requirements of this Security Target, and the interface facilitates only the selection of folders to be crawled by the defined crawler.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1a: The TOE restricts the ability to modify and change the default access level settings and role assignments to Authorized Project Administrators as defined above.
- FMT_MSA.1b: The TOE restricts the ability to modify the access settings and the moderator, crawler and owner attributes of specific objects to Authorized Object Administrators, as defined above, and the object owner (if applicable).
- FMT_MTD.1a: The TOE restricts the ability to modify, delete, move, and create projects to Collaboration Administrators (except that Collaboration Project Administrators can also create projects).
- FMT_MTD.1b: The TOE restricts the ability to archive, restore, and create projects to Collaboration Project Administrators (except that Collaboration Administrators can also create projects).
- FMT_SMF.1a: The TOE provides web-based interfaces that allowed the authorized administrators to manage the security functions as described above.
- FMT_SMR.1a: The TOE has three pre-defined roles for projects - Project Leader, Project Member, and Project Guest – and also recognizes two roles implemented within ALI – Collaboration Administrator and Collaboration project Administrator. The three pre-defined roles correspond to Authorized project Administrator and Authorized Object Administrator when administrative access is granted to the applicable roles for specific projects and/or objects as described above. The TOE also realizes crawler and crawler definer roles by virtue of distinct interfaces provided exclusively to support the crawling and crawler definition functions.

6.1.3 Protection of the TSF

The interfaces offered by the TOE have all been carefully designed, implemented, and tested to ensure that they do not offer opportunities to tamper with or interfere with the operation of the security functions and also to ensure that they do not offer any access to protected resources that is not subject to the access control policies and activity rights.

Collaboration is designed to operate in security domains provided by the underlying Tomcat web server. It relies on the environment to protect components from interference and tampering by untrusted subjects.

Collaboration relies on ALI to identify and authenticate all users attempting to access Collaboration. ALI defines, maintains, and manages the administrators and administrative groups of Collaboration, the users, user groups, and community members which can be assigned to roles in Collaboration, and the administrative objects used to implement the ALI-Collaboration integration. Examples of these administration objects are portlets, content sources, remote server, and web services. ALI uses the Collaboration activity rights to limit the access to the Collaboration administrative interfaces. Collaboration enforces the privileges allowed by the activity right.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_RVM.1a: The TOE enforces access control mechanisms to ensure that the TOE security functions are not bypassed.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL 2 augmented with ALC_FLR.2 assurance requirements:

- Configuration Management;
- Delivery and operation;
- Development;
- Guidance documents
- Lifecycle Support;
- Tests; and
- Vulnerability Assessment.

6.2.1 Configuration management

The configuration management measures applied by BEA ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. BEA performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, delivery and operations, life cycle support, vulnerability assessment and the CM documentation.

These activities are documented in:

- AquaLogic® User Interaction Configuration Management

The Configuration management assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

BEA provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. BEA's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. BEA also provides documentation that describes the steps necessary to install the TOE in the evaluated configuration.

These activities are documented in:

- AquaLogic® User Interaction Delivery and Operation
- Release Notes for AquaLogic Interaction Collaboration 4.2 MP1
- BEA AquaLogic Interaction Collaboration Installation and Upgrade Guide, Version 4.2 MP1
- Collaboration 4.2 Installation Worksheet
- Deployment Guide for BEA AquaLogic™ User Interaction – this information is divided into 5 separate guides as follows:
    - BEA AquaLogic User Interaction Deployment Overview
    - BEA AquaLogic User Interaction Deployment Planning
    - BEA AquaLogic User Interaction Customization Overview
    - BEA AquaLogic User Interaction Deployment Maintenance Guide
    - BEA AquaLogic User Interaction Networking and Authentication Guide

The Delivery and operation assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

BEA has documents describing all facets of the design of the TOE. These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

These activities are documented in:

- AquaLogic Interaction Collaboration 4.2 MP1 Functional Specification (ADV_FSP)
- AquaLogic Interaction Collaboration 4.2 MP1 High Level Design (ADV_HLD)
- AquaLogic Interaction Collaboration 4.2 MP1 Representation Correspondence (ADV_RCR)

The Development assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

BEA provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- AquaLogic Interaction Collaboration 4.2 MP1 Guidance Documents (AGD)
- BEA AquaLogic Interaction Collaboration Administrator Guide, Version 4.2
- AquaLogic Interaction Collaboration 4.2 Online Help

The Guidance documents assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

BEA has procedures that define the process for accepting and acting upon user reports of security flaws. These procedures describe the acceptance criteria for security flaws, how all security flaws and the status of fixes for each security flaw are tracked, and how corrections and corrective measures are made available as applicable.

These activities are documented in:

- AquaLogic® User Interaction Flaw Remediation

The Life cycle support assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 assurance requirements:

- ALC_FLR.2

6.2.6 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- AquaLogic® Interaction Collaboration 4.2 MP1 Testing Documentation

The Tests assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

BEA performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- AquaLogic® Interaction Collaboration 4.2 MP1 Vulnerability Assessment

The Vulnerability assessment assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

The ST does not claim compliance to a Protection Profile.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

Table 8-1: Environment to Objective Correspondence

	P.ACCESS	P.MANAGE	A.AUTH_USERS	A.INSTALL	A.NOEVIL	A.PHYSICAL	A.OPE_ENV	A.TRANSMIT	A.USER
O.ACCESS	X	X							
O.MANAGE		X							
OE.ACCESS	X	X							
OE.AUTH			X						
OE.MANAGE		X							
OE.OPE_ENV							X		
OE.ADMIN					X				
OE.INSTALL				X					
OE.PHYSICAL						X			
OE.TRANSMIT								X	
OE.USER									X

8.1.1.1 P.ACCESS

Protected objects must be controlled so that they are accessible only to authorized users.

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The objective ensures that the TOE restricts access to the TOE objects to the authorized users.
- OE.ACCESS: The objective ensures that the environment protects the objects in the underlying product to help ensure that the TOE can effectively protect its own objects.

8.1.1.2 P.MANAGE

Authorized administrators must have the utilities necessary to effectively manage the security-related functions of the system.

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The objective ensures that the TOE provides the tools to allow an authorized administrator to determine who may have access to the objects.
- OE.ACCESS: The objective ensures that the environment provides the tools to allow an authorized administrator to determine who may have access to its objects.
- O.MANAGE: This objective ensures that the TOE provides the tools necessary for the authorized administrator to manage the security-related functions.
- OE.MANAGE: This objective ensures that the environment provides the tools necessary for the authorized administrator to manage the security functions in the environment.

8.1.1.3 A.AUTH_USERS

Only the users authorized to access the information within the TOE may access the TOE.

This Assumption is satisfied by ensuring that:

- OE.AUTH: The objective ensures that users of the TOE are identified and authenticated before access to the TOE and its functions is allowed.

8.1.1.4 A.INSTALL

Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner to maintain to the IT security objectives.

This Assumption is satisfied by ensuring that:

- OE.INSTALL: The objective ensures that the TOE will be installed, managed and operated in a manner that maintains the security objectives.

8.1.1.5 A.NOEVIL

The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance.

This Assumption is satisfied by ensuring that:

- OE.ADMIN: This objective ensures that the TOE is managed and administered in a secure manner by competent and security aware personnel in accordance with the administrator documentation.

8.1.1.6 A.PHYSICAL

The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: The objective ensures that the TOE is protected from physical attacks.

8.1.1.7 A.OPE_ENV

The TOE operating environment shall provide the mechanism to isolate the TOE components and resources, ensure the TOE cannot be tampered with or bypassed and the TOE data is protected from unauthorized deletions.

This Assumption is satisfied by ensuring that:

- OE.OPE_ENV: The objective ensures that the TOE's operating environment protects the TOE and it associated data.

8.1.1.8 A.TRANSMIT

The operating environment will protect the data transmitted to and from the TOE.

This Assumption is satisfied by ensuring that:

- OE.TRANSMIT: The objective ensures that the TSF data imported to and exported from the TOE is protected from disclosure.

8.1.1.9 A.USER

The authorized users will not be negligent or malicious and will follow the guidance provided.

This Assumption is satisfied by ensuring that:

- OE.USER: The objective ensures that the user of the TOE will work co-operatively and will follow the provided guidance.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that Table 8-2 indicates the requirements that effectively satisfy the individual objectives.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

Table 8-2: Objective to Requirement Correspondence

	O.ACCESS	O.MANAGE	OE.ACCESS	OE.AUTH	OE.MANAGE	OE.OPE_ENV
FDP_ACC.1a	X					
FDP_ACF.1a	X					
FMT_MSA.1a	X	X				
FMT_MSA.1b	X	X				
FMT_MSA.3a	X					
FMT_MTD.1a		X				
FMT_MTD.1b		X				
FMT_SMF.1a		X				
FMT_SMR.1a		X				
FPT_RVM.1a	X	X				
FDP_ACC.1b			X			

	O.ACCESS	O.MANAGE	OE.ACCESS	OE.AUTH	OE.MANAGE	OE.OPE_ENV
FDP_ACF.1b			X			
FIA_ATD.1				X		
FIA_UAU.2				X		
FIA_UID.2				X		
FMT_MSA.1c					X	
FMT_MSA.3b			X			
FMT_SMF.1b					X	
FMT_SMR.1b					X	
FPT_RVM.1b						X
FPT_SEP.1						X

8.2.1.1 O.ACCESS

The TSF shall restrict access of the TOE defined objects to authorized users. The TSF must allow authorized administrators to specify which users may access the objects and the actions performed on the objects.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.1: The requirement helps meets the objective by identifying the objects and subjects subjected to the access control policy.
- FDP_ACF.1: The requirement meets this objective by ensuring the TOE only allows access to objects based on the defined access control policy.
- FMT_MSA.1a: The TOE allows the project leader role to determine who will have access to the objects and what actions the user can be perform.
- FMT_MSA.1b: The TOE allows the project leader to determine which users will act as moderator of the discussion and document folder objects.
- FMT_MSA.3a: The TOE enforces a restrictive access when a new object is created. The TOE has a default access level which is assigned to all newly-created objects.
- FPT_RVM.1a: The TOE enforces the access control policy to ensure that objects are accessed by authorized users and only permitted actions are allowed.

8.2.1.2 O.MANAGE

The TOE shall allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized users with the administrative privileges are able to access the security functions.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MSA.1a: The TOE will restrict the ability to manage the access level to authorized administrators.
- FMT_MSA.1b: The TOE will restrict the ability to assign the moderator attribute to the project leader.
- FMT_MTD.1a: The TOE restricts the ability assign the users to roles to the authorized administrator.
- FMT_MTD.1b: The TOE restricts the ability to create a project to the project administrators.
- FMT_SMF.1a: The TOE will provide the interfaces to manage the TOE.
- FMT_SMR.1a: The TOE has pre-defined roles.
- FPT_RVM.1a: The TOE limits access to the interfaces that manage the security functions to users with appropriate administrative activity rights.

8.2.1.3 OE.ACCESS

The IT Environment shall restrict access to objects to identified users and groups. The IT Environment must allow authorized administrator to specify which users and groups may access the objects and the operations that may be performed.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.1b: The requirement helps meets the objective by identifying the user objects subject to the access control policy.
- FDP_ACF.1b: The requirement meets this objective by ensuring the IT environment only allows access to user objects based on the defined access control policy.
- FMT_MSA.3b: The IT environment enforces a restrictive access when a new object is created. Newly-created objects inherit the ACL from the parent folder.

8.2.1.4 OE.AUTH

The IT environment shall ensure that all users have been identified and authenticated before access to the TOE is permitted.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The IT Environment will maintain, at the minimum, the username and the password of TOE defined user accounts.
- FIA_UAU.2: The IT Environment ensures that TOE-defined users are authenticated before access to the TOE is permitted. New users are able to create a new account before access is granted.
- FIA_UID.2: The IT Environment ensures that TOE-defined users are identified before access to the TOE is permitted. New users are able to create a new account before access is granted.

8.2.1.5 OE.MANAGE

The IT environment shall allow environment administrators to effectively manage the environment and its security functions.

This IT Environment Security Objective is satisfied by ensuring that:

- FMT_MSA.1c: The environment will restrict the ability to assign the TOE-related activity rights to environment administrators.
- FMT_SMF.1b: The environment will provide the interfaces to administrator the environment.
- FMT_SMR.1b: This requirement ensures the environment defines an authorized administrator.

8.2.1.6 OE.OPE_ENV

The operating environment shall provide the mechanism to isolate the TOE components and resources, ensure that the TOE cannot be tampered with or bypassed, the TOE data is protected from unauthorized deletions.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_RVM.1b: The IT environment will enforce mechanisms to ensure that the TOE security functions can not be bypassed.
- FPT_SEP.1: The IT environment will protection TOE and its data and ensure that it is not tampered with by untrusted subject.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL 2 augmented with ALC_FLR.2 assurance package. The EAL chosen is based on the statement of the security environment (assumptions, and organizational policy) and the security objectives defined in this ST. The sufficiency of the EAL chosen is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. The users are conscientious, non-hostile and will follow the guidance (A.NOEVIL, A.USER, OE.ADMIN, OE.USER). The TOE server component is

physically protected and properly and securely configured (A.INSTALL, OE.INSTALL). Given these aspects, a TOE based on good commercial development practices is sufficient. EAL 2 augmented with ALC_FLR.2 is an appropriate level of assurance for the TOE described in this ST.

8.4 Strength of Functions Rationale

The TOE does not implement any other functions that are of a permutational or probabilistic nature. Therefore, a minimum SOF claim is not made for the TOE.

8.5 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria. Table 8-3: Security Requirement Dependencies lists each requirement from Sections 5.1 and 5.2 and indicates which requirements were included to satisfy the dependencies, if any.

Table 8-3: Security Requirement Dependencies

ST Requirement	CC Dependencies	ST Dependencies
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a
FDP_ACF.1a	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1a and FMT_MSA.3a
FMT_MSA.1a	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1a and FMT_SMF.1a and FDP_ACC.1a
FMT_MSA.1b	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1a and FMT_SMF.1a and FDP_ACC.1a
FMT_MSA.3a	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1a and FMT_MSA.1b and FMT_SMR.1a
FMT_MTD.1a	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1a and FMT_SMR.1b and FMT_SMF.1a
FMT_MTD.1b	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1a and FMT_SMR.1b and FMT_SMF.1a
FMT_SMF.1a	none	none
FMT_SMR.1a	FIA_UID.1	FIA_UID.2
FPT_RVM.1a	none	none
FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b
FDP_ACF.1b	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1band FMT_MSA.3b
FIA_ATD.1	none	none
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	none	none
FMT_MSA.1c	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1b and FMT_SMF.1b and FDP_ACC.1b
FMT_MSA.3b	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1c and FMT_SMR.1b
FMT_SMF.1b	none	none
FMT_SMR.1b	FIA_UID.1	FIA_UID.2
FPT_RVM.1b	none	none
FPT_SEP.1	none	none

8.6 Explicitly Stated Requirements Rationale

All requirements included in this ST are drawn from the CC Part 2 and Part 3. The Security Target does not define explicitly stated requirements.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 8-4 Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

Table 8-4: Security Functions vs. Requirements Mapping

	User data protection	**Security management**	**Protection of the TSF**
FDP_ACC.1	X		
FDP_ACF.1	X		
FMT_MSA.1a		X	
FMT_MSA.1b		X	
FMT_MSA.3a	X		
FMT_MTD.1a		X	
FMT_MTD.1b		X	
FMT_SMF.1a		X	
FMT_SMR.1a		X	
FPT_RVM.1a			X

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.

Appendix A: Terminology

Activity Rights	Activity rights are ALI permissions that confer system-wide privileges maintained in ALI. Activity rights are not assigned directly to individual users, rather activity rights are assigned to groups. Then users are also assigned to groups and the users acquire the associated group activity rights conferred by their specific group membership.
Community	A community is a ALUI workspace that contains pages, portlet and sub-communities. ALI users can be assigned to communities.
Content crawler	An ALI admin object used to import content into the ALI Knowledge Directory from external content repositories. Content crawlers import from back-end content sources, such as Collaboration, document records that contain descriptive information, such as content type and properties, document ACL (read access only), and links to the documents. Configuring a content crawler requires selection of a content source admin object. There are two types of Content Crawlers: Remote and WWW. Collaboration installs a remote content source object into ALI so that crawlers can be configured for the Collaboration project folders.
Content Source	A remote content source allows users to import content from an external content repository into the portal through remote content crawlers.
Groups	A group is a set of user and or other groups defined in ALI. Groups are used to assigned activity rights and can be assigned to roles in the Collaboration projects and in object ACLs.
Knowledge Directory	An ALI area where users can browse and view documents that have been uploaded by users or imported by content crawlers. This information is organized into subfolders in a manner similar to file storage systems. The Knowledge Directory (KD) does not store documents, instead the KD stores links to docs, it stores the name, description, URL, in the ALI database
System	The system is the TOE and its operating environment.
WebDAV	**Web-based Distributed Authoring and Versioning**, or **WebDAV**, is a set of extensions to the Hypertext Transfer Protocol (HTTP) which allows users to collaboratively edit and manage files on remote World Wide Web servers.

Appendix B: Acronyms

ACL	Access Control List
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
EAL	Evaluation Assurance Level
FDP	User Data Protection CC Class
FIA	Identification and Authentication CC Class
FMT	Security Management CC Class
FSP	Functional Specification
HLD	High Level Design
IT	Information Technology
MOF	Management of Functions
MTD	Management of TSF Data
OSP	Organization Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Security Management
SMR	Security Management Roles
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection