National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

AquaLogic® Interaction Collaboration 4.2 MP1

Report Number: CCEVS-VR-10104-2009
Dated: 20 February 2009
Version: 1.2

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

Table of Contents

List of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of AquaLogic® Interaction Collaboration 4.2. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the AquaLogic® Collaboration 4.2. product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in January 2009. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 2.3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 2 augmented with ALC_FLR.2. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

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. Collaboration is one of several products in the AquaLogic User Interaction suite.

The TOE is dependent on the correct operation of the environment and on its underlying ALI portal, neither of which are included within the scope of the evaluation. It should also be noted that the access control policy implemented by the TOE is enforced only on access attempts made through the TOE's interfaces. The TOE does not and cannot control attempts to access data directly (e.g., via the underlying OS).

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the AquaLogic Collaboration 4.2 MP1 Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	AquaLogic® Interaction Collaboration 4.2 MP1
Sponsor:	BEA Systems, Inc 475 Sansome Street

San Francisco, CA 94111

Developer:
BEA Systems, Inc
475 Sansome Street
San Francisco, CA 94111

CCTL:
Science Applications International Corporation
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Kickoff Date: June 27, 2005

Completion Date: 13 January 2009

CC: Common Criteria for Information Technology Security Evaluation, Version 2.3

Interpretations: None

CEM: Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.3, August 2005.

Evaluation Class: EAL 2 augmented with ALC_FLR.2

Description: AquaLogic® Interaction Collaboration 4.2 MP1 is a web application that works in the context of an owning AquaLogic Interaction (ALI) 6.1 MP1 portal.

Disclaimer: The information contained in this Validation Report is not an endorsement of the AquaLogic Interaction Collaboration 4.2 MP1 product by any agency of the U.S. Government and no warranty of the ALI product is either expressed or implied.

PP: None

Evaluation Personnel:
Science Applications International Corporation:
Anthony J. Apted
Lisa Vincent

Validation Body: National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Organizational Security Policies

The ST identifies the following organizational security policies with which the TOE is intended to comply.

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.

2 Identification

The evaluated product is **AquaLogic® Interaction Collaboration 4.2 MP1**.

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the Collaboration security policy has been extracted and reworked from the BEA AquaLogic Interaction Collaboration 4.2 MP1 ST and Final ETR.*

3.1 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.

3.2 Security Management

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

3.3 Protection of the TSF

The TOE enforces the access control mechanisms to ensure that the security functions cannot 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.

4 Assumptions

The following assumptions are identified in the ST:

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.

4.1 Clarification of Scope

The Target of Evaluation (TOE) is AquaLogic Interaction Collaboration 4.2 MP1, henceforth referred to as Collaboration.

The TOE is dependent on the correct operation of the environment and on its underlying OS and AquaLogic Interaction 6.1 MP1 owning portal server, none of which are included within the scope of the evaluation. It should also be noted that the access control policy implemented by the TOE is enforced only on access attempts made through the TOE's interfaces. The TOE does not and cannot control attempts to access data directly (e.g., via the underlying OS).

5 Architectural Information

The Target of Evaluation (TOE) is AquaLogic Interaction Collaboration 4.2 MP1, henceforth referred to as 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

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

users. A collection of Collaboration web services provide the communication mechanism for this exchange of portlet data between ALI and Collaboration.

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 (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

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.

6 Documentation

BEA provides an extensive set of documentation describing the installation, configuration, management and operation of the TOE. This set comprises documentation for the Collaboration which comprises the TOE. The Collaboration documentation is available from the BEA edocs website, http://edocs.bea.com/alui/collaboration/docs42/index.html. Additionally, installation worksheets for AquaLogic Interaction Collaboration Windows and Unix installations are available.

The guidance documentation examined during the course of the evaluation and therefore included in the TOE is as follows:

Guidance

- AquaLogic Interaction Collaboration 4.2 MP1 Administrator Guide
- AquaLogic Interaction Collaboration 4.2 MP1 Online Help
- AquaLogic Interaction Collaboration 4.2 MP1 Release Notes
- AquaLogic Interaction Collaboration 4.2 MP1 Installation and Upgrade Guide
- AquaLogic Interaction Collaboration 4.2 MP1 Installation Worksheet for Windows Installations
- AquaLogic Interaction Collaboration 4.2 MP1 Installation Worksheet for UNIX Installations
- Deployment Guide for AquaLogic User Interaction

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for AquaLogic Interaction Collaboration 4.2 MP1.

7.1 Developer Testing

The developer’s approach to testing for Collaboration is based on TOE Security Function (TSF) interface testing. BEA has developed a test suite comprising various manual tests to exercise the TSF at both the user interfaces and the portal Application Programming Interfaces (APIs) as described in the TOE Functional Specification. The vendor addressed test depth by analyzing the functionalities addressed in the high-level design and associating test cases that cover the addressed functionalities. The high-level design addressed the general functions of the TOE subsystems, identifying the security functionality of each subsystem, as appropriate. The testing documentation maps security functions to specific test suites and tests, while the development documentation maps security functions to subsystems. The combination of the two mappings shows how the tests map to the subsystems.

The vendor ran the TOE manual tests in various configurations, consistent with the test environment described in the testing documentation, and provided the evaluation team with the actual results. The test configurations were representative of the operating systems supported and the application environment. All tests passed.

While performing the ATE_FUN work units, the evaluation team examined in detail a sample (amounting to slightly over 20%) of the vendor test cases and determined that all actual results matched the expected results. These results provided sufficient confidence that the entire test suite results match as well.

7.2 Evaluation Team Independent Testing

The TOE Test Environment was installed on Microsoft Windows XP Professional and team personnel accessed the following test configurations via virtual machines using VMWare Lab Manager 2.5. The two (2) test configurations selected comprised:

- Microsoft Windows Server 2003 SP1 using Tomcat Server 5.0.28, with AquaLogic Interaction 6.1 MP1 and Internet Explorer (7.0)
- Red Hat Enterprise Linux 4.0 Update 3 (x86) with AquaLogic Interaction 6.1 MP1 and Internet Explorer (7.0).

The TOE testing environments were equipped with the following software:

- Tomcat Server 5.0.28 (as deployed with the TOE, but is a separate web application server and not part of the TOE)
- Shared database server (provided as part of the ALI installation) as either Microsoft SQL Server 2005 (with SQL Server 2000 compatibility level) or Oracle 10g R2 (10.2.0.1 and above) in default or Oracle RAC configuration
- Microsoft Internet Explorer (IE) 6.0 SP2 or 7.0; or Mozilla Firefox 2.0.

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The test environments described above were used with team generated test procedures and team analysis to determine the expected results.

The evaluation team performed the following additional functional tests:

- **User Roles and Object Access**— The vendor's ST and design documentation describes various user roles (i.e., Collaboration Administrator (administrator), Collaboration Project Administrator (Project Leader) and describes access functions that can be done by an administrator versus a project leader. Performed various actions as Administrator and Project Leader to verify various functionality per role and associated access. The in-depth tests demonstrated that the TSF behaves as expected for various user roles and object accesses as specified in the functional specification and satisfies the requirements specified in the ST.
- **Project Creation and Manipulation**—Within the TOE, users access the Project Explorer interface to view projects for which they have been granted membership and only authorized users may create new projects. Within the Project Explorer page, creation of a new project requires assigning groups, users, and functional areas for which members will have access to within the created project. Additionally, only those users with the appropriate privileges may move projects. Accessed Project Explorer via the Home Page and created new projects, assigned groups, members and functional areas, as well as, moved the created project. The test demonstrated that the TOE allows a defined user to create a new project, assign groups and members and assign functional areas, as well, as move the created project as specified in the functional specification and satisfies the requirements specified in the ST.

- **Read Access**—the vendor's ST describes the access levels that can be assigned as Admin, Edit, Write, Read and No Access and Table 6-2 indicates that the allowed actions with the Read access include viewing all objects. Logged on as a project guest with only read access, by default, and attempted to access and modify settings. The test demonstrated that the TSF enforces the Read access and allows all users to view objects; however, when the user attempts to change any of the settings, an error message is displayed that user only has read access and any changes will not be saved as specified.
- **Editing Document Properties by Owner—** The ST specifies that 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. Additionally, the ST specifies that the owner (based on identity) of an identified document or file is granted all operations. Attempted to modify an ACL on an object as the owner (creator) and the TSF allowed the owner of the document to modify the document properties as specified in the functional specification and ST. The test further demonstrated that the TOE allows a non-administrative user who created an object to modify the properties as the owner.
- **Crawlers and Crawler Definer Subject Restrictions**—The ST specifies that the primary distinction between Users, Crawler Definers and Crawlers is the interface used to access protected objects and the interfaces applicable to each type of subject are protected by the underlying ALI product. The Crawler interface is for special purpose content crawlers that serve to catalog available information for subsequent use (via the other interface); 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 Definers are treated as Crawler Definer (e.g., user); 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. Crawler Definers are able to set document folders to be subsequently crawled by the resulting crawler. Further, Project Leaders or users with Admin access to folders can enable or disable a folder property called "accessible to crawlers" that controls whether files in the folder can be 'crawled' into the ALI Knowledge Directory by a content crawler. This property is enabled by default. 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). The crawler definer special-purpose interface is made available to support the definition of crawlers and users of this interface are able to select document folders to which they have at least the read access level, to be subsequently crawled by the resulting crawler. The test demonstrated that the ST definition of a Crawler Definer being a separate and distinct security role is appropriate. Administrator's (users granted the 'Admin' access) can create new crawlers and define the project(s) and/or folder(s) for which the crawler crawls documents managed by the TOE. However, the user defining the crawler must have Collaboration project access and at least READ access to the source folder; otherwise the source folder does not appear as an option for selection.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product that searched four (4) additional well known vulnerability web sites and extended the search parameters used by the developer. The evaluation team did not discover any new open source vulnerabilities/bugs that pertain to the TOE that have not been corrected. The evaluation team conducted the following additional penetration test for the reasons specified:

- **Replay vulnerability**—During the validation of the AquaLogic Interaction TOE (VID10103), and as a result of an investigation performed by the evaluation team in response to validator questions, the evaluation team identified that remote servers that were integrated with AquaLogic Interaction via a portlet were potentially susceptible to replay attacks. This vulnerability was not applicable directly to the evaluated version of AquaLogic Interaction, as it does include remote servers. However, Publisher 6.4 is deployed as a remote server of AquaLogic Interaction, and so was potentially vulnerable. The test demonstrated that a user able to access a browser session previously used by an Administrator, within a reasonable period of time, could reuse URLs to exploit the replay vulnerability and essentially perform some action as if they were the Administrator.

8 Evaluated Configuration

The evaluated version of the TOE is AquaLogic Interaction Collaboration 4.2 MP1.

The TOE is a web application that works with the portal technology platform (ALI).

Collaboration is evaluated on the following platforms and with the following other IT environment 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.*

IT Environment Components	**Supported Versions/Descriptions**
AquaLogic Interaction (ALI)	6.1 MP1 *ALI Includes the following components:* • ***Administrative Portal****. 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****. The API Service enables remote client applications to call into ALI from other machines on the network. Collaboration is one such remote client.* • ***Automation Service****. Runs jobs and other automated ALI tasks.*
	• ***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.*

IT Environment Components	Supported Versions/Descriptions
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 *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, 7.0 Mozilla Firefox 1.5 tested on v2.0 *Web browsers are used by clients to access functions of the product.*

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3 and CEM version 2.3. The evaluation determined AquaLogic® Interaction Collaboration 4.2 MP1 to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements augmented with ALC_FLR.2. The rationale supporting each CEM work unit verdict is recorded in the **Evaluation Technical Report for AquaLogic® Interaction Collaboration 4.2 MP1 Part 2** which is considered proprietary.

10 Validator Comments/Recommendations

Note that there are no security functional requirements for collection of audit data. The start of this evaluation predates the CCEVS policy to require audit, if the evaluation began today this would not be permitted.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **AquaLogic® Interaction Collaboration 4.2 MP1 Security Target,** Version 1.0, dated 17 March 2008.

13 Glossary

The following acronyms beyond those in the CC or CEM are supplied; however, no additional definitions are supplied:

- **ACL**—Access Control List
- **ALI**—AquaLogic Interaction
- **ALUI**—AquaLogic User interaction
- **API**—Application Programming Interface
- **MP**—Maintenance Pack
- **UI**—User Interface

14 Bibliography

URLs

- NIAP Common Criteria Evaluation and Validation Scheme (http://www.niap-ccevs.org/cc-scheme/)
- SAIC CCTL (http://www.saic.com/infosec/common-criteria/)
- BEA Systems, Inc. (http://www.bea.com)

NIAP CCEVS Documents:

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.3, August 2005
- *Common Evaluation Methodology for Information Technology Security*, version 2.3, August 2005.

Other Documents:

- *AquaLogic® Interaction Collaboration 4.2 MP1 Security Target*, Version 1.0, 17 March 2008.