WebSphere Application Server EAL2 Security Target

Date: 1 December 2004
Issue: 2.9
Reference: LFF/WAS/EAL2/ST/29

This Page Intentionally Left Blank.

Table of Contents

GLOSSARY AND TERMINOLOGY IV

1 INTRODUCTION 1

1.1 TARGET OF EVALUATION OVERVIEW 1
1.2 CC CONFORMANCE 2
1.3 STRENGTH OF FUNCTIONS 2
1.4 REFERENCES 2
1.5 STRUCTURE 2

2 DESCRIPTION 3

2.1 DESCRIPTION OF THE PRODUCT 3
2.1.1 Product Server 3
2.1.2 Product Client 5
2.1.3 Product Admin Console Tool 5
2.1.4 Product wsadmin Tool 5
2.1.5 Product Additional Tools 5
2.1.6 Product HTTP Server Plug-In 6
2.1.7 Product Included Software 6
2.2 IDENTIFICATION OF THE TOE 6
2.3 DESCRIPTION OF THE TOE EVALUATED CONFIGURATION 7
2.3.1 TOE 7
2.3.2 Software Environment of the TOE 9
2.4 DESCRIPTION OF THE TOE SECURITY FUNCTIONS 12
2.4.1 Identification 12
2.4.2 Access Control 12
2.4.3 System Management 13

3 TOE SECURITY ENVIRONMENT 14

3.1 INTRODUCTION 14
3.2 THREATS 14
3.2.1 Threats countered by the TOE 14
3.2.2 Threats countered by the TOE Environment 14
3.3 ORGANISATIONAL SECURITY POLICIES (OSPS) 14
3.4 ASSUMPTIONS 14
3.4.1 Physical aspects 15
3.4.2 Personnel Aspects 15

4 SECURITY OBJECTIVES 16

4.1 SECURITY OBJECTIVES FOR THE TOE 16
4.2 SECURITY OBJECTIVES FOR THE TOE ENVIRONMENT 16

5 SECURITY REQUIREMENTS 17

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 17
5.1.1 Access Control (FDP) 18
5.1.2 Identification 19
5.1.3 Security Management (FMT) 19
5.2 STRENGTH OF FUNCTION (SOF) 20

5.3 TOE SECURITY ASSURANCE REQUIREMENTS 20
5.4 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 20
5.4.1 Identification and Authentication (FIA) *20*
6 TOE SUMMARY SPECIFICATION 21
6.1 SECURITY FUNCTIONS (SF) 21
6.1.1 Identification (Ident.1) *21*
6.1.2 Access Control (AC.1) *22*
6.1.3 Security Management (SM.1, SM.2, and SM.3) *24*
6.2 ASSURANCE MEASURES 25
7 RATIONALE 27
7.1 CORRELATION OF THREATS, POLICIES, ASSUMPTIONS AND OBJECTIVES 27
7.2 SECURITY OBJECTIVES RATIONALE 28
7.2.1 Threats *28*
7.2.2 Security Policy *29*
7.2.3 Assumptions *30*
7.3 SECURITY REQUIREMENTS RATIONALE 31
7.3.1 Security Functional Requirements Rationale *31*
7.3.2 Security Environment Requirements Rationale *32*
7.3.3 Security Assurance Requirements Rationale *32*
7.4 SFR DEPENDENCIES 33
7.5 TOE SUMMARY SPECIFICATION RATIONALE 33
7.5.1 TSF correspondence to SFRs *34*

Glossary and Terminology

API	Application Programming Interface
Authorised Client	A client user who may, in accordance with the TSP, perform an operation.
CC	Common Criteria
DB	DataBase
EAL	Evaluation Assurance Level
EJB	Enterprise Java Bean
Enterprise bean component	A server application component that conforms to the J2EE V1.3 specification. The component contains one or more enterprise beans. The enterprise beans are packaged in a JAR file and configured with an ejb-jar.xml file.
Enterprise application	A server application that conforms to the J2EE V1.3 specification. The application consists of one or more web server application components, enterprise bean components, or both. The components optionally can be packaged in an EAR file and configured with an application.xml file.
Enterprise bean	A server module that is included in an enterprise bean component. The module is coded in the Java programming language and conforms to the EJB architecture identified in the J2EE V1.3 specification.
IT	Information Technology
J2EE	Java 2 Enterprise Edition
J2SE	Java 2 Standard Edition
JCA	Java Connection Architecture
JDBC	Java DataBase Connectivity
JNDI	Java Naming Directory Interface
JSP	Java Server Page, a server module that is included in a web server application component. The module is coded in the Java scripting language and conforms to the JSP architecture identified in the J2EE V1.3 specification. web server application component JVM Java Virtual Machine
OS	Operating System
OSP	Organisational Security Policy
Protected Resources	Methods in enterprise beans, methods and HTML pages in web server applications, the Administration Service, and the Naming Service.

RMI	Remote Method Invocation protocol (RMI). A Java protocol for transforming the data in a Java method into a serial data stream so that the data can be transmitted remotely.
Role	A logical grouping of users that are defined by an application component provider or assembler
SDK	Software Development Kit
Servlet	A server module that is included in a web server application component. The module is coded in the Java programming language and conforms to the servlet architecture identified in the J2EE V1.3 specification.
SF	Security Function. A part or parts of the TOE that have been relied upon for enforcing a closely related subset of rules from the TSP.
SFR	Security Functional Requirement
SOF	Strength Of Function
ST	Security Target
TOE	Target Of Evaluation. An IT product or system and its associated administrator and user guidance documentation that is the subject of the evaluation.
TSC	TSF Scope of Control
TSF	TOE Security Function. A set consisting of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TSP	TOE Security Policy. A set of rules that regulate how assets are managed, protected and distributed within the TOE.
User Guidance document	The document entitled "Websphere Application Server AGD - Guidance"
Web server application	A servlet, JSP, or HTML page.
Web server application component	A server application component that conforms to the J2EE V1.3 specification. The component contains one or more web server applications. The web server applications are packaged in a WAR file and configured with a web.xml file.

1 Introduction

Security Target (ST) Title: WebSphere Application Server EAL2 Security Target

Version: 2.9

Version Date: 1 December, 2004

TOE identification: WebSphere Application Server version 5.0.2.8

Common Criteria Identification: Common Criteria for Information Technology Security Evaluation, CCIMB-99-031, Version 2.1, August 1999.

Evaluated Assurance Level: EAL2, augmented with ALC_FLR.1 (Basic Flaw Remediation).

1.1 Target of Evaluation Overview

WebSphere Application Server v5.0.2.8 (hereafter referred to as *the product*) is a Java 2 Enterprise Edition (J2EE) 1.3 compliant run-time environment. The primary purpose of the product is to provide an environment for running and managing the components of user-supplied enterprise applications. In addition to its primary purpose, the product provides an environment for running clients to enterprise applications and provides tools for doing useful functions such as assembling and troubleshooting enterprise applications.

The TOE consists of a subset of the components provided with the product. This subset is comprised of those product components that are used to deploy and run user-supplied enterprise applications and to manage these applications by means of a scripting tool.

J2EE is a comprehensive set of specifications for designing, developing and deploying multi-tier, server-based applications. The J2EE specifications are the result of an industry-wide effort that involves a large number of contributors.

The following Operating Systems (OS) are supported within this evaluation, but outside its scope:

- AIX 5.2;
- HP-UX 11i;
- Linux SuSE Enterprise Edition (SLES) 8;
- Linux Red Hat 2.1
- Sun Solaris 8; and
- Microsoft Windows 2003.

It is assumed that all hardware used within the operating environment is secured such that no potential vulnerabilities could be introduced that would circumvent the functionality described within this ST.

1.2 CC Conformance

This ST is [CC] Part 2 conformant and Part 3 conformant to a claimed Evaluation Assurance Level of EAL2, *augmented with* ALC_FLR.1.

1.3 Strength of Functions

There is no strength of function claim because the TOE does not identify any security functional requirements for which an explicit Strength Of Function (SOF) is appropriate and does not identify any functions that are of a permutational or probabilistic nature. Therefore, a minimum SOF claim is not included for the TOE.

1.4 References

[CC] Common Criteria for Information Technology Security Evaluation, CCIMB-99-031, Version 2.1, August 1999.

1.5 Structure

The structure of this document is as defined by [CC] Part 1, Annex C:

- Section 2 is the TOE description;
- Section 3 provides a statement of the TOE security environment;
- Section 4 provides the statement of IT security objectives;
- Section 5 provides a statement of IT security requirements;
- Section 6 provides the TOE summary specification, which includes the detailed specification of the IT functions; and
- Section 7 provides the rationale for the security objectives, security requirements and TOE summary specification.

2 Description

This section provides the following information:

- Description of the product;
- Identification of the TOE;
- Description of the TOE evaluated configuration;
- Description of the TOE security functions.

2.1 Description of the Product

The product is a J2EE V1.3 compliant run-time environment. The primary purpose of the product is to provide an environment for running and managing user-supplied enterprise applications and their components. In addition to its primary purpose, the product provides an environment for running clients to enterprise applications and provides tools for doing useful functions such as assembling and troubleshooting enterprise applications.

The product consists of the following components:

- Product Server
- Product Client;
- Product Admin Console Tool;
- Product wsadmin Tool;
- Product Additional Tools;
- Product HTTP Server Plug-Ins;
- Product Included Software.

Note: See the Glossary of this document for a definition of enterprise applications and for definitions of enterprise application components, which are web server applications components and enterprise bean components.

2.1.1 Product Server

The Product Server component is a set of containers, services, and resources that provide an environment for running enterprise applications and their components and for programmatically managing enterprise applications and their components.

The containers are runtime wrappers that handle system functions, such as communications and security, for enterprise application components and some types of resources. The following containers are included:

- Enterprise bean container--handles system functions for enterprise beans.
- Web server container (contains an embedded HTTP server)--handles system functions for web server applications.

- Resource adapter container--handles system functions for resources that conform to the Java Container Architecture (JCA).

The services are Java API and remote interface implementations. They provide useful functions, such as directory and security, that components of enterprise applications can use. A few of these services also are remotely available so that clients also can use them. The following services are included:

- Services defined and documented in Java specifications. The following is a list of these services:
  - Document Object Model (DOM) 2.0
  - Enterprise JavaBean (EJB) 2.0
  - Java 2 Enterprise Edition (J2EE) 1.3
  - J2EE Connector Architecture (JCA) 1.0
  - JavaMail 1.2
  - Java API for XML Parsing (JAXP) 1.1
  - Java DataBase Connectivity (JDBC) 2.0
  - Java Messaging Service (JMS) 1.0.2
  - Java Management Extensions (JMX) 1.0
  - Java Naming and Directory Interface (JNDI) 1.2
  - JavaServer Pages (JSP) 1.2
  - Java Transaction API (JTA) 1.0.1
  - Java Transaction Services (JTS) 1.0
  - Simple API for XML (SAX) 2.0
  - Servlet (JSDK) 2.3
  - Transformation API for XML (TRAX) 1.1.3
  - COSNaming, which is defined as part of Java 2 Standard Edition (J2SE) 1.3
- Services defined and documented in the formal product documentation. The following table lists these services and contains links to the documentation of these services:

Services	**Documentation**
Application Server	http://publib.boulder.ibm.com/infocenter/wasinfo/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/javadoc/ae/index.html
Java Management Extensions	http://publib.boulder.ibm.com/infocenter/wasinfo/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/javadoc/ae/index.html
MBean	http://publib.boulder.ibm.com/infocenter/wasinfo/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/javadoc/mbean/index.html
Server Configuration	http://publib.boulder.ibm.com/infocenter/wasinfo/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/javadoc/wccm/index.html
Web services	http://publib.boulder.ibm.com/infocenter/wasinfo/index.jsp?

Services	Documentation
	topic=/com.ibm.websphere.base.doc/info/aes/javadoc/wsi/index.html

Note: Application Server is a group of services.

The resources are software modules that are used by some of the services for back-end processing. The following resources are included:

- WebSphere Relational Resource Adapter--handles back-end processing for the product Java Database Connectivity (JDBC) API service.
- WebSphere Java Messenger Service (JMS) Provider--handles back-end processing for the product JMS API service.
- Build-in Mail Provider--handles back-end processing for the product JavaMail API service.
- A naming resource--handles back-end processing for the product JNDI and COSNaming services.
- Security resources--handles back-end processing for the product security services.

2.1.2 Product Client

The Product Client component is a set of application programming interfaces (APIs) that provide an environment for running clients to enterprise applications.

2.1.3 Product Admin Console Tool

The Product Admin Console component is a tool that provides a graphical user interface for managing enterprise applications and their components.

2.1.4 Product wsadmin Tool

The Product wsadmin Tool is a tool that provides a scripting interface for managing enterprise applications and their components.

2.1.5 Product Additional Tools

The Product Additional Tools component is a set of additional tools for doing the following functions:

- Installing, upgrading, and migrating the product
- Assembling enterprise applications
- Monitoring and tuning the runtime environment of enterprise applications
- Troubleshooting the runtime environment of enterprise applications

2.1.6 Product HTTP Server Plug-In

The Product HTTP Server Plug-In component is a set of plug-ins for external HTTP servers. An HTTP Server Plug-in re-routes requests from an external HTTP server to the embedded HTTP server included in the web server container of the Product Server component.

2.1.7 Product Included Software

The Product Included Software Component is a set of external software products and technologies that are included with the product. This set of external software products and technologies include the following:

- Java 2 Software Development Kit (SDK)--contains implementations of all the Java APIs defined in the J2SE V1.3 specification.
- Cloudscape--a database server.
- IBM HTTP Server--an HTTP server.

2.2 Identification of the TOE

The following table lists the product components and indicates whether each component is included in or excluded from the TOE.

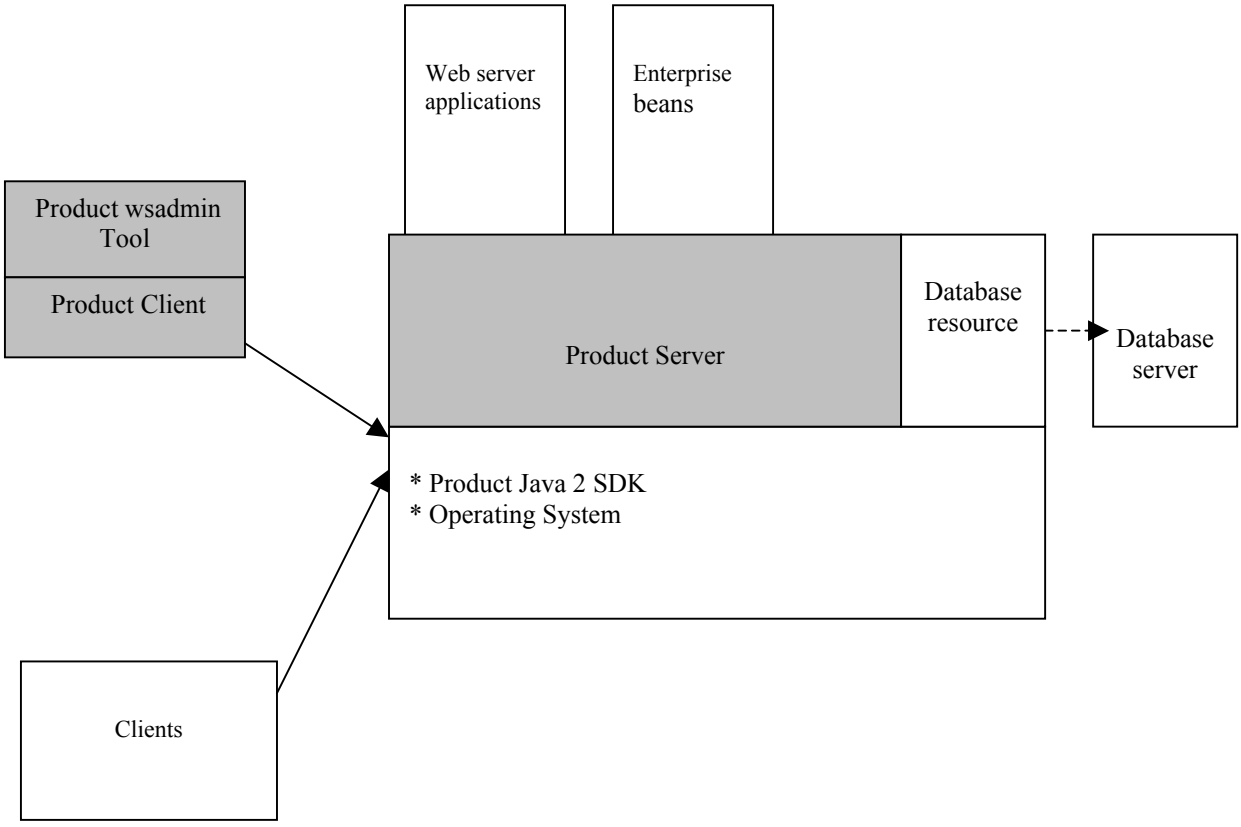
Product Component	**Included in TOE**	**Excluded from TOE**
Product Server	X	
Product Client	X	
Product Admin Console Tool		X
Product wsadmin Tool	X	
Product Additional Tools		X
Product HTTP Server Plug-In		X
Product Included Software		X

The Product Server is included in the TOE because it implements the primary purpose of the product, which is to provide an environment for running enterprise applications and their components and for programmatically managing enterprise applications and their components. The Product wsadmin Tool is included in the TOE because it provides a scripting tool that facilitates the management of enterprise applications. The Product Client is included in the TOE because it is required by the wsadmin Tool.

The remaining product components are excluded from the TOE during installation because they do not implement the primary purpose of the product and are not required to facilitate the product management functions.

2.3 Description of the TOE Evaluated Configuration

The following figure illustrates the evaluated configuration of the TOE. The shaded components are the TOE. The non-shaded components are required or optional in the software environment of the TOE.



2.3.1 TOE

This sub-section describes the TOE components. The TOE components are:

- Product Server
- Product wsadmin Tool
- Product Client

2.3.1.1 Product Server

The Product Server is included in the TOE and required in the evaluated configuration. The Product Server is briefly described in the section "Product Server" of this document.

The following provides additional information about the Product Server and its required configuration.

2.3.1.1.1 Description of the Product Server

In the evaluated configuration, the Product Server performs the following functions:

- Starts up
- Loads local components
- Accepts local and remote requests
- Processes requests for services
- Processes requests for mapped methods and HTML pages

Starts up. The Product Server is started using the Java command provided by the Product Java 2 SDK. The Product Server is run in a single operating system process and JVM.

Loads local components. The Product Server starts the following components:

- Web server applications, and
- Enterprise beans.

These components are run in the same operating system process and JVM that the Product Server is using. Therefore, these components are called "local components."

Accepts local and remote requests. The Product Server accepts requests over its local and remote interfaces. The requests over its local interfaces come from the local components (web server applications and enterprise beans). The Product Server receives these requests directly. The requests over its remote interfaces come from clients. The Product Server receives these requests indirectly by means of the Product Java 2 SDK.

Processes requests for services. If the Product Server receives a request for a service, the Product Server processes any required security and, if security is successful, processes the requested service.

Processes requests for mapped methods and HTML pages. If the Product Server receives a request for a mapped method or HTML page in a local component (web server application or enterprise bean), the Product Server processes any required security and then, if security processing is successful, invokes the mapped method or HTML page.

2.3.1.1.2 Required configuration of the Product Server

In the evaluated configuration, the Product Server must be configured as follows:

- Security:
    - Global security: Enabled;
    - Security Protocol: CSIv2 with basic authentication required and no SSL;
    - User Registry: Operating system (OS);
    - Authentication mechanism: Simple WebSphere Authentication Mechanism (SWAM);

- Java 2 security: Enabled

- JMX connector: RMI
- Resources: All of the following types of resources provided by WebSphere Application Server must be disabled: JDBC Provider, JavaMail Provider, JMS provider, and Resource Adapter.

2.3.1.2 Product wsadmin Tool

The Product wsadmin Tool is included in the TOE and required in the evaluated configuration. It must reside on the same operating system as the Product Client and is run in the same operating system process and JVM as the Product Client.

The Product wsadmin Tool is briefly described in the section Product wsadmin Tool of this document. The following provides additional information about the Product wsadmin Tool and how it is configured in the evaluated configuration.

The Product wsadmin Tool is a Java client application. The administrator starts the Product wsadmin Tool by running a wsadmin.bat file as described in the next section. After the Product wsadmin Tool starts, an administrator can use this tool to execute administrative scripting commands. The Product wsadmin Tool processes these commands by calling the AdminClient API of the Product client.

2.3.1.3 Product Client

The Product Client is included in the TOE and is required in the evaluated configuration. It resides in the same system unit as the Product Server. However, it is considered to be remote from the Product Server because it is run in a different operating system process and JVM from that in which the Product Server is run.

The Product Client is briefly described in the section Product Client of this document. The following provides additional information about the Product Client and how it is used and configured in the evaluated configuration.

In the evaluated configuration, the administrator starts the Product Client using the wsadmin command file. The wsadmin command file causes the Java 2 SDK to start the Product Client and then causes the Product Client to start Product wsadmin Tool. The product wsadmin tool must be configured to communicate with the Product Server by means of the RMI protocol.

Both the Product Client and the Product wsadmin Tool run in a single process and use a single JVM. After the Product Client starts, it accepts AdminClient API requests from the Product wsadmin Tool and processes these requests by calling a remote interface to the Administration Service of the Product Server.

2.3.2 Software Environment of the TOE

This sub-section describes the components that are either required or optional in the software environment of the TOE. (Note that the components described in this sub-section are **not** included in the TOE.) There are no restrictions on the hardware environment of the TOE.

The components that are required or optional in the software environment of the TOE are:

- Product Java 2 SDK

- Operating system
- Database provider and database server
- Web server applications and enterprise beans
- Clients

2.3.2.1 Product Java 2 SDK

The Product Java 2 SDK is included with the product and is required in the evaluated configuration. The Product Java 2 SDK must reside on the system unit of the Product Server.

The TOE uses the following functions of the Product Java 2 SDK:

- The administrator uses the Java command provided by the Java 2 SDK to start the Product Server and the Product Client.
- The Product Server uses the APIs provided by the Java 2 SDK to accept requests from the Product Client and any other clients.
- The Product Client uses the APIs provided by the Java 2 SDK to send requests to the Product Server.
- The Product Server, Product Client, and Product wsadmin Tool use the APIs provided by the Product Server to handle system functions, such as threads.

The APIs provided by the Java 2 SDK are all defined in the J2SE V1.3 specification. None of these APIs are relevant to the TSF.

2.3.2.2 Operating System

The operating system is required in the evaluated configuration. It must reside in the system unit of the Product Server.

The operating system must be one of the following external products:

- AIX 5.2;
- HP-UX 11i;
- Linux SuSE Linux Enterprise Edition (SLES) 8;
- Linux Red Hat 2.1
- Sun Solaris 8; and
- Microsoft Windows 2003.

The TOE components uses the following functions of the operating system:

- The Product Server, as well as all the local components started by the Product Server, run in a process and JVM provided by the operating system.
- The Product Client and Product wsadmin Tool run in a process and JVM provided by the operating system.
- The Product Server uses the user registry provided by the operating system to validate the passwords of clients and to get user and group IDs of clients. The location of the user registry is defined by the operating system. In the evaluated

configuration, the user registry must contain the ID of each user and group that has permission to access a resource protected by the TOE. The user registry must also contain a password for each user ID.

- The Product Server uses the file system provided by the operating system to store and retrieve configuration and naming data.

2.3.2.3 Database Resource and Database Server

If any of the web server applications or enterprise beans use the JDBC API, a database resource is required. If the database resource requires an external database server, the database server also is required. In all other cases, the database resource and database server are not required.

The database resource can be any of the external database resources supported by the product. The Product Server uses this resource to handle back-end processing for the JDBC API. The database server, if required, must be a server supported by the database resource. The evaluated configuration does not have any restrictions as to how to configure the database resource or the database server.

2.3.2.4 Web Server Applications and Enterprise Beans

The web server applications and enterprise beans are developed by application developers and are optional in the evaluated configuration. The following provides a definition of a web server application and an enterprise bean and then describes an assumption that this evaluation makes about these applications.

A *web server application* is any of the following modules: servlets, JSPs, and HTML pages. The modules are packaged and configured as *web server application components*, and the web server application components optionally are packaged and configured as *enterprise applications*. See the Glossary of this document for definitions of servlet, JSP, web server application, web server application component, and enterprise application.

An enterprise bean is a server module. The enterprise beans are packaged and configured as *enterprise bean components*, and the enterprise bean components optionally are packaged and configured as *enterprise applications*. See the Glossary of this document for definitions of enterprise bean, enterprise bean component, and enterprise application.

This evaluation makes an assumption that the developers of the web server applications and enterprise beans have complied with the guidelines listed in the "Assumptions" section of this document. These guidelines describe how to code and configure the web server applications and enterprise beans so that the TSF will be enforced. The person responsible for the TOE needs to ensure that the developers of all web server applications and enterprise beans have followed these guidelines.

2.3.2.5 Clients

The clients are optional in the evaluated configuration. They are entities that are remote from the JVM and operating system process that the Product Server is using and that are attempting to access the resources of the TOE. These resources are:

- Methods and HTML pages in web server applications
- Methods in enterprise beans

- Services of the Product Server

The term "remote" has to do with the operating system process and JVM that the clients are using rather than system unit where the clients are located. If a client is located on the same system unit as the Product Server but is using a different operating system process and JVM than the Product Server is using, the client is considered to be remote.

In the evaluated configuration, the only way that clients can request access to any of these resources is to issue requests to remote interfaces that are implemented by the Product Server.

2.4 Description of the TOE Security Functions

The TOE provides security functionality and mechanisms to protect sensitive resources. A sensitive resource (i.e. protected) is a resource in the TOE that is security relevant and can be accessed, directly or indirectly, by a client. The sensitive resources are:

- A resource (method) in an enterprise bean;
- A resource (method or HTML page) in a web server application;
- The Administration Service;
- The Naming Service;

The Administration Service is implemented by the Product Server and is one of its Application Server services. The Naming Service is implemented by the Product Server and is a generic name that encompasses both the COSNaming and JNDI services, which are both implemented

Note: The Java 2 SDK also implements a COSNaming service. However, in the evaluated configuration, the COSNaming service of the Product Server overrides the COSNaming service of the Java 2 SDK.

2.4.1 Identification

When a client issues a request to the TOE to access a protected resource, the TOE identifies the client before performing any other TSF mediated action for the client. The client passes its user ID to the TOE. The TOE uses the user registry to validate the user ID and gain the group ID(s) for which the client user is a member. The User/group IDs, are maintained within the environment. If the client does not pass its user ID to the TOE, or if the TOE is not able to validate the user ID, the TOE does not process the request. See Section 6.1.1, "Identification (Ident.1)" for more information.

2.4.2 Access Control

The TOE provides one access control function: AC.1. This function permits a client to access a protected resource only if a user or group ID of the user is mapped to a role that has permission to access the resource. See Section 6.1.2, "Access Control (AC.1)" for more information.

2.4.3 System Management

An authorised role can use the wsadmin Tool to configure the following security parameters that are used by the TOE. These parameters are:

- Mappings of user and group IDs to administration roles;
- Mappings of user and group IDs to naming roles; and
- Mappings of user and group IDs to the roles used by each web server application and enterprise bean.

See Section 6.1.3, "System Management (SM.1, SM.2, and SM.3)" for more information.

3 TOE Security Environment

3.1 Introduction

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

The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organisational security policies which the product is designed to comply.

3.2 Threats

The assumed security threats are listed below:

3.2.1 Threats countered by the TOE

[T.ACCESS_RES] A client gains access to a resource without the correct authority to access that resource.

[T.ACCESS_TOE] An unidentified client gains access to a protected resource.

3.2.2 Threats countered by the TOE Environment

[T.APP] The applications and operating system that the TOE interfaces compromises the TOE.

[T.NETWORK] Data transferred between workstations is disclosed to, or modified by unidentified users or processes, either directly or indirectly.

3.3 Organisational Security Policies (OSPs)

The TOE complies with the following OSP:

[P.ACCESS] The right to access a resource is determined on the basis of association of user or group IDs to roles and of roles to resources.

3.4 Assumptions

This section provides the minimum physical and procedural measures required to maintain security of the WebSphere Application Server product.

3.4.1 Physical aspects

[A.APP] It is assumed that the applications and operating system that the TOE interfaces, will not compromise the security of the TOE and where applicable, that they have been configured in accordance with the manufacturer's installation guides and/or its evaluated configuration. It also is assumed that the developers of all local applications (web server applications and enterprise beans) will comply with all the guidelines and restrictions specified in the User Guidance document.

[A.PROTECT] It is assumed that all software and hardware, including network and peripheral devices, have been approved for the transmittal of protected data. Such items are to be physically protected against threats to the confidentiality and integrity of the data. It is assumed that all hardware used in the operating environment is secured.

3.4.2 Personnel Aspects

[A.ADMIN] It is assumed that there are one or more competent individuals that are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, wilfully negligent or hostile.

4 Security Objectives

4.1 Security Objectives for the TOE

[O.ACCESS] The TOE must ensure that only those clients with the correct authority are able to access an object.

[O.IDENTIFY] The TOE must ensure that all clients are identified before they access a protected resource.

[O.MANAGE] The TOE must allow administrators to effectively manage the TOE and that this can be performed remotely only by authorised clients.

4.2 Security Objectives for the TOE Environment

[O.ADMIN] Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

[O.APP] Those responsible for the TOE must ensure that the interfacing applications do not compromise the security of the TOE and that they are installed and configured in accordance with the manufacturer's instructions and/or the evaluated configuration where applicable. In addition, those responsible for the TOE must ensure that the developers of the applications are trusted to comply with the Guidelines listed in the assumption A.APP.

[O.ATTR] The IT Environment shall maintain User and Group mappings for clients.

[O.PROTECT] Those responsible for the TOE must ensure that procedures exist to ensure that data transferred between workstations is secured from disclosure, interruption or tampering.

[O.RECOVER] Those responsible for the TOE must ensure that procedures are provided to ensure that after system failure or other discontinuity, recovery without a security compromise is obtained.

5 Security Requirements

This section specifies the Security Functional Requirements (SFRs) for the TOE and organises the SFRs by class.

Within the text of each SFR, the selection, assignment, and refinement operations (as defined within [CC]) are *italicised*. Iteration of requirements is indicated by a letter in parenthesis placed at the end of the component.

Note: FIA_ATD.EXP is an explicitly stated IT Environment security requirement, and although based on [CC], it has not been specified using CC Part 2 functional components

The International Interpretations that have been applied for the Security Requirements are 058, 064, 065, 103, 201, and 202.

5.1 TOE Security Functional Requirements

The following table summarises the SFRs:

CLASS	FAMILY	COMPONENT	ELEMENT
FDP	FDP_ACC	FDP_ACC.2	FDP_ACC.2.1
			FDP_ACC.2.2
	FDP_ACF	FDP_ACF.1	FDP_ACF.1.1
			FDP_ACF.1.2
			FDP_ACF.1.3
			FDP_ACF.1.4
FIA	FIA_UID	FIA_UID.2	FIA_UID.2.1
	FIA_USB	FIA_USB.1	FIA_USB.1.1
FMT	FMT_MSA	FMT_MSA.1	FMT_MSA.1.1
		FMT_MSA_.3(a)	FMT_MSA_.3.1(a)
			FMT_MSA_.3.2(a)
		FMT_MSA_.3(b)	FMT_MSA_.3.1(b)
			FMT_MSA_.3.2(b)
		FMT_MSA_.3(c)	FMT_MSA_.3.1(c)

CLASS	FAMILY	COMPONENT	ELEMENT
			FMT_MSA_.3.2(c)
	FMT_SMF	FMT_SMF.1	FMT_SMF.1.1
	FMT_SMR	FMT_SMR.1	FMT_SMR.1.1
			FMT_SMR.1.2

5.1.1 Access Control (FDP)

FDP_ACC.2.1 The TSF shall enforce the *access control policy* on *protected resources i.e.:*

- *methods in enterprise beans;*
- *methods and HTML pages in web server applications;;*
- *Administration Service; and*
- *Naming Service),*

and clients and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1.1 The TSF shall enforce the *access control policy* to objects based on the following:

Subject/Object	*Security Attributes*
Client[1]	*User/Group IDs and* *Role*
Protected resources: • *methods in enterprise beans;* • *methods and HTML pages in web server applications;* • *Administration Service; and* • *Naming Service).*	*Role*

[1] A client is a user from a remote JVM.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *A client is granted access to a protected resource if*:

- *The user ID of the client is mapped to a role; or*
- *A group ID of the client is mapped to a role;*

and

- *the role has permission to access the protected Resource.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no additional rules*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the: *no additional rules.*

5.1.2 Identification

FIA_UID.2.1 The TSF shall require each client to identify itself before allowing any other TSF mediated actions on behalf of that client

FIA_USB.1.1 The TSF shall associate the appropriate user attributes with subjects acting on behalf of that client.

5.1.3 Security Management (FMT)

FMT_MSA.1.1 The TSF shall enforce the *access control policy* to restrict the ability to *write or delete* the security *attributes that map user/group IDs* to *roles* to *only* the *clients that are mapped to the administration role with the correct permission.*

FMT_MSA.3.1(a) The TSF shall enforce the *Access Control Policy* to provide *restrictive* default values *for the mappings of user/group IDs to administration roles* security attributes that are used to enforce the SFP.

FMT_MSA.3.2(a) The TSF shall allow the [no user role] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1(b) The TSF shall enforce the *Access Control Policy* to provide *permissive* default values *for the mappings of user/group IDs to naming roles* security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b) The TSF shall allow the [no user role] to specify alternative initial values to override the default values when an object or information is created

FMT_MSA.3.1(c)	The TSF shall enforce the *Access Control Policy* to provide *restrictive* default values *for the mappings of user/group IDs to application-defined roles* security attributes that are used to enforce the SFP.
FMT_MSA.3.2(c)	The TSF shall allow the [application developer] to specify alternative initial values to override the default values when an object or information is created.
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: *configuration of mappings of user and group IDs to roles*
FMT_SMR.1.1	The TSF shall maintain the roles: o *application-defined roles,* o *naming roles, and* o *administration roles.*
FMT_SMR.1.2	The TSF shall be able to associate user and group IDs with roles.

5.2 Strength Of Function (SOF)

There is no strength of function claim because the TOE does not identify any security functional requirements for which an explicit Strength of Function (SOF) is appropriate and does not identify any functions that are of a permutational or probabilistic nature. Therefore, a minimum SOF claim is not included for the TOE.

5.3 TOE Security Assurance Requirements

The target evaluation assurance level for this product is EAL2, augmented with ALC_FLR.1 (Basic Flaw Remediation).

5.4 Security Requirements for the IT Environment

This section specifies the Security Requirements for the IT environment.

5.4.1 Identification and Authentication (FIA)

FIA_ATD.EXP	The environment shall provide services to the TSF to validate the password of individual clients and to obtain the following attributes belonging to individual clients: *User ID and Group IDs.*

6 TOE Summary Specification

6.1 Security Functions (SF)

6.1.1 Identification (Ident.1)

The TOE provides one identification function: Ident.1. This function identifies a client before performing any other mediated TSF function for the client. The client passes its user ID to the TOE. The TOE uses the user registry to validate the user ID and gain the group ID(s) for which the client user is a member. The User/group IDs, are maintained within the environment. If the client does not pass its user ID to the TOE, or if the TOE is not able to validate the user ID, the TOE does not process the request. The following sub-sections provide details on how the identification function is processed for each type of protected resource.

6.1.1.1 Resource in a Web Server Application

When a client requests access to a resource in a web server application, the client issues the request to a remote interface of the TOE. The TOE uses the configuration data to obtain the authentication method configured in the application configuration file. In the evaluated configuration, this method is configured with a value of BASIC or FORM and the TOE uses the value to determine how to obtain the user ID and password of the client.

After getting the value, the TOE then does one of the following:

- If the value is BASIC, the TOE uses the HTTP Basic Authentication Protocol, which is defined in the J2EE V1.3 specification, to obtain the user ID and password of the client. Using this protocol, the TOE sends a challenge to the client requesting the client user ID and password, and the client responds to the challenge by sending its user ID and password. (Despite the name of this protocol, the TOE uses the protocol only to obtain the user ID and password of the client and not to perform any type of authentication.)
- If the value is FORM, the TOE sends an HTML form to the client requesting the client user ID and password, and the client completes this form with its user ID and password.

After obtaining the user ID and password of the client, the TOE processes this information as follows:

1. Issues a request to the operating system user registry inquiring whether the user ID and password are valid. The operating system makes this determination and returns the results to the TOE.

2. Uses the operating system user registry to look up all the groups to which the client is a member.

3. Associates the following identity attributes with the client: user ID of the client and the IDs of all the groups to which the client is a member. The TOE also associates the following special group IDs with the client: "Everyone" and "AllAuthenticated."

If the client does not supply a user ID and password or if the operating system determines that the user ID and password are not valid, the TOE does not process the request.

6.1.1.2 Resource in an Enterprise Bean, the Administration Service, or the Naming Service

When a client requests access to a resource in an enterprise bean, the Administration Service, or the Naming Service, the client must issue the request to a remote interface of the Product Java 2 SDK and, in the evaluated configuration, the client must send its user ID and password with the request. When the Java 2 SDK receives the request, it passes the request to the TOE. The TOE then obtains the user ID and password from the request and processes this information in the same way as described in the previous section.

If the request does not contain a user ID and password or if the operating system determines that the user ID and password are not valid, the TOE returns a fatal error to the Java 2 SDK. The Java 2 SDK then returns this fatal error to the client.

6.1.2 Access Control (AC.1)

The TOE provides one access control function: AC.1. This function permits a client to access a protected resource only if a user or group ID of the user is mapped to a role that has permission to access the resource. The following describes the processing of this function for each type of protected resource.

6.1.2.1 Resource in a Web Server Application

When a client requests access to a resource in a web server application, the TOE does the following:

- Uses the application configuration file to obtain the security constraints configured for the protected resource. Using this information, determines the roles that have permission to access the resource.
- Uses the TOE configuration data to determine if a user or group ID of the client can be mapped to a role that has permission to access the protected resource.

If a user or group ID associated with the client can be mapped to a role that has permission to access the protected resource, the TOE invokes the resource on behalf of the client. Otherwise, the TOE does not invoke the resource.

6.1.2.2 Resource in an Enterprise Bean

When a client requests access to a resource in an enterprise bean, the TOE does the following:

- Uses the application configuration file to obtain the permissions that are configured for the protected resource. Using this information, determines the roles that have permission to access the resource.

- Uses the TOE configuration data to determine if a user or group ID of the client can be mapped to a role that has permission to access the protected resource.

If a user or group ID of the client can be mapped to a role that has permission to access the protected resource, the TOE invokes the resource on behalf of the client. Otherwise, the TOE does not invoke the resource.

6.1.2.3 Administration Service

The Administration Service maintains administration roles and permissions. When a client requests access to the Administration Service, the TOE uses the configuration data to determine all the administration roles that can be mapped to the user and group IDs of the client. If a user or group ID associated with the client can be mapped to a role that has permission to do the requested operation, the TOE processes the request. Otherwise, the TOE does not process the request.

The following are the roles and permissions for the administration service.

Administration Role	**Permission**
Monitor	Permission to read configuration attributes and runtime state
Operator	Monitor permission plus permission to affect runtime state
Configurator	Monitor permission plus permission to write configuration attributes with the exception of the highly sensitive configuration attributes
Administrator	Operator and Configurator permission plus permission to write highly sensitive configuration attributes

6.1.2.4 Naming Service

The Naming Service maintains naming roles and permissions. When a client requests access to the Naming Service, the TOE uses the configuration data to determine all the naming roles that can be mapped to the user and group IDs associated with the client. If a user or group ID associated with the client can be mapped to a role that has permission to do the requested operation, the TOE processes the request. Otherwise, the TOE does not process the request.

The following are the roles and permissions for the naming service:

Naming Role	**Permission**
CosNamingRead	Permission to read from the naming directory
CosNamingWrite	CosNamingRead permission plus permission to write to the naming directory
CosNamingCreate	CosNamingWrite permission plus permission to insert entries in the naming directory

Naming Role	Permission
CosNamingDelete	CosNamingCreate permission plus permission to delete entries in the naming directory

6.1.3 Security Management (SM.1, SM.2, and SM.3)

SM.1 The TOE shall maintain predefined security attributes: *special group IDs, naming roles, and administrator roles.*

The special group IDs are:

- *Everyone*
- *AllAuthenticated*

The naming roles are:

- *COSNamingRead*
- *COSNamingWrite*
- *COSNamingCreate*
- *COSNamingDelete*

The administration roles are:

- *Monitor*
- *Configurator*
- *Operator*
- *Administrator*

SM.2 On initiation of the TOE by default, there are the following mappings of user/group IDs to roles:

- Mappings of user/group IDs to naming roles:

Naming Role	Mapped user/group IDs
COSNamingRead	*Everyone group ID*
COSNamingWrite	*AllAuthenticated group ID*
COSNamingCreate	*AllAuthenticated group ID*
COSNamingDelete	*AllAuthenticated group ID*

- Mappings of user/group IDs to administration roles:

Administration Role	Mapped user/group IDs by default
Monitor	*None*
Operator	*None*
Configurator	*None*
Administrator	*None*

- Mappings of user/group IDs to application-defined roles:

Application-Defined Role	Mapped user/group IDs by default
Each application-defined role	*None or defined by application developer*

SM.3 A client in the Administrator role, via the Product wsadmin Tool, can configure the attributes that map user/group IDs to administration roles. A client in the Administrator or Configurator role, via the Product wsadmin Tool, can configure the attributes that map user/group IDs to the naming roles. A client in the Administrator or Configurator role, via the Product wsadmin Tool, can configure the attributes that map user/group IDs to the appllication-defined roles.

.

6.2 Assurance Measures

Assurance measures will be adopted to address each of the EAL2 assurance requirements, as summarised in table B.1 within [CC] and the International Interpretations 003, 004, 016, 019, 027, 051 (Rev.1). The following table provides a summary:

Assurance Component	Description of how Requirement will be met
ACM_CAP.2	A description of the configuration management used by the developers will be provided with a configuration list that will identify the items that comprise the TOE. This document will uniquely reference the TOE stated within Section 1 of this ST. Confirmation that the TOE is labelled with the correct reference will be provided during testing.
ADO_DEL.1	The developers will provide the delivery procedures used to ensure that security is maintained when distributing versions of the TOE to the user's site.
ADO_IGS.1	Procedures for the secure installation, generation and start-up of the TOE shall be provided.

Assurance Component	Description of how Requirement will be met
ADV_FSP.1	An informal description of the TSF and its external interfaces, describing effects, exceptions and interfaces will be provided.
ADV_HLD.1	A high-level design will be provided that informally describes the security of each component within the TSF. All hardware, software and firmware required by the TOE will be identified. A presentation of the functions provided by the supporting protection mechanisms implemented in these, will also be included. Identification of the interfaces between the components and which of these are externally visible will be provided.
ADV_RCR.1	This correspondence information will be contained within the Functional Specification and high-level design. This will provide a correspondence analysis between the TOE summary specification, the functional specification and the high level design.
AGD_ADM.1	The product operational documentation that describes to the administrator how to operate the TOE in a secure manner will be provided. This will describe the administrative security functions and interfaces available to the administrator. All details of any warnings about functions and privileges and assumptions about user behaviour are included.
AGD_USR.1	The product user guidance documentation will be provided in the product InfoCenter that describes to trusted developers the interfaces that can be called from web server applications and enterprise beans.
ALC_FLR.1	The flaw remediation procedures shall be provided, which describe the procedures used to track all reported security flaws in each release of the TOE. Details of the nature and effect of each flaw shall be provided as well as the status of finding a correction to that flaw. The methods used to provide flaw information; correction and guidance on corrective actions to users shall be described.
ATE_COV.1	Coverage of the TSF by the developers functional testing to the functional specification will be provided as part of the testing documentation.
ATE_FUN.1	Test documentation will be provided, which describes the functional tests performed by the developers. This document will include test plans, test procedures, expected and actual test results, It will also identify the security functions to be tested.
ATE_IND.2	Resources will be made available to the evaluators so that they are able to perform additional, independent testing.
AVA_SOF.1	There are no functions within the TOE that have a strength and therefore no Strength of Functions analysis will be produced.
AVA_VLA.1	A description and analysis of any potential vulnerability identified within the TOE will be performed. This will be documented together with an explanation of why the vulnerabilities cannot be exploited.

7 Rationale

This chapter presents the evidence used in the ST evaluation and supports the claims that the ST is a complete and cohesive set of requirements.

7.1 Correlation of Threats, Policies, Assumptions and Objectives

The following table provides a correspondence of the threats, policies, assumptions and objectives:

Objectives:	O.ACCESS	O.IDENTIFY	O.MANAGE	O.ADMIN	O.APP	O.ATTR	O.PROTECT	O.RECOVER
T.ACCESS_RES	x		x			x	x	x
T.ACCESS_TOE		x	x			x	x	x
T.APP				x	x		x	x
T. NETWORK					x		x	
P.ACCESS	x		x	x	x	x		
A.ADMIN				x				
A.APP				x	x			
A.PROTECT							x	

7.2 Security Objectives Rationale

This section demonstrates that the security objectives stated in Section 4 of this ST are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them.

7.2.1 Threats

This section provides evidence demonstrating coverage of the threats by both the IT and non-IT security objectives.

[T.ACCESS_RES]

A client gains access to a resource without the correct authority to access that resource.

The objective O.ACCESS counters this directly by ensuring that only those clients with the correct authority can access an object. This is supported by O.MANAGE, which ensures that privileged actions are performed effectively.

The following environmental objectives support O.ACCESS in countering the threat:

- O.ATTR – ensures that the correct role to resource association is maintained, and thus preventing any access to a resource that the client is not authorised.
- O.PROTECT – ensures that no objects can be accessed by the cabling between the workstations;
- O.RECOVER – ensures that following a system failure, the TOE is not operating in an insecure state whereby an unauthorised client can gain access to objects they are not authorised to access.

[T.ACCESS_TOE]

An unidentified client gains access to a protected resource.

O.IDENTIFY is the primary objective that counters this threat, by ensuring that all clients are identified before they can access a protected resource. O.MANAGE also supports this by ensuring effective management of the TOE.

The following environmental objectives support O.IDENTIFY in countering the threat:

- O.ATTR – ensures that a UID is maintained thus allowing correct operation of the identification functionality;
- O.PROTECT – ensures that an unidentified client cannot gain access to the TOE via the cabling between the workstations;
- O.RECOVER – ensures that following a system failure, the TOE is not operating in an insecure state whereby an unauthorised client can gain access to the TOE.

[T.APP]

The applications and operating system that the TOE interfaces compromises the TOE.

It is essential that the administrator manages the applications interfacing to the TOE in a secure manner, so that vulnerabilities do not exist, which may lead to compromise of the TOE. The objectives O.APP, O.PROTECT and O.RECOVER all ensure that the operating system is managed in a secure manner. O.ADMIN further supports this threat by ensuring that the administrator is a competent individual that will apply the latest patch information and therefore ensuring that any vulnerabilities that may compromise the security of the operating system becomes known, will be countered.

[T.NETWORK]

Data transferred between workstations is disclosed to, or modified by unidentified clients or processes, either directly or indirectly.

Administrators must ensure that data transferred between workstations i.e. along network cabling, is suitably protected against physical or other (e.g. Sniffing) attacks that may result in the disclosure, modification or delay of information transmitted between workstations. Objective O.PROTECT ensures that this is achieved. O.APP ensures that the protocols used in the transmission of data have been correctly configured within the operating systems.

7.2.2 Security Policy

This section provides evidence demonstrating coverage of the organisational security policy by both the IT and non-IT security objectives.

[P.ACCESS]

The right to access a resource is determined on the basis of association of user or group IDs to roles and of roles to resources.

This policy is implemented through the objective O.ACCESS, which provides the means of controlling access to objects by users and processes. O.MANAGE supports this policy by the administrators ensuring that the policy is maintained.

The environmental objectives O.ADMIN and O.APP further support the policy by ensuring that the interfacing applications are configured in a secure manner so that no vulnerability may exist that enables an unauthorised client to gain an authorised identity.

O.ATTR ensures that the association of roles to resources is maintained, and thus supporting this policy.

7.2.3 Assumptions

This section provides evidence demonstrating coverage of the assumptions by both the IT and non-IT security objectives.

[A.ADMIN]

It is assumed that there are one or more competent individuals that are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, wilfully negligent or hostile.

O.ADMIN is the primary objective that meets this assumption, which ensures that the administrator is a competent and trustworthy person whom is capable of managing the TOE in a secure manner.

[A.APP]

It is assumed that the applications and operating system that the TOE interfaces, will not compromise the security of the TOE and where applicable, that they have been configured in accordance with the manufacturer's installation guides and/or its evaluated configuration. In addition, it is assumed that the developers of the applications comply with the guidelines defined in the following sections of this document: "Web Server Applications" and "Enterprise Beans."

O.APP is the primary environmental objective that satisfies the assumption. This ensures that the administrator installs and configures the supporting operating systems in accordance with:

- The manufacturers instructions; and
- Any evaluated configurations were applicable.

This also ensures that the developers of the applications comply with the guidelines defined in this document.

O.ADMIN supports this by ensuring that the Administrator is a competent and trustworthy person and that the users have been set up appropriately.

[A.PROTECT]

It is assumed that all software and hardware, including network and peripheral devices, have been approved for the transmittal of protected data. Such items are to be physically protected against threats to the confidentiality and integrity of the data.

The environmental objective O.PROTECT ensures that the network cabling is suitably protected against threats of modification, tampering or interruption of the data transmitted via this medium. Also, it is assumed that all hardware used within the operating environment is secured.

7.3 Security Requirements Rationale

7.3.1 Security Functional Requirements Rationale

This section demonstrates that the functional components selected for the TOE provide complete coverage of the defined security objectives. The mapping of components to security objectives is illustrated in the table below.

Security Objective	Functional Component
O.ACCESS	Complete Access Control (FDP_ACC.2) Security Attribute Based Access Control (FDP_ACF.1) User-subject binding (FIA_USB.1) Management of Security Attributes (FMT_MSA.1) Static Attribute Initialisation (FMT_MSA.3(a))
O.IDENTIFY	User Identification before any action (FIA_UID.2)
O.MANAGE	Management of Security Attributes (FMT_MSA.1) Static Attribute Initialisation (FMT_MSA.3(a)(b)(c) Specification of Management Functions (FMT_SMF.1) Security Roles (FMT_SMR.1)

[O.ACCESS]

The TOE must ensure that only those clients with the correct authority are able to access an object.

Association [FIA_USB.1] of user security attributes must be performed in order that the access control mechanism can operate.

The access control mechanism must have a defined scope of control [FDP_ACC.2] with defined rules [FDP_ACF.1]. Authorised clients [FMT_SMR.1] must be able to control who has access to the objects [FMT_MSA.1]. Protection of these objects must be continuous, starting from object creation [FMT_MSA.3(a)]

[O.IDENTIFY]

The TOE must ensure that all clients are identified before they access a protected resource.

Before clients can access a protected resource, they need to be identified [FIA_UID.2].

[O.MANAGE]

The TOE must allow administrators to effectively manage the TOE and that this is only performed by authorised clients.

The TSF must restrict the ability to manage the TOE to authorised administrators [FMT_MSA.1] with default values [FMT_MSA.3(a)(b)(c)] and the security attributes [FMT_MSA.1]. [FMT_SMF.1] specifies the management functions provided by the TOE. [FMT_SMR.1] defines roles in order that the TOE is managed effectively.

7.3.2 Security Environment Requirements Rationale

This section demonstrates that the functional components provided by the environment for the TOE, provide complete coverage of the defined security objectives. The mapping of requirements to security objectives is illustrated in the table below.

Security Objective	Requirement for Environment
O.ATTR	User Attribute Mapping (FIA_ATD.EXP)

[O.ATTR]

The IT Environment shall maintain User and Group mappings for clients.

The User/Group IDs mapping belonging to individual clients must be maintained int eh IT Environment (FIA_ATD.EXP).

7.3.3 Security Assurance Requirements Rationale

This ST contains assurance requirements from the CC EAL2 assurance package.

The EAL chosen is based on the impact that the statements of the security environment and objectives within this ST have on the assurance level. The administrator shall be capable of managing the TOE such that the security is maintained (O.ADMIN) particularly within the operating system that the TOE relies (O.APP), and that the physical environment protects the TOE from any potential vulnerability (O.PROTECT). This EAL level also provides a low to moderate level of independently assured security without demanding additional effort by the developers.

Given the amount of assurance required to meet the TOE environment and the intent of EAL2, this assurance level was considered most applicable for the TOE described within this ST.

EAL2 augmented with ALC_FLR.1, was chosen to provide further assurance in the flaw remediation procedures provided by the developers.

7.4 SFR Dependencies

The below table identifies all of the dependencies of the SFRs included in the ST. Only those SFRs that have a dependency, or are depended upon are shown in the table.

	FDP_ACC.1	FDP_ACF.1	FIA_ATD.EXP	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1
FDP_ACC.2		x						
FDP_ACF.1	x					x		
FIA_UID.2								
FIA_USB.1			x					
FMT_MSA.1	o						x	x
FMT_MSA.3(a)(b)					x			x
FMT_SMR.1				x				

The key to the symbols used, are:

x required dependency

o optional dependency

It should be noted that where there is a dependency on FDP_ACC.1 and FIA_UID.1, then these are provided by FDP_ACC.2 and FIA_UID.2 respectively as these SFRs are hierarchical.

As shown in [CC], all dependencies are satisfied by the TOE, with the exception of FIA_ATD.1. The attributes necessary to support FIA_USB.1 have been included in the explicitly stated requirement FIA_ATD.EXP, which is met by the IT environment of the TOE.

FIA_ATD.EXP has been explicitly stated and was not specified using CC Part 2 functional components. The reason for this is because the TOE requires very specific functionality from the IT Environment and explicitly stating a requirement was the clearest way to express that required functionality.

7.5 TOE Summary Specification Rationale

This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

7.5.1 TSF correspondence to SFRs

This section demonstrates that the combination of the specified TSFs work together so that the SFRs are satisfied. The table below shows the TOE security functions, which together satisfy each SFR element.

SFR	**TSFs**
FDP_ACC.2	AC.1
FDP_ACF.1	AC.1
FIA_UID.2	Ident.1
FIA_USB.1	Ident.1
FMT_MSA.1	SM.3
FMT_MSA.3(a)(b)(c)	SM.2
FMT_SMF.1	SM.3
FMT_SMR.1	SM.1

End of Document