BEA Systems, Inc.

BEA WebLogic Server® V7.0 SP6

with BEA05-107.00 advisory patch

Common Criteria

Security Target

Version 2-0-00

---

29 November 2005

TABLE OF CONTENTS

TABLE OF FIGURES AND TABLES

TABLE/FIGURE **PAGE**

1 SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET IDENTIFICATION

TOE Identification: BEA WebLogic Server® V7.0 SP6 with BEA05-107.00 advisory patch (hereafter referred to as WLS)

ST Identification: BEA WebLogic Server® V7.0 SP6 with BEA05-107.00 advisory patch Common Criteria Security Target

ST Version Number: Version 2-0-00

ST Authors: Paul Ferwerda and Paul Patrick, BEA Systems, Inc.; Kristina C. Rogers and Gary Grainger, CygnaCom Solutions, Inc.

Assurance level: EAL2 augmented by ALC_FLR.1

Registration: <To be filled in upon registration>

Keywords: Application Server

1.2 SECURITY TARGET OVERVIEW

BEA WebLogic Server is an application server that provides a foundation for an enterprise to build and integrate applications and databases. BEA WebLogic Server has a J2EE-compliant tiered architecture. It supports tool sets that facilitate the separation of presentation, business logic, and data, while providing the underlying core functionality necessary for the development and deployment of business-driven applications. Its capabilities support an integrated infrastructure that can connect legacy systems, as well as Web Services.

The scope of this evaluation is the WebLogic Security Subsystem that provides security services to WebLogic Server and hosted applications. The WebLogic Security Subsystem provides the following security functionality:

- Security audit,
- User data protection,
- Identification and authentication,
- Security management, and
- Protection of TSF security functions.

1.3 COMMON CRITERIA CONFORMANCE

This ST has been built with Common Criteria (CC) Version 2.2 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements).

This ST is Common Criteria Version 2.2, Part 2 extended, Part 3 conformant, and EAL2 augmented by ALC_FLR.1. The explicitly stated security functional requirements used in this ST are identified in Table 5.1 and Table 5.5.

1.4 INTERPRETATIONS

CC version 2.2 has 10 final interpretations (editorial changes, and agreed new material) since its publication and the completion of this evaluation. Out of the 10 final interpretations, only *RI 243 – Must Test Setup And Cleanup Code Run Unprivileged?* is applicable to this ST and evaluation.

1.5 DOCUMENT ORGANIZATION

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5 identifies the TOE Security Requirements, which include the TOE Security Functional Requirements (SFR), the Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable. This product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Acronym definitions and references are provided in the Appendices.

1.6 DEFINITION OF TERMS

Group

A group is a set of users. An administrator can specify the conditions under which the membership of a group can hold a role.

Principal

A principal is an identity assigned to a user or group as a result of authentication. Principals are stored in subjects representing each user.

Provider

Security providers are modules that "plug into" the WebLogic Server security framework to provide security services to applications.

Realm

A security realm consists of a set of configured security providers, users, groups, security roles, WebLogic Server entities, and security policies.

Role

A security role is a privilege granted to users or groups based on Username, group membership, and the time of day. WebLogic Server also supports administrative roles as defined under security function SM-1.

Subject

A subject is the representation of a user in WebLogic Server.

User

A user can be a person, such as application end user, or a software entity, such as a client application or other instances of WebLogic Server.

WebLogic resource

A WebLogic resource represents an underlying WebLogic Server entity that can be protected from unauthorized access using security roles and security policies.

2 TOE DESCRIPTION

2.1 PRODUCT OVERVIEW

The BEA WebLogic Server is an application server that provides a foundation for an enterprise to build and integrate applications and databases. BEA WebLogic Server is designed to have a J2EE-compliant tiered architecture, and support for tool sets facilitate the separation of presentation, business logic, and data, providing the underlying core functionality necessary for the development and deployment of business-driven applications. Its capabilities support an integrated infrastructure that can connect legacy systems, as well as Web Services.

WebLogic Server is an application server: a platform for developing and deploying multi-tier distributed enterprise applications. WebLogic Server centralizes application services such as Web server functionality, business components, and access to backend enterprise systems. WebLogic Server also provides enterprise-level security and administration facilities.

Security functionality is provided by the WebLogic Security Subsystem (known hereafter as WebLogic Security Framework (WSF)), which provides security services for the WebLogic Server V7.0 SP6 with BEA05-107.00 advisory patch and hosted application programs. The WSF is an integral subset of the BEA WebLogic Server product.

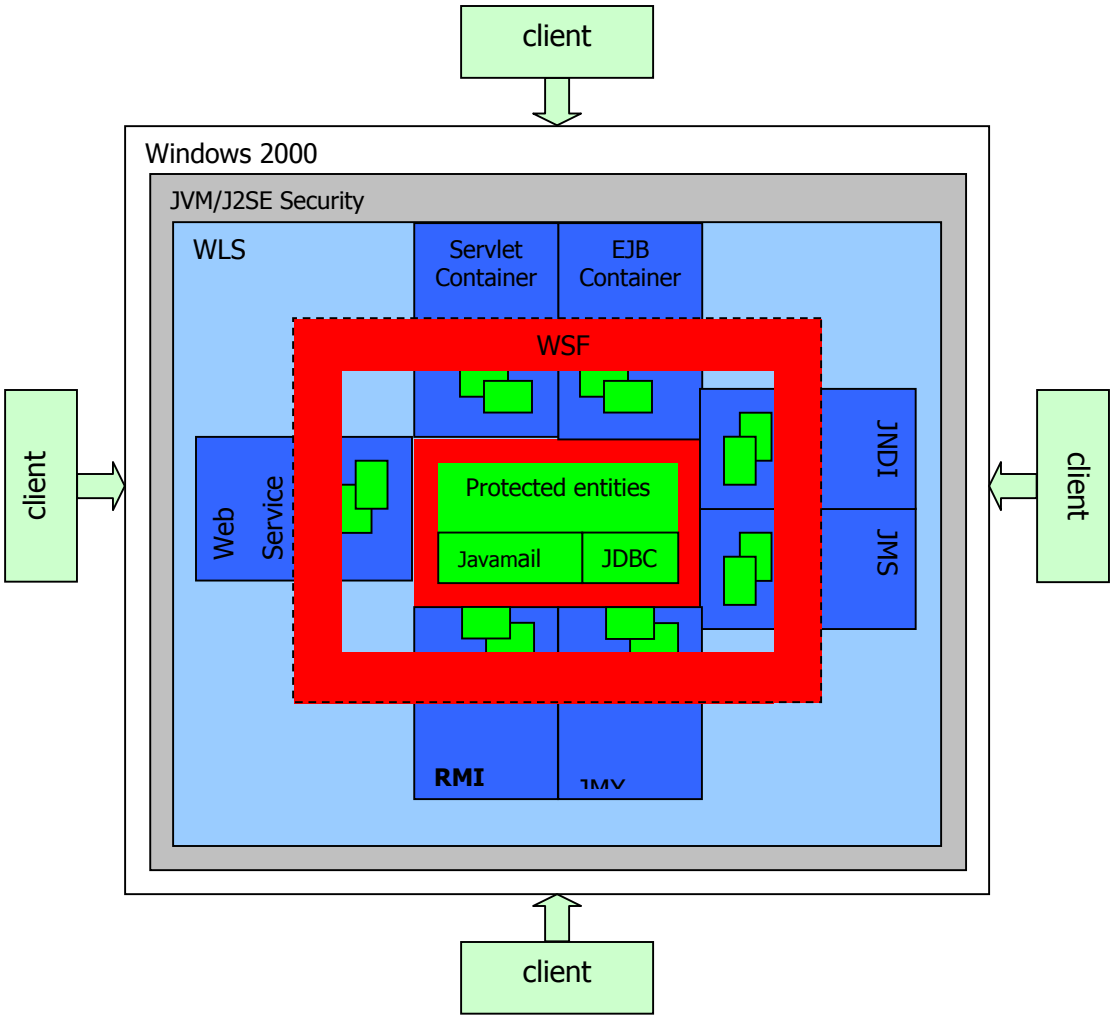
WebLogic Server is made up of various components that may be accessed by clients using various protocols. Figure 2-1 illustrates the WebLogic Server components and their relationship to the WebLogic Security Framework. When a client connects to WebLogic Server to access a WebLogic entity (e.g., application, Enterprise JavaBean), the various WebLogic Server components first check the security policy with the WSF. This ensures that the caller should be granted access to the WebLogic entity. If the WSF grants access, then the WebLogic Server component grants access to the client to access the entity. WSF allows WebLogic Server components to check access for the following types of entities:

- Administrative (represented by AdminResource),
- Application (represented by ApplicationResource),
- Component Object Model (represented by COMResource),
- Enterprise Information System (represented by EISResource),
- Enterprise JavaBean (represented by EJBResource),
- Java Database Connectivity (represented by JDBCResource),
- Java Message Service (represented by JMSResource),
- Java Naming and Directory Interface (represented by JNDIResource),
- Server (represented by ServerResource),
- Web (URL) (represented by URLResource), and
- Web Services (represented by WebServiceResource).

If an entity attempts to access other entities within WebLogic Server, the WSF mediates access based on the access controls configured by the WebLogic Server administrator.

The implementation of WSF security policy decisions by the WebLogic Server components is outside the scope of this evaluation.

Figure 2-1. Relationship of the WebLogic Security Framework to WebLogic Server



In Figure 2-1 HTTP, HTTPS, T3, T3S, RMI-IIOP, SOAP, JCOM and WTC are various protocols that can be used by clients to access WebLogic Server running within the JVM on the physical machine.

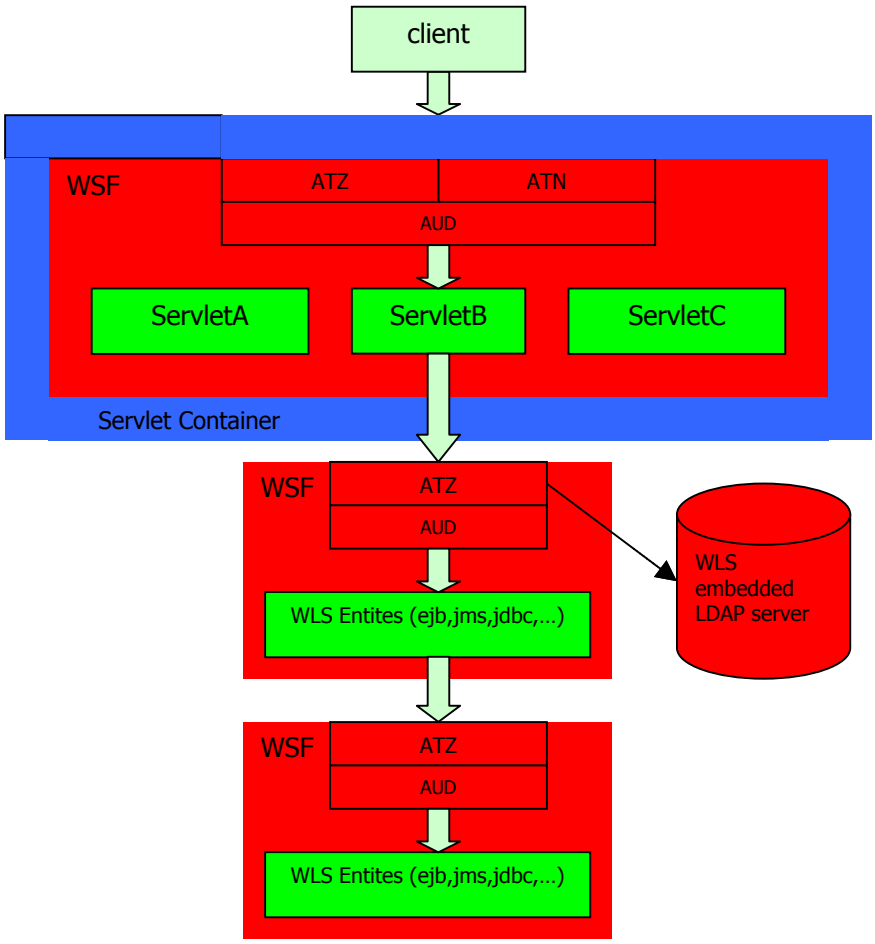
The color code for Figure 2-1 is as follows:

- Gray represents the IT Environment: the physical machine, the operating system, the Java Virtual Machine (JVM) and the J2SE Security sandbox model (See Section 2.4 TOE Environment).
- Light blue represents WLS.
- Dark blue represents the containers for entities that may be accessed by client. Containers interact with the WSF to check whether access to the entity desired by the client is restricted

and grants or denies access as directed by the WSF. It is the responsibility of the containers to enforce the access decision.

- Red represents the WSF which provides the security functions within WLS to protect the entities to be protected. The WSF is responsible for the access control decision.
- Green represents protected entities. Entities within containers may attempt to access other resources and that access attempt will be restricted by the WSF as configured by the WLS administrator.

Figure 2-2 Servlet Container Interaction with WebLogic Security Framework.



As can be seen from Figure 2-2 above a container invokes the WSF in protecting access to application code inside the container (in this example ServletB) from being accessed by a client if the servlet has been protected by the WLS administrator. The Authentication (ATN) and Authorization (ATZ) WSF functions are invoked and all security decisions are audited by the Auditing (AUD) function. Additionally, if the application code needs to access other entities within WLS, the container consults the WSF before access is granted. The WSF as configured for this evaluation uses the WLS embedded LDAP server as its security data store. The Authorization (ATZ) and Authentication (ATN) WSF functions use the WLS embedded LDAP server, but for purposes of keeping the diagram simple, only a single arrow is shown from one of the ATZ functions. The WLS Administration Console (not shown) is also protected by the WSF.

Red represents the WSF. Blue represents the servlet container. Green represents the entity to be protected.

The scope of this evaluation is the red part of the diagram that provides: security audit, user data protection, identification and authentication, security management and protection of TSF.

2.2 TOE PHYSICAL BOUNDARY AND SCOPE OF THE EVALUATION

The evaluated configuration consists of one instance of a WebLogic Server and its associated Administration Console (GUI) running on a single machine connected to a network.

The TOE consists of the WSF including out-of-the-box (as installed by default) security providers together with the Administration Console, and the embedded WLS LDAP server for TSF data. The following WebLogic Server security providers are included in the TOE:

- WebLogic Authentication provider
- WebLogic Identity Assertion provider
- WebLogic Credential Mapping provider
- WebLogic Authorization provider
- WebLogic Adjudication provider
- WebLogic Role Mapping provider
- WebLogic Auditing provider

Section 2.3 below describes the TOE security functionality provided by each security provider.

Figure 2-1 above shows the TOE components (in red) in relation to the entire WebLogic Server product (in blue). Figure 2-2 above provides additional detail about the relationships between a container (in blue) and the TOE (in red) illustrating security functions (SF) authentication (ATN), authorization (AZN), and auditing (AUD) from the security providers.

WebLogic Server carries a J2EE 1.3 Certification, which means that it correctly implements J2EE 1.3 and the various standards that are part of J2EE (EJB, Connectors, JDBC, JMS, JNDI, Servlets, Web Services, etc.), however the claim of J2EE compliance is not part of this evaluation and the WSF itself does not ensure J2EE compliance.

The physical boundary of the TOE is the hardware platform. See section 2.4 for a description of the hardware platform on which the TOE relies.

Table 2-1 indicates what is and what is not part of the TOE.

Table 2-1 What is and is not part of the TOE

TOE Component	Not Included in the TOE Scope			
	Physical Machine #	Operating System	Other supporting software on the same machine	Non-TOE WebLogic Server Components

WebLogic Security Framework from the WLS 7.0 SP6 with BEA05-107.00 advisory patch Administration Console WLS Embedded LDAP server WebLogic Security Providers • Authentication provider • Identity Assertion provider • Credential Mapping provider • Authorization provider • Adjudication provider • Role Mapping provider • Auditing provider	Physical Machine #1 Pentium-based machine with at least: • 400 MHz processor speed, • 512 MB of RAM (1 GB recommended for performance), • 215 MB of disk storage for WebLogic Server plus audit log storage space, and • Clock.	Windows 2000 Server SP4	Sun 1.3.1 JVM Java 2 Security Sandbox	WebLogic Server components other than WSF, such as the servlet container, the EJB container, diagnostic services, the weblogic.Admin client, etc. from the WLS 7.0 SP6 with BEA05-107.00 advisory patch

2.3 TOE LOGICAL BOUNDARY

The TOE provides the following Common Criteria security functions:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions (TSF)

2.3.1 Security Audit

Auditing provides an electronic trail of security-relevant events. The WebLogic Auditing provider supplies these services.

2.3.2 User data protection

The TOE implements access control decision functionality, which WebLogic Server containers use to restrict access to protected WebLogic entities, using the following services supplied by security providers.

Authorization

Authorization is the process whereby the interactions between users and WebLogic entities are controlled. The WebLogic Authorization provider supplies these services.

The TOE access control decision functionality takes a subject, any roles, the specific resources (i.e., representation of an underlying WebLogic Server entity) for which access is being attempted, and renders a decision denying or permitting access. Username and groups assigned at authentication (by the WebLogic Authentication provider) and any roles (determined by the WebLogic Role Mapping provider when access is requested) are matched against policies stored in

the WebLogic Authorization provider to determine whether access should be denied or granted to the requested entity represented by the resource.

Role Mapping

Roles are computed for a requestor for a given resource at a given point in time based on administrator-configured information in the security provider database. The Role Mapping provider supplies the Authorization provider with this information so that the Authorization provider can answer the "is access allowed?" question for WebLogic resources that use role-based security (for example, Web applications and Enterprise JavaBeans (EJBs)).

Adjudication

When multiple Authorization providers are configured, each may return a different answer to the "is access allowed" question for a given resource. Determining what to do if multiple Authorization providers do not agree is the primary function of an Adjudication provider.

The WebLogic Adjudication provider resolves the conflict that might occur when some Authorization providers return PERMIT and some return ABSTAIN. For the purposes of this evaluation the WebLogic Adjudicator will only be dealing with results from the single WebLogic Authorization provider. A DENY or ABSTAIN result from the Authorization provider will be treated as a DENY. A PERMIT result from the Authorization provider will be treated as a PERMIT.

2.3.3 Identification and authentication

Both administrative users and users associated with applications are identified and authenticated by the TOE. The TOE also may be configured to allow anonymous users (but not anonymous administrative users). The TOE implements identification and authentication using the following services supplied by security providers.

Authentication

Authentication is the process whereby the identity of users or system processes are proved or verified. The TOE supports username and password authentication. The WebLogic Authentication provider supplies username / password authentication.

Identity Assertion

An Authentication provider that performs perimeter authentication—a special type of authentication using tokens—is called an Identity Assertion provider. Identity assertion involves establishing a client's identity through the use of client-supplied tokens that may exist outside of the request. Thus, the function of an Identity Assertion provider is to validate and map a CORBA Common Secure Interoperability version (CSIv2) token to a username. The WebLogic Identity Assertion provider supplies these services.

2.3.4 Security Management

The Administration Console is the interface for performing TOE security management functions. The TOE supports four global roles: administrator, deployer, operator, and monitor. These roles provide the capabilities needed to manage the TOE security functions. An anonymous user cannot be assigned a role, and hence, cannot perform any security management functions.

The TOE includes a security provider database to store data used by the security providers. In the evaluated configuration, an embedded LDAP server is used for the security provider database. WebLogic Server, including the TOE, is designed to ensure that only a user acting in an appropriate role can modify or review TOE configuration data.

Credential Mapping

A credential map is a mapping of credentials used by the TOE to credentials used in a legacy or remote system, which tells the TOE how to connect to a given resource in that system. In other words, a credential map allows the TOE to log into a remote system on behalf of a subject that has already been authenticated. The WebLogic Credential Mapping provider supplies this service. The TOE security management functions provide administrators with the capabilities needed to manage credential mapping.

2.3.5 Protection of TSF Security Functions

The WebLogic Server encapsulates the applications it protects within the WebLogic Server security framework to ensure that the security mechanisms are always invoked when resources are requested. WebLogic Server operates as a collection of Java applications that operate in their own domains distinct from one another and also from other potentially untrusted entities.

Hence, the TOE relies on the IT environment for the majority of the services that protect the TSF. The TSF does ensure that, when invoked, it performs its security policy enforcement functions successfully.

2.4 TOE ENVIRONMENT

Because WebLogic Server is a Java-based application server, it must rely upon a Java Virtual Machine (JVM) to interpret the Java byte code for both the application server itself (including the TOE), as well as the applications that are hosted within the application server. The TOE relies upon the Sun 1.3.1 JVM, which is included in the distribution kit.

The TOE was evaluated on the Windows 2000 Server SP4 operating system. Audit records are stored in the operating system files. In addition, WebLogic Server, including the TOE, relies on the operating system to help protect its program and data, to prevent the TOE security functions from being bypassed, and to provide reliable time stamps.

The TOE runs in the Java Run-Time environment. The Java 2 Security Sandbox provides for separate domains for security providers and application code within the JVM.

The hardware platform supporting the TOE may be any Pentium-based machine with at least:

- 400 MHz processor speed,
- 512 MB of RAM (1 GB recommended for performance),
- 215 MB of disk storage for WebLogic Server plus audit log storage space, and
- Clock.

The following are not considered part of the TOE:

- JVM (Sun 1.3.1),
- Windows 2000 Server SP4,
- Java 2 Security Sandbox,
- Hardware platform and any network, and
- WebLogic Server components other than WSF, such as the servlet container, the EJB container, diagnostic services, the weblogic.Admin client, etc.from the WLS 7.0 SP6 with BEA05-107.00 advisory patch

3 SECURITY ENVIRONMENT

This section identifies Secure Usage Assumptions and Threats to Security

3.1 SECURE USAGE ASSUMPTIONS

This section contains the secure usage assumptions.

A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.NO_UNTRUSTED	There are no untrusted user accounts or software on the server platform.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

3.2 THREATS TO SECURITY

This section contains threats to security.

T.BYPASS	An attacker may be able to bypass TOE protection mechanisms through WebLogic Server containers, the JVM, or Windows 2000 Server operating system.
T.EXCESS_AUTHORITY	An administrative user may be granted more authority than they are trained to handle.
T.EAVESDROP	An attacker may be able to observe authentication data transmitted from a user to the TOE.
T.NO_TIME	Those responsible for the TOE may not be able to determine the sequence of security relevant events.
T.STORAGE	Audit data and other TSF data may be lost or modified.
T.TAMPER	An attacker may be able to tamper with TSF programs and data.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNACCOUNTABLE	Users of the TOE may not be held accountable for their actions.
T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNDETECTED_ACTIONS	The administrator may not have the ability to detect potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNIDENTIFIED_USERS	An attacker may gain access to the TOE without being reliably identified allowing them to gain unauthorized access to data or TOE resources.

4 SECURITY OBJECTIVES

The section contains the following subsections:

- Security Objectives for the TOE, which by convention are identified by the O.* labels,
- Security Objectives for the IT Environment, which by convention are identified by the OE.* labels, and
- Security Objectives for the Non-IT Environment, which by convention are identified by the ON.* labels.

4.1 SECURITY OBJECTIVES FOR THE TOE

This section contains the security objectives for the TOE.

O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.
O.ID_AND_AUTH:	The TOE will provide identification and authentication mechanisms that provide the basis for controlling a user's logical access to the TOE and the resources it protects.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the TOE security functions and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE will provide access control decisions for user data in accordance with the WebLogic Server security policy.
O.ROLES	The TOE will support user roles for the management of TOE security functions.
O.SUCCEED	The TOE will ensure that, when invoked, it performs its security policy enforcement functions successfully.

4.2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT

The security objectives for the IT environment are as follows:

OE.AUDIT_REVIEW	The IT environment will provide a capability to review audit trails produced by the TSF.
OE.AUTH_INVOKE	The IT environment will invoke the WSF to identify and authenticate WebLogic Server users.
OE.ENFORCE_POLICY	The WebLogic Server containers will enforce the access control decisions provide by the TOE.
OE.OS_STORAGE	The operating system will provide files for the storage of audit records and other TSF data.
OE.TIME	The operating system platform and JVM will provide support for reliable time stamps.

OE.TSF_PROTECT	The JVM and underlying operating system will protect TSF code and data structures from unauthorized modification and prevent TSF security functions from being bypassed through IT environment interfaces.

4.3 SECURITY OBJECTIVES FOR THE NON-IT ENVIRONMENT

The security objectives for the non-IT Environment are as follows:

ON.NO_EVIL	Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
ON.NO_UNTRUSTED	Those responsible for the TOE will ensure that there are no untrusted user accounts or software on the server platform.
ON.PHYSICAL	Those responsible for the TOE will provide physical security of the WebLogic Server and its hardware platform for the value of the protected IT assets and the value of the stored, processed, and transmitted information.
ON.SEC_COMM	Those responsible for the TOE will ensure that transmissions between users and the TOE are protected from observation.

5 IT SECURITY REQUIREMENTS

This section contains the following:

- TOE Security Functional Requirements
- TOE Security Assurance Requirements, and
- Security Functional Requirements for the IT Environment.

The ST author used the following conventions for operations on Security Functional Requirements:

- Completed assignments are represented by [***bold italic text in square brackets.***]
- Completed selections are represented by **[bold text in square brackets].**
- Refinements are represented *by underlined italic text*.
- Iterations are represented by a semi-colon followed by an integer and **[identifying text]** added to the component title in square brackets.
- Explicitly stated requirements are marked with "_EXP" in their short name.
- Application notes, which are informative, are represented by "Application Note:" followed by a colon and the text of the application note.

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This section contains the security functional requirements for the TOE. The functional components are listed in Table 5.1, which identifies the explicitly stated security functional requirements used in this ST.

Table 5.1 – TOE Security Functional Requirements

No.	Component	Component Name	Source
1	FAU_GEN.1	Audit data generation	CC v2.2 Part 2
2	FDP_ACF_EXP.1	Security attribute based access control decision	Explicitly stated
3	FIA_AFL.1	Authentication failure handling	CC v2.2 Part 2
4	FIA_ATD.1	User attribute definition	CC v2.2 Part 2
5	FIA_UAU.1	Timing of authentication	CC v2.2 Part 2
6	FIA_UAU.5	Multiple authentication mechanisms	CC v2.2 Part 2
7	FIA_UID.1	Timing of identification	CC v2.2 Part 2
8	FMT_MOF.1	Management of security functions behaviour	CC v2.2 Part 2
9	FMT_MSA.1	Management of security attributes	CC v2.2 Part 2
10	FMT_MSA.3	Static attribute initialisation	CC v2.2 Part 2
11	FMT_MTD.1	Management of TSF data	CC v2.2 Part 2
12	FMT_SMF.1	Specification of Management Functions	CC v2.2 Part 2
13	FMT_SMR.1	Security roles	CC v2.2 Part 2
14	FPT_RVM_EXP.1	Non-bypassability of the WSF TSP	Explicitly stated

5.1.1 FAU – Audit

5.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [**not specified**] level of audit; and

c) [***the following auditable events***

1. ***Simple authentication (username/password),***
2. ***Perimeter authentication (based on tokens),***
3. ***User account lockout for failed logons,***
4. ***User account automatic lockout removal,***
5. ***User account explicit lockout removal***
6. ***Access attempt,***
7. ***Obtain roles,***
8. ***Role deployment,***
9. ***Role undeployment,***
10. ***Policy deployment, and***
11. ***Policy undeployment.***]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***severity and server name.***]

Dependencies: FPT_STM.1 Reliable time stamps

5.1.2 FDP – User Data Protection

5.1.2.1 FDP_ACF_EXP.1 Security attribute based access control decision

Hierarchical to: No other components.

FDP_ACF_EXP.1.1 The TSF shall provide WebLogic Server Access Control SFP access control decisions to objects based on:

- Subject attributes:
    1) Username
    2) Group Membership
    3) Roles
- Object attributes:

1) Type of entity
2) Entity name
3) Security policy
4) Security constraints in the deployment descriptor

Application note: In FDP_ACF_EXP.1.2, keep in mind that a resource is the representation in WSF of a WebLogic Server entity, i.e., an object.

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

A) A security policy is a policy statement, which is a Boolean expression of policy expressions.

B) A policy expression is true if

1. The policy condition is “User Name of the Caller” and the subject username matches the username specified by the administrator when constructing the policy condition,
2. The policy condition is “Caller is a Member of the Group” and at least one group to which the subject belongs matches the group specified by the administrator when constructing the policy condition,
3. The policy condition is “Caller is Granted the Role” and at least one of the subject’s roles as determined at the time of the request matches the role specified by the administrator when constructing the policy condition, or
4. The policy condition is “Hours of Access are Between” and the time of the request falls within the allowed time interval specified by the administrator when constructing the policy condition.

C) A policy statement is satisfied if the Boolean expression made up of policy expressions is true when evaluated from left to right.

D) A subject is allowed to access an object if

1. The resource type is URL (Web) or EJB resource, value of the fullyDelegateAuthorization configuration flag is false, and either
    a. The subject satisfies the security constraints in the deployment descriptor associated with the resource or
    b. There is no deployment descriptor associated with the resource; or
2. The resource type is URL (Web) or EJB resource, the value of fullyDelegateAuthorization configuration flag is true, the Ignore Security Data in Deployment Descriptors configuration check box is checked, and either
    a. The subject satisfies the security constraints in the deployment descriptor associated with the resource or
    b. There is no deployment descriptor associated with the resource; or
3. There is a policy statement associated with the resource and the subject satisfies that policy statement; or
4. There is no policy statement associated with the resource and the subject satisfies the policy statement associated with the resource type.

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

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

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

Application note: The term “resource” has special meaning in WebLogic Server context. A resource is a representation of an underlying WebLogic Server entity. Hence, the term “entity” is used to describe objects in this ST instead of “resource.”

Application note: The Servlet and EJB Containers know when an object’s access is unchecked (i.e., wide-open) or excluded (i.e., denied to all). If the fullDelegateAuthorization configuration flag is false, the containers can render access decisions for unchecked or excluded objects without consulting the WSF. If the flag is set to false, then the containers must consult the WSF for all access decisions. See also requirement FDP_ACF.1 for the IT environment.

5.1.3 FIA – Identification and Authentication

5.1.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1: The TSF shall detect when [**an administrator configurable positive integer within** [***the range 1 to unlimited***]] unsuccessful authentication attempts occur related to [***password authentication within the configured lockout reset duration***].

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

Dependencies: FIA_UAU.1 Timing of authentication

Application note: The lockout reset duration is the number of minutes within which invalid login attempts must occur in order for the user’s account to be locked. An account is locked if the number of invalid login attempts set by an administrator happens within the amount of time defined by the lockout reset duration.

5.1.3.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

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

1. ***Username,***
2. ***Password,***
3. ***Group membership,***
4. ***Legacy system credentials, and***
5. ***Account lock status***].

Dependencies: No dependencies

5.1.3.3 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [***actions authorized for the anonymous subject***] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

Application note: There is one anonymous subject per WLS instance. The anonymous subject acts as a tag on the thread of control to mark the fact that there is no authentication associated with the thread. The anonymous subject is a member of the special group named *everyone*. See Table 6.4 – WebLogic Server Resources for details on what access is available to the group *everyone*. Access for the anonymous subject is identical to the access for the group *everyone*.

5.1.3.4 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide [***the following authentication mechanisms:***

1. ***Password-based authentication and***
2. ***Token-based authentication with CORBA Common Secure Interoperability version (CSIv2) identify assertion, and***
3. ***None.***]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [***following rules:***

1. ***The TSF shall use the password-based authentication mechanism when a WebLogic Server container requests user authentication and provides username/password data;***
2. ***The TSF shall use token-based authentication with CSIv2 identity assertion when a WebLogic Server container requests authentication and provides a CSIv2 token;***
3. ***The TSF shall use no authentication mechanism when a WebLogic Server container requests an anonymous subject and provides no authentication data.***]

Dependencies: No dependencies.

Application note: FIA_UAU.5.2 rules 1 and 2 are not mutually exclusive. An administrator must configure either the WebLogic Authentication provider or the WebLogic Identity Assertion provider in order to satisfy FIA_UAU.1.

5.1.3.5 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [***actions authorized for the anonymous subject***] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

Application note: There is one anonymous subject per WLS instance. The anonymous subject acts as a tag on the thread of control to mark the fact that there is no authentication associated with the thread. The anonymous subject is a member of the special group named *everyone*. See Table 6.4 – WebLogic Server Resources for details on what access is available to the group *everyone*. Access for the anonymous subject is identical to the access for the group *everyone*.

5.1.4 FMT – Security Management

5.1.4.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [**enable and disable**] the functions [***the TSF***] to [***administrator and operator roles***].

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Application note: In the context of WSF, “enable” corresponds to the operations boot and unlock and “disable” corresponds to the operations shutdown and lock. These operations apply to the WebLogic Server as a whole, and hence, to all the functions of the TSF.

5.1.4.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [***WebLogic Server Access Control SFP***] to restrict the ability to [***perform operations listed in Table 5.2 on***] the security attributes [***as specified in Table 5.2***] to [***authorised identified roles as specified in Table 5.2***].

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Application note: The dependency on FDP_ACC.1 or FDP_IFC.1 is met by FDP_ACC.1 in this security target.

Table 5.2 – Management of Security Attributes

Operation	Security Attribute	Authorized Roles
Create, modify, and delete	User account attributes	Administrator
View	User account attributes	Administrator, Deployer, Operator, and Monitor
Unlock	A user account	Administrator

5.1.4.3 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [***WebLogic Server Access Control SFP***] to provide [***deployment descriptor-based***] default values for security attributes that are used to enforce the *SFP*.

FMT_MSA.3.2 The TSF shall allow the [***administrator role***] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

5.1.4.4 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [***perform operations listed in Table 5.3 on***] the [***TSF data specified in Table 5.3***] to [***authorised identified roles as specified in Table 5.3***].

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Table 5.3 – Management of TSF data

Operation	TSF Data	Authorized Roles
View	Server configuration including encrypted attributes	Administrator
View	Server configuration, except for encrypted attributes	Deployer, Operator, and Monitor
Deploy	Applications, EJBs, startup and shutdown classes, J2EE Connectors and Web Service components	Administrator Deployer
Edit	Deployment descriptors	Administrator Deployer
Create, modify, nest, and delete	Groups	Administrator
View	Groups	Administrator, Deployer, Operator, and Monitor
Create, modify, and delete	Roles	Administrator
View	Roles	Administrator, Deployer, Operator, and Monitor
Set	fullyDelegateAuthorization Flag	Administrator
View	fullyDelegateAuthorization Flag	Administrator, Deployer, Operator, and Monitor
Set	Ignore Security Data in Deployment Descriptors Check Box	Administrator
View	Ignore Security Data in Deployment Descriptors Check Box	Administrator, Deployer, Operator, and Monitor
Set	Require Unanimous Permit attribute	Administrator
View	Require Unanimous Permit attribute	Administrator, Deployer, Operator, and Monitor
Create. Modify, and delete	A security policy	Administrator

Operation	TSF Data	Authorized Roles
View	Security policy	Administrator, Deployer, Operator, and Monitor
Set	Lockout attributes for a security realm[1]	Administrator
View	Lockout attributes for a security realm	Administrator, Deployer, Operator, and Monitor
Configure	SSL[2]	Administrator
View	SSL configuration	Administrator, Deployer, Operator, and Monitor

5.1.4.5 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

1) ***Manage TOE security functions as specified in FMT_MOF.1;***
2) ***Manage security attributes as specified in Table 5.2 – Management of Security Attributes;***
3) ***Manage TSF data as specified in Table 5.3 – Management of TSF data.***]

Dependencies: No Dependencies.

5.1.4.6 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [

1. ***Administrator,***
2. ***Deployer,***
3. ***Operator, and***
4. ***Monitor***].

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

Dependencies: FIA_UID.1 Timing of identification

5.1.5 FPT – Protection of the TOE Security Functions

5.1.5.1 FPT_RVM_EXP.1 Non-bypassability of the WSF TSP

Hierarchical to: No other components.

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

---

[1] Reference for evaluator to be deleted in final version: See Managing WebLogic Security, Section 7

[2] [2] Reference for evaluator to be deleted in final version: See Managing WebLogic Security, Section 6

Dependencies: No Dependencies.

5.1.6 Strength of Function (SOF) Requirement

The minimum strength of function (SOF) level for the TOE security functional requirements level is SOF-basic.

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.1, Flaw remediation. All of the assurance components are drawn from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5.4.

Table 5.4 – Assurance Components

Component	Title
ACM_CAP.2	Configuration Items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_FLR.1	Flaw remediation
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

5.3 IT SECURITY ENVIRONMENT SECURITY REQUIREMENTS

Table 5.5 lists the security functional requirements for the IT environment.

In accordance with CC interpretation #58, "TSF" has been changed to " *IT environment*" in the security functional requirements for the IT environment in this section. This refinement is made more specific in FDP_ACF.1 to identify the WebLogic Server containers as the components in the IT environment that provide the functionality. This refinement is indicated by underlined, italic text.

Table 5.5 – Security Functional Requirements for the IT Environment

Ref	Component	Component Name	Source
1E	FAU_SAR.1	Audit review	CC v2.2 Part 2
2E	FAU_STG_EXP.1	Protected WebLogic Server audit trail storage	Explicitly Stated
3E	FDP_ACC.1	Subset access control	CC v2.2 Part 2
4E	FDP_ACF.1	Security attribute based access control	CC v2.2 Part 2
5E	FIA_UAU_EXP.1	Timing of authentication request	Explicitly Stated
6E	FIA_UID_EXP.1	Timing of identification request	Explicitly Stated
7E	FPT_RVM_EXP.2	Non-bypassability of the IT environment security policy	Explicitly Stated
8E	FPT_SEP.1	TSF domain separation	CC v2.2 Part 2
9E	FPT_STM.1	Reliable time stamps	CC v2.2 Part 2

5.3.1 FAU – Audit

5.3.1.1 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The *IT environment* shall provide [***WebLogic Server administrators***] with the capability to read [***all WebLogic Server audit information***] from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

5.3.1.2 FAU_STG_EXP.1 Protected WebLogic Server audit trail storage

Hierarchical to: No other components.

FAU_STG_EXP.1.1 The IT environment shall protect the stored WebLogic Server audit records from unauthorised deletion.

FAU_STG_EXP.1.2 The IT environment shall be able to prevent unauthorised modifications to the audit records in the WebLogic Server audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.3.2 FDP – User data protection

5.3.2.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The *IT environment* shall enforce the [***WebLogic Server Access Control SFP***] on [

- ***Subjects: Instances of the Java class Subject representing WebLogic users***
- ***Objects: WebLogic Server entities. WebLogic Server controls access to the following types of entities:***
    1. ***Application: Enterprise Application aRchive (EAR)***

2. ***Component Object Model (COM): Java objects to be exported as COM objects to be accessed by COM client applications***
3. ***Enterprise Information System (EIS): Resource Adapter aRchive (RAR)***
4. ***Enterprise JavaBean (EJB):***
    a. ***EJB JARs,***
    b. ***Individual EJBs within an EJB JAR,***
    c. ***Individual methods of an EJB.***
5. ***Java Database Connectivity (JDBC):***
    a. ***ConnectionPool Java objects***
    b. ***MultiPool Java objects***
6. ***Java Message Service (JMS):***
    a. ***Queue Java objects***
    b. ***Topic Java objects***
7. ***Java Naming and Directory Interface (JNDI): naming contexts***
8. ***Universal Resource Locator (URL):***
    a. ***Web Application aRchive (WAR) file***
    b. ***Individual modules of a Web application (servlets, JSPs).***
9. ***Web Service:***
    a. ***Entire Web service***
    b. ***Individual methods of a Web service.***

- ***Operations: As specified in Table 5.6.***]*Error! Reference source not found.*

Table 5.6 – Operations corresponding to Objects

Entities	*Operation*
Application	***Access***
Component Object Model	***Export***
EIS	***Access***
EJB	***Access***
JDBC	***Reserve, admin, shrink, reset***
JMS	***Send, receive, browse***
JNDI	***Lookup, list, modify***
URL	***Access***
WebService	***Access***

Dependencies: FDP_ACF.1 Security attribute based access control

Application note: The term “access” in Table 5.6 denotes invoke services provided by the corresponding object to the granularity indicated in the subject list.

Application note: The term “resource” has special meaning in a WebLogic Server context. A resource is a representation of an underlying WebLogic Server entity. Hence, the term “entity” is used to describe objects in this ST instead of “resource.”

Application note: The functions for enforcing the WebLogic Server Access Control SFP are divided between the TOE and the IT environment. WebLogic Server containers pass WSF access request information (c.f. FDP_ACF_EXP.1 in section 5.1.2.1)

Application note: WebLogic Server has administrative entities (i.e., Administration console, weblogic.Admin client, and MBean APIs) and server entities in addition to the entities listed in FDP_ACC.1. These entities are accessible only to users with administrative roles as specified in 5.1.4 FMT – Security Management.

5.3.2.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The *WebLogic Server containers security functions* shall enforce the [***WebLogic Server Access Control SFP***] to objects based on [

- ***Subject attributes:***
    1) ***Username***
    2) ***Group Membership***
    3) ***Roles***
- ***Object attributes:***
    1) ***Type of Entity***
    2) ***Entity name***
    3) ***Security policy***
    4) ***Security constraints in the deployment descriptor***]

FDP_ACF.1.2 The *WebLogic Server containers security functions* shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

1. ***A WebLogic container will grant a subject access to an entity represented by a resource if the WSF returns TRUE in response to the container resource request.***]

FDP_ACF.1.3 The *WebLogic Server containers security functions* shall explicitly authorise access of subjects to objects based on the following additional rules: [

1. ***The resource type is URL (Web) or EJB resource, value of the fullyDelegateAuthorization configuration flag is false, and the deployment descriptor indicates the resource is unchecked.***]

FDP_ACF.1.4 The *WebLogic Server containers security functions* shall explicitly deny access of subjects to objects based on the [

1. ***The resource type is URL (Web) or EJB resource, value of the fullyDelegateAuthorization configuration flag is false, and the deployment descriptor indicates the resource is excluded.***]

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF_EXP.1 Security attribute based access control decision

Application note: The dependency on FDP_ACF_EXP.1 is specific to WLS because the TSF and the IT environment cooperate to implement access control policy.

5.3.3 FIA – Identification and authentication

5.3.3.1 FIA_UAU_EXP.1 Timing of authentication request

Hierarchical to: No other components.

FIA_UAU_EXP.1.1 The WebLogic Server container security functions shall allow actions authorized for anonymous subjects on behalf of the user to be performed before the user is authenticated.

FIA_UAU_EXP.1.2 The WebLogic Server container security functions shall require each user to be successfully authenticated before allowing any other actions mediated by the WebLogic Server container security functions on behalf of that user.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID_EXP.1 Timing of identification request

5.3.3.2 FIA_UID_EXP.1 Timing of identification request

Hierarchical to: No other components.

FIA_UID_EXP.1.1 The WebLogic Server container security functions shall allow actions authorized for anonymous subjects on behalf of the user to be performed before the user is identified.

FIA_UID_EXP.1.2 The WebLogic Server container security functions shall require each user to be successfully identified before allowing any other actions mediated by the WebLogic Server container security functions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

5.3.4 FPT – Protection of the TSF

5.3.4.1 FPT_RVM_EXP.2 Non-bypassability of the IT environment security policy

Hierarchical to: No other components.

FPT_RVM_EXP.2.1 The IT environment shall ensure that its security policy enforcement functions are invoked and succeed before each function within the scope of control of the IT environment is allowed to proceed.

Dependencies: No Dependencies.

5.3.4.2 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

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

FPT_SEP.1.2 The *IT environment* shall enforce separation between the security domains of subjects in the *IT environment scope of control*.

Dependencies: No Dependencies.

5.3.4.3 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The *IT environment* shall be able to provide reliable time stamps for its own use.

Dependencies: No Dependencies.

6 TOE SUMMARY SPECIFICATION

6.1 IT SECURITY FUNCTIONS

6.1.1 Security Audit

AUD-1 Audit Generation

WebLogic Server security audit events are generated by the WSF in the evaluated configuration. The Auditing provider offers auditing functions used by the other WSF components. WSF components invoke the Auditor (which in turn invokes the Auditing provider) when a security-relevant event occurs, providing all pertinent information, with the time stamp obtained from the hosting IT environment (i.e., Java methods and host OS). The WebLogic Auditing provider makes the decision about whether to record an audit record of a particular event based on the audit severity levels. A security-related event is only recorded when its severity meets or exceeds the severity level specified in the configuration of the Auditing provider. The WebLogic Auditing provider records the event data associated with these security events.

(FAU_GEN.1)

AUD-2 Auditable Events

The WSF can generate audit records for the auditable events listed in FAU_GEN.1.1. The correspondence between the SFR auditable events and WebLogic Server documentation terminology is given in Table 6.1 – Auditable Events.

Table 6.1 – Auditable Events

SFR Auditable Event	Event Type
Start-up of the audit functions	Server startup with audit provider enabled
Shutdown of the audit functions	Server shutdown with audit provider enabled
Simple authentication (username/password)	AUTHENTICATE
Perimeter authentication (based on tokens)	ASSERTIDENTITY
User account lockout for failed logons	USERLOCKED
User account automatic lockout removal	USERLOCKOUTEXPIRED
User account explicit lockout removal	USERUNLOCKED
Access attempt	ISAUTHORIZED
Obtain Roles	ROLEVENT
Role deployment	ROLEDEPLOY
Role undeployment	ROLEUNDEPLOY
Policy deployment	POLICYDEPLOY
Policy undeployment	POLICYUNDEPLOY

(FAU_GEN.1)

AUD-3 Audit Record Fields

Audit records contain the fields listed in Table 6.2

Table 6.2 – Audit Record Fields

Message Field	Field Description
Timestamp	The time and date when the message originated, in a format that is specific to the locale.
Severity	Indicates the degree of impact or seriousness of the event reported by the message.
Event type	Indicates the type of security event being reported
Event	Contains information about the specific security event, including identify of subject whose action caused the event. The content of the event is specific to the type of the event.

The name of the WebLogic Server is contained in the path to the audit trail file itself (e.g., "yourserver" in WL_HOME\yourdomain\yourserver\DefaultAuditRecorder.log).

(FAU_GEN.1)

AUD-4 Severity Attribute

Table 6.3 lists the possible values of the severity attribute and their meanings. The values are listed in order with FAILURE being the most severe.

Table 6.3 – Severity Attribute

Severity	Meaning
INFORMATION	Used for reporting normal operations.
WARNING	A suspicious operation or configuration has occurred but it may not have an impact on normal operation.
ERROR	A user error has occurred. The system or application is able to handle the error with no interruption, and limited degradation, of service.
SUCCESS	Used to report that a security decision occurred and the requested security action was permitted
FAILURE	Used to report that a security decision occurred and the requested action was not permitted

(FAU_GEN.1)

AUD-5 Audit Record Format

When a WebLogic Server instance outputs a security event, the first line of each event record in the audit log begins with "#### Audit Record Begin" followed by the event information and terminated with the text "Audit Record End ####". Each attribute of the event information is contained between angle brackets. The following is an example of an audit event record:

Audit Record Begin <Jun 2, 2002 10:23:02 AM> <Severity =FAILURE> <EventType=Authentication Audit Event> <baduser> <AUTHENTICATE> Audit Record End

In this example, the attributes are: Timestamp, Severity, Event Type, username, and type of authentication event.

(FAU_GEN.1)

AUD-6 WebLogic Server Log Files

WSF writes the messages to audit files. These files can be viewed with a standard text editor.

Each WSF instance writes all event records to an audit file that is located on the local host machine. All auditing information recorded by the WebLogic Auditing provider is saved in WL_HOME\yourdomain\yourserver\DefaultAuditRecorder.log.

(FAU_GEN.1)

6.1.2 User data protection - Authorization (Access Control)

ACC-1 Access Decisions

The TSF includes the default WebLogic Authorization provider for making access control decisions. WLS components invoke the WSF for access control decisions. The WSF computes a list of roles for the subject and then invokes the WebLogic Authorization provider to obtain an access decision. The WebLogic Authorization provider uses a policy-based authorization engine to determine if a particular user is allowed access to a protected WebLogic resource. The WebLogic Authorization provider also supports the deployment and undeployment of security policies within the system.

The WSF also invokes the WebLogic Adjudicator provider, which is used to mediate decisions when multiple authorization providers are configured. (However, multiple authorization providers are not part of the TOE.)

The WSF returns a boolean value to the caller with a result of true indicating that access is allowed and a result of false indicating that access is denied.

Application Note: The enforcement of the access control decision lies within the Containers as described in Section 2. The containers were outside the scope of this evaluation.

(FDP_ACF_EXP.1)

ACC-2 Security Policies

A security policy is an association between a WebLogic entity and one or more users, groups, or security roles. A security policy consists of a set of policy statements, each of which is a boolean combination of expressions. An expression is a policy condition together with specific information (e.g., the actual role to be used in the policy condition). The policy conditions that are available in the TSF are:

1. “User Name of the Caller” and the information matches the username specified by the administrator when constructing the policy condition,
2. “Caller is a Member of the Group” and the information matches the group specified by the administrator when constructing the policy condition,
3. “Caller is Granted the Role” and information matches the role specified by the administrator when constructing the policy condition, or
4. “Hours of Access are Between” and the information falls within the allowed time interval specified by the administrator when constructing the policy condition.

Security policies can be assigned to

1. A type of WebLogic entity,

2. WebLogic entities, or
3. Attributes or operations of a WebLogic entity.

If a security policy is assigned to a type of WebLogic entity, all new instances of that entity inherit that security policy. Security policies assigned to individual entities or attributes override security policies assigned to a type of WebLogic entity.

The TSF WebLogic Authorization provider stores security policies in the security provider database. The default security policies are based on security roles and default global groups.

(FDP_ACF_EXP.1)

ACC-3 Subject Roles

Security policy expressions may include role-based conditions. Security roles are computed and granted to users or groups dynamically. The TSF includes a WebLogic Role Mapping provider for computing and granting roles dynamically.

The role mapping process is initiated when a user or system process requests a WebLogic entity on which it will attempt to perform a given operation. The entity container that handles the type of WebLogic entity being requested receives the request. The entity container calls the WebLogic Security Framework and passes in the request parameters, including:

- Subject of the request
- WebLogic resource representing the entity being requested, and
- Request-specific information.

The WSF calls the Role Mapping provider to obtain a list of the roles that apply. If a security policy specifies that the requestor is entitled to a particular role, the role is added to the list of roles that are applicable to the subject. This process continues until all security policies that apply to the WebLogic entity or the entity container have been evaluated.

The list of roles is returned to the WSF, where it is used in access decisions.

The WebLogic Role Mapping provider supports the deployment and undeployment of roles within the system. The WebLogic Role Mapping provider uses the same security policy engine as the WebLogic Authorization provider.

Users may be placed into groups that are associated with security roles, or be directly associated with security roles. Security roles can be scoped to specific WebLogic resources within a single application in a WebLogic Server domain (unlike groups, which are always scoped to an entire WebLogic Server domain.)

(FDP_ACF_EXP.1, FMT_MOF.1, FMT_MSA.1, FMT_MTD.1)

ACC-4 WebLogic Resources

A WebLogic resource is a structured object used to represent an underlying WebLogic Server entity, which can be protected from unauthorized access using security roles and security policies. The WebLogic Server protects the eleven types of resources listed in Table 6.4.

Table 6.4 – WebLogic Server Resources

Type of Resource	Description and how protected	Default Security Policy

Type of Resource	Description and how protected	Default Security Policy
Administrative	Protected public interfaces Access can be granted to: 1. The Administrative console, 2. weblogic.admin, and/or 3. MBean APIs	Default global roles: Admin, Deployer, Operator, and Monitor
Application	Resources that represent enterprise applications, packaged as EAR (Enterprise Application aRchive) files. Use this type of WebLogic resource to protect all EJBs (Enterprise JavaBeans) within an entire application.	None
COM	Resources that are designed as program component objects according to Microsoft's framework. Grant the COM client user access to the classes that the COM client application needs to access. [3]	Default group: everyone
EIS	Resources that are designed as connectors, which allow for the integration of Java applications with existing enterprise information systems. If the resource adapter has not defined specific security policies, WebLogic Server overrides the runtime environment for the resource adapter with the default security policies specified in the J2EE Connector Architecture Specification. If the resource adapter has defined specific security policies, WebLogic Server first overrides the runtime environment for the resource adapter first with a combination of the default security policies for resource adaptors and the specific policies defined for the resource adapter. Resource adapters define specific security policies using the security-permission-spec element in the ra.xml deployment descriptor file. [4]	Default group: everyone
EJB	Resources that are related to EJBs. Use this type of WebLogic resource when you want to protect: 1. EJB JARs, 2. individual EJBs within an EJB JAR, or 3. individual methods on an EJB.	Default group: everyone
JDBC	Resources that are related to JDBC. To secure JDBC database access, you can create security policies and security roles for all connection pools as a group, individual connection pools, and MultiPools. When you secure individual connection pools, you can choose whether to protect all operations on the connection pool, or specify one of the following operations: 1. Admin 2. reserve 3. shrink 4. reset	Default group: everyone
JMS	Resources that are related to JMS.	Default group:

[3] Reference for evaluator to be deleted in final version: see Configure Access Control in *Programming WebLogic jCO*M. (jcom.pdf)

[4] Reference for evaluator to be deleted in final version: See Security in *Programming WebLogic J2EE Connectors*. (jconnector.pdf)

Type of Resource	Description and how protected	Default Security Policy
	To secure JMS destinations, you can create security policies and security roles for all destinations (JMS queues and JMS topics) as a group, or an individual destination (JMS queue or JMS topic) on a JMS server. When you secure a particular destination on a JMS server, you can choose whether to protect all operations on the destination, or specify the send, browse, or receive operations (for a JMS queue) and the send and receive operations (for a JMS topic).	everyone
JNDI	Resources that use the industry-standard JNDI API to enable connectivity to heterogeneous enterprise naming and directory services To secure access to the JNDI tree, create security policies and security roles for the entire JNDI tree, or an individual branch of that tree. Regardless, you can choose whether to protect all operations, or specify the lookup, modify, or list operations.	Default group: everyone
Server	WebLogic Server instances. The allowed operations are Boot, Shut down, Lock, and Unlock	Default global roles: Admin Operator
Universal Resource Locator (URL)	Resources that are related to Web applications. To secure Web applications, create security policies and security roles for a WAR (Web Application aRchive) file or individual components of a Web application (such as servlets and JSPs).	Default group: everyone
Web Service	Resources that are related to services, which can be shared by and used as components of distributed, Web-based applications. This type of WebLogic resource can be an entire Web service or individual components of a Web Service. WebLogic Web services are packaged as standard J2EE Enterprise applications. Consequently, access to the Web service is secured by securing access to some or all of the J2EE components that make up the Web service: the web service, the web service URL, the stateless session EJB that implements the Web service, and a subset of the methods of the stateless session EJB. [5]	Default group: everyone

(FDP_ACF_EXP.1)

ACC-5 Configuration Options for EJB and URL (Web) Resources

Access to EJB and URL (Web) Resources can be controlled using either the Administration Console or Deployment Descriptors or a combination.

This is controlled using the *fullyDelegateAuthorization Flag* and *Ignore Security Data in Deployment Descriptors Check Box.*

fullyDelegateAuthorization Flag

[5] Reference for evaluator to be deleted in final version: See Configuring Security in *Programming WebLogic Web Services (webserv.pdf)*

When the value of the fullyDelegateAuthorization flag is false, the WebLogic Security Service *only* performs security checks on URL and EJB resources that have security specified in their associated deployment descriptors. This is the default.

When the value of the fullyDelegateAuthorization flag is true, the WebLogic Security Service performs security checks on all URL (Web) and EJB resources, regardless of whether there are any security settings in the deployment descriptors for these WebLogic resources.

Ignore Security Data in Deployment Descriptors Check Box

If the Ignore Security Data in Deployment Descriptors check box is checked, the security policy for URL and EJB resources is determined by the WebLogic Server Administration Console.

If the Ignore Security Data in Deployment Descriptors check box is not checked, the security policy for URL and EJB resources is determined by the deployment descriptors (that is, the ejb-jar.xml, weblogic-ejb-jar.xml, web.xml, and weblogic.xml files).

(FDP_ACF_EXP.1, FMT_MTD.1)

6.1.3 Identification and Authentication

IA-1 Identity

The username is the unique identifier for a user within a security realm. No username is associated with the anonymous subject.

(FIA_UID.1)

IA-2 User Attributes

WebLogic Server maintains the following user attributes:

1. Username,
2. Password,
3. Group membership,
4. Legacy system credentials, and
5. Account lock status

(FIA_ATD.1)

IA-3 Authentication Process

A container supplies a user's claimed identity and credential to the WSF. The WSF verifies the identity of the user based on that credential. Upon successful authentication, the WSF associates the principal assigned to the user with the thread of execution running on behalf of the user.

The verification mechanism used by the WSF depends upon the type of credentials provided by the WebLogic Server container.

1. If the credential is a password, the WSF calls upon the WebLogic Authentication provider to verify username with the password.
2. If the credential is a CORBA CSIv2 identity assertion, the WSF calls upon the WebLogic Identity Assertion provider to validate the token.

In the case of anonymous subjects, a WebLogic Server container requests a subject but provides neither a username nor authentication credentials. WSF creates the subject without username or group principals, which identifies the subject as an anonymous subject.

(FIA_UAU.1, FIA_UAU.5, FIA_UID.1)

IA-4 Password-based authentication

The WSF performs authentication based on username and password by calling the WebLogic Authentication provider.

The minimum password length is eight (8) characters.

Application note: The administrator may set the minimum password length to less than 8 characters. To maintain CC compliance the password must be set to 8 or greater.

WebLogic Server stores passwords in the security provider database. (The WSF stores hashed versions of the passwords, but the cryptographic hash functionality is not claimed as TOE functionality.)

The IT environment (i.e., WebLogic Server containers) requests user ID and password from the user and sends them to the WSF. When WSF receives an authentication request, the password presented by the IT environment is hashed and WSF compares it to the already hashed password to see if it matches.

This provider allows the administrator to edit, list, and manage users and group membership.

(FIA_UAU.5)

IA-5 Token-based authentication

The Identity Assertion provider is a specific form of Authentication provider called by the WSF that allows users or system processes to assert their identity using tokens. The function of the Identity Assertion provider is to validate and map a token to a username. Once this mapping is complete, the default Authentication provider's LoginModule is used to convert the username to principals within the subject representing the user.

In the evaluated configuration, the WebLogic Identity Assertion provider supports token-based authentication using CORBA Common Secure Interoperability version 2 (CSIv2) identity assertion.

(FIA_UAU.5)

IA-6 Authentication Failure Handling

WSF defines a set of attributes to protect user accounts as listed in Table 6.5. If a user account exceeds the values set for the attributes on the User Lockout Tab, the user account becomes locked. The User Lockout attributes apply to the security realm and all its security providers. Only administrators can configure User Lockout attributes. (See security function SM-1 Administrative Roles.)

Table 6.5 – User Lockout Attributes

Attribute	Description	Default
Lockout Enabled	Requests the locking of a user account after invalid attempts to log in to that account exceed the specified Lockout Threshold during a period less than the Lockout Reset Duration attribute.	Enabled
Lockout	A positive integer number of failed user password entries that can be	5

Attribute	Description	Default
Threshold	tried before that user account is locked. Any subsequent attempts to access the account (even if the username/password combination is correct) raise a Security exception; the account remains locked until it is explicitly unlocked by the system administrator or another login attempt is made after the Lockout Duration period ends.	
Lockout Duration	Number of minutes that a user's account remains inaccessible after being locked in response to several invalid login attempts within the amount of time specified by the Lockout Reset Duration attribute.	30 minutes
Lockout Reset Duration	Number of minutes within which invalid login attempts must occur in order for the user's account to be locked. An account is locked if the number of invalid login attempts defined in the Lockout Threshold attribute happens within the amount of time defined by this attribute.	5 minutes
Lockout Cache Size	Specifies the intended cache size of unused and invalid login attempts.	5
Lockout GC Threshold	The maximum number of invalid login records that the server keeps in memory. If the number of invalid login records is equal to or greater than the value of this attribute, the server's garbage collection purges the records that have expired. A record expires when a user is unlocked or when the Lockout Reset Duration has expired for that record.	400 records.

(FIA_AFL.1)

6.1.4 Security Management

SM-1 Administrative Roles

Table 6.6 describes the four global roles that WSF uses to determine access privileges for system administration operations, and the permissions granted to each role.

Table 6.6 – Global Roles and Permissions

Global Role	Global Role Permissions
Administrator	View the server configuration, including the encrypted value of encrypted attributes. Modify the entire server configuration: Deploy applications, EJBs, startup and shutdown classes, J2EE Connectors, and Web Service components, and edit deployment descriptors. Start, resume, and stop servers by default. [6]
Deployer	View the server configuration, except for encrypted attributes: Deploy applications, EJBs, startup and shutdown classes, J2EE Connectors, and Web Service components, and edit deployment descriptors.
Operator	View the server configuration, except for encrypted attributes. Start, resume, and stop servers by default.
Monitor	View the server configuration, except for encrypted attributes.

Server configuration includes:

1. Roles

[6] Reference for evaluator to be deleted in final version: "Permissions for Starting and Shutting Down a WebLogic Server" on page 3-8, provides more information.

2. Groups and group membership
3. WebLogic resources
4. Deployment descriptors
5. Security policies
6. User account attributes,
7. Encrypted value of attributes in server configuration,
8. fullyDelegateAuthorization Flag
9. Ignore Security Data in Deployment Descriptors Check Box
10. Lockout attributes for a security realm
11. Require Unanimous Permit attribute
12. SSL configuration

No user, regardless of role membership, can view the non-encrypted version of an encrypted attribute.

While any number of additional roles can be created for use in by applications, only the roles in Table 6.6 have permission to view or change the configuration of a WebLogic Server.

The assignment of roles to users is accomplished either directly or via the assignment of groups associated with roles. Conversely, each role is associated with groups that serve to grant access to applicable WLS resources.

Access to view or modify TSF data, including that used to define the operation of the TOE, is restricted to one or more of the administrative roles identified above. Of particular note, user definitions (users, credentials, groups and group memberships), role definitions, and security policy settings for audit, identification and authentication, and user data protection are all restricted to one or more of the identified administrator roles.

Furthermore, the TOE offers interfaces that allow an administrator to effectively manage the TOE; including, viewing configuration data, managing user accounts and their attributes; managing roles; and, management of the access control settings.

(FMT_MOF.1, FMT_MSA.1, FMT_MTD.1, FMT_SMR.1, FPT_RVM_EXP.1)

SM-2 Default Security Attributes of Entities

By default, WebLogic Server defines the security policies shown in Table 6.7:

Table 6.7– Default Security Policy

WebLogic Entity	Security Policy
Administrative resources	Default global role: Admin
Application resources	None
COM resources	None
EIS resources	Default group: Everyone
EJB resources	Default group: Everyone
JDBC resources	Default group: Everyone
JMS resources	Default group: Everyone
JNDI resources	Default group: Everyone
Server resources	Default global roles: Administrator, Operator

WebLogic Entity	Security Policy
URL resources	Default group: Everyone
Web Services	Default group: Everyone

When the value of the fullyDelegateAuthorization flag is false, the WebLogic Security Service only performs security checks on URL and EJB resources that have security specified in their associated deployment descriptors. This is the default setting.

A user in the administrator role can override the default setting of the fullyDelegateAuthorization flag and Ignore Security Data in Deployment Descriptors Check Box. (See Configuration Options for EJB and URL (Web) Resources.)

(FMT_MSA.3)

SM-3 Default Groups

By default, WebLogic Server defines the groups shown in Table 6.8. The four administrative groups correspond to the four administrative global roles.

Table 6.8 – Default Groups

Group Name	Membership	Corresponding Role
Users	If a user identifies himself or herself when they log in (for example, through a Web page), the user is a member of this group. The users group includes all users except the <anonymous> user.	-
Everyone	Regardless of whether a user identifies himself or herself when they log in, the user is a member of this group.	-
Administrators	By default, this group contains the user information entered as part of the installation process, and the system user if the WebLogic Server instance is running Compatibility security. Any user assigned to the Administrators group is granted the Administrator security role by default.	Administrator
Deployers	By default, this group is empty. Any user assigned to the Deployers group is granted the Deployer security role by default.	Deployer
Operators	By default, this group is empty. Any user assigned to the Operators group is granted the Operator security role by default.	Operator
Monitors	By default, this group is empty. Any user assigned to the Monitors group is granted the Monitor security role by default.	Monitor

(FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1)

SM-4 Security Provider Database

The security provider database provides support for storage and management of security attributes and TSF data. It contains the users, groups, security roles, security policies, and credentials used by some types of security providers to provide security services

The security provider database used by the WSF security providers is implemented using the embedded LDAP server.

The security provider database is initialized the first time security providers are used. This initialisation is done:

- When a WebLogic Server instance boots, and
- When a call is made to one of the security provider's MBeans.

At minimum, the security provider database is initialized with the default users, groups, security roles, and security policies provided by WebLogic Server.

(FMT_SMF.1)

Table 6.9 lists the security attributes and TSF data stored in the security provider database for each type of security provider.

Table 6.9 – WebLogic Security Provider Database Usage

Security Provider	Database Information
Authentication	Stores user and group information.
Authorization	Stores security roles, security policies, and predicate information.
Role Mapping	Supports dynamic role associations by obtaining a computed set of roles granted to a requestor for a given WebLogic resource.
Auditing	None.
Credential Mapping	Stores Username-Password credential mapping information.
Identity Assertion	Stores user and group information.

(FMT_SMF.1)

SM-5 Credential Mapping Provider

The provider maps a user's authentication identity to those required for legacy applications, so that the legacy application gets the necessary credential information.

WSF provides administrators with the capability to manage users' credentials for legacy applications.

(FMT_MSA.1)

6.1.5 Protection of the TOE Security Functions

PT-1 Non-Bypassability

The WSF ensures that its security functions are invoked and succeed before allowing a thread to continue processing.

(FPT_RVM_EXP.1)

PT-2 Principal Validation

As part of a successful authentication, principals are signed and stored in a subject for future use. The WSF calls a Principal Validation provider to sign principals, and calls the Authentication provider's LoginModule to actually store the principals in the subject.

Later, when a caller attempts to access a principal stored within a subject, the WSF calls a Principal Validation provider to verify that the principal has not been altered since it was signed, and the principal is returned to the caller (assuming all other security conditions are met).

The WebLogic Principal Validation provider signs and verifies WebLogic Server principals that represent WebLogic Server users or WebLogic Server groups.

(FPT_RVM_EXP.1)

6.2 STRENGTH OF FUNCTION REQUIREMENT

The minimum strength of function (SOF) level for the TOE security functional requirements level is SOF-basic. The strength of function requirement is applicable to the passwords for IA-4 Password-based authentication. This IT security function has an SOF level of SOF-basic.

6.3 ASSURANCE MEASURES

Table 6.10 lists the evaluation evidence that was provided to meet EAL2 assurance requirements augmented with ALC_FLR.1.

Table 6.10 – Assurance Measures

Component	Title	Evidence
ACM_CAP.2	Configuration Items	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Configuration Management Version v1-0-03, November 29, 2005. Filename: BEA WLS 7.0 ACM v1-0-03 2005-11-29.doc
ADO_DEL.1	Delivery procedures	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Delivery Procedures and Installation Overview Version v1-0-01, November 29, 2005. Filename: BEA WLS 7.0 ADO v1-0-01 2005-11-29.doc
ADO_IGS.1	Installation, generation, and start-up procedures	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Delivery Procedures and Installation Overview Version v1-0-01, November 29, 2005. Filename: BEA WLS 7.0 ADO v1-0-01 2005-11-29.doc BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Administrator and User Guidance Version v1-0-03, November 29, 2005. Filename: BEA WLS 7.0 AGD v1-0-03 2005-11-29.doc
ADV_FSP.1	Informal functional specification	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Functional Specification Version v1-0-03, November 29, 2005. Filename: BEA WLS 7.0 FSP v1-0-03 2005-11-29.doc
ADV_HLD.1	Descriptive high-level design	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, High Level Design Version v1-0-02, November 29, 2005

Component	Title	Evidence
		Filename: BEA WLS 7.0 HLD v1-0-02 2005-11-29.doc
ADV_RCR.1	Informal correspondence demonstration	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Representation Correspondence Version v1-0-02, November 29, 2005 Filename: BEA WLS 7.0 HLD v1-0-02 2005-11-29.doc
AGD_ADM.1	Administrator guidance	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Administrator and User Guidance Version v1-0-03, November 29, 2005. Filename: BEA WLS 7.0 AGD v1-0-03 2005-11-29.doc
AGD_USR.1	User guidance	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Administrator and User Guidance Version v1-0-03, November 29, 2005. Filename: BEA WLS 7.0 AGD v1-0-03 2005-11-29.doc
ALC_FLR.1	Flaw remediation	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Flaw Remediation Version v1-0-01, November 29, 2005. Filename: BEA WLS 7.0 ALC_FLR v1-0-01 2005-11-29.doc
ATE_COV.1	Evidence of coverage	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Testing Documentation Version v1-0-01, November 29, 2005. Filename: BEA WLS 7.0 ATE v1-0-01 2005-11-29.doc
ATE_FUN.1	Functional testing	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Testing Documentation Version v1-0-01, November 29, 2005. Filename: BEA WLS 7.0 ATE v1-0-01 2005-11-29.doc
ATE_IND.2	Independent testing – sample	TOE for Testing
AVA_SOF.1	Strength of TOE security function evaluation	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Vulnerability Assessment Version v1-0-01, November 29, 2005. Filename: BEA WLS 7.0 AVA v1-0-01 2005-11-29.doc
AVA_VLA.1	Developer vulnerability analysis	BEA WebLogic Server™ 7.0 SP6 with BEA05-107.00 advisory patch, Vulnerability Assessment Version v1-0-01, November 29, 2005. Filename: BEA WLS 7.0 AVA v1-0-01 2005-11-29.doc

7 PP CLAIMS

This Security Target was not written to address any existing Protection Profile.

8 RATIONALE

This section contains the following rationale sections:

- Security Objectives Rationale
- Security Requirements Rationale
- TOE Summary Specification Rationale

8.1 SECURITY OBJECTIVES RATIONALE

This section consists of two subsections. Section 8.1.1 shows that all of the secure usage assumptions and threats to security have been addressed. Section 8.1.2 shows that each IT security objective and each non-IT security objective addresses at least one threat, policy, or assumption.

8.1.1 All Threats and Assumptions Addressed by Objectives

Table 8.1 shows that all the identified assumptions and threats to security have been addressed. Note that TOE threats, policies, and assumptions have the prefixes “T”, “P”, and “A,” respectively. The rationale for these mappings is provided below.

Table 8.1 – All Threats and Assumptions Addressed by Objectives

Threat	Threat Text	Objective
T.BYPASS	An attacker may be able to bypass TOE protection mechanisms through WebLogic Server containers, the JVM, or Windows 2000 Server operating system.	O.SUCCEED OE.TSF_PROTECT
T.EXCESS_AUTHORITY	An administrative user may be granted more authority than they are trained to handle.	O.ROLES
T. EAVESDROP	An attacker may be able to observe authentication data transmitted from a user to the TOE.	ON.SEC_COMM
T.NO_TIME	Those responsible for the TOE may not be able to determine the sequence of security relevant events.	OE.TIME
T.STORAGE	Audit data and other TSF data may be lost or modified.	O.MANAGE OE.OS_STORAGE OE.TSF_PROTECT
T.TAMPER	An attacker may be able to tamper with TSF programs and data.	O.MANAGE OE.TSF_PROTECT
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).	O.MANAGE OE.TSF_PROTECT
T.UNACCOUNTABLE	Users of the TOE may not be held accountable for their actions.	O.AUDIT_GENERATION O.ID_AND_AUTH OE.AUDIT_REVIEW OE.AUTH_INVOKE
T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.	O.MEDIATE OE.ENFORCE_POLICY
T.UNDETECTED_ACTIONS	The administrator may not have the ability to detect potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.	O.AUDIT_GENERATION OE.AUDIT_REVIEW OE.OS_STORAGE
T.UNIDENTIFIED_USERS	An attacker may gain access to the TOE without being reliably identified allowing them to gain unauthorized access to data or TOE resources.	O.ID_AND_AUTH O.SUCCEED OE.AUTH_INVOKE
Assumption Name	**Assumption Description**	**Objective for the IT Environment**
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.	ON.NO_EVIL
A.NO_UNTRUSTED	There are no untrusted user accounts or software on the server platform.	ON.NO_UNTRUSTED
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	ON.PHYSICAL

T.BYPASS states, "An attacker may be able to bypass TOE protection mechanisms through WebLogic Server containers, the JVM, or Windows 2000 Server operating system.". This threat is countered by O.SUCCEED and OE.TSF_PROTECT.

O.SUCCEED prevents one TOE security function from being used to bypass another. OE.TSF_PROTECT prevents bypassing the TSF through the JVM, OS, or their interfaces.

T.EXCESS_AUTHORITY states, “An administrative user may be granted more authority than they are trained to handle. ”This threat is countered by O.ROLES, which ensures that the TOE supports user roles.

T.EAVESDROP states, “An attacker may be able to observe authentication data transmitted from a user to the TOE.” This threat is countered by ON.SEC_COMM, which ensures that communication between users and the TSF is protected from observation.

T.NO_TIME states, “Those responsible for the TOE may not be able to determine the sequence of security relevant events.” This threat is countered by OE.TIME, which ensures that the underlying operating system platform and JVM provide support for reliable time stamps. The TSF calls the operating system via Java classes to obtain the time based on the system clock.

T.STORAGE states, “Audit data and other TSF data may be lost or modified.” This threat is countered by O.MANAGE, OE.OS_STORAGE, and OE.TSF_PROTECT.

OE.OS_STORAGE ensures that the OS provides storage for TOE audit data and other TSF data. O.MANAGE prevents unauthorized users from modifying or deleting audit data or other TSF data using TOE functions. OE.TSF_PROTECT prevents unauthorized modification or deletion of this data through the JVM, OS, or their interfaces.

T.TAMPER states, “An attacker may be able to tamper with TSF programs and data. ” This threat is countered by O.MANAGE and OE.TSF_PROTECT.

O.MANAGE protects TSF management functions to prevent tampering with TSF data using those functions. OE.TSF_PROTECT prevents tampering with TSF program and data through the JVM, OS, or their interfaces.

T.TSF_COMPROMISE states, “A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).” This threat is countered by O.MANAGE and OE.TSF_PROTECT.

O.MANAGE prevents unsophisticated attackers from using the TSF itself to inappropriately access TSF data. OE.TSF_PROTECT prevents inappropriate access to the TSF through the JVM, OS, or their interfaces.

T.UNACCOUNTABLE states, “Users of the TOE may not be held accountable for their actions. ” This threat is countered by O.ID_AND_AUTH, O.AUDIT_GENERATION, OE.AUDIT_REVIEW, and OE.AUTH_INVOKE.

O.ID_AND_AUTH and OE.AUTH_INVOKE prevent a user from accessing protected WebLogic Server entities anonymously or with a false identify. Anonymous access is allowed to an unprotected entity as specified in the entity’s security policy. O.AUDIT_GENERATION provides accountability through its records of security-relevant events associated with users. OE.AUDIT_REVIEW ensures that WebLogic Server administrators have the capability to use the audit trail to identify inappropriate actions and the users performed those actions.

T.UNAUTHORIZED_ACCESS states, “A user may gain access to user data for which they are not authorized according to the TOE security policy.” This threat is countered by O.MEDIATE and OE.ENFORCE_POLICY.

OE.ENFORCE_POLICY prevents this attack by enforcing the access control policy decisions provided by O.MEDIATE, which provides access control decisions in accordance with the WebLogic Server security policy.

T.UNDETECTED_ACTIONS states, “The administrator may not have the ability to detect potential security violations, thus limiting the administrator’s ability to identify and take action against a possible security breach. ” This threat is countered by O.AUDIT_GENERATION, OE.AUDIT_REVIEW, and OE.OS_STORAGE.

O.AUDIT_GENERATION prevents the threat by providing administrators with a record of security relevant. OE.OS_STORAGE ensures this record is available for administrator review. OE.AUDIT_REVIEW provides the capability for an administrator to review the audit trail with a text editor to look for potential security violations.

T.UNIDENTIFIED_USERS states “An attacker may gain access to the TOE without being reliably identified allowing them to gain unauthorized access to data or TOE resources.” This threat is countered by O.ID_AND_AUTH, O.SUCCEED, and OE.AUTH_INVOKE.

O.ID_AND_AUTH and OE.AUTH_INVOKE prevent a user from accessing protected WebLogic Server entities anonymously or with a false identify. Anonymous access is allowed to an unprotected entity as specified in the entity’s security policy. O.SUCCEED ensures that identification and authentication are successful before performing any other TOE function.

A.NO_EVIL states “Administrators are non-hostile, appropriately trained and follow all administrator guidance.” This assumption is addressed by ON.NO_EVIL, which restates that assumption as an objective to be fulfilled by those responsible for the TOE.

A.NO_UNTRUSTED states, “There are no untrusted user accounts or software on the server platform.” This assumption is addressed by ON.NO_UNTRUSTED, which restates that assumption as an objective to be fulfilled by those responsible for the TOE.

A.PHYSICAL states, “Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.” This assumption is addressed by ON.PHYSICAL, which restates that assumption as an objective to be fulfilled by those responsible for the TOE.

8.1.2 All Objectives Necessary

Table 8.2 shows that there are no unnecessary IT security objectives for the TOE, since each objective addresses at least one threat or secure usage assumption. Mapping rationale is discussed in the previous section and is not repeated here.

Table 8.2 – All IT Security Objectives Necessary

Objective Name	Objective Description	Threat or Policy or Assumption
	Objectives for the TOE	
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.	T.UNACCOUNTABLE T.UNDETECTED_ACTIONS
O.ID_AND_AUTH	The TOE will provide identification and authentication mechanisms that provide the basis for controlling a user's logical access to the TOE and the resources it protects.	T.UNACCOUNTABLE T.UNIDENTIFIED_USERS
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the TOE security functions and restrict these functions and facilities from unauthorized use.	T.STORAGE T.TAMPER T.TSF_COMPROMISE
O.MEDIATE:	The TOE will provide access control decisions for user data in accordance with the WebLogic Server security policy.	T.UNAUTHORIZED_ACCESS
O.ROLES	The TOE will support user roles for the management of TOE security functions.	T.EXCESS_AUTHORITY
O.SUCCEED	The TOE will ensure that, when invoked, it performs its security policy enforcement functions successfully.	T.BYPASS T.UNIDENTIFIED_USERS
	Objectives for the IT Environment	
OE.AUDIT_REVIEW	The IT environment will provide a capability to review audit trails produced by the TSF.	T.UNACCOUNTABLE T.UNDETECTED_ACTIONS
OE.AUTH_INVOKE	The IT environment will invoke the WSF to identify and authenticate WebLogic Server users.	T.UNACCOUNTABLE T.UNIDENTIFIED_USERS
OE.ENFORCE_POLICY	The WebLogic Server containers will enforce the access control decisions provide by the TOE.	T.UNAUTHORIZED_ACCESS
OE.OS_STORAGE	The operating system will provide files for the storage of audit records and other TSF data.	T.STORAGE T.UNDETECTED_ACTIONS
OE.TIME	The operating system platform and JVM will provide support for reliable time stamps.	T.NO_TIME
OE.TSF_PROTECT	The JVM and underlying operating system will protect TSF code and data structures from unauthorized modification and prevent TSF security functions from being bypassed through IT environment interfaces.	T.BYPASS T.STORAGE T.TAMPER T.TSF_COMPROMISE
	Objectives for the Non-IT Environment	

Objective Name	Objective Description	Threat or Policy or Assumption
ON.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.	A.NO_EVIL
ON.NO_UNTRUSTED	There are no untrusted user accounts or software on the server platform.	A.NO_UNTRUSTED
ON.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	A.PHYSICAL
ON.SEC_COMM	Those responsible for the TOE will ensure that transmissions between users and the TOE are protected from observation.	T.EAVESDROP

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 All Objectives Met by Security Requirements

Table 8.3 maps IT security objectives to functional requirements. Objectives for the TOE are identified by an "O." prefix and the corresponding requirements are TOE requirements. Objectives for the IT environment are identified by an "OE." prefix and the corresponding requirements are for requirements for the IT environment. The rationale for the mappings is discussed below.

Table 8.3 – Mapping of IT Security Objectives to Requirements

Objective Name	Objective Description	Security Requirement
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.	FAU_GEN.1
O.ID_AND_AUTH	The TOE will provide identification and authentication mechanisms that provide the basis for controlling a user's logical access to the TOE and the resources it protects.	FIA_AFL.1 FIA_ATD.1 FIA_UAU.1 FIA_UAU.5 FIA_UID.1
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the TOE security functions and restrict these functions and facilities from unauthorized use.	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1
O.MEDIATE	The TOE will provide access control decisions for user data in accordance with the WebLogic Server security policy.	FDP_ACF_EXP.1
O.ROLES	The TOE will support user roles for the management of TOE security functions.	FMT_SMR.1
O.SUCCEED	The TOE will ensure that, when invoked, it performs its security policy enforcement functions successfully.	FPT_RVM_EXP.1
	Objectives for the IT Environment	
OE.AUDIT_REVIEW	The IT environment will provide a capability to review audit trails produced by the TSF.	FAU_SAR.1

OE.AUTH_INVOKE	The IT environment will invoke the WSF to identify and authenticate WebLogic Server users.	FIA_UAU_EXP.1 FIA_UID_EXP.1
OE.ENFORCE_POLICY	The WebLogic Server containers will enforce the access control decisions provide by the TOE.	FDP_ACF.1 FDP_ACC.1
OE.OS_STORAGE	The operating system will provide files for the storage of audit records and other TSF data.	FAU_STG_EXP.1
OE.OS_TIME	The operating system platform and JVM will provide support for reliable time stamps.	FPT_STM.1
OE.TSF_PROTECT	The JVM and underlying operating system will protect TSF code and data structures from unauthorized modification and prevent TSF security functions from being bypassed through IT environment interfaces.	FPT_RVM_EXP.2 FPT_SEP.1

O.AUDIT_GENERATION states, “The TOE will provide the capability to detect and create records of security relevant events associated with users.” This objective is met by FAU_GEN.1 (Audit data generation), which requires that the TSF be able to generate audit records for specified auditable events.

O.ID_AND_AUTH states, “The TOE will provide identification and authentication mechanisms that provide the basis for controlling a user’s logical access to the TOE and the resources it protects.” This objective is met by identification and authentication requirements: FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, and FIA_UID.1.

FIA_UID.1 (Timing of identification) and FIA_UAU.1 (Timing of authentication) specify identification and authentication to meet O.ID_AND_AUTH for protected WebLogic Server entitles. Anonymous access is allowed to an unprotected entity as specified in the entity’s security policy. FIA_UAU.5 (Multiple authentication mechanisms) specifies when authentication mechanisms are to be applied. It specifies password-based and token-based mechanisms for authentication and the rules used to apply them. FIA_AFL.1 (Authentication failure handling) prevents brute-force attacks against the authentication mechanisms. FIA_ATD.1 (User attribute definition) specifies the user attributes used to enforce the TSP or managed by the TSF.

O.MANAGE states, “The TOE will provide all the functions and facilities necessary to support the administrators in their management of the TOE security functions and restrict these functions and facilities from unauthorized use.” This objective is met by requirements for security management: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

FMT_SMF.1 (Specification of management functions) identifies the security management functions needed to manage the TSF, with details provided by FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1. FMT_MOF.1 (Management of security function behaviour) restricts the capability to start and stop the TSF. FMT_MSA.1 (Management of security attributes) specifies capabilities for and restrictions on managing user accounts (user security attributes) and WebLogic resources. FMT_MTD.1 (Management of TSF data) specifies the capabilities for and restrictions on managing security policies, WebLogic entities, and configuration data. FMT_MSA.3 (Static attribute initialisation) specifies how default security attributes are assigned to new objects (i.e., WebLogic entities) and permits administrators to override the defaults. These management requirements are expressed using roles defined in FMT_SMR.1 (Security roles).

O.MEDIATE states, “The TOE will provide access control decisions for user data in accordance with the WebLogic Server security policy.” This objective is met by: FDP_ACF_EXP.1.

FDP_ACF_EXP.1 (Security attribute based access control decision) specifies the rules used by the TSF to make access control decisions.

O.ROLES states, “The TOE will support user roles for the management of TOE security functions.” FMT_SMR.1 (Security roles) meets this objective by identifying the roles supported by the TOE.

O.SUCCEED states, “The TOE will ensure that, when invoked, it performs its security policy enforcement functions successfully.” FPT_RVM_EXP.1 (Non-bypassability of the WSF TSP) meets this objective by specifying that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

OE.AUDIT_REVIEW states, “The IT environment will provide a capability to review audit trails produced by the TSF.” FAU_SAR.1 (Audit review) meets this objective by requiring the IT environment to provide WebLogic Server administrators with the capability to read the WSF audit trail

Application note: The WSF audit trail is a plain text document. The IT environment need only provide WebLogic Server administrators with a text editor in order to review the audit trail.

OE.AUTH_INVOKE states, “The IT environment will invoke the WSF to identify and authenticate WebLogic Server users.” This objective is met by identification and authentication requirements FIA_UAU_EXP.1 and FIA_UID_EXP.1.

FIA_UID_EXP.1 (Timing of identification request) and FIA_UAU_EXP.1 (Timing of authentication request) specify that WebLogic Server containers invoke the WSF identification and authentication functions before allowing access to protected WebLogic Server entities.

Application note: The functionality to invoke the WSF identification and authentication functions is built into WebLogic Server containers. Containers invoke the WSF even when creating anonymous subjects. However, these containers are outside the scope of the current evaluation.

OE.ENFORCE_POLICY states, “The WebLogic Server containers will enforce the access control decisions provide by the TOE.” This objective is met by: FDP_ACF.1 and FDP_ACC.1.

FDP_ACC.1 (Subset access control) specifies access control policy for the WebLogic Server, including the TOE, in terms of applicable subjects, objects, and controlled operations. FDP_ACF.1 (Security attribute based access control) specifies access control functions that enforce access control decisions made by the TSF.

Application note: The access control policy enforcement functionality is built into WebLogic Server containers. However, these containers are outside the scope of the current evaluation.

OE.OS_STORAGE states, “The operating system will provide files for the storage of audit records and other TSF data.” FAU_STG_EXP.1 (Protected WebLogic Server audit trail storage) meets this requirement by specifying the IT environment provide storage and protection for the WebLogic Server audit trail.

Application note: The WebLogic Server audit trail is a plain text document. The IT environment needs to limit access to the files containing the audit trail to WebLogic Server administrators.

OE.OS_TIME states, “The operating system platform and JVM will provide support for reliable time stamps.” FPT_STM.1 (Reliable time stamps) meets this requirement by specifying the IT environment provide reliable time stamps.

Application note: The TSF calls standard Java time methods to obtain timestamps for audit records.

OE.TSF_PROTECT states, “The JVM and underlying operating system will protect TSF code and data structures from unauthorized modification and prevent TSF security functions from being

bypassed through IT environment interfaces." This objective is met by FPT_RVM_EXP.2 and FPT_SEP.1.

FPT_SEP.1 (TSF domain separation) specifies domain separation for subjects within the scope of control of the IT environment, which prevents unauthorized subjects from modifying TSF code and data structures. FPT_RVM_EXP.2 (Non-bypassability of the IT Environment Security Policy) specifies that the security functions of the IT environment always be invoked and succeed. This prevents bypassing of the TSF through the IT environment.

Application note: Although details of the IT environment are outside the scope of the evaluation, it may be helpful to integrators to understand some details of the dependency of the TSF on the IT environment. The WSF relies on both the JVM and the operating system to provide domain separation. The Java 2 Security Sandbox provides domain separation for subjects within the JVM scope of control. That is, it provides separate domains for WebLogic security providers and application code within the JVM. The operating system provides domain separation for its subjects, i.e., processes.

8.2.2 All Functional Components Necessary

Table 8.4 shows that each functional requirement is necessary, since it is used to address at least one of the IT security objectives. Note that functional requirements for the TOE map to objectives with an "O." prefix and functional requirements for the environment map to an "OE." prefix. Discussion of the mapping is provided in the previous section.

Table 8.4 – Mapping of Functional Requirements to IT Security Objectives

	Component	Component Title	Objective
1	FAU_GEN.1	Audit data generation	O.AUDIT_GENERATION
2	FDP_ACF_EXP.1	Security attribute based access control decision	O.MEDIATE
3	FIA_AFL.1	Authentication failure handling	O.ID_AND_AUTH
4	FIA_ATD.1	User attribute definition	O.ID_AND_AUTH
5	FIA_UAU.1	Timing of authentication	O.ID_AND_AUTH
6	FIA_UAU.5	Multiple authentication mechanisms	O.ID_AND_AUTH
7	FIA_UID.1	Timing of identification	O.ID_AND_AUTH
8	FMT_MOF.1	Management of security functions behaviour	O.MANAGE
9	FMT_MSA.1	Management of security attributes	O.MANAGE
10	FMT_MSA.3	Static attribute initialisation	O.MANAGE
11	FMT_MTD.1	Management of TSF data	O.MANAGE
12	FMT_SMF.1	Specification of Management Functions	O.MANAGE
13	FMT_SMR.1	Security roles	O.MANAGE O.ROLES
14	FPT_RVM_EXP.1	Non-bypassability of the WSF TSP	O.SUCCEED
		Requirements for the IT Environment	
1E	FAU_SAR.1	Audit Review	OE.AUDIT_REVIEW
2E	FAU_STG_EXP.1	Protected WebLogic Server audit trail storage	OE.OS_STORAGE
3E	FDP_ACC.1	Subset access control	OE.ENFORCE_POLICY
4E	FDP_ACF.1	Security attribute based access control	OE.ENFORCE_POLICY
5E	FIA_UAU_EXP.1	Timing of authentication request	OE.AUTH_INVOKE
6E	FIA_UID_EXP.1	Timing of identification request	OE.AUTH_INVOKE
7E	FPT_RVM_EXP.2	Non-bypassability of the IT environment security policy	OE.TSF_PROTECT
8E	FPT_SEP.1	TSF domain separation	OE.TSF_PROTECT
9E	FPT_STM.1	Reliable time stamps	OE.OS_TIME

8.2.3 Explicitly Stated Requirements

Components from CC version 2.2 Part 2 are used to express security functional requirement in this ST whenever possible. However, it was not possible to use the CC components for six security functional requirements. This section provides rationale for explicitly stating those six requirements.

8.2.3.1 FAU_STG_EXP.1 Protected WebLogic Server audit trail storage

The IT environment provides storage and protection for the WebLogic Server audit trail. FAU_STG_EXP.1 restricts FAU_STG.1 to the WebLogic Server audit trail and levies it upon the IT environment. The restriction would be a refinement except for the fact that there are other audit trails within the IT environment (i.e., the OS audit trail). It would be inappropriate to levy FAU_STG.1 on all the audit trails, since the OS is outside the scope of this evaluation. Thus, it is necessary to explicitly state FAU_STG_EXP.1.

The Security audit event storage (FAU_STG) family describes requirements for storing audit data for later use. FAU_STG_EXP.1 is adequate to specify both audit storage and protection of that storage, since is follows the model of the FAU_STG family and in particular FAU_STG.1.

FAU_STG_EXP.1 is a restriction in scope of FAU_STG.1. Hence, FAU_STG_EXP.1 is measurable and states objective evaluation requirements. Likewise, the EAL2 assurance requirements are adequate for FAU_STG_EXP.1 and no additional security assurance requirements are needed.

Because FAU_STG_EXP.1 is a restriction of FAU_STG.1, it also has a dependency of FAU_GEN.1 to specify generation of WebLogic Server audit records.

8.2.3.2 FDP_ACF_EXP.1 Security attribute based access control decision

Typically, access control functions are specified using FDP_ACF.1 (Security attribute based access control). In this case, the TSF and the IT environment (i.e., WebLogic Server containers) each implement part of FDP_ACF.1. The IT environment requests access control decisions from the TSF and enforces those decisions. The TSF provides access control decisions based on information provided by the IT environment.

There are no CC security functional requirements that could be used to specify this decomposition of the functionality specified by FDP_ACF.1. Hence, it is necessary to explicitly state FDP_ACF_EXP.1 to split the functionality of FDP_ACF.1 between the TSF and the IT environment. FDP_ACF_EXP.1 is defined to specify the decision-making aspect of FDP_ACF.1. FDP_ACF.1 itself (with appropriate assignments) is used to specify requesting and enforcing those decisions.

FDP_ACF_EXP.1 is closely modeled after FDP_ACF.1. FDP_ACF_EXP.1 is measurable and states objective evaluation requirements, since it specifies a subset of the functionality specified by FDP_ACF.1. Likewise, the EAL2 assurance requirements are adequate for FDP_ACF_EXP.1 and no additional security assurance requirements are needed.

Because of the close relationship between FDP_ACF_EXP.1 and FDP_ACF.1, FDP_ACF_EXP.1 also has dependencies of FDP_ACC.1 to specify the necessary security policy definition and FMT_MSA.3 to specify default security attributes for objects.

8.2.3.3 FIA_UID_EXP.1 Timing of identification request and FIA_UAU_EXP.1 Timing of authentication request

Often, identification is specified using FIA_UID.1 (Timing of identification) and authentication is specified using FIA_UAU.1 (Timing of authentication). In this case, the TSF and the IT environment (i.e., WebLogic Server containers) each contribute to implementing FIA_UID.1 and FIA_UAU.1. WebLogic Server containers are the interfaces to WebLogic Server users, but the WSF provides the identification and authentication functionality.

There are no CC security functional requirements that could be used to specify this decomposition of the functionality specified by FIA_UID.1 and FIA_UAU.1. Hence, it is necessary to explicitly state FIA_UID_EXP.1 and FI_UAU_EXP.1 to specify the requirement on WebLogic Servers to invoke the WSF. FIA_UID.1 and FIA_UAU.1 are adequate and appropriate for the TOE, since they apply only to TSF-mediated actions. This follows current guidance from the U.S. Common Criteria Evaluation and Validation Scheme. (See Instruction 2 in *Consistency Instruction Manual For Development Of US Government Protection Profiles (PP) For Use In Basic Robustness Environments*.)

FIA_UID_EXP.1 and FIA_UAU_EXP.1 are closely modeled after FIA_UID.1 and FIA_UAU.1, respectively. Each explicitly stated requirement is measurable and states objective evaluation requirements, since each specifies a subset of the functionality specified by the original

requirements. Likewise, the EAL2 assurance requirements are adequate for FIA_UID_EXP.1 and FIA_UAU_EXP.1 and no additional security assurance requirements are needed.

FIA_UID_EXP.1 has a dependency on FIA_UID.1 for the identification functionality invoked by the WebLogic Server containers. FIA_UAU_EXP.1 has dependencies on FIA_UID_EXP.1 for identification functionality and on FIA_UAU.1 for authentication functionality invoked by the WebLogic Server containers.

8.2.3.4 FPT_RVM_EXP.1 Non-bypassability of the WSF TSP and FPT_RVM_EXP.2 Non-bypassability of the IT environment security policy

Typically, non-bypassability is specified using FPT_RVM.1 (Non-bypassability of the TSP). In this case, the TSF and the IT environment (i.e., WebLogic Server containers, JVM, and OS) each contribute to implementing FPT_RVM.1. WebLogic Server containers, the JVM, and the OS each include functionality to ensure that their security policy enforcement functions cannot be bypassed. The TSF includes functionality to ensure that its enforcement functions succeed. No single component addresses all of FPT_RVM.1.

There are no CC security functional requirements that could be used to specify this decomposition of the functionality specified by FPT_RVM.1. Hence, it is necessary to explicitly state FPT_RVM_EXP.1 and FPT_RVM_EXP.2 to split the functionality of FPT_RVM.1 between the TSF and the IT environment. The explicitly stated requirements specify the contribution of each component. This follows current guidance from the U.S. Common Criteria Evaluation and Validation Scheme. (See Instruction 2 in *Consistency Instruction Manual For Development Of US Government Protection Profiles (PP) For Use In Basic Robustness Environments*.)

FPT_RVM_EXP.1 and FPT_RVM_EXP.2 are closely modeled after FPT_RVM.1. Each explicitly stated requirement is measurable and states objective evaluation requirements (to the extent that FPT_RVM.1 is measurable), since each specifies a subset of the functionality specified by FPT_RVM.1. Likewise, the EAL2 assurance requirements are adequate for FPT_RVM_EXP.1 and FPT_RVM_EXP.2 and no additional security assurance requirements are needed.

Because of the close relationship between FPT_RVM_EXP.1 and FPT_RVM_EXP.2 and FPT_RVM.1, the explicitly stated requirements have no dependencies on other requirements.

8.2.4 Mutual Support

Table 8.5 shows that all of the dependencies between the functional requirements are satisfied. Dependencies satisfied by hierarchical components are mark with “(H)”.

Table 8.5 – Functional Requirements Dependencies

No	Component	Component Name	Dependencies	Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	9E
2	FDP_ACF_EXP.1	Security attribute based access control decision	FDP_ACC.1 FDP_MSA.3	3E 10
3	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	5
4	FIA_ATD.1	User attribute definition	None	-
5	FIA_UAU.1	Timing of authentication	FIA_UID.1	7
6	FIA_UAU.5	Multiple authentication mechanisms	None	-
7	FIA_UID.1	Timing of identification	None	-

No	Component	Component Name	Dependencies	Reference
8	FMT_MOF.1	Management of security functions behaviour	FMT_SMF.1, FMT_SMR.1	12 13
9	FMT_MSA.1	Management of security attributes	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	3E 12 13
10	FMT_MSA.3	Secure attribute initialisation	FMT_MSA.1 FMT_SMR.1	9 13
11	FMT_MTD.1	Management of TSF data	FMT_SMF.1 FMT_SMR.1	12 13
12	FMT_SMF.1	Specification of Management Functions	None	-
13	FMT_SMR.1	Security roles	FIA_UID.1	7
14	FPT_RVM_EXP.1	Non-bypassability of the WSF TSP	None	-
		Requirements for the IT Environment		
1E	FAU_SAR.1	Audit review	FAU_GEN.1	1
2E	FAU_STG_EXP.1	Protected WebLogic Server audit trail storage	FAU_GEN.1	1
3E	FDP_ACC.1	Subset access control	FDP_ACF.1	2 4E
4E	FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FDP_MSA.3 FDP_ACF_EXP.1	3E 10 2
5E	FIA_UAU_EXP.1	Timing of authentication request	FIA_UAU.1 FIA_UID_EXP.1	5 6E
6E	FIA_UID_EXP.1	Timing of identification request	FIA_UID.1	7
7E	FPT_RVM_EXP.2	Non-bypassability of the IT environment security policy	None	-
8E	FPT_SEP.1	TSF domain separation	None	-
9E	FPT_STM.1	Reliable time stamps	None	-

Mutual support is provided by:

- FPT_RVM_EXP.1 and FPT_RVM_EXP.2 in place of FPT_RVM.1, which ensure that the TSF security functions cannot be bypassed,
- FPT_SEP.1, which ensures that TSF programs and data cannot be tampered with, and
- FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1, which ensure that security functions cannot be disabled.

8.2.5 Strength of Function

A strength of function level of SOF-Basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

8.2.6 Assurance Rationale

EAL2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. The security objectives defined for the TOE are consistent with an EAL2 assurance level and EAL2 is sufficient to satisfy the security objectives of the TOE.

EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behavior. The analysis is supported by:

- Independent testing of the TOE security functions,
- Evidence of developer testing based on the functional specification,
- Selective independent confirmation of the developer test results,
- Strength of function analysis, and
- Evidence of a developer search for obvious vulnerabilities (e.g., those in the public domain).

EAL2 also provides assurance through a configuration list for the TOE and evidence of secure delivery procedures. The TOE and related documentation have all of the characteristics required for EAL2.

EAL2 was augmented by ALC_FLR.1, because flaw remediation procedures provide greater assurance that bugs will be fixed in a widely distributed commercial product.

8.3 TOE SUMMARY SPECIFICATION RATIONALE

8.3.1 All TOE Security Functional Requirements Satisfied

Table 8.6 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements. The mappings are discussed in detail in Section 6. As described in Section 6, all functional components map to a TOE Security Function.

Table 8.6 – Mapping of Functional Requirements to TOE Summary Specification

No	Functional Component	Functional Requirement	TOE Security Function
1	FAU_GEN.1	Audit data generation	AUD-1 Audit Generation
			AUD-2 Auditable Events
			AUD-3 Audit Record Fields
			AUD-4 Severity Attribute
			AUD-5 Audit Record Format
			AUD-6 WebLogic Server Log Files
2	FDP_ACF_EXP.1	Security attribute based access control decision	ACC-1 Access Decisions
			ACC-2 Security Policies
			ACC-3 Subject Roles
			ACC-4 WebLogic Resources
			ACC-5 Configuration Options for EJB and URL (Web) Resources
3	FIA_AFL.1	Authentication failure handling	IA-6 Authentication Failure Handling
4	FIA_ATD.1	User attribute definition	IA-2 User Attributes
5	FIA_UAU.1	Timing of authentication	IA-3 Authentication Process
6	FIA_UAU.5	Multiple authentication mechanisms	IA-3 Authentication Process
			IA-4 Password-based authentication
			IA-5 Token-based authentication
7	FIA_UID.1	Timing of identification	IA-1 Identity

			IA-3 Authentication Process
8	FMT_MOF.1	Management of security functions behaviour	SM-1 Administrative Roles
			SM-3 Default Groups
			ACC-3 Subject Roles
9	FMT_MSA.1	Management of security attributes	SM-1 Administrative Roles
			SM-3 Default Groups
			ACC-3 Subject Roles
			SM-5 Credential Mapping Provider
10	FMT_MSA.3	Static attribute initialisation	SM-2 Default Security Attributes of Entities
			SM-3 Default Groups
11	FMT_MTD.1	Management of TSF data	SM-1 Administrative Roles
			SM-3 Default Groups
			ACC-3 Subject Roles
			ACC-5 Configuration Options for EJB and URL (Web) Resources
12	FMT_SMF.1	Specification of Management Functions	SM-4 Security Provider Database
13	FMT_SMR.1	Security roles	SM-1 Administrative roles
14	FPT_RVM_EXP.1	Non-bypassability of the WSF TSP	SM-1 Administrative roles
			PT-1 Non-bypassability
			PT-2 Principal Validation

FAU_GEN.1 Audit data generation: This requirement is implemented by the following IT security functions:

1) AUD-1 Audit Generation: Process by which the WSF generates and stores audit records.
2) AUD-2 Auditable Events: WebLogic Server audit events corresponding to events listed in FAU_GEN.1.1.
3) AUD-3 Audit Record Fields: WebLogic Server audit event data that provides information specified in FAU_GEN.1.2.
4) AUD-4 Severity Attribute: Semantics of severity attribute.
5) AUD-5 Audit Record Format: Semantics of audit record.
6) AUD-6 WebLogic Server Log Files: Storage of audit trail.

FDP_ACF_EXP.1 Security attribute based access control decision: This requirement is implemented by the following IT security functions:

1) ACC-1 Access Decisions: Process by which access control policy decisions are made.
2) ACC-2 Security Policies: Basis for security policy decisions.
3) ACC-3 Subject Roles: Process of dynamically granting roles to subjects for use in access decisions
4) ACC-4 WebLogic Resources: Entities to which security policies apply

5) ACC-5 Configuration Options for EJB and URL (Web) Resources: Semantics of *fullyDelegateAuthorization Flag* and *Ignore Security Data in Deployment Descriptors Check Box.*

FIA_AFL.1 Authentication failure handling: This requirement is met by IA-6 Authentication Failure Handling, which implements the policy for locking user accounts after failed login attempts.

FIA_ATD.1 User attribute definition: This requirement is met by IA-2 User Attributes, which defines the user security attributes maintained by WSF.

FIA_UAU.1 Timing of authentication: This requirement is implemented by IA-3 Authentication process, which either provides an anonymous subject or authenticates the identity claimed by a user before allowing other WSF functions.

FIA_UAU.5 Multiple authentication mechanisms: This requirement is implemented by the following IT security functions:

1) IA-3 Authentication Process: Implements rules for applying appropriate authentication mechanism.
2) IA-4 Password-based authentication: Implements password-based authentication mechanism.
3) IA-5 Token-based authentication: Implements token-based authentication mechanisms.

FIA_UID.1 Timing of identification: This requirement is met by

1) IA-1 Identity: Definition of WSF identity.
2) IA-3 Authentication Process: Implements identification as integral part of authentication.

FMT_MOF.1 Management of security functions behaviour: This requirement is implemented by the following IT security functions:

1) SM-1 Administrative Roles: Defines capabilities of each security management role to affect security functions
2) SM-3 Default Groups: Associates security management roles with WebLogic Server groups
3) ACC-3 Subject Roles: Process of dynamically granting roles to subjects for use in access decisions

FMT_MSA.1 Management of security attributes: This requirement is implemented by the following IT security functions:

1) SM-1 Administrative Roles: Defines capabilities of each security management role to affect security attributes
2) SM-3 Default Groups: Associates security management roles with WebLogic Server groups
3) ACC-3 Subject Roles: Process of dynamically granting roles to subjects for use in access decisions
4) SM-5 Credential Mapping Provider: Capability to manage users' credentials for legacy applications.

FMT_MSA.3 Static attribute initialisation: This requirement is implemented by the following IT security functions:

1) SM-2 Default Security Attributes of Entities
2) SM-3 Default Groups

FMT_MTD.1 Management of TSF data: this requirement is implemented by the following TI security functions:

1) SM-1 Administrative Roles: Defines capabilities of each security management role to affect TSF data
2) SM-3 Default Groups: Associates security management roles with WebLogic Server groups
3) ACC-3 Subject Roles: Process of dynamically granting roles to subjects for use in access decisions
4) ACC-5 Configuration Options for EJB and URL (Web) Resources: Semantics of *fullyDelegateAuthorization Flag* and *Ignore Security Data in Deployment Descriptors Check Box.*

FMT_SMF.1 Specification of Management Functions: This requirement is implemented by SM-4 Security Provider Database, which provides a database to support management of security functions, security attributes, and TSF data.

FMT_SMR.1 Security roles: This requirement is implemented by SM-1 Administrative roles

FPT_RVM_EXP.1 Non-bypassability of the WSF TSP: This requirement is implemented by:

1) PT-1 Non-bypassability,
2) PT-2 Principal Validation, and
3) SM-1 Administrative Roles.

8.3.2 All TOE and Environment Summary Specification (TSS) Functions Necessary

Table 8.7 shows that all of the IT Security Functions in the TOE Summary Specification (TSS) are necessary. Mappings are provided in Sections 6.1 and 8.3.1 and rationale is provided in Section 8.3.1.

Table 8.7 – Mapping of TOE and Environment Summary Specification to Functional Requirements

IT Security Function	Component	Component Title
ACC-1 Access Decisions	FDP_ACF_EXP.1	Security attribute based access control decision
ACC-2 Security Policies	FDP_ACF_EXP.1	Security attribute based access control decision
ACC-3 Subject Roles	FDP_ACF_EXP.1	Security attribute based access control decision
	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MTD.1	Management of TSF data
ACC-4 WebLogic Resources	FDP_ACF_EXP.1	Security attribute based access control decision
ACC-5 Configuration Options for EJB and URL (Web) Resources	FDP_ACF_EXP.1	Security attribute based access control decision
	FMT_MTD.1	Management of TSF data
AUD-1 Audit Generation	FAU_GEN.1	Audit data generation

IT Security Function	Component	Component Title
AUD-2 Auditable Events	FAU_GEN.1	Audit data generation
AUD-3 Audit Record Fields	FAU_GEN.1	Audit data generation
AUD-4 Severity Attribute	FAU_GEN.1	Audit data generation
AUD-5 Audit Record Format	FAU_GEN.1	Audit data generation
AUD-6 WebLogic Server Log Files	FAU_GEN.1	Audit data generation
IA-1 Identity	FIA_UID.1	Timing of identification
IA-2 User Attributes	FIA_ATD.1	User attribute definition
IA-3 Authentication Process	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
IA-4 Password-based Authentication	FIA_UAU.5	Multiple authentication mechanisms
IA-5 Token-based Authentication	FIA_UAU.5	Multiple authentication mechanisms
IA-6 Authentication Failure Handling	FIA_AFL.1	Authentication failure handling
PT-1 Non-Bypassability	FPT_RVM_EXP.1	Non-bypassability of the WSF TSP
PT-2 Principal Validation	FPT_RVM_EXP.1	Non-bypassability of the WSF TSP
SM-1 Administrative Roles	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MTD.1	Management of TSF data
	FMT_SMR.1	Security roles
	FPT_RVM_EXP.1	Non-bypassability of the WSF TSP
SM-2 Default Security Attributes of Entities	FMT_MSA.3	Static attribute initialisation
SM-3 Default Groups	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
SM-4 Security Provider Database	FMT_SMF.1	Specification of management functions
SM-5 Credential Mapping Provider	FMT_MSA.1	Management of security attributes

8.3.3 Strength of Function Rationale

The strength of function requirement is applicable to the passwords for IA-4 Password-based authentication. This IT security function claims an SOF level of SOF-basic, which satisfies the overall minimum SOF level of SOF-basic.

8.3.4 Assurance Measures Rationale

Table 6.9 – Assurance Measures in section 6.3 shows how all assurance requirements were satisfied.

8.4 PP CLAIMS RATIONALE

Not applicable.

9 ACRONYMS

API	Application Program Interface
ATN	Authentication
ATZ	Authorization
AUD	(Security) Audit
CC	Common Criteria for IT Security Evaluation
CM	Configuration Management
COM	Component Object Model
EAL	Evaluation Assurance Level
ERP	Enterprise Resource Planning
EJB	Enterprise Java Beans
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
J2EE	Java 2 Enterprise Edition
J2SE	Java 2 Standard Edition
JCOM	Java COM
JDBC	Java Database Connectivity
JMS	Java Message Service
JMX	Java Management eXtension
JNDI	Java Naming and Directory Interface
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
MBean	Management Java Bean
OOTB	Out of the Box
RMI	Remove Method Invocation
RMI-IIOP	Remove Method Invocation-Internet Inter-ORB Protocol
SF	Security Function
SFP	Security Function Policy
SOAP	Simple Object Access Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation

TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
WSF	WebLogic Security Framework

References

Reference	Filename
BEA WebLogic Server™ and WebLogic Express ® *Administration Guide*, Release 7.0, Document Revised: September 6, 2002.	Adminguide.pdf
BEA WebLogic Server™ and WebLogic Express™ *Installation Guide*, Version 7.0 SP6, Document Revised: March 5, 2005, Part Number: 860-001001-011.	Install.pdf
BEA WebLogic Server™, *Creating and Configuring WebLogic Server Domains*, Release 7.0, Revised: September 4, 2002.	Admin_domain.pdf
BEA WebLogic Server™, *Developing Security Providers for WebLogic Server*, Release 7.0, Document revised: March 28, 2002.	Dvspisec.pdf
BEA WebLogic Server™, *Introduction to WebLogic Security,* Release 7.0, Document Revised: June 13, 2003	secintro.pdf
BEA WebLogic Server™, *Introduction to WebLogic Server™ and WebLogic Express™,* Release 7.0, Document Revised: September 3, 2002, Part Number:860-001001-011	Intro.pdf
BEA WebLogic Server™, *Managing WebLogic Security,* Release 7.0, Document Revised: February 7, 2003	secmanage.pdf
BEA WebLogic Server™, *Programming WebLogic Security,* Release 7.0, Document Revised: August, 2005	security.pdf
BEA WebLogic Server™, *Securing a Production Environment,* Release 7.0, Document Revised: February 7, 2003	lockdown.pdf
BEA WebLogic Server™, *Securing WebLogic Resources,* Release 7.0, Document Revised: July 18, 2003	secwlres.pdf
BEA WebLogic Server™, *Security Functional Specification Version 7.0, March 21, 2004*	Functional spec.doc
Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.2 Revision 256, CCIMB-2004-01-001, January 2004	http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part1.pdf
Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, CCIMB-2004-01-002, January 2004	http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part2.pdf
Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, CCIMB-2004-01-003, January 2004	http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part3.pdf
Consistency Instruction Manual For development of US Government Protection Profiles (PP) For use in Basic Robustness Environments, Information Assurance Directorate, Release 2.0, 1 March 2004	http://niap.nist.gov/pp/basic_rob_manual.pdf