Pivotal, Inc.
tc Server Standard Edition v2.8.2

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.2

Prepared for:

Pivotal, Inc.
875 Howard St., 5th Floor
San Francisco, CA 94103
United States of America

Phone: +1 650 475 5000

http://www.gopivotal.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050

http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the Pivotal tc Server[1] Standard Edition v2.8.2, and will hereafter be referred to as the TOE throughout this document. The TOE is a lightweight application web server designed for virtual and cloud environments. The TOE is based on open-source Apache Tomcat and allows for compatibility with users' existing web Tomcat applications. It also provides performance enhancements for traditional Java Enterprise Edition (JEE) architectures enabling more efficient web application deployment.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	Pivotal, Inc. tc Server Standard Edition v2.8.2 Security Target
ST Version	Version 1.2
ST Author	Corsec Security, Inc.
ST Publication Date	5/23/2013
TOE Reference	Pivotal tc Server Standard Edition v2.8.2.RELEASE

[1] Formerly called VMware vFabric tc Server

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

Pivotal tc Server Standard Edition v2.8.2 is a web application server that is based on open-source Apache Tomcat. It preserves the best of Tomcat and adds many mission-critical operational capabilities that are unavailable in the open-source product. tc Server modernizes the power of traditional JEE architectures and eliminates their complexity and performance drawbacks, making it easier, faster, and more cost-effective to build and run cloud-ready applications. As shown below in Figure 1, tc Server integrates seamlessly into existing customer environments. With its lean architecture and small memory footprint, the tc Server requires significantly fewer resources than conventional web application servers, allowing for greater server density in virtual and cloud environments.

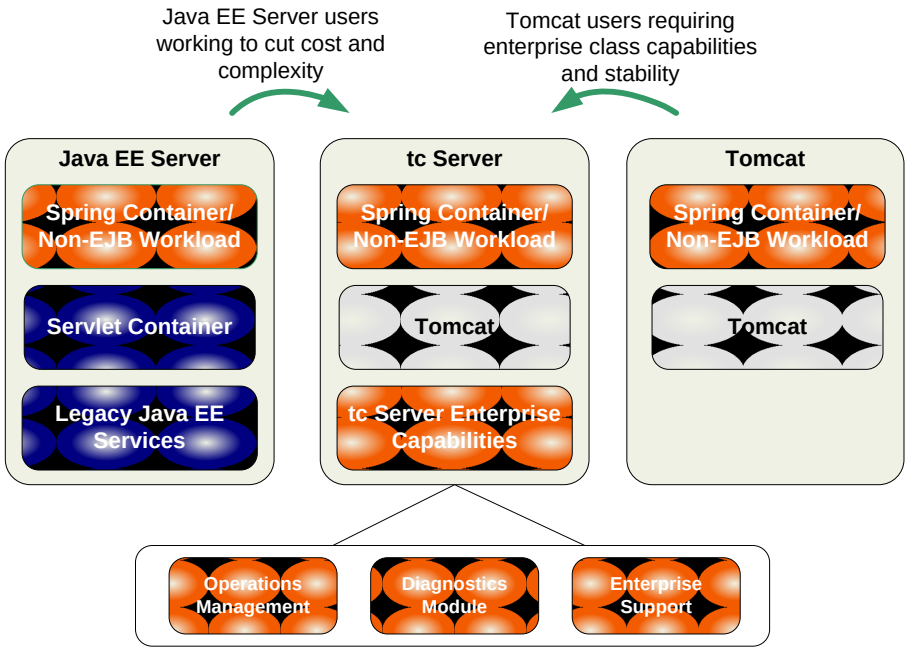

Figure 1 tc Server Integration

tc Server provides additional capabilities not found in a standard Apache Tomcat deployment. Improved out-of-the-box configuration enables customers to rapidly deploy one or more instances of the web server. When using multiple instances of tc Server, instances can be grouped into clusters providing high-availability and load-balancing features. tc Server includes pre-packaged templates that can be leveraged during the deployment phase by using optional command line parameters. Custom templates can also be created, greatly reducing the configuration work during deployment. Multiple instances of tc Server can be deployed at a time using a single tc Server Standard Edition installation. tc Server is automatically configured to use a high-concurrency Java Database Connectivity connection pool whenever a new instance is deployed. tc Server also exposes custom Managed Beans (MBeans) through a Java Management Extension (JMX) agent allowing customers with a JMX client to invoke commands, view configuration, and view real time monitoring statistics.

tc Server can be installed on Windows or Linux-based operating systems. Table 2 below specifies the minimum system requirements for the proper operation of tc Server.

Table 2 tc Server Minimum System Requirements

Operating System	Major Version	Chip Architecture	Java
RedHat Enterprise Linux (RHEL)	V5	x86 32-bit	Java SE Runtime Environment 7
		x86 64-bit	
	V6	x86 32-bit	
		x86 64-bit	
Ubuntu	10.04 LTS	x86 64-bit	Java SE Runtime Environment 7
Microsoft Windows	Server 2008 SP2	x86 32-bit	Java SE Runtime Environment 7
		x86 64-bit	
	Server 2003 SP2 and newer	x86 32-bit	

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is a web application server based on open-source Apache Tomcat. The TOE can be run in a stand-alone configuration or in clustered-mode configuration. Deploying the TOE in clustered-mode will ensure user sessions are not ended abruptly and continue to operate without interruption in the event of a web server crash.

The TOE provides Hypertext Transfer Protocol (HTTP), Apache JServ Protocol (AJP), and JMX interfaces through which users may connect. All interfaces support authentication. Authentication to the HTTP and AJP interfaces require a username and password combination that may be entered in either a form or a browser-based method. The HTTP and AJP Connector interfaces also support X.509 certificate authentication. The configuration of the protocols and ports for the HTTP and AJP Connectors is retrieved by the TOE from the *server.xml* file. There is no way to manipulate the *server.xml* file from within the TOE and therefore any configuration of this file must take place through the TOE environment. The JMX interface requires the use of a third party JMX client such as JConsole and passes username and password credentials to the JMX interface for authentication. Access to JMX interface is restricted to only those users on the same local area network as the TOE itself.

Accounts for HTTP and AJP Connector interface are maintained by the TOE in the *tomcat-users.xml* file. This file can be edited via the TOE environment using a text editor such as NotePad. The contents of this file are read to create the UserDatabase MBean. These accounts represent the users of the TOE that invoke resource requests on web applications that are hosted by the TOE. The user accounts located in the UserDatabase MBean may be edited through the TOE using JConsole to access the JMX Socket Listener interface. Changes made to the user accounts located in the UserDatabase MBean will be reflected in the *tomcat-users.*xml for persistence.

Accounts for the JMX Socket Listener interface are maintained by the TOE in the *jmxremote.access* and *jmxremote.password* files. These accounts represent the administrators of the TOE. These files can only be edited via the TOE environment and there is no configuration or management of the files provided by the TOE.

TOE security functionality (TSF) data is accessible to only authorized TOE users and is also protected using Access Control Security Functional Policies (SFPs). The Access Control SFPs are used to mediate the TSF data exposed through the HTTP, AJP, and JMX interfaces.

Figure 2 shows the details of the deployment configuration of the TOE and contains the following previously undefined acronym:

- OS – Operating System

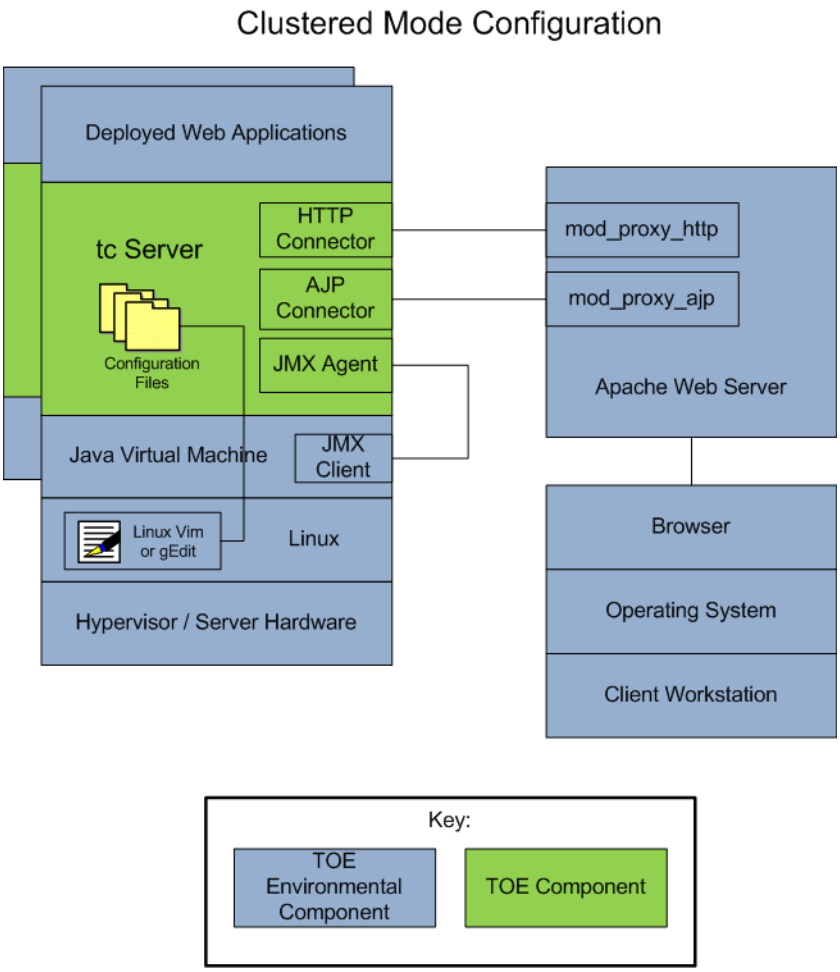

Figure 2 Deployment Configuration of the TOE

1.4.1 TOE Environment

The TOE is intended to be deployed in a physically secure cabinet room or data center with the appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms, etc.) The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE is installed on a physical or virtual platform that is outside of the TOE boundary. The underlying operating system and Java Virtual Machine (JVM) of the host platform are parts of the TOE environment. All configuration of the TOE is performed through the environment via XML and configuration files. The entire management workstation, its browsers, and JMX clients are considered part of the TOE environment as well.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE boundary consists of only the application web server software (the Pivotal tc Server Standard Edition v2.8.2.RELEASE binary). There are two instances of the TOE in the evaluated configuration. Each instance of the TOE is installed on the RHEL v5 OS running on physical or virtual hardware. Additionally, each installation of the RHEL v5 OS must have Java version 7 update 10 or later installed. The deployment configuration of the TOE is shown as depicted in Figure 3 below. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- Physical or virtual hardware running RHEL v5 x86 64-bit for each instance of the TOE
- Client workstation used to connect to the TOE, installed with:
  - Mozilla Firefox 10 or newer, Internet Explorer 9.0 or newer
- VMware vFabric Web Server 5.2 or later configured to support both HTTP and AJP requests
- Java SE Runtime Environment 7 must be installed on the RHEL v5 OS

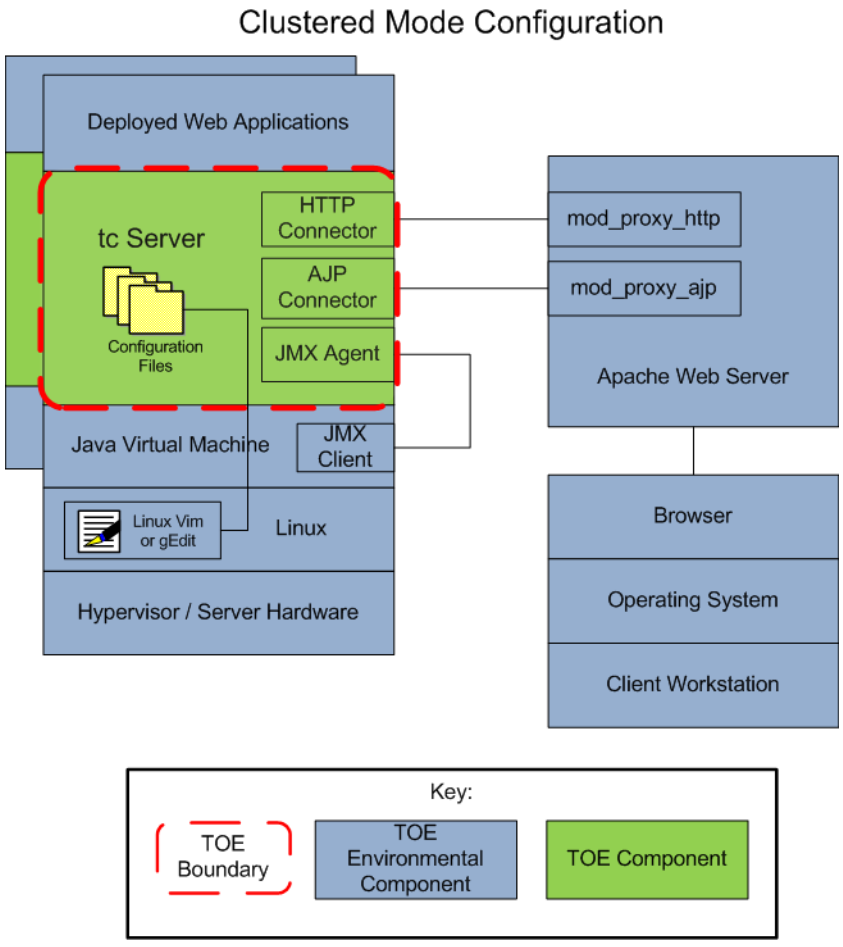

Figure 3 Physical TOE Boundary

1.5.1.1 Guidance Documentation

Table 3 lists the TOE Guidance Documentation to install, configure, and maintain the TOE.

Table 3 Guidance Documentation

Document Name	Description
Getting Started with vFabric tc Server, VMware vFabric Cloud Application Platform 5.0, VMware vFabric tc Server 2.8	Includes steps for the basic initialization and setup of the TOE.
vFabric tc Server Administration, VMware vFabric Cloud Application Platform 5.0, VMware vFabric tc Server 2.8	Contains detailed steps for how to properly configure and maintain the TOE.
tc Server 2.8 Release notes, http://www.vmware.com/support/vfabric-tcserver/doc/vfabric-tcserver-rn-2.8.0.html	Contains release notes for tc Server 2.8.x and the versions leading up to it.
Apache Tomcat 7 Documentation, http://tomcat.apache.org/tomcat-7.0-doc/index.html	Contains detailed documentation on the underlying Apache Tomcat functionality.
Pivotal Inc. tc Server Standard Edition v2.8.2 Guidance Supplement v0.2	Contains information regarding specific configuration for the TOE evaluated configuration.

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access

1.5.2.1 Security Audit

The TOE generates log files to record audit events. The audit data contains events such as web server access and records the source Internet Protocol (IP) address, requested Uniform Resource Locator (URL), response code, bytes transferred, success or failure of the transfer, and a timestamp for each event. Additionally, this log records startup and shutdown of the web server, web application deployment and removal, and errors trapped by web applications or tc Server itself.

1.5.2.2 User Data Protection

The TOE allows authorized administrators to enforce rigid Access Control SFPs for users accessing TOE resources. The TOE enforces administrator-configurable policies on access to sensitive data:

- Access to web applications hosted by the TOE via the HTTP interface.

- Access to web applications hosted by the TOE via the AJP interface.
- Access to Managed Beans exposed by the TOE through the JMX Agent interface.

Each instance of the TOE contains identical user data providing high availability in the event of a TOE crash. User data consists of user security attributes and any data related to the deployed applications hosted by the TOE. If the instance of the TOE currently serving user requests crashes, the TOE ensures that the instance of the TOE selected to take over the session will contain the same user security attributes and deployed application data.

1.5.2.3 Identification and Authentication

The TOE enforces identification and authentication on users attempting to access restricted content. Only TOE resources that have an Access Control SFP with the <url-pattern> (found in the resources *web.xml* file) set to "unchecked/*" may be accessed prior to this process. The unauthenticated access allowed when the <url-pattern> is set to "unchecked/*" is specific to only the HTTP and AJP Connector interfaces and does not apply to the JMX Socket Listener interface. Authorized administrators are responsible for configuring the identification and authentication method that occurs. This method can be configured in one of three ways: form-based, browser-based, or certificate-based. The TOE maintains the following list of attributes for each user: a username, a secret (password or X.509 certificate depending on the authentication method specified), and a role. Upon successful identification and authentication, the user is permanently associated with these attributes during the active session. The TOE provides additional security through the use of a configurable strike-out policy allowing the TOE to deny a user access based on a predefined number of unsuccessful login attempts. The TOE also provides obscured authentication feedback during login.

1.5.2.4 Security Management

The TOE provides management capabilities via JMX, accessible through the JMX Socket Listener Interface. The TOE enforces the JMX Access Control SFP to restrict the ability to configure and manage the security attributes of HTTP and AJP Connector subject attributes. The TOE user accounts that may be edited via JMX are the HTTP and AJP Connector accounts found in the *tomcat-users.xml* file. When using JMX to configure security attributes used by the HTTP Access Control SFP and the AJP Access Control SFP, the TOE provides restrictive default values that will be denied by the these SFPs respectively.

The TOE provides authorised users with write permissions the ability to manage the security attributes surrounding the HTTP and AJP Connector subject attributes. The TOE maintains a set of administrator-configured roles used to determine the access privileges during user authentication with the JMX Socket Interface.

1.5.2.5 Protection of the TSF

The TOE is configured in a clustered-mode deployment replicating data across each instance of the TOE. This configuration enables the TOE to continue to function in a secure state if an instance of the TOE crashes or is taken out of service.

Each instance of the TOE contains identical TSF data ensuring all Access Control SFPs are still enforced. If the instance of the TOE currently serving user requests crashes, the TOE ensures that the instance of the TOE selected to take over the session will continue to implement the same Access Control SFPs.

1.5.2.6 Resource Utilization

The TOE enforces maximum quotas on the number of processing threads that users can use simultaneously. Subsequent user requests will be forced to wait until an active processing thread is terminated allowing another request to be handled.

1.5.2.7 TOE Access

The TOE has the ability to terminate inactive user sessions.

1.5.3 Product Physical and Logical Features and Functionality not included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- All the web applications (and the corresponding *web.xml* files published by these applications) that are deployed and hosted on tc Server
- Underlying physical or virtual hardware on which the TOE is installed.
- RHEL v5 Operating system on which the TOE is installed.
- Web browsers (Firefox 10 or newer, or IE 9 or newer) used to submit resource requests via the HTTP or AJP Connectors.
- JMX Client used to access the JMX Socket Interface.

2 Conformance Claims

This section and Table 4 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2012/05/18 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.3)

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[2] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 5 below lists the applicable threats.

Table 5 Threats

Name	Description
T.AUDIT_COMPROMISE	A malicious user or process may modify the timestamp source in order to conceal malicious events.
T.FAILURE	A TOE user or attacker may cause an instance of the TOE to fail in an attempt to prevent the TOE from meeting the TSF.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorised access to data or TOE resources.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.
T.TSF_COMPROMISE	A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.UNAUTHORIZED _ACCESS	An unauthorized user may attempt to bypass the security of the TOE to access and use security functions and/or other functionality provided by the TOE.

[2] IT – Information Technology

3.2 Organizational Security Policies

There are no Organizational Security Policies for this evaluation.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 Assumptions

Name	Description
A.CERTIFICATE	The TOE will be able to authenticate users with X.509 certificates as an authentication credential.
A.LOCATE	The connection between the two clustered instances of the TOE an any TOE environmental components (the Apache Web Server, Remote Administrator workstation) are all located within a controlled access facility on a secured network.
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the Linux OS in the TOE environment (where the TOE is installed), other than those services necessary for the operation, administration, and support of the TOE.
A.PHYSICAL	The TOE environment will provide physical security commensurate with the value of the TOE and the data it contains.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMPS	The TOE environment will provide the TOE with the necessary reliable timestamps.
A.XML_CONFIGURATION	The TOE environment is assumed to provide protection for the administration of TOE's XML configuration files by unauthorized users.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7 below.

Table 7 Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must prevent unauthenticated users from accessing configuration data and resources that require authentication.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.
O.AUTHENTICATE	The TOE must require identification and authentication before any access to the JMX Socket Listener is granted and if a resource data request matches an HTTP or AJP access control SFP rule which requires identification and authentication.
O.LOCKOUT	The TOE must protect user passwords from being obtained through brute-force attack methods through account lockout thresholds.
O.MANAGE	The TOE must provide all the functions and facilities necessary to support the authorized administrator in management of the security attributes as discussed in FMT_MSA.1, and restrict these functions and facilities from unauthorized use.
O.PROTECT	The TOE must protect the TSF in the event of failure of a single TOE instance in a clustered node configuration.
O.QUOTA	The TOE shall prevent resource exhaustion attacks through the use of maximum connection quotas.
O.REPLICATION	The TOE must export user session data to other TOE instances whenever a session changes. This guarantees data consistency between the TOE instances.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

Table 8 IT Security Objectives

Name	Description
OE.CRYPTO	The TOE Environment must provide the cryptographic functionality and protocols required to generate and verify X.509 certificates to be used by the TOE for certificate authentication.
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.NO_GENERAL_PURPOSE	There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on the Linux OS in the TOE environment (where the TOE is installed), other than those services necessary for the operation, administration, and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the TOE environment.
OE.PROTECT	The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.
OE.TIMESTAMPS	The operational environment will provide reliable time stamps.
OE.XML_CONFIGURATION	The TOE environment will provide all the functions and facilities necessary to support administrators responsible for management and configuration of the TOE's XML files, and the TOE environment will restrict these functions and facilities from unauthorized users.

4.2.2 Non-IT Security Objectives

Table 9 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 Non-IT Security Objectives

Name	Description
NOE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
NOE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the TOE environment.

5 Extended Components

There are no extended SFRs and extended SARs for this TOE.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FDP_ACC.1(a)	Subset access control - HTTP		✓		✓
FDP_ACC.1(b)	Subset access control - JMX		✓		✓
FDP_ACC.1(c)	Subset access control - AJP		✓		✓
FDP_ACF.1(a)	Security attribute based access control - HTTP		✓		✓
FDP_ACF.1(b)	Security attribute based access control - JMX		✓		✓
FDP_ACF.1(c)	Security attribute based access control - AJP		✓		✓
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.5	Multiple authentication mechanism		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.1	Timing of Identification		✓		

Name	Description	S	A	R	I
FIA_USB.1	User-subject binding		✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation - JMX	✓	✓		
FMT_SMF.1(a)	Specification of management functions - JMX		✓		✓
FMT_SMF.1(b)	Specification of management functions - XML		✓		✓
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of a secure state		✓		
FPT_ITA.1	Inter-TSF availability within a defined availability metric		✓	✓	
FRU_RSA.1	Maximum quotas	✓	✓		
FTA_SSL.3	TSF initiated termination		✓	✓	

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps
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) [*HTTP and AJP Connector resource requests, web application deployment and removal, and errors trapped by deployed applications or the TOE*].

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 (if applicable), 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, [*the additional information found in Table 11 for HTTP and AJP Connector requests only*].

Table 11 Additional Information Recorded for HTTP or AJP Connector Requests

Field	Content
Client host name	IP address of the client connection
Remote logical username	A dash (-) character is used to represent the remote logical username for actions that do not require the user to be unauthenticated. The username present in the *tomcat-users.xml* file is used to represent the logical username for actions that do require the user be authenticated.
Method and Resource	The HTTP method and the location of the requested resource
Response	The HTTP response status code
Response size	The HTTP response size in bytes (excluding the HTTP response headers)

6.2.2 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control – HTTP
Hierarchical to: No other components.
Dependencies: FDP_ACF.1(a) Security attribute based access control – HTTP
FDP_ACC.1.1a
The TSF shall enforce the [*HTTP access control SFP*] on
[*Subjects: Calling entity that has been assigned to a specific role,*
Objects: Resource data located at the specified Uniform Resource Locator (URL),
Operations: HTTP methods consisting of: GET, POST, PUT, TRACE, DELETE, HEAD].

FDP_ACC.1(b) Subset access control – JMX
Hierarchical to: No other components.
Dependencies: FDP_ACF.1(b) Security attribute based access control – JMX
FDP_ACC.1.1b
The TSF shall enforce the [*JMX access control SFP*] on
[*Subjects: Calling entity that has been assigned to a specific role,*
Objects: JMX Socket Listener
Operations: JMX Remote Method Invocation (RMI) operations supported by the TSF's Management Bean Server].

FDP_ACC.1(c) Subset access control – AJP
Hierarchical to: No other components.
Dependencies: FDP_ACF.1(c) Security attribute based access control – AJP
FDP_ACC.1.1c
The TSF shall enforce the [*AJP access control SFP*] on
[*Subjects: Calling entity that has been assigned to a specific role,*
Objects: Resource data located at the specified URL
Operations: HTTP methods encapsulated in the following AJP methods: SEND_HEADERS, SEND_BODY_CHUNK, GET_BODY_CHUNK, END_RESPONSE].

FDP_ACF.1(a) Security attribute based access control – HTTP
Hierarchical to: No other components.
Dependencies: FDP_ACC.1(a) Subset access control – HTTP
FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1a
The TSF shall enforce the [*HTTP Access Control SFP*] to objects based on the following:
[*Subjects: Calling entity*
Attributes: Role
Objects: resource data located at the specified URL
Attributes: Role, HTTP method, and URL].
FDP_ACF.1.2a
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*the calling entity may invoke the HTTP operation on the stored resources at the specified URL if the following conditions are met:*

1. *The role associated with the calling entity (defined in the tomcat-users.xml) file matches one of the allowed roles specified in the <auth-constraint>, a sub-element of the <security-constraint> element in the web application's web.xml file.*
2. *The HTTP operation submitted by the calling entity must be listed as an available <http-method> under the <web-resource-collection> in the web application's web.xml file.*

3. *The transport guarantee method used by the calling entity must at least cover the transport guarantee method as defined by the <user-data-constraint> element for the specified URL in the in the web application's web.xml file, requiring NONE, INTEGRAL, or CONFIDENTIAL in order of ascending security]*.

FDP_ACF.1.3a

The TSF shall explicitly authorise access of subjects to objects based on the following additional rule: [*when the <url-pattern> is configured to "/unchecked/*" or there is no <security-constraint> in the web application's web.xml file, all authorized entities may access any URL and its associated resource data*].

FDP_ACF.1.4a

The TSF shall explicitly deny access of subjects to objects based on the following additional rules [*no additional rules*].

FDP_ACF.1(b) Security attribute based access control – JMX

Hierarchical to: No other components.

Dependencies: FDP_ACC.1(b) Subset access control – JMX
FMT_MSA.3 Static attribute initialization – JMX

FDP_ACF.1.1b

The TSF shall enforce the [*JMX Access Control SFP*] to objects based on the following:

[*Subjects: Calling entity*
Attributes: Role
Objects: JMX Socket Listener
Attributes: Role (every MBean method is accessible if the subject is associated with the appropriate role].

FDP_ACF.1.2b

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*the calling entity may invoke JMX RMI operations via the JMX Socket Listener if the following conditions are met:*

1. *The username of the calling entity has the appropriate role (defined in the jmxremote.access file).*
2. *The calling entity is on the same local subnet as the TOE*.

FDP_ACF.1.3b

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

FDP_ACF.1.4b

The TSF shall explicitly deny access of subjects to objects based on the following additional rules [*no additional rules*].

Note to Evaluator: While listed as a dependency, the FMT_MSA.3 requirement is not met for this SFR. There are no management capabilities provided by the TOE through this interface that would allow the subject attributes defined in this SFP to be configured or managed at all. The configuration and management of subject attributes used by the HTTP Access Control SFP and AJP Access Control SFP can only be accomplished through the JMX interface or through the TOE environment. Therefore, this dependency has been met by the TOE environment, via XML file configuration.

FDP_ACF.1(c) Security attribute based access control – AJP

Hierarchical to: No other components.

Dependencies: FDP_ACC.1(c) Subset access control – AJP
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1c

The TSF shall enforce the [*AJP Access Control SFP*] to objects based on the following:
[*Subjects: Calling entity*
Attributes: Role
Objects: resource data located at the specified URL
Attributes: Role, HTTP method, and URL].

FDP_ACF.1.2c

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*the calling entity may invoke the AJP encapsulated HTTP operation on the stored resources at the specified URL if the following conditions are met:*

1. *The role associated with the calling entity (defined in the tomcat-users.xml) file matches one of the allowed roles specified in the <auth-.constraint>, a sub-element of the <security-constraint> element in the web application's web.xml file.*
2. *The HTTP operation submitted by the calling entity must be listed as an available <http-method> under the <web-resource-collection> in the web applications web.xml file.*
3. *The transport guarantee method used by the calling entity must at least cover the transport guarantee method as defined by the <user-data-constraint> element for the specified URL in the in the web application's web.xml file, requiring NONE, INTEGRAL, or CONFIDENTIAL in order of ascending security].*

FDP_ACF.1.3c

The TSF shall explicitly authorise access of subjects to objects based on the following additional rule: [*when the <url-pattern> is configured to "/unchecked/*" or there is no <security-constraint> in the web application's web.xml file, all authorized entities may access any URL and its associated resource data*].

FDP_ACF.1.4c

The TSF shall explicitly deny access of subjects to objects based on the following additional rules [*no additional rules*].

6.2.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_AFL.1.1
The TSF shall detect when [[an administrator configurable positive integer within [*1 to 5*]] unsuccessful authentication attempts occur related to [*authentication to the web server*].
FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the user account for an administrator configurable amount of time*].

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users: [*username, password or X.509 certificate (HTTP and AJP users only), and role*].

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.1.1
The TSF shall allow [*HTTP operations on resource data URLs that do not have a <url-pattern> defined in the web application's web.xml*] 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.

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_UAU.5.1
The TSF shall provide [*the following multiple authentication mechanisms for the HTTP and AJP Connector interfaces:*
- *form-based,*
- *browser-based, and*
- *certificate-based*

] to support user authentication.
FIA_UAU.5.2
The TSF shall authenticate any user's claimed identity according to the [*internally stored identity and credential information*].

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_UAU.7.1
The TSF shall provide only [*bullets (form-based) and asterisks (browser-based)*] to the user while authentication is in progress.

FIA_UID.1 Timing of identification
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_UID.1.1

The TSF shall allow [*HTTP operations on resource data URLs that do not have a <security-constraint> defined in the web application's web.xml file*] 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.

FIA_USB.1: User-subject binding
Hierarchical to: No other components
Dependencies: FIA_ATD.1 User Attribute Definition
FIA_USB.1.1:

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*username and role*].

FIA_USB.1.2:

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*the user must authenticate successfully with the TOE before any associations are made*].

FIA_USB.1.3:

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*there are to be no changes to user security attributes after the user-subject binding has occurred*].

6.2.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*JMX Access Control SFP*] to restrict the ability to [create, delete, modify] the security attributes [*specified in the FIA_ATD.1, excluding X.509 certificates*] to [*administrator-configurable roles*].

Dependencies: FDP_ACC.1(b) Subset access control – JMX
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MSA.3 Static attribute initialisation – JMX

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*JMX Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*no one*] 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

FMT_SMF.1a Specification of management functions – JMX

Hierarchical to: No other components.

FMT_SMF.1.1a

The TSF shall be capable of performing the following management functions: [*management of security attributes as described in FIA_ATD.1]*.

Dependencies: No Dependencies

FMT_SMF.1b Specification of management functions – XML

Hierarchical to: No other components.

FMT_SMF.1.1b

The TSF shall be capable of performing the following management functions: [*management of HTTP, AJP, and JMX account security attributes as described in FIA_ATD.1, clustered-mode configuration, maximum resource quotas for Connectors, audit log name and path, the multiple authentication mechanisms, HTTP and AJP session timeouts, and Connector authentication failure parameters by editing the configuration files of the TOE]*.

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*administrator-configurable roles*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*crash of one instance of the TOE*].

FPT_ITA.1 Inter-TSF availability within a defined availability metric
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_ITA.1.1

The TSF shall ensure the availability of [*user session data*] provided to another trusted IT product within [*within five seconds and prior to completing the user request*] given the following conditions *[both instances of the TOE are operational and available*].

6.2.6 Class FRU: Resource Utilization

FRU_RSA.1 Maximum quotas
Hierarchical to: No other components.
Dependencies: No dependencies
FRU_RSA.1.1

The TSF shall enforce maximum quotas of the following resources: [*HTTP Connector and AJP Connector queues*] that [subjects] can use [simultaneously].

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_SSL.3.1

The TSF shall terminate an interactive **user** session after an [*administrator-configurable time, in minutes, of user inactivity*].

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.3. Table 12 Assurance Requirements summarizes the requirements.

Table 12 Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.3 Basic Flaw Remediation
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Complete functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Focused Vulnerability analysis

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 13 lists the security functions and their associated SFRs.

Table 13 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
User Data Protection	FDP_ACC.1(a)	Subset access control - HTTP
	FDP_ACC.1(b)	Subset access control - JMX
	FDP_ACC.1(c)	Subset access control - AJP
	FDP_ACF.1(a)	Security attribute based access control - HTTP
	FDP_ACF.1(b)	Security attribute based access control - JMX
	FDP_ACF.1(c)	Security attribute based access control - AJP
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanism
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of Identification
	FIA_USB.1	User-subject binding
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation - JMX
	FMT_SMF.1(a)	Specification of management functions - JMX
	FMT_SMF.1(b)	Specification of management functions - XML
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of a secure state
	FPT_ITA.1	Inter-TSF availability within a defined availability metric

TOE Security Function	SFR ID	Description
Resource Utilization	FRU_RSA.1	Maximum quotas
TOE Access	FTA_SSL.3	TSF initiated termination

7.1.1 Security Audit

The TOE is capable of auditing a variety of events, including startup and shutdown of the system, HTTP and AJP resource requests to the TOE, web application deployment and removal, and errors trapped by deployed web application or the TOE itself.

Although the TOE does not explicitly generate an audit event for startup and shutdown of the audit functionality, it does audit the startup and shutdown of the system. Since the system starts up and shuts down at the same time as the audit function, these records can be considered to provide equivalent notice.

With each auditable event, the TOE must record the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. Web application resources requests received by the TOE over the HTTP and AJP connectors will also be recorded with the following additional information found below in Table 14. :

Table 14 Additional Information Recorded for HTTP or AJP Connector Requests

Field	Content
Client host name	IP address of the client connection
Remote logical username	A dash (-) character is always used to represent the remote logical username.
Method and Resource	The HTTP method and the location of the requested resource
Response	The HTTP response status code
Response size	The HTTP response size in bytes (excluding the HTTP response headers)

TOE Security Functional Requirements Satisfied: FAU_GEN.1.

7.1.2 User Data Protection

The TOE enforces HTTP and AJP Access Control SFPs to manage access to resource data within or hosted by the TOE. Authorized users possessing the appropriate permissions may execute HTTP or AJP (used to encapsulate HTTP) methods. The HTTP and AJP Access Control SFPs determine if the user is allowed to access the resource by comparing the role of the user with the role that the resource requires. If the user has the correct permissions to access the resource, the TOE must ensure that the user is using the appropriate transport guarantee method as required by the resource. The HTTP and AJP Access Control SFPs allow authorized users access to some resource data if the <url-pattern> in the web application's *web.xml* is set as "/unchecked/*".

The TOE also enforces a JMX Access Control SFP to manage access to the JMX Socket Listener. Authorized users possessing the appropriate permissions may access the JMX Socket Listener and invoke

JMX RMI methods on the TOE's Managed Beans. The username and role of the user are compared to a local list of authorized JMX users and their permissions defined in the "jmxremote.access" file. The JMX Socket Listener requires authentication and the password of the user and compares them to username and password combinations found in the local "jmxremote.password" file. There is no explicit access given to the JMX Socket Listener and access to this resource always requires authentication.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACC.1(c), FDP_ACF.1(a), FDP_ACF.1(b), FDP_ACF.1(c),.

7.1.3 Identification and Authentication

The TOE requires users and administrators to identify and authenticate before allowing access to TOE functionality; however, there are some resources that do not require authentication. Web applications that do not have a "<security-constraint>" explicitly defined in the web application's *web.xml* file may be accessed by any user or administrator prior to authentication. The TOE supports multiple authentication mechanisms. Users and administrators can use passwords in both form and browser-based authentication, or users and administrators can use certificates for authentication. The TOE also provides obscured authentication feedback during login.

The TOE stores the credentials associated with each user and administrator locally Credentials for users accessing the HTTP and AJP interfaces consist of a user ID, password (or x.509 certificate), and a role. The user ID, password, and role are all stored in the *tomcat-users.xml* file and can be edited through the TOE environment or via a JMX session. If an X.509 certificate has been configured for use, this credential is stored in the *tcserver.keystore* file. This file is only editable via the TOE environment. Credentials for JMX accounts consist of a user ID, password, and role. The JMX credentials are stored in two files: the user ID and role are stored in the *jmxremote.access* file and the user ID and password are stored in the *jmxremote.password* file.

The TOE tracks authentication attempts and has the ability to lock a user out after an administrator configurable amount of failed attempts, for an administrator-configurable period of time. Upon successful identification and authentication, the user is permanently associated with these attributes during the active session. JMX clients acting on behalf of authenticated users inherit the username and role security attributes of the user. In this way, users bind to the JMX clients rather than issuing commands directly.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.7, FIA_UID.1, FIA_USB.1.

7.1.4 Security Management

The TOE provides management capabilities via JMX, accessible through the JMX Socket Listener Interface. The TOE enforces the JMX Access Control SFP to restrict the ability to configure and manage MBeans. The MBeans accessible via JMX allow for the configuration and management of the security attributes of HTTP and AJP Connector subject attributes. The TOE user accounts that may be edited via the JMX Socket Interface are the HTTP and AJP Connector accounts found in the *tomcat-users.xml* file. The JMX Socket Interface does not provide direct access to the *tomcat-users.xml file*, but rather changes made to the UserDatabase MBean will be reflected in this file after the changes have been committed. When using JMX to configure security attributes used by the HTTP Access Control SFP and the AJP Access Control SFP, the TOE provides restrictive default values that will be denied by the these SFPs respectively. The JMX interface does provide any capability to deploy web applications or edit the security attributes of web applications in the web application's *web.xml* file.

The TOE provides authorised users with write permissions the ability to manage the security attributes surrounding the HTTP and AJP Connector subject attributes. The TOE maintains a set of administrator-

configured roles used to determine the access privileges during user authentication with the JMX Socket Interface.

In addition to managing the TOE through the JMX interface, the TOE also provides management capabilities via directly editing the configuration files through a Linux text editor. Only trusted administrators will have access to the workstation where the TOE resides, and therefore only trusted administrators will be able to directly access these files. Like the JMX interface, administrators may manage all HTTP and AJP user accounts, but the Linux text editor interface allows JMX accounts to be managed as well. Through the manipulation of the configuration files, the TOE also provides management capabilities for the following TOE features: clustered mode configuration, maximum resource quotas for Connectors, audit log name and path, the multiple authentication mechanisms, HTTP and AJP session timeouts, and Connector authentication failure parameters.
TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1(a), FMT_SMF.1(b), FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE provides a secure state in the event that one instance of the TOE crashes when the TOE is configured in a clustered mode of operation.

In the evaluated configuration, the TOE is deployed in a clustered-mode configuration. Each instance of the TOE that is a member of the cluster is required to be configured with the same multicast IP address. All TOE instances that are members of the same cluster contain identical TSF data. TSF data, or user session data, is kept consistent across multiple instances of the TOE through replication updates that occur each time a user modifies the session. The TOE exports the TSF data to other instances of the TOE that are members of the cluster using TCP unicast messages. If a user is currently interacting with an instance of the TOE that suddenly crashes, any other TOE instance in the same cluster group can take over the request handling and begin providing TOE services. The Apache Web Server in the TOE environment is responsible for redirecting the request; however, the TOE implements the actual TSF data replication process.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_ITA.1.

7.1.6 Resource Utilization

The TOE enforces maximum quotas on the queue sizes associated with the HTTP Connector and AJP Connectors for incoming connection requests. When all processing threads are in use, users' requests go into either the HTTP or the AJP Connector queues. . Once the HTTP or AJP Connector queues have reached the administrator-configurable length, subsequent user requests will receive a "Connection Refused" error message and be forced to wait until there is space in the queue.

TOE Security Functional Requirements Satisfied: FRU_RSA.1.

7.1.7 TOE Access

The TOE automatically ends user sessions after an administrator-configurable time, in minutes, of inactivity. Users are required to re-authenticate after a session timeout.

TOE Security Functional Requirements Satisfied: FTA_SSL.3.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 15 below provides a mapping of the objects to the threats they counter.

Table 15 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.AUDIT_COMPROMISE A malicious user or process may modify the timestamp source in order to conceal malicious events.	OE.PROTECT The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.	The OE.PROTECT objective counters this threat by protecting the IT Environment that provides reliable time stamps and thereby making it impossible for a malicious user to tamper with the source of time stamps. This guarantees that the date and time that the event occurred is accurate and the audit logs are not compromised.
T.FAILURE A TOE user or attacker may cause an instance of the TOE to fail in an attempt to prevent the TOE from meeting the TSF.	O.PROTECT The TOE must protect the TSF in the event of failure of a single TOE instance in a clustered node configuration.	O.PROTECT mitigates this threat by protecting the TSF in the event of a failure of a single TOE instance in a clustered mode configuration.
	O.REPLICATION The TOE must export user session data to other TOE instances whenever a session changes. This guarantees data consistency between the TOE instances.	The O.REPLICATION counters this threat by ensuring that in the event of a TOE instance crashing, there is another instance of the TOE able with identical session data able to replace the failed instance without outside visibility a crash occurred.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorised access to data or TOE resources.	O.AUTHENTICATE The TOE must require identification and authentication before any access to the JMX Socket Listener is granted and if a resource data request matches an HTTP or AJP access control SFP	The O.AUTHENTICATE ensures login credentials of an identity and authentication credential are supplied and verified before being granted access to services or information, thereby reducing the risk of access by masquerading.

Threats	Objectives	Rationale
	rule which requires identification and authentication.	
	O.LOCKOUT The TOE must protect user passwords from being obtained through brute-force attack methods through account lockout thresholds.	The O.LOCKOUT counters this threat by protecting users' passwords from brute-force guessing by attackers by locking users' accounts after a configurable number of failed authentication attempts for an administrator configurable period of time, thereby reducing the risk of someone being able to masquerade as another user.
	O.MANAGE The TOE must provide all the functions and facilities necessary to support the authorized administrator in management of the security attributes as discussed in FMT_MSA.1, and restrict these functions and facilities from unauthorized use.	
T.RESOURCE_EXHAUSTION A process or user may deny access to TOE services by exhausting critical resources on the TOE.	O.QUOTA The TOE shall prevent resource exhaustion attacks through the use of maximum connection quotas.	The O.QUOTA objective counters this threat by providing maximum connection quotas to mitigate user attempts to intentionally or inadvertently exhaust TOE resources.
T.TSF_COMPROMISE A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).	O.ACCESS The TOE must prevent unauthenticated users from accessing configuration data and resources that require authentication.	The O.AUDIT objective ensures that configuration data will not be accessible to a malicious user or process and that only authenticated users will have access to these resources.
T.UNAUTHORIZED _ACCESS An unauthorized user may attempt to bypass the security of the TOE to access and use security functions and/or other functionality provided by the TOE.	O.ACCESS The TOE must prevent unauthenticated users from accessing configuration data and resources that require authentication.	The O.ACCESS counters this threat by ensuring that users gain only authorized access to it and to resources that it controls.
	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	The O.AUDIT_GENERATION objective ensures that security relevant events that may indicate attempts to gain unauthorised access to the TOE are recorded.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no organizational security policies defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 16 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.CERTIFICATE The TOE will be able to authenticate users with X.509 certificates as an authentication credential.	OE.CRYPTO The TOE Environment must provide the cryptographic functionality and protocols required to generate and verify X.509 certificates to be used by the TOE for certificate authentication.	OE.CRYPTO satisfies this assumption by stating that the TOE environment will provide all the necessary functions and facilities to generate and verify X.509 certificates that will be imported into the TOE and used as an authentication credential by users authenticating to the TOE.
A.LOCATE The connection between the two clustered instances of the TOE an any TOE environmental components (the Apache Web Server, Remote Administrator workstation) are all located within a controlled access facility on a secured network.	OE.PROTECT The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.	OE.PROTECT satisfies this assumption by stating that the TOE environment will provide all the necessary protection for the network that TOE communications will be traversing.
A.NO_EVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	OE.NO_EVIL Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	OE.NO_EVIL upholds this assumption by ensuring that administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the Linux OS in the TOE environment (where the TOE is installed), other than those services necessary for the operation, administration, and support of the TOE.	OE.NO_GENERAL_PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on the Linux OS in the TOE environment (where the TOE is installed), other than those services necessary for the operation, administration, and support of the TOE.	OE.NO_GENERAL_PURPOSE satisfies the assumption by ensuring there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the Linux OS (where the TOE is installed), other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	OE.PHYSICAL	OE.PHYSICAL satisfies the

Assumptions	Objectives	Rationale
The TOE environment will provide physical security commensurate with the value of the TOE and the data it contains.	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the TOE environment.	assumption that the TOE environment provides protection from unauthorized modification.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.	OE.PROTECT satisfies the assumption that the TOE environment provides protection from unauthorized modification.
A.TIMESTAMPS The TOE environment will provide the TOE with the necessary reliable timestamps.	OE.TIMESTAMPS The operational environment will provide reliable time stamps.	OE.TIME_STAMPS satisfies this assumption by stating that the environment will maintain reliable timestamps and those will be used by the TOE to stamp each audit record with a date and time.
A.XML_CONFIGURATION The TOE environment is assumed to provide protection for the administration of TOE's XML configuration files by unauthorized users.	OE.XML_CONFIGURATION The TOE environment will provide all the functions and facilities necessary to support administrators responsible for management and configuration of the TOE's XML files, and the TOE environment will restrict these functions and facilities from unauthorized users.	OE.XML_CONFIGURATION satisfies this assumption by stating that the TOE environment will provide all the necessary functions and facilities to support authorised administrators responsible for the configuration and management of the TOE's XML files.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

No extended security functional requirements have been defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended security functional requirements have been defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 below shows a mapping of the objectives and the SFRs that support them.

Table 17 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must prevent unauthenticated users from accessing configuration data and resources that require authentication.	FDP_ACC.1(a) Subset access control - HTTP	The TOE is required to enforce an HTTP Access Control SFP on a list of subjects acting on the behalf of users attempting to gain access to a list of named objects. All the operations between subjects and objects covered are defined by the TOE's Access Control SFP.
	FDP_ACC.1(b) Subset access control - JMX	The TOE is required to enforce a JMX Access Control SFP on a list of subjects acting on the behalf of users attempting to gain access to a list of named objects. All the operations between subjects and objects covered are defined by the TOE's Access Control SFP.
	FDP_ACC.1(c) Subset access control - AJP	The TOE is required to enforce an AJP Access Control SFP on a list of subjects acting on the behalf of users attempting to gain access to a list of named objects. All the operations between subjects and objects covered are defined by the TOE's Access Control SFP.
	FDP_ACF.1(a) Security attribute based access control - HTTP	The TOE is required to enforce the Access Control SFP on objects based on the security attributes defined in this SFR.
	FDP_ACF.1(b) Security attribute based access control - JMX	The TOE is required to enforce the Access Control SFP on objects based on the security attributes defined in this SFR.
	FDP_ACF.1(c) Security attribute based access control - AJP	The TOE is required to enforce the Access Control SFP on objects based on the security attributes defined in this SFR.
	FIA_ATD.1 User attribute definition	The TOE is required to maintain a list of the security attributes of subjects used to enforce the Access Control SFP of the TOE.
	FIA_USB.1 User-subject binding	The TOE is required to ensure that all subjects that act on behalf

Objective	Requirements Addressing the Objective	Rationale
		of users will have a binding that associates the subjects with a user uniquely.
	FTA_SSL.3 TSF initiated termination	The TOE is required to protect TSF data by ensuring that unauthorised users do not gain access to the TOE through an unattended session.
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	FAU_GEN.1 Audit data generation	The TOE is required to record audit events as defined in this SFR. This requirement ensures that the administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event.
	FIA_USB.1 User-subject binding	The TOE is required to ensure that all subjects that act on behalf of users have a binding that associates the subjects with a user. This is necessary to be able to associate audit records with user identities.
O.AUTHENTICATE The TOE must require identification and authentication before any access to the JMX Socket Listener is granted and if a resource data request matches an HTTP or AJP access control SFP rule which requires identification and authentication.	FIA_ATD.1 User attribute definition	The TOE is required to maintain a list of the security attributes of subjects used to enforce the authentication policy of the TOE.
	FIA_UAU.1 Timing of authentication	The TOE is required to authenticate users requesting access to TSF data before any actions may be taken on the behalf of that user.
	FIA_UAU.5 Multiple authentication mechanism	The TOE is required to authentication users requesting access to TSF data before any actions may be taken on the behalf of that user. There are multiple mechanisms supported as specified in this SFR.
	FIA_UAU.7 Protected authentication feedback	The TOE is required to obscure the feedback of passwords entered by users of the TOE during authentication.
	FIA_UID.1 Timing of Identification	The TOE is required to identify all users requesting access to TSF

Objective	Requirements Addressing the Objective	Rationale
		data before the user may perform any actions on TSF data.
	FIA_USB.1 User-subject binding	The TOE is required to ensure that all subjects that act on behalf of users have a binding that associates the subjects with a user uniquely.
O.LOCKOUT The TOE must protect user passwords from being obtained through brute-force attack methods through account lockout thresholds.	FIA_AFL.1 Authentication failure handling	The TOE is required to protect TSF data from unauthorized access. After an administrator configurable number of failed attempts, the TOE will lock a user account for a configurable amount of time.
O.MANAGE The TOE must provide all the functions and facilities necessary to support the authorized administrator in management of the security attributes as discussed in FMT_MSA.1, and restrict these functions and facilities from unauthorized use.	FMT_MSA.1 Management of security attributes	The TOE requires that the ability to perform operations on security attributes is restricted to particular roles.
	FMT_MSA.3 Static attribute initialisation - JMX	The TOE requires restrictive values for security attributes.
	FMT_SMF.1(a) Specification of management functions - JMX	The TOE is required to include administrative functions over the JMX interface to facilitate the management of security attributes.
	FMT_SMF.1(b) Specification of management functions - XML	The TOE is required to include administrative functions by editing the configuration files of the TOE using a Linux Text editor to facilitate the management of security attributes.
	FMT_SMR.1 Security roles	The TOE is required to provide access to TSF management functions and data based on the roles assigned to users during authentication.
O.PROTECT The TOE must protect the TSF in the event of failure of a single TOE instance in a clustered node configuration.	FPT_FLS.1 Failure with preservation of a secure state	The TOE is required to protect TSF data in the event of a failure.
O.QUOTA The TOE shall prevent resource exhaustion attacks through the use of maximum connection quotas.	FRU_RSA.1 Maximum quotas	The TOE is required to enforce a maximum quota on the number of active simultaneous connections to the TOE to protect the TOE from resource exhaustion attacks.

Objective	Requirements Addressing the Objective	Rationale
O.REPLICATION The TOE must export user session data to other TOE instances whenever a session changes. This guarantees data consistency between the TOE instances.	FPT_ITA.1 Inter-TSF availability within a defined availability metric	The TOE is required to automatically replicate session data every time the session is updated.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.3 was chosen to give greater assurance of the developer's on-going flaw remediation processes, including flaw reporting procedures.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 18 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 18 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included because time stamps are provided by the TOE environment. An environmental objective states that the TOE will receive reliable time stamps.
FDP_ACC.1(a)	FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FDP_ACC.1(c)	FDP_ACF.1(c)	✓	
FDP_ACF.1(a)	FDP_ACC.1(a)	✓	
	FMT_MSA.3	No	FMT_MSA.3 is not included with respect to the HTTP Connector interface because the

SFR ID	Dependencies	Dependency Met	Rationale
			management of the subject's security attributes (as used in the HTTP Access Control SFP) cannot take place over the HTTP interface and must be done via the TOE environment or via the JMX Socket Listener Interface.
FDP_ACF.1(b)	FDP_ACC.1(b)	✓	
	FMT_MSA.3	✓	
FDP_ACF.1(c)	FMT_MSA.3	✓	FMT_MSA.3 is not included with respect to the AJP Connector interface because the management of the subject's security attributes (as used in the AJP Access Control SFP) cannot take place over the AJP Connector interface and must be done via the TOE environment or via the JMX Socket Listener Interface.
FIA_AFL.1	FIA_UAU.1	✓	
FIA_ATD.1	None	N/A	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.5	None	N/A	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.1	None	N/A	
FIA_USB.1	FIA_ATD.1	✓	
FMT_MSA.1	FDP_ACC.1(b)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1(a)	None	N/A	
FMT_SMF.1(b)	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FPT_FLS.1	None	N/A	
FPT_ITA.1	None	N/A	
FRU_RSA.1	None	N/A	
FTA_SSL.3	None	N/A	

9 Acronyms and Terms

Table 19 and Table 20 below define the acronyms and terms used throughout this document.

9.1 Acronyms

Table 19 Acronyms

Acronym	Definition
AJP	Apache JServ Protocol
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
JEE	Java Enterprise Edition
JMX	Java Management eXtensions
JVM	Java Virtual Machine
OS	Operating System
PP	Protection Profile
RHEL	RedHat Enterprise Linux
RMI	Remote Method Invocation
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
URL	Uniform Resource Locator

Table 20 defines the terms used in this document.

Table 20 Terms

Term	Definition
auth-constraint	This is a sub-element of the <security-constraint>. This element determines what roles are allowed access to the stored resource at the specified URL
CONFIDENTIAL	This application requires the data to be transmitted in a fashion that prevents other entities from observing the contents of the transmissions. In most cases, the presence of CONFIDENTIAL indicates that the use of SSL is required.
http-method	This element is found in the web application's *web.xml* file. This is a sub-element of the <web-resource-collection>. This element defines what HTTP operations are on the resource URLs as defined by the <url-pattern> and what roles may invoke these operations based on the <auth-constraint>.
INTEGRAL	This application requires that the data be sent between the client and server to be sent in such a way that it can't be modified in transit. In most cases, the presence of INTEGRAL indicates that the use of SSL is required.
NONE	This application does not require any transport guarantees.
security-constraint	This element, located in the web application's *web.xml* file, is a declarative way to annotate the intended protection of Web content. A security-constraint consists of a web-resource-collection, an <auth-constraint>, and a <user-data-constraint>.
user-data-constraint	This element is found in the web application's *web.xml* file. This is a sub element of the security-constraint. This element determines what guarantees are applied to transmissions between the server and client: NONE, INTEGRAL, or CONFIDENTIAL.
url-pattern	This element is found in the web application's *web.xml* file. This is a sub element of the <web-resource-collection>. This element defines what resource data URLs will be governed by the <security-constraint>.
web-resource-collection	This element is found in the web application's *web.xml* file. This is a sub element of the security-constraint. This element defines what resources will be protected by Access Control SFPs and what methods will be allowed for these resources. This element contains <url-pattern>s and <http-methods>s as its sub elements.

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com