Marimba Desktop/Mobile Management and Server Change Management Security Target

Version 2.0

26 May 2005

Prepared for:
BMC Software, Inc.
440 Clyde Ave.
Mt. View, CA 94043

Prepared by:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Security Target Introduction

BMC Software provides a family of Desktop/Mobile Management (DMM) and Server Change Management (SCM) products, which provide change and configuration management services for client and server devices.

The Desktop/Mobile Management (DMM) and Server Change Management (SCM) products (collectively known as marimba's change and configuration products) are capable of deploying and maintaining a wide variety of information, called packages, whether it is individual files or documents, entire software suites, JAVA applications, or web sites.

BMC's change and configuration products for both desktop and server management are packaged as a single suite with common components.

This section identifies the Security Target (ST) and Target of Evaluation (TOE), specifies ST conventions and conformance claims, and describes how the ST is organized.

1.1 Security Target, TOE and CC Identification

ST Title – Marimba Desktop/Mobile Management and Server Change Management Security Target

ST Version – Version 1.17

ST Date – 1 February 2005

TOE Identification – The TOE is composed of the following product modules:

Marimba Infrastructure 6.0.2.1

Marimba Policy Manager 6.0.2

Marimba Deployment Manager 6.0.2

Collectively known as "Marimba Control Center by BMC Software"

Evaluation Assurance Level (EAL) – EAL 3

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.
    - Part 3 Conformant
    - Evaluation Assurance Level 3 (EAL3)

1.3 Conventions

The following conventions have been applied in this document:

- All requirements in this ST are reproduced relative to the requirements defined in CC v2.1.
- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once, with varying operations. In the ST, iteration is indicated by a letter in parenthesis, placed at the end of the component. For example, FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement: a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using underlined text and surrounded by brackets (e.g., [selection]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").

Other sections of the ST use bolding and italics to highlight text of special interest, such as captions.

1.4 Security Target Organization

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description: This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – Security Environment: This section details the expectations of the environment, the threats that are countered by DMM/SCM and it environment and the organizational policy that the DMM/SCM must fulfill.
- Section 4 – Security Objectives: This section details the security objectives of the DMM/SCM and its environment.
- Section 5 – IT Security Requirements: This section presents the security functional requirements (SFR) for DMM/SCM and IT Environment that supports the TOE, and details the requirements for EAL3.
- Section 6 – TOE Summary Specification: This section describes the security functions represented in the DMM/SCM that satisfy the security requirements.
- Section 7 – Protection Profile Claims: This section identifies a Protection Profile in which conformance is being claimed.
- Section 8 – Rationale: This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness and suitability.

2. TOE Description

The Desktop/Mobile Management (DMM) and Server Change Management (SCM) products are software change management packages produced by BMC Software, Inc., 440 Clyde Ave., Mt. View, CA 94043, herein called simply DMM/SCM. The SCM software is designed for use with groups of servers, while the DMM software is designed for use with groups of desktop machines. For the evaluated configuration, both products must be installed and configured.

The DMM/SCM allows administrators to perform change management of software packages across an enterprise. For example, they can package applications and application updates to automate their distribution. DMM/SCM also allows administrators to perform OS migration and perform hardware and software inventories of connected machines.

Due to its development in Java, DMM/SCM products are capable of managing these packages from a single location in a heterogeneous environment, including Windows and Solaris platforms.

2.1 Product Type

The Marimba Desktop/Mobile Management (DMM) and Server Change Management (SCM) (DMM/SCM) products are a collection of Java-based applications that distribute and maintain software applications and content within a company or across the Internet. For instance, the DMM/SCM products centralize and automate change management and configuration management tasks such as Operating System migration, software updates (such as OS patches or anti-virus software updates), and IT inventory management.

2.2 Product Description

The TOE includes modules that make up the Marimba Desktop/Mobile Management (DMM) and Server Change Management (SCM) software products. Both products rely on a pair of applications called the Tuner and the Transmitter, which serves channels (applications or files) over a network. The majority of software components are identical between the DMM and SCM products.

The Tuner component serves two purposes: Firstly, the Tuner provides a Java execution environment for running all other Marimba products. The main service the Tuner provides, in addition to a Java Virtual Machine, is updating capabilities for all application running in the Tuner environment. These applications can be both Marimba products, and third party packaged application such as Microsoft Office XP. Due to the updating services provided, the tuner is present on managed client endpoints, in addition to the server and administration computers.

The Transmitter operates as a data server, providing the content for updated and distributed software packages. Since the Transmitter is a Marimba Java based product, it also runs in the Tuner environment. This can sometimes be confusing, since the Tuner operates both as the client component, and as the Java environment for the Server component.

Both products are capable of gathering and generating reports of inventory data (for example, operating system versions) on enterprises' connected machines and packaging applications for distribution across a network. The products also contain software APIs for developers to use for integration with custom third-party applications.

The Desktop/Mobile Management product also allows administrators to define "subscription policies," which allow different applications to be distributed, based on the identities of users and their group memberships

The Common Management Services (CMS) is a part of the DMM architecture that provides a Servlet/JSP-based application server, on top of which Marimba applications are run. CMS also provides centralized services such as database and LDAP connection pooling and user role support.

2.3 Product Features

The TOE implements the following features:

- Events within the Transmitter are logged, including security events. Audit records include the name of the user associated with the event, a description of the event, and the date and time of the event. Authorized administrators may view DMM/SCM audit logs using the Report Center component.
- Access to the various channels is controlled by the identity of the user and/or group membership and the access control attributes associated with the named object. Channel based access control is implemented by the Transmitter component.
- DMM/SCM provides user identification mechanisms for all administrative applications. In DMM, the user is authenticated against an external user database such as LDAP. The LDAP server is external to the TOE. In SCM, the administrative user is authenticated against a user database, which is part of the TOE.

2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

2.4.1 Physical Boundaries

The TOE is a suite of software applications operating on server and client machines. The supported hardware and operating system platforms include Windows and Solaris platforms. The physical boundary for each component of the TOE is the environment that each component requires for effective operation. The operating system, external Relational Database Management System (RDBMS), Light-weight Directory Access Protocol (LDAP), and NT Domain controller, and hardware are included by assumption and are not part of the TOE. Following is a description of the components that comprise the TOE.

The DMM components include the Tuner, the Transmitter, the Infrastructure Administrator, Subscription Policy Manager and the Report Center. These components are described below:

- The Tuner component is the application in which users subscribe to channels that have been published on the Transmitter component. The Tuner downloads the channel files or the updates to the channel files, to the user's workstation. In addition, the Tuner provides a Java execution environment for running all other Marimba products, including the Transmitter. For that reason the Tuner is present on all computers running the Marimba software, i.e. client endpoints, servers, and administrative computers. Figure 1, shows the Tuner running on all four computer systems, and providing application change management to the computer designated as the "Client Computer".
- The Transmitter component is a server that delivers channels to its clients' Tuners. The Transmitter itself runs in the Tuner environment, and operates as the server in the DMM distributed environment. The Transmitter is running on the computer designated as "Server Components" in Figure 1, and is providing application change management services to the "Client Computer".
- The Infrastructure Administrator (contained in the CMS) provides the administrator with the ability to install, configure, and manage the components of the TOE. They are shown in Figure 1 running on the computer designated as the "Administrator's Workstation".
- Subscription Policy Manager (contained in the CMS) is the application for assigning channels and otherwise managing the subscription capabilities.
- The Report Center (contained in the CMS) provides the interface for scheduling data collection and otherwise administering the inventory process, as well as searching the collected data for specific information and reporting the results. Since this tool is used by administrators, it is shown in Figure 1, running on the computer designated as the "Administrator's Workstation".

The TOE is comprised of the following product modules, which each contain external interfaces that are applicable to DMM, SCM or both, as indicated in the following table:

Module Name	Channel Name	Product Category
Marimba Infrastructure	Channel Manager	DMM/SCM
	Infrastructure Administration	DMM/SCM
	Console Window	DMM/SCM
	Help Channel	DMM/SCM
	License Installer	DMM/SCM
	Infrastructure Service	DMM/SCM
	Schema Manager	DMM/SCM
	Certificate Manager	DMM/SCM
	Channel Copier	DMM/SCM
	Publisher	DMM/SCM

	Transmitter	DMM/SCM
	Proxy	DMM/SCM
	Browser Integration Module	DMM/SCM
	Subnet Repeater Policy	DMM/SCM
	Logging Service	DMM/SCM
	Inventory Service	DMM/SCM
	NT Domain Authenticator	DMM/SCM
	Report Center	DMM/SCM
	Common Management Services	DMM/SCM
Policy Manager	Subscription Policy Manager	DMM
	Subscription Policy Service	DMM
	Subscription Reporter	DMM
Deployment Manager	Deployment Manager	SCM
	Deployment Service	SCM
	Deployment Manager Command Line	SCM

The following diagram depicts the DMM component boundaries. The evaluated configuration shows the Marimba DMM products distributed amongst four computers. The RDBMS and LDAP server are not part of the TOE, but are part of the environment required to operate the products.

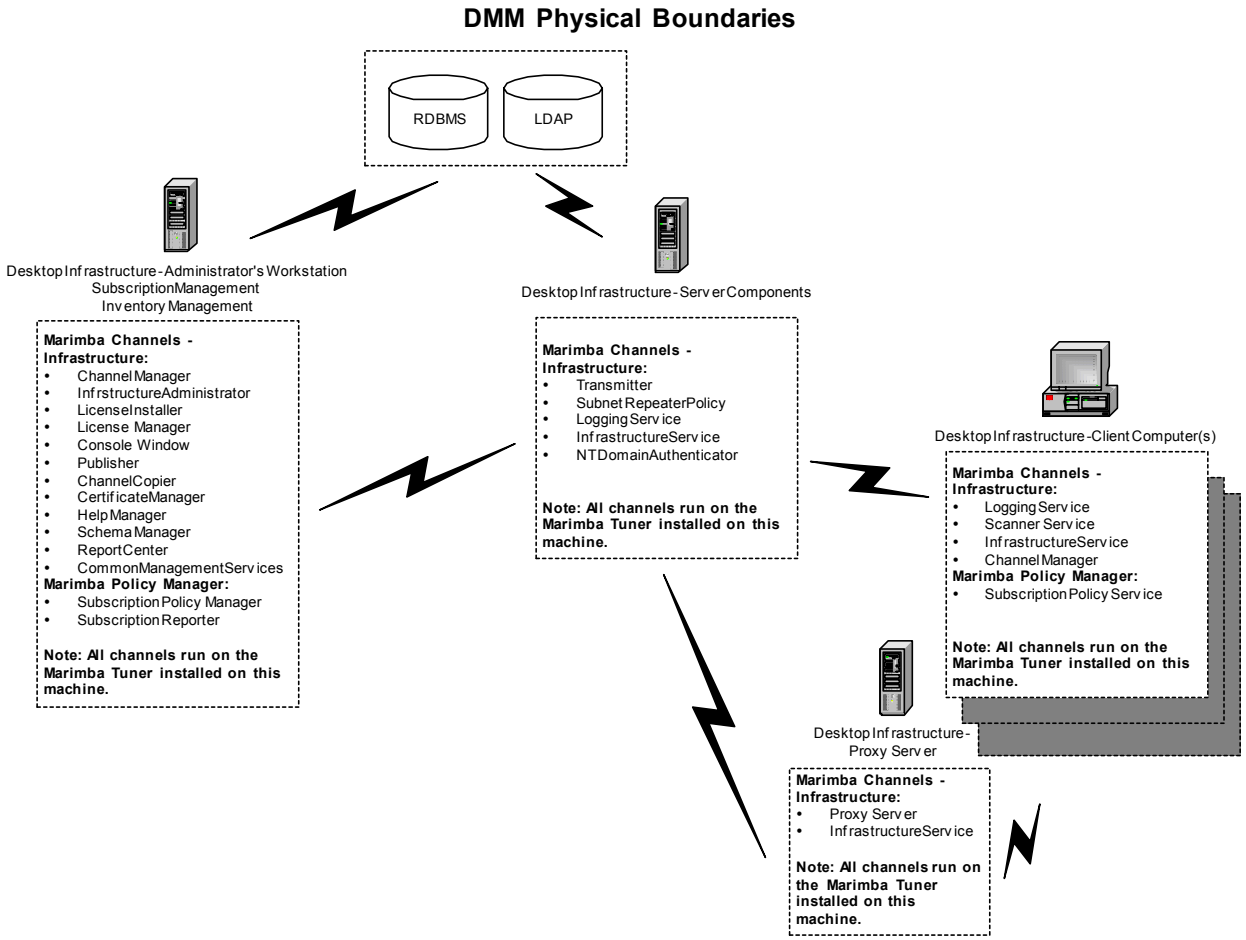

Figure 1: DMM Physical Boundaries

The SCM components are the Tuner, the Transmitter, the Infrastructure Administrator, the Deployment Manager/Service, and the Content Replicator. These components are described below:

- The Tuner component is the application in which users subscribe to channels that have been published on the Transmitter component. The Tuner downloads the channel files or the updates to the channel files, to the managed server endpoint. In addition, the Tuner provides a Java execution environment for running all other Marimba products, including the Transmitter. For that reason the Tuner is present of all computers running the Marimba software, i.e. managed server endpoints, servers and administrative computers. Figure 1 shows the Tuner running on all five computer systems and providing application change management to the computer designated as the "Managed Server Endpoint".
- The Transmitter component is a server that delivers channels to its clients' Tuners. The Transmitter itself runs in the Tuner environment, and operates as the server in the SCM distributed environment. The Transmitter is running on the computer designated as "Server Components" in Figure 1, and is providing application change management services to the "Managed Server Endpoint".
- The Infrastructure Administrator (contained in the CMS) provide the administrator with the utilities to install, configure, and manage the components of the TOE. They are shown in Figure 1 running on the computer designated as the "Administrator's Workstation".

- The Deployment Manager component of Server Management provides centralized control and monitoring of content distribution. Since this tool is used by administrators, it is shown in Figure 1, running on the computer designated as the "Administrator's Workstation".
- The Content Replicator component (Content Distribution module) performs the tasks of installing data and content on managed server endpoints, and rolling back installations. Deployment Manager is used to run Content Replicator remotely. Since the Content Replicator component is used to manage the endpoint, it is shown running on the computer designated as the "Managed Server Endpoint" in Figure 1.

The following diagram depicts the SCM component boundaries. The evaluated configuration shows the marimba SCM products distributed amongst five computers. The RDBMS and LDAP server are not part of the TOE, but are part of the environment required to operate the products.

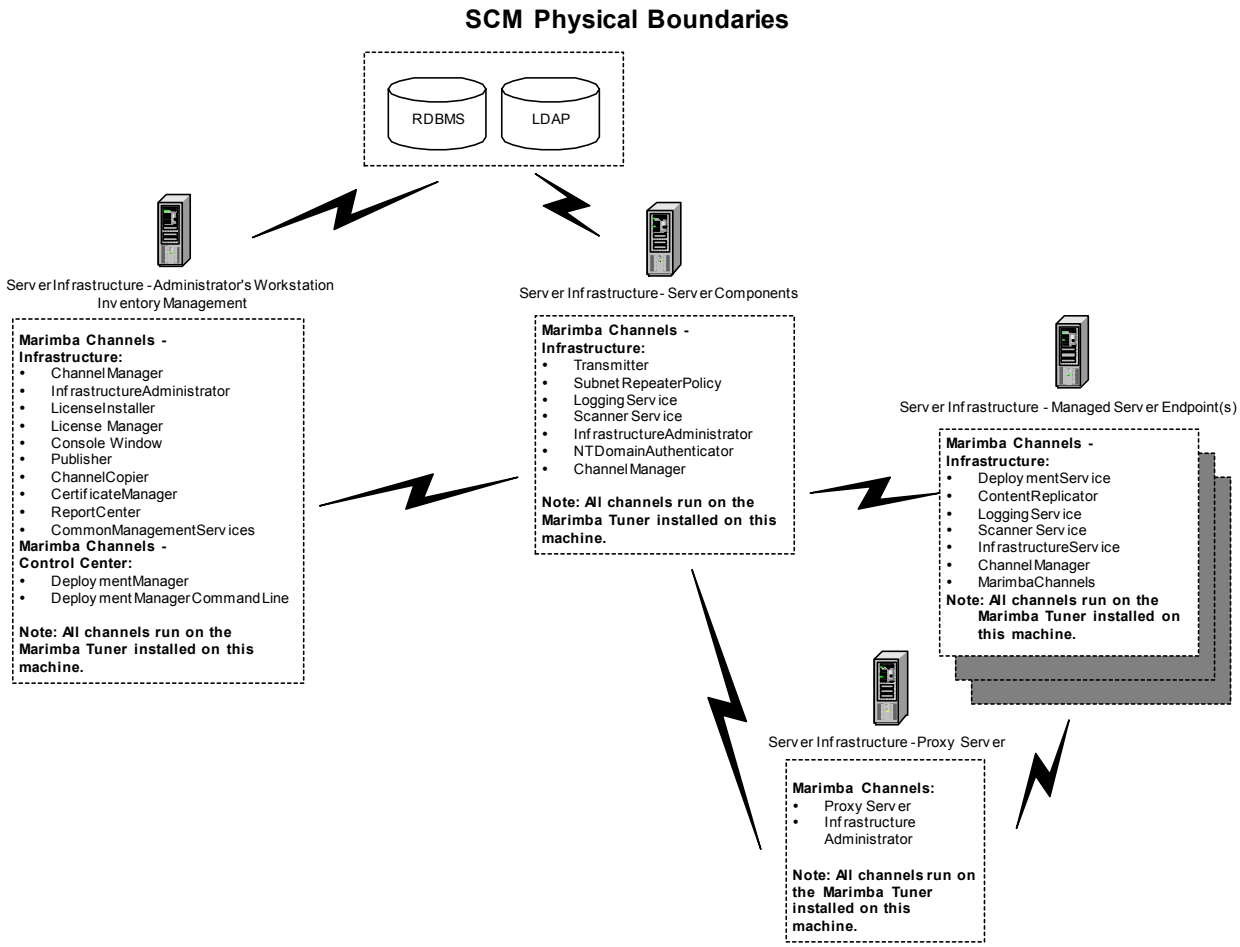

Figure 2: SCM Physical Boundaries

2.4.2 Logical Boundaries

The logical boundaries of the TOE include the functions of the TOE interfaces. These functions include audit, user data protection, identification and authentication, and the management of the security configurations.

2.4.2.1 Security Audit

DMM/SCM audits the actions that occur on the Transmitter. The log files contain information about events such as starting the Transmitter and modifying access control attributes associated to channels, as well as any problems associated with those events.

2.4.2.2 User Data Protection

DMM/SCM access privileges for the user, hence, access to the various channels and other named objects are controlled by the combination of user and group identification and the access control attributes associated to the named objects.

2.4.2.3 Identification and Authentication

The DMM/SCM requires users to be identified and authenticated before they can access the TOE and the TOE security-relevant data.

2.4.2.4 Security Management

The TOE provides a number of interfaces to manage the configuration and implementation of the policy enforced by the TOE. Security management includes managing the following items: access control of channels and configuring termination of inactive sessions.

2.4.2.5 TOE Access

The CMS component monitors an established session for activity and if the session is inactive for the specified time period, the CMS will terminate the session.

3. Security Environment

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

The statement of TOE security environment defines the following:

- Threats that the product is designed to counter
- Organizational security policies with which the product is designed to comply
- Assumptions made on the operational environment and the method of use intended for the product.

The TOE, DMM/SCM, has been developed for an operating environment with a low level of risk to identified assets. The assurance requirements of EAL 3 and the minimum strength of function of SOF-basic were chosen to be consistent with that level of risk.

3.1 Threats to Security

T.ACCESS	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.AUDIT_CORRUPT	Unauthorized users may tamper with audit data by gaining unauthorized access to the audit trail.
T. PRIVILEGE	An authorized user of the TOE may gain access to a resource or channel without having permission.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to DMM/SCM.

P.ACCOUNTABILITY	The Administrator of the system shall be held accountable for their security relevant actions within the system.
P.MANAGE	The system must provide authorized administrators with utilities to effectively manage the security functions of the TOE.

3.3 Secure Usage Assumptions

This section describes the security aspects of the environment in which the TOE will be utilized. This includes information about the physical, personnel, and system aspects of the environment.

3.3.1 Physical Assumptions

A.CONNECT Any network resources used for communication between TOE components will be adequately protected from unauthorized access.

A.PROTECT The components of TOE hardware and software critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

3.3.2 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

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

3.3.3 System Assumptions

A.HARDWARE The TOE will be installed on a hardware system that meets or exceeds the following constraints:

DMM:

- Windows:
  - Pentium 133 MHz minimum, 266 MHz or higher recommended. Windows NT 4.0 (SP6a or higher), Windows 2000, and Windows XP for managed desktop endpoints.
  - Pentium 400 MHz minimum, 750 MHz or higher recommended. Windows NT 4.0 or Windows 2000 for the Marimba Infrastructure and Policy Manager server-side components.
- Solaris: (for all DMM components)
  - SPARC Netra T1 266Mhz or higher
  - Solaris 8 or 9
    - Common Desktop Environment (CDE)

SCM:

- Windows:
  - Windows operating system:
    - Pentium 133 MHz minimum, 266 MHz or higher recommended. Windows NT 4.0 (SP6a or higher), Windows 2000, and Windows XP for managed server endpoints.
    - Pentium 400 MHz minimum, 750 MHz or higher recommended. Windows NT 4.0 or Windows 2000 for the Marimba Infrastructure and Deployment Manager server-side components
- Solaris: (for all SCM components)
  - SPARC Netra T1 266Mhz or higher
  - Solaris 8 or 9
    - Common Desktop Environment

A.IDENT The operating environment will provide a method of identification and authentication.

A.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.
A.SYSPROTECT	The operating environment will provide protection to the TOE and its related data.
A.TIME	The operating environment will provide reliable system time.

4. Security Objectives

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

4.1 IT Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

O.AUTHORIZATION	The TSF must ensure that only authorized users gain access to the TOE and its resources.
O.OBJ_ACCESS	The TSF must limit access to named objects maintained by the TOE to users with authorization and appropriate privileges. The TSF must allow authorized users to specify which users may access their objects and the actions performed on the objects.
O.AUDIT	The TOE must record security-relevant events, associate these events with users, dates and times, and make audit information available to authorized administrators.
O.MANAGE	The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

4.2 IT Security Objectives for the Environment

The following security objectives for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

OE.AUTH_ACCESS	The TOE operating environment must ensure that only authorized users gain access to the TOE.
OE.SEP	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.
OE.TIME_SOURCE	The IT environment for the TOE must provide a reliable time source for the TOE to generate accurate timestamps for audit records.

4.3 Security Objectives of the Non-IT Environment

The following security objectives are intended to be satisfied by the environment of the TOE.

OE.HARDWARE	The TOE will be installed on a hardware system that meets or exceeds the following constraints:

DMM:

- Windows:

- Pentium 133 MHz minimum, 266 MHz or higher recommended. Windows NT 4.0 (SP6a or higher), Windows 2000, and Windows XP for managed desktop endpoints.
- Pentium 400 MHz minimum, 750 MHz or higher recommended. Windows NT 4.0 or Windows 2000 for the Marimba Infrastructure and Policy Manager server-side components.

- Solaris: (for all DMM components)
  - SPARC Netra T1 266Mhz or higher
  - Solaris 8 or 9
    - Common Desktop Environment (CDE)

SCM:

- Windows:
  - Windows operating system:
    - Pentium 133 MHz minimum, 266 MHz or higher recommended. Windows NT 4.0 (SP6a or higher), Windows 2000, and Windows XP for managed server endpoints.
    - Pentium 400 MHz minimum, 750 MHz or higher recommended. Windows NT 4.0 or Windows 2000 for the Marimba Infrastructure and Deployment Manager server-side components.
- Solaris: (for all SCM components)
  - SPARC Netra T1 266Mhz or higher
  - Solaris 8 or 9
    - Common Desktop Environment

OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.
OE.PERSON	Authorized Administrators of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided. These users are not careless, negligent, or hostile.
OE.PHYCAL	Those responsible for the TOE must ensure that the parts of the TOE critical to security policy are protected from physical attack that might compromise the TOE security objectives.

5. IT Security Requirements

This section of the ST details the security functional requirements (SFR) for the TOE and the IT Environment that will support the TOE. The SFR were drawn from the CC Part 2.

CC defined operations for assignment, iteration, selection, and refinement were used to tailor the requirements to the level of detail necessary to meet the stated security objectives. Refer to Conventions section for the format definition. Each SFR was also changed, when necessary, to conform to International Interpretations.

5.1 TOE Security Functional Requirements

Security Functional Class	Security Functional Components
Security audit (FAU)	Audit data generation (FAU_GEN.1)
	User identity association (FAU_GEN.2)
	Audit review (FAU_SAR.1)
	Selective audit (FAU_SEL.1)
User data protection (FDP)	Subset access control (FDP_ACC.1)

Security Functional Class	Security Functional Components
	Security attribute based access control (FDP_ACF.1)
Identification and authentication (FAI)	User attribute definition (FIA_ATD.1)
	User authentication before any action (FIA_UAU.2)
	User identification before any action (FIA_UID.2)
Security management (FMT)	Management of security attributes (Named objects, except channels and policy manager targets) (FMT_MSA.1(a))
	Management of security attributes (Channels) (FMT_MSA.1(b))
	Management of security attributes (Policy manager targets) (FMT_MSA.1(c)))
	Static attribute initialization (FMT_MSA.3)
	Management of TSF data (Audit) (FMT_MTD.1(a))
	Management of TSF data (Access Control) (FMT_MTD.1(b))
	Specification of management functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
TOE access (FTA)	TSF-initiated termination (FTA_SSL.3)

Table 1: Security Functional Components

5.1.1 Security Audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

5.1.1.1.1 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) [**Auditable events in Table 2 below.**].

Component	Auditable Event
FMT_MSA.1(b)	Use of the functions listed in this requirement

Table 2: Auditable Events

5.1.1.1.2 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

a) b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**object identity (channel),** and **severity**].

5.1.1.2 User identity association (FAU_GEN.2)

5.1.1.2.1 FAU_GEN.2.1

The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 Audit review (FAU_SAR.1)

5.1.1.3.1 FAU_SAR.1.1

The TSF shall provide [**Primary Administrator, Administrator, Operator**] with the capability to read [**all audit trail data**] from the audit records.

5.1.1.3.2 FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.4 FAU_SEL.1 Selective audit (FAU_SEL.1)

5.1.1.4.1 FAU_SEL.1.1

The TSF shall be able to include or exclude auditable events **as instructed by a Primary Administrator, Administrator, or Operator** from the set of audited events, based on the following attributes:

b) [event type]
c) [**severity and event type ranges**].

5.1.2 User Data Protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

5.1.2.1.1 FDP_ACC.1.1

The TSF shall enforce the [**Access Control SFP**] on [**subject: users and process acting on behalf of the user, objects: named objects; Transmitter folders, Deployment Manager Folders, deployments, task groups, server groups, server keychains, channels, policy manager targets and all operations, except read, using the command line interface].**

5.1.2.2 Security attribute based access control (FDP_ACF.1)

5.1.2.2.1 FDP_ACF.1.1

The TSF shall enforce the [**Transmitter access control, Deployment Manager access control and create permissions, and Policy Manager access control**] to objects based on [

- **Transmitter access control for read, write and delete operations on Channel and Transmitter Folder named objects. Access is controlled by an ACL containing a single attribute, that can have the following values:**
  - **A user (not specified) authenticated by an external source.**
  - **A specific user authenticated by an external source.**
  - **A group, of which only authenticated members have access.**
- **Deployment Manager access control for Deployment Manager Folders, Deployments, Server Groups, Server Keychains, Task Group named objects. Each of these named objects maintains an ACL containing the following attributes:**
  - **A user or group name.**
  - **Four boolean permission bits representing Read (r), Write (w), Execute (x) and Owner (o), associated with each user or group.**
- **Deployment Manager create permissions for Deployment Manager Folders, Deployments, Server Groups, Server Keychains, Task Group named objects. Each user and group managed by the Deployment Manager has a series of attributes with the following values associated with it:**
  - **Five create attributes, one each for: Deployment Manager Folders, Deployments, Server Groups, Server Keychains, Task Groups.**
  - **Each of these attributes can have three possible values: None, Create, Revoke.**
- **Policy Manager access control for Policy Manager Targets. Each user or group of users (stored and authenticated by an external source) has an ACL associated with it, containing the following attributes:**

- **One or more Policy Manager Targets**
- **Four Boolean permission bits associated with each Policy Manager Target for the following permissions: ACL read, ACL write, subscription policy read, subscription policy write.]**

5.1.2.2.2 FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed**:** [

- **Named object access is allowed if at least one of the following conditions is true:**
  - **an ACL entry explicitly grants access to a user**
  - **an ACL entry explicitly grants access to a group of which the subject is a member**
  - **the subject is the object owner (folders, keychains, task groups, server groups, and deployments)**].

5.1.2.2.3 FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**Only a Primary Administrator or Administrator can delete a channel**].

5.1.2.2.4 FDP_ACF.1.4

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

5.1.3 Identification and Authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

5.1.3.1.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

- [**user identity**
- **group membership**
- **home (default) folder**
- **password (authentication data)**.
- **Create permissions (for folders, keychains, task groups, server groups, and deployments)].**

5.1.3.2 User authentication before any action (FIA_UAU.2)

5.1.3.2.1 FIA_UAU.2.1

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

5.1.3.3 User identification before any action (FIA_UID.2)

5.1.3.3.1 FIA_UID.2.1

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1(a))

5.1.4.1.1 FMT_MSA.1.1(a)

The TSF shall enforce the [**Access Control SFP**] to restrict the ability to [change_default, modify,] the security attributes [**access control attributes associated with a named object, except channels and policy manager targets, and create permissions associated with users**] to [**Deployment Manager Administrator and object owners**].

5.1.4.2 Management of security attributes (FMT_MSA.1(b))

5.1.4.2.1 FMT_MSA.1.1(b)

The TSF shall enforce the [Access Control SFP**] to restrict the ability to [change_default, modify, delete] the security attributes [**access control attributes associated with channels**] to [**Primary Administrator, Administrator**].**

5.1.4.3 Management of security attributes (FMT_MSA.1(c))

5.1.4.3.1 The TSF shall enforce the [Access Control SFP] to restrict the ability to [change default, modify, delete] the security attributes [access control attributes associated with policy manager targets] to [Primary Administrator, users with ACL write permissions]

5.1.4.4 Static attribute initialization (FMT_MSA.3)

5.1.4.4.1 FMT_MSA.3.1

The TSF shall enforce the [**Access Control SFP**] to provide [**permissive values for Transmitter Administration, restrictive values for Deployment Manager, restrictive values for Policy Manager**] default values for security attributes that are used to enforce the SFP.

5.1.4.4.2 FMT_MSA.3.2

The TSF shall allow the **[(a) Primary Administrator, or Administrator (channel objects), or (b)Deployment Manager Administrator or folder owner (folders, keychains, task groups, server groups, and deployments), or (c) Primary Administrator or users with ACL write permissions (policy manager targets)]** to specify alternative initial values to override the default values when an object or information is created.

5.1.4.5 Management of TSF data (FMT_MTD.1(a))

5.1.4.5.1 FMT_MTD.1.1(a)

The TSF shall restrict the ability to [**query**] the [**audit data]** to the **[the Primary Administrator, Administrator, Operator**].

5.1.4.6 Management of TSF data (FMT_MTD.1(b))

5.1.4.6.1 FMT_MTD.1.1(b)

The TSF shall restrict the ability to [**modify, delete, initialize**] [**user's security attributes**] to **[the Deployment Manager Administrator and users**[1]].

[1] **Users are only permitted to modify their own passwords.**

5.1.4.7 Specification of Management Functions (FMT_SMF.1)

5.1.4.7.1 FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:

- [**Management of access control to named objects**
- **Configure idle user timeout**].

5.1.4.8 Security roles (FMT_SMR.1)

5.1.4.8.1 FMT_SMR.1.1

The TSF shall maintain the roles:

- **[Deployment Manager - Deployment Manager Administrator, Regular User**
- **Transmitter component - Primary Administrator, Administrator**
- **CMS - Primary Administrator, Administrator, Operator**].

5.1.4.8.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.1.5 TOE access (FTA)

5.1.5.1 TSF-initiated termination (FTA_SSL.3)

5.1.5.1.1 FTA_SSL.3.1

The TSF shall terminate an interactive session after a [**a Deployment Manager Administrator or Primary Administrator specified time**].

5.2 Security Functional Requirements for the IT Environment

Security Functional Class	Security Functional Components
Identification and Authentication (FIA)	User attribute definition (FIA_ATD.1)
	User authentication before any action (FIA_UAU.2)
	User identification before any action (FIA_UID.2)
Protection of the TSF (FPT)	TSF domain separation (FPT_SEP.1)
	Reliable time stamp (FPT_STM.1)

Table 3: Security Functional Components for the Environment

5.2.1 Identification and Authentication (FIA)

5.2.1.1 User attribute definition (FIA_ATD.1)

5.2.1.1.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

- [**user identity**
- **group membership**
- **password (authentication data)**].

5.2.1.2 User authentication before any action (FIA_UAU.2)

5.2.1.2.1 FIA_UAU.2.1

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

5.2.1.3 User identification before any action (FIA_UID.2)

5.2.1.3.1 FIA_UID.2.1

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

5.2.2 Protection of the TSF (FPT)

5.2.2.1 TSF domain separation (FPT_SEP.1)

5.2.2.1.1 FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

5.2.2.1.2 FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2.2.2 Reliable time stamps (FPT_STM.1)

5.2.2.2.1 FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 3 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components

Assurance Class	Assurance Components
Configuration Management (ACM)	Authorization controls (ACM_CAP.3)
	TOE CM coverage (ACM_SCP.1)
Delivery and Operations (ADO)	Delivery procedures (ADO_DEL.1)
	Installation, generation, and start-up procedures (ADO_IGS.1)
Development (ADV)	Informal functional specification (ADV_FSP.1)
	Security enforcing high-level design (ADV_HLD.2)
	Informal correspondence demonstration (ADV_RCR.1)
Guidance Documents (AGD)	Administrator guidance (AGD_ADM.1)
	User guidance (AGD_USR.1)
Life Cycle Support (ALC)	Identification of security measures (ALC_DVS.1)
Tests (ATE)	Analysis of coverage (ATE_COV.2)
	Testing: high-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)

Assurance Class	Assurance Components
Vulnerability Assessment (AVA)	Examination of guidance (AVA_MSU.1)
	Strength of TOE security function evaluation (AVA_SOF.1)
	Developer vulnerability analysis (AVA_VLA.1)

Table 4: EAL3 Assurance Components

5.3.1 Configuration Management (ACM)

5.3.1.1 Authorization Controls (ACM_CAP.3)

5.3.1.1.1 ACM_CAP.3.1D

The developer shall provide a reference for the TOE.

5.3.1.1.2 ACM_CAP.3.2D

The developer shall use a CM system.

5.3.1.1.3 ACM_CAP.3.3D

The developer shall provide CM documentation.

5.3.1.1.4 ACM_CAP.3.1C

The reference for the TOE shall be unique to each version of the TOE.

5.3.1.1.5 ACM_CAP.3.2C

The TOE shall be labeled with its reference.

5.3.1.1.6 ACM_CAP.3.3C

The CM documentation shall include a configuration list and a CM plan.

5.3.1.1.7 ACM_CAP.3.RI3

The configuration list shall uniquely identify all configuration items that comprise the TOE.[2]

5.3.1.1.8 ACM_CAP.3.4C

The configuration list shall describe the configuration items that comprise the TOE.

5.3.1.1.9 ACM_CAP.3.5C

The CM documentation shall describe the method used to uniquely identify the configuration items.

5.3.1.1.10 ACM_CAP.3.6C

The CM system shall uniquely identify all configuration items.

5.3.1.1.11 ACM_CAP.3.7C

The CM plan shall describe how the CM system is used.

[2] This requirement element has been added to comply with International Interpretation RI #3.

5.3.1.1.12 ACM_CAP.3.8C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

5.3.1.1.13 ACM_CAP.3.9C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

5.3.1.1.14 ACM_CAP.3.10C

The CM system shall provide measures such that only authorized changes are made to the configuration items.

5.3.1.1.15 ACM_CAP.3.1E

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

5.3.1.2 TOE CM Coverage (ACM_SCP.1)

5.3.1.2.1 ACM_SCP.1.1D

~~The developer shall provide CM documentation~~ The developer shall provide a list of configuration items for the TOE.[3]

5.3.1.2.2 ACM_SCP.1.1C

~~The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.~~ **The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.[4]**

~~5.3.1.2.3 ACM_SCP.1.2C~~

~~The CM documentation shall describe how configuration items are tracked by the CM system.~~[5]

5.3.1.2.4 ACM_SCP.1.1E

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

5.3.2 Delivery and Operation (ADO)

5.3.2.1 Delivery Procedures (ADO_DEL.1)

5.3.2.1.1 ADO_DEL.1.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

5.3.2.1.2 ADO_DEL.1.2D

The developer shall use the delivery procedures.

[3] This requirement has been modified to comply with International Interpretation RI #4.
[4] This requirement has been modified to comply with International Interpretation RI #4.
[5] This requirement has been removed to comply with International Interpretation RI #4.

5.3.2.1.3 ADO_DEL.1.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

5.3.2.1.4 ADO_DEL.1.1E

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

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

5.3.2.2.1 ADO_IGS.1.1D

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

5.3.2.2.2 ADO_IGS.1.1C

The **installation, generation and start-up** documentation shall describe **all** the steps necessary for secure installation, generation, and start-up of the TOE.[6]

5.3.2.2.3 ADO_IGS.1.1E

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

5.3.2.2.4 ADO_IGS.1.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal Functional Specification (ADV_FSP.1)

5.3.3.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

5.3.3.1.2 ADV_FSP.1.1C

The functional specification shall describe the TSF and its external interfaces using an informal style.

5.3.3.1.3 ADV_FSP.1.2C

The functional specification shall be internally consistent.

5.3.3.1.4 ADV_FSP.1.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.1.5 ADV_FSP.1.4C

The functional specification shall completely represent the TSF.

[6] This requirement has been modified to comply with International Interpretation RI #51.

5.3.3.1.6 ADV_FSP.1.1E

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

5.3.3.1.7 ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

5.3.3.2.1 ADV_HLD.2.1D

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

5.3.3.2.2 ADV_HLD.2.1C

The presentation of the high-level design shall be informal.

5.3.3.2.3 ADV_HLD.2.2C

The high-level design shall be internally consistent.

5.3.3.2.4 ADV_HLD.2.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

5.3.3.2.5 ADV_HLD.2.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

5.3.3.2.6 ADV_HLD.2.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

5.3.3.2.7 ADV_HLD.2.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

5.3.3.2.8 ADV_HLD.2.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

5.3.3.2.9 ADV_HLD.2.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.2.10 ADV_HLD.2.9C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.3.3.2.11 ADV_HLD.2.1E

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

5.3.3.2.12 ADV_HLD.2.2E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

5.3.3.3.1 ADV_RCR.1.1D

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

5.3.3.3.2 ADV_RCR.1.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.3.3.3.3 ADV_RCR.1.1E

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

5.3.4 Guidance Documents (AGD)

5.3.4.1 Administrator Guidance (AGD_ADM.1)

5.3.4.1.1 AGD_ADM.1.1D

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

5.3.4.1.2 AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

5.3.4.1.3 AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

5.3.4.1.4 AGD_ADM.1.3C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

5.3.4.1.5 AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

5.3.4.1.6 AGD_ADM.1.5C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

5.3.4.1.7 AGD_ADM.1.6C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

5.3.4.1.8 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.3.4.1.10 AGD_ADM.1.1E

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

5.3.4.2 User Guidance (AGD_USR.1)

5.3.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

5.3.4.2.2 AGD_USR.1.1C

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

5.3.4.2.3 AGD_USR.1.2C

The user guidance shall describe the use of user-accessible security functions provided by the TOE.

5.3.4.2.4 AGD_USR.1.3C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

5.3.4.2.5 AGD_USR.1.4C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

5.3.4.2.6 AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.2.7 AGD_USR.1.6C

The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.3.4.2.8 AGD_USR.1.1E

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

5.3.5 Life Cycle Support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

5.3.5.1.1 ALC_DVS.1.1D

The developer shall produce development security documentation.

5.3.5.1.2 ALC_DVS.1.1C

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

5.3.5.1.3 ALC_DVS.1.2C

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.3.5.1.4 ALC_DVS.1.1E

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

5.3.5.1.5 ALC_DVS.1.2E

The evaluator shall confirm that the security measures are being applied.

5.3.6 Security Testing (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

5.3.6.1.1 ATE_COV.2.1D

The developer shall provide an analysis of the test coverage.

5.3.6.1.2 ATE_COV.2.1C

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

5.3.6.1.3 ATE_COV.2.2C

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.3.6.1.4 ATE_COV.2.1E

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

5.3.6.2 Testing: high-level design (ATE_DPT.1)

5.3.6.2.1 ATE_DPT.1.1D

The developer shall provide the analysis of the depth of testing.

5.3.6.2.2 ATE_DPT.1.1C

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

5.3.6.2.3 ATE_DPT.1.1E

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

5.3.6.3 Functional testing (ATE_FUN.1)

5.3.6.3.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

5.3.6.3.2 ATE_FUN.1.2D

The developer shall provide test documentation.

5.3.6.3.3 ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

5.3.6.3.4 ATE_FUN.1.2C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

5.3.6.3.5 ATE_FUN.1.3C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

5.3.6.3.6 ATE_FUN.1.4C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

5.3.6.3.7 ATE_FUN.1.5C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.3.6.3.8 ATE_FUN.1.1E

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

5.3.6.4 Independent testing – sample (ATE_IND.2)

5.3.6.4.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

5.3.6.4.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

5.3.6.4.3 ATE_IND.2.2C

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.3.6.4.4 ATE_IND.2.1E

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

5.3.6.4.5 ATE_IND.2.2E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

5.3.6.4.6 ATE_IND.2.3E

The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability Assessment (VLA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

5.3.7.1.1 AVA_MSU.1.1D

The developer shall provide guidance documentation.

5.3.7.1.2 AVA_MSU.1.1C

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

5.3.7.1.3 AVA_MSU.1.2C

The guidance documentation shall be complete, clear, consistent and reasonable.

5.3.7.1.4 AVA_MSU.1.3C

The guidance documentation shall list all assumptions about the intended environment.

5.3.7.1.5 AVA_MSU.1.4C

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

5.3.7.1.6 AVA_MSU.1.1E

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

5.3.7.1.7 AVA_MSU.1.2E

The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

5.3.7.1.8 AVA_MSU.1.3E

The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

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

5.3.7.2.1 AVA_SOF.1.1D

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

5.3.7.2.2 AVA_SOF.1.1C

For each mechanism with strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

5.3.7.2.3 AVA_SOF.1.2C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.3.7.2.4 AVA_SOF.1.1E

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

5.3.7.2.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

5.3.7.3.1 AVA_VLA.1.1D

~~The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.~~ **The developer shall perform a vulnerability analysis.**[7]

5.3.7.3.2 AVA_VLA.1.2D

~~The developer shall document the disposition of obvious vulnerabilities.~~ **The developer shall provide vulnerability analysis documentation.**[8]

5.3.7.3.3 AVA_VLA.1.1C

~~The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.~~ **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.**[9]

5.3.7.3.4 AVA_VLA.1.2C

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.[10]

5.3.7.3.5 AVA_VLA.1.3C

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. [11]

---

[7] This requirement has been modified to comply with International Interpretation RI #51.
[8] This requirement has been modified to comply with International Interpretation RI #51.
[9] This requirement has been modified to comply with International Interpretation RI #51.
[10] This requirement has been added to comply with International Interpretation RI #51.
[11] This requirement has been added to comply with International Interpretation RI #51.

5.3.7.3.6 AVA_VLA.1.1E

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

5.3.7.3.7 AVA_VLA.1.2E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by describing how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

All events, as identified in **Table 2: Auditable Events**, are logged by the Transmitter. Auditable security events include when the Transmitter is stopped and started. The audit records are stored both local to the Transmitter, on the file system of the computer running that component, and also in a central log repository; the external Relational Database Management System (RDBMS). The centralized logging component acts as a collection agent, collecting the Transmitter's audit logs and sending them to the repository. The centralized location allows the Primary Administrator, Administrator, or Operator access to review them using the Report Center interface, which is part of the Marimba Infrastructure component. This audit data is presented in such a manner that the Primary Administrator, Administrator, or Operator can read and interpret the content of the information; hence the information is presented in a manner suitable for human interpretation. Each audit record records the user that performed the action, as well as the action (event), the date/time the action was performed, as well as the outcome of either success or failure, the channel (object identity), and severity level,

The centralized logging component is configured using the Report Center interface. Report Center includes a log-filtering feature in which the Primary Administrator, Administrator, or Operator can specify which audit log messages they want collected by the centralized logging component, and what the minimum severity level should be (for example, MAJOR or CRITICAL messages only). Once the Primary Administrator, Administrator, or Operator has set specific logging filters based on severity and event type ranges, only messages with specified ID codes and severity levels are sent to the central log repository. Report Center is the used to review the audit log entries present in the log repository.

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

- FAU_GEN.1
- FAU_GEN.2
- FAU_SAR.1
- FAU_SEL.1

6.1.2 User Data Protection

The TSF mediates access between subjects and the named objects. Subjects consist of users and processes acting on behalf of users. The following table lists the named objects under the control of the access control policy for the TOE.

Name	Description
Deployment Manager Folder	Serves as an organizer of the Deployment, Task Group, Server Group and Server Keychain objects
Deployment	A set of jobs that distribute and manage content and applications on sets of servers. Each deployment job maps one task to at least one server group.
Task group	An object that contains the instructions for what you want to accomplish on your endpoints. For example, you could create a task group called Web Content, which contains instructions for managing the content (data files) on your website. Within this task group, you might create three related tasks: •A task called Stage, which would download but not activate the content •A task called Install, which would activate the content only if the Stage task was successful on all the servers •A task called Rollback, which would revert the content to a previous version if necessary Within each task, you would then create the specific commands to carry out that task.
Server group	A set of target servers on which you want to execute commands.
Server keychain	A server keychain specifies the user names and passwords (also called server credentials) that you want to use for accessing the servers.
Channel	An application or content that is published to a Transmitter. A channel can be: •An application of any type (Windows, Java, Visual Basic, and so on) or a Java applet •One or more content files, containing HTML or any data •A combination of the above
Transmitter Folder	Serves as an organizer of the Channel objects
Policy Manager Target	An object used by the policy manager interface to assign a group of application to. Typically the policy manager target object will correspond to a user or machine group in a directory system. A typical use-case would be “assign SFA applications to the sales group in active directory”.

Table 5: Named Objects

The access control policy is the mechanism by which access to the named objects is controlled based solely on the identity of the user and/or group membership, create permissions associated with that user or group and the security attributes associated with the named object.

In the SCM product, the implementation of the access policy is accomplished by association of permission bits, which are specific to the named object. Such as, permissions restrict the access that a user (subject) has to a

particular object (server group, server keychain, task group, deployment, or folder), and consequently restrict the operations (such as, read (r), write (w), execute (x), delete (d) and the ability to change permissions by virtue of being designated an object's owner (o)). Additionally, global create permissions, known as *privileges* can be associated with users and groups of users to explicitly grant or revoke create permissions for named objects.

In the DMM product, the access policy is implemented using an ACL, which contains an attribute indicating the user or user group that can access a channel, and for policy manager targets an ACL containing a list of targets a user or user group can access.

Users, or groups of users can gain access to the objects as long as they have the appropriate permissions. Access checks are performed on every reference to the named object.

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1
- FDP_ACF.1

6.1.3 Identification and Authentication

Users accessing DMM and SCM components in common with the DMM are identified and authenticated via the LDAP server, or NT Domain Controller in the environment and the identity is used by the TOE. When users access the TOE via the SCM Deployment Manager, the TOE is performing identification and authentication.

Before any security management functions can be performed on SCM Deployment Manager, users must be successfully identified and authenticated. The identification and authentication is performed via the GUI Deployment Manager tool and via the Deployment Manager Command Line interface. The users are presented with a dialog box and once the logon dialog is displayed, the user enters their user ID and password. With the Deployment Manager Command Line interface, users submit their user IDs and passwords as command line parameters to be validated by the Deployment Manger. All other SCM components are common with DMM, and therefore users for these components are identified and authenticated via the LDAP server, or NT Domain Controller in the environment.

All users, regardless of where identification and authentication take place, they must be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of the user and gaining access to the TOE.

The user attributes for Deployment Manager are stored in the local user database, which is stored on the machine where Deployment Manager is installed. The following attributes are maintained for each user entry stored in the TOE:

- User ID – user name to uniquely identify a user
- Password – the password assigned must be more than 8 characters.
- Home (default) folder – when the user account is created, a home or default folder must be specified.
- Group membership - all users are associated with groups to assist in defining roles as well as access permissions. By adding a user to a group, the user will have all the permissions assigned to that group.
- Create permissions, or privileges – when a user account or a group is created, you specify whether that user or group can create each type of named object (server group, server keychain, task group, deployment, or deployment manager folder).

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2

6.1.4 Security Management

The TSF provides the ability to manage the security functions of the TOE. The functions include the following:

- Management of access control to named objects
- Configure idle user timeout

All management functions can be performed via the GUI or via command line operations. Either interface requires successful identification and authentication of the authorized administrator before any security management functions can be performed.

All security functions are controlled through the assignment of roles, which is determined through user and group membership. By default, for Deployment Manager, the owner of a named object has read, write, execute permission on the new objects and all other users have read permission. Folder owners can set default permissions that will be applied to all objects created within the folder.. To grant access, the Deployment Manager Administrator associates users or user groups to the named objects. Only those users and/or user groups requiring access to named objects are granted access. By default, permissions for Deployment Manager Folders, deployments, task groups, server groups, and server keychains named objects are restrictive.

For channels, Transmitter folders and policy manager targets the Primary Administrator and Administrator, and users with ACL write permissions (in the case of policy manager targets only) associates users or user groups to the named objects. Only those users and/or user groups requiring access to named objects are granted access. By default, permissions for channels and Transmitter folders are permissive, while permissions for policy manager targets are restrictive.

The following roles are available, together with an indication of which product they apply to:

- Primary Administrator (CMS) - Primary Administrators have access to all product features available in the components. The security functions available to the Primary Administrator are the ability to assign the roles “Primary Administrator”, “Administrator” and “Operator” to other users, and the ability to configure the authentication source (LDAP) used by the Common management Services (CMS) component of the TOE. For the evaluated configuration, this source is an LDAP server external to the TOE environment.
- Administrator (CMS) - Administrators can log in to the TOE and have access to most product features available, except those reserved for Primary Administrators. In Report Center, for example, the Configuration page is not available to Administrators, only Primary Administrators. In addition, Administrators cannot modify the system settings, so they cannot perform tasks like giving login access to new users or configuring directory server settings.
- Operator (CMS) - Operators can log in to the applications and perform certain tasks, but they cannot make changes or save any changes in the applications. For the most part, they have read-only access to the applications.
- Deployment Manager Administrator (SCM) - Can modify the Deployment Manager’s system settings, and can grant new users and groups, access to the Deployment Manager, including specifying a default folder for them. In addition, the Deployment Manager can modify users’ security attributes. The Deployment Manager Administrator has the ability to modify, change default settings, and delete the security control attributes associated with named objects, except channels.
- Regular Users (SCM) – Non-administrative users can perform operations only on objects that they have sufficient permissions to do so. Each object in the Deployment Manager can have the following combination of permissions: read, write, execute and owner Non-administrative users can also change their own passwords.

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

- FMT_MSA.1

- FMT_MSA.3
- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1

6.1.5 TOE Access

The TSF provides the ability for the Deployment Manager Administrator in SCM, and the Primary Administrator in DMM to specify a user session timeout value. The TSF monitors an established session for activity and if the session is inactive for the specified time period, the TSF will terminate the session. On the SCM, the default time is 15 minutes, on the DMM, the default time is 60 minutes. To reestablish a session, the user must re-enter their user ID and password and be successfully identified and authenticated.

The TOE Access function is designed to satisfy the following security functional requirement:

- FTS_SSL.3

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL3 assurance requirements.

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The CM documentation describes the processes and procedure that are followed and automated tools that are utilized in the tracking and monitoring the changes to the CM items and the generation of the TOE. The configuration management measures applied by Marimba ensure that configuration items are uniquely identified. Marimba ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. Marimba performs configuration management on the TOE implementation representation, design, tests, vulnerability analysis, delivery, installation, user and administrator guidance, lifecycle, and the CM documentation. These activities are documented in:

- Marimba Configuration Management Guide, version 2.x

6.2.1.2 Life Cycle Support

Marimba ensures the adequacy of the procedures used during the development and maintenance of the TOE. Marimba includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. Marimba achieves this through the use of documented procedures. These procedures are documented in:

- Marimba Configuration Management Guide, version 2.x

The Process Assurance measures satisfy the following assurance requirements:

- ACM_CAP.3
- ACM_SCP.1

- ALC_DVS.1

6.2.2 Delivery and Operation

Marimba provides documentation that explains how the TOE is delivered, the carriers utilized, and the procedures that are followed to maintain security when distributed to the user's site. Marimba's installation procedures describe the steps used for the secure installation, generation, and start-up of the TOE along with configuration settings to secure the TOE privileges and functions. These procedures are documented in:

- Sales Orders and Delivery Guide, version 2.x

Marimba Documentation Addendum, version 2.x[12]

The Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Design Documentation

Marimba provides design documentation that identifies and describes the external interfaces and the decomposition of the TOE into subsystems. The design documentation consists of the following documents:

- ADV_FSP.1: The Marimba Functional Specification, Version 2.x describes all the external interfaces of the TSF. The description includes the purpose and method of use of the interface, applicable parameters, effects, error messages, and exceptions as appropriate.
- ADV_HLD.2: The Marimba High Level Design, Version 2.x decomposes the TOE into TSP-enforcing and other subsystems. Each subsystem will describe the purpose and method of use of all interfaces to the subsystems of the TSF. The description includes the purpose and method of use of the interface, applicable parameters, effects, error messages, and exceptions as appropriate.
- ADV_RCR.1: The way that this correspondence is evident within the design documentation is:
    - ST-TSS to FSP: The Marimba Correspondence Matrix identifies the interfaces that provide the security functions as described in the ST.
    - FSP to HLD: The Marimba Correspondence Matrix identifies the interfaces of the subsystems that provide the security functions as described in the FSP.

The Design assurance measure satisfies the following Assurance requirements

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1

6.2.4 Guidance Documentation

Marimba provides administrator guidance on how to utilize the TOE security functions, the interfaces available to the administrator, and warnings to authorized administrators about actions that can compromise the security of the TOE. The procedures, included in the administrator guidance, describe the steps necessary to operate DMM/SCM in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration, and assumptions about the environment.

The user guidance describes the procedures to use the TOE security-related functions and the interfaces that are available to the non-administrative users.

[12] The Addendum specifies the Common Criteria specific evaluation settings.

- The administrator and user guidance is documented in:
- *Marimba Documentation Addendum, version 2.x*
- *Marimba Infrastructure Administrator's Guide, version 6.0.2 (040628)*
- *Marimba Infrastructure & Console Release Notes, version 6.0.2 (040625)*
- *Marimba Infrastructure Patch Page, version 6.0.2 (040625)*
- *Planning Guide, version 6.0 (031219)*
- *Deployment Guide, version 6.0.2 (040708)*
- *Upgrade Guide, version 6.0.2 (040708)*
- *Marimba Reference Guide, June 2004 (400628)*
- *Policy Management Administrator's Guide, version 6.0.2 (040625)*
- *Policy Management Release Notes, version 6.0.2 (040625)*
- *Policy Management Patch Page, version 6.0.2 (040623)*
- *Report Center Administrator's Guide, version 6.0.2 (040628)*
- *Report Center/Inventory Release Notes, version 6.0.2 (040624)*
- *Report Center/Inventory Patch Page, version 6.0.2 (040628)*
- *Server Management Administrator's Guide, version 6.0.2 (040621)*
- *Server Management Guide to the Command Line Interface, version 6.0.2 (040621)*
- *Server Management Release Notes, version 6.0.2 (040625)*
- *Server Management Patch Page, version 6.0.2 (040625)*
- *Marimba Server Management Advanced Topics Guide, version 6.0.2 (040621)*
- *System Requirements for Marimba Products, version 6.0.2 (040701)*
- *Introduction to Marimba Products, September 2004 (040916)*

The Guidance assurance measure satisfies the following Assurance requirements

- AGD_ADM.1
- AGD_USR.1

6.2.5 Test Documentation

Marimba provides test documentation that describes how each of the TOE security functions is tested, as well as the actual results of applying the tests. The test documentation consists of the following document:

Marimba Desktop/Mobile Management and Server Change Management Test Plan and Test Cases, version 2.x

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.2: The Test Cases descriptions describe the test cases for each of the security-relevant interfaces of the TOE. The descriptions indicate which tests are used to satisfy the test cases identified for each interface.
- ATE_DPT.1: The Test Cases descriptions include more detailed test case descriptions that demonstrate that the test are sufficient to demonstrate that the TSF operates in accordance with the high-level design and that all of the corresponding interfaces are appropriately exercised

- ATE_FUN.1: The Test Plan describes the security functions to be tested, how to successfully test all of them, the expected results, and the actual test results after exercising all of the tests.
- ATE_IND.2: The TOE and test documentation will be available for independent testing.

6.2.6 Vulnerability Assessment

6.2.6.1 Evaluation of Misuse

The Evaluation Team's misuse analysis will demonstrate that the administrative and user guidance completely addresses managing the TOE in a secure configuration.

6.2.6.2 Strength of TOE Security Functions and Vulnerability Analysis

Marimba performs a SOF analysis of the authentication mechanism. The strength of TOE security function analysis demonstrates that the SOF claims made in the ST for all probabilistic or permutation mechanisms are correct. The TOE security function analysis is provided in the Section 8.7 of this ST.

Marimba's vulnerability assessment provides the status of each identified vulnerability and demonstrates that each one cannot be exploited in the intended environment and that DMM/SCM is resistant to obvious penetration attacks.

The vulnerability analysis is documented in:

- Marimba Desktop/Mobile Management and Server Change Management Vulnerability Analysis, Version 2.x

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

There are no Protection Profile conformance claims for the TOE.

8. Rationale

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

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Explicitly Stated Requirements;
- Security Requirements Dependencies Rationale;
- TOE Summary Specification;
- Internal Consistency and Support Rationale; and
- Strength of Function (SOF) Rationale.

8.1 Security Objectives Rationale

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

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

8.1.1 Security Objective for the TOE Rationale

Table 6: Mapping of TOE Security Objectives to Threats or Organizational Security Policies provides a mapping of TOE security objectives to those threats that the security objectives that the TOE is designed to counter and organizational security policies that the TOE must enforce.

TOE Security Objectives	Threats and Organizational Policies
O.AUTHORIZATION	T.ACCESS
O.OBJ_ACCESS	T.PRIVILEGE
O.AUDIT	P.ACCOUNTABILITY T.AUDIT_CORRUPT
O.MANAGE	P.MANAGE
	T.AUDIT_CORRUPT

Table 6: Mapping of TOE Security Objectives to Threats or Organizational Security Policies

The following objectives will address the threats and organizational policies listed in the ST.

O.AUTHORIZATION - This objective counters the threat T.ACCESS by requiring each user be identified and authenticated before any access to the TOE and its protected resources is granted.

O.OBJ_ACCESS - This objective counters the threat T. PRIVILEGE by ensuring access to named objects is explicitly granted, preventing an unauthorized user from gaining access to the named object.

O.AUDIT – This objective implements the security policy P.ACCOUNTABILITY, ensuring that all relevant TOE security actions are recorded. This objective also counters the threats T.AUDIT_CORRUPT by restricting access to all audit records to only authorized administrators.

O.MANAGE – This objective implements the security policy P.MANAGE, by ensuring that only authorized administrators can use the provided utilities for managing the security functions of the TOE and its resources. This objective also counters the threats T.AUDIT_CORRUPT by restricting access to all audit records to only authorized administrators.

8.1.2 Security Objectives for Environment Rationale

8.1.2.1 Security Objectives for the IT Environment Rationale

Table 7: Security objectives for the IT environment mapped to assumptions identifies security objectives for the IT environment in which the TOE is designed to operate and provides a mapping to assumptions that are made about that environment.

TOE Security Objectives for the IT Environment	Assumptions

TOE Security Objectives for the IT Environment	Assumptions
OE.AUTH_ACCESS	A.IDENT A.SYSPROTECT T.ACCESS
OE.SEP	A.CONNECT A.SYSPROTECT T.ACCESS
OE.TIME_SOURCE	A.TIME

Table 7: Security objectives for the IT environment mapped to assumptions

OE.AUTH_ACCESS - This objective ensures that only authorized users have access to the TOE, thus countering T.ACCESS and assuring that A.IDENT and A.SYSPROTECT are addressed.

OE.SEP - This objective provides the support needed by the TOE to counter threats T.ACCESS by ensuring that the TOE cannot be tampered with or bypassed and assuring A.CONNECT and A.SYSPROTECT is addressed.

OE.TIME_SOURCE - The IT environment must provide a reliable time source for the TOE to provide an accurate timestamp for all audit records, thus assuring A.TIME is addressed.

8.1.2.2 Security Objectives for the Non-IT Environment Rationale

Table 8: Security objectives for the non-IT environment mapped to assumptions identifies security objectives for the non-IT environment in which the TOE is designed to operate and provides a mapping to assumptions that are made about that environment.

TOE Security Objectives for the Non-IT Environment	Assumptions
OE.HARDWARE	A.HARDWARE
OE.INSTALL	A.INSTALL A.PROTECT
OE.PERSON	A.NOEVIL A.MANAGE
OE.PHYCAL	A.CONNECT A.PROTECT

Table 8: Security objectives for the non-IT environment mapped to assumptions

OE.HARDWRE - This objective ensures that the TOE is operating on the hardware, operating system, and associated software that would ensure the TOE operates correctly and has sufficient space to execute the security functions correctly. This objective addresses A.HARDWRE

OE.INSTALL - Ensuring proper installation, management, and operation of the TOE to protect both itself and its resources addresses the assumption A.INSTALL and A.PROTECT.

OE.PERSON - This objective ensures that the TOE is operated in a secure manner by competent, trained personnel, which addresses A.NOEVIL assumption. This objective also ensures that there are TOE administrators and they are properly trained and competent which addresses the A.MANAGE objective.

OE.PHYCAL - This objective ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the information generated. This objective addresses A.CONNECT and A.PROTECT.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target.

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

8.2.1 Security Functional Requirements Rationale

Table 9: SFRs mapped to Security Objectives provides the correspondence mapping between security objectives for the TOE and the security functional requirements that satisfy them.

SECURITY FUNCTIONAL REQUIREMENT	O.AUTHORIZATION	O.OBJ_ACCESS	O.AUDIT	O.MANAGE	OE.AUTH_ACCESS	OE.SEP	OE.TIME_SOURCE
FAU_GEN.1			X				
FAU_GEN.2			X				
FAU_SAR.1			X				
FAU_SEL.1			X				
FDP_ACC.1		X					
FDP_ACF.1		X					
FIA_ATD.1	X	X			X		
FIA_UAU.2	X				X		
FIA_UID.2	X				X		
FMT_MSA.1(a)		X		X			
FMT_MSA.1(b)		X		X			
FMT_MSA.1(c)				X			
FMT_MSA.3				X			
FMT_MTD.1(a)				X			
FMT_MTD.1(b)		X		X			
FMT_SMF.1				X			
FMT_SMR.1				X			
FPT_SEP.1						X	
FPT_STM.1							X
FTA_SSL.3				X			

Table 9: SFRs mapped to Security Objectives

O.AUTHORIZATION

FIA_UAU.2 and FIA_UID.2 require a user be successfully be identified and authenticated before any access to the TOE and TOE-protected resources is allowed.

FIA_ATD.1 defines the unique attributes that are associated with individual users.

O.OBJ_ACCESS

FDP_ACC.1 and FDP_ACF.1 define the Access Control Policy, the subjects and objects that the policy covers, the security attributes that access to objects is based on, and the rules of access between subjects and objects. The Access Control Policy allows for the control of access to resources based on the user identity and group membership.

FIA_ATD.1 defines the security attributes that are associated to the user and used by the SFP.

FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.1(c), FMT_MSA.3, and FMT_MTD.1(b) restrict the ability to change_default, query, modify, create, and delete security attributes to authorized users and ensures that restrictive default values are defined for the security attributes used to enforce the SFP.

O.AUDIT

FAU_GEN.1 and FAU_GEN.2 define the TOE events that will be audited, along with the details that will be recorded along with the event.

FAU_SAR.1 restricts access to the audit trail to authorized administrators and provides them a method for viewing the data according to various criteria. FAU_SEL.1 provides the capability for the authorized administrator to include or exclude records based on the channel as well as the severity and error code ranges.

O.MANAGE

FMT_MSA.1(a) restricts the ability to manage the associated security attributes (associated with a named object, except channels) of the Access Control SFP to the Deployment Manager Administrator.

FMT_MSA.1(b) restricts the ability to manage the associated security attributes (access control attributes associated with channels) of the Access Control SFP to the Primary Administrators and Administrators.

FMT_MSA.1(c) restricts the ability to manage the associated security attributes (access control attributes associated with policy manager targets) of the Access Control SFP to Primary Administrator and users with ACL write permissions.

FMT_MSA.3 enforces the restrictive default values for security attributes associated with a named object.

FMT_MTD.1(a) provides the ability for the Primary Administrator, Administrator, and Operator to view the audit data

FMT_MTD.1(b) provides the ability for the Deployment Manager Administrator to manage the security attributes of other users. Users are not restricted when modifying their own user account security attributes.

FMT_SMR.1 requires the TOE to provide the ability to set roles for security relevant authority; Primary Administrator, Administrator, Operator, Deployment Manager Administrator, Transmitter Administrator, and Regular User.

FMT_SMF.1 requires that the TOE provide the ability to manage the security functions of TOE. Those functions include management of Access Control SFP and configuring idle user timeout.

FTA_SSL.3 provides the Deployment Manager Administrator and the Primary Administrator the ability to configure an idle user timeout; will automatically log out the current user after a specified period of time.

OE.AUTH_ACCESS

FIA_ATD.1 defines the unique attributes that are associated with individual users.

FIA_UAU.2 and FIA_UID.2 require a user be identified and authenticated before any access to the TOE is allowed.

OE.SEP

FPT_SEP.1 ensures the TOE maintains a separate execution domain to protect from external tampering.

OE.TIME_SOURCE

FPT_STM.1 ensures that an accurate time source will be available to the TOE.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL3 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a medium level of risk to the assets. The security environment in which the TOE operates assumes physical protection. DMM/SCM provides a level of protection that is appropriate for IT environments that require secure automated change management, such as the distribution of application updates and patches throughout an enterprise. As such, it is believed that EAL3 provides an appropriate level of assurance in the security functions offered by the TOE.

8.4 Security Requirements Dependencies Rationale

The table below maps the TOE security functional requirements to the corresponding requirements they are dependent on. The dependencies of the TOE security functional requirements are, for the most part, met through the functionality of the TOE and/or by the security functionality of the IT environment.

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	Included (environment)
FAU_GEN.2	FAU_GEN.1	Included
	FIA_UID.2	Included
FAU_SAR.1	FAU_GEN.1	Included
FAU_SEL.1	FAU_GEN.1	Included
	FMT_MTD.1	Included (FMT_MTD.1(a))
FDP_ACC.1	FDP_ACF.1	Included
FDP_ACF.1	FDP_ACC.1	Included
	FMT_MSA.3	Included
FIA_ATD.1	None	
FIA_UAU.2	FIA_UID.2	Included
FIA_UID.2	None	
FMT_MSA.1(a, b & c)	FDP_ACC.1 or FDP_IFC.1	Included
	FMT_SMF.1	Included
	FMT_SMR.1	Included
FMT_MSA.3	FMT_MSA.1	Included
	FMT_SMR.1	Included
FMT_MTD.1 (a & b)	FMT_SMR.1	Included
	FMT_SMF.1	Included
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.2	Included
FPT_SEP.1	None	
FPT_STM.1	None	
FTA_SSL.3	None	

Table 10: Requirement Dependency Rationale

8.5 TOE Summary Specification Rationale

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

This Section in conjunction with TOE Summary Specification section provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE Summary Specification are all necessary for the required security functionality in the TSF. **Table 11: Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Audit	User Data Protection	Identification and Authentication	Security Management	TOE Access
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1	X				
FAU_SEL.1	X				
FDP_ACC.1		X			
FDP_ACF.1		X			
FIA_ATD.1			X		
FIA_UAU.2			X		
FIA_UID.2			X		
FMT_MSA.1(a)				X	
FMT_MSA.1(b)				X	
FMT_MSA.1(c)				X	
FMT_MSA.3				X	
FMT_MTD.1(a)				X	
FMT_MTD.1(b)				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FTA_SSL.3					X

Table 11: Security Functions vs. Requirements Mapping

8.6 Internal Consistency and Support Rationale

The selected functional requirements for the TOE and IT Environment are internally consistent. All the operations performed are in accordance with the CC. The ST does not include any instances of a requirement that conflicts with or contradicts another requirement. In instances where multiple requirements apply to the same functions, the requirements and their operations do not cause a conflict between each other.

The selected requirements are mutually supportive by supporting the dependencies as demonstrated in the **Table 10: Requirement Dependency Rationale**. The rationale of the suitability of the requirements to meet the objectives; the inclusion of architectural requirements FPT_SEP.1, to protect the TOE; the inclusion of audit requirements to

detect unauthorized actions and/or events, the inclusion of user data protection for access control, and the inclusion of security management requirements to provide a means to properly configure and manage the other security requirements.

8.7 Strength of Function (SOF) Rationale

The TOE minimum strength of function of SOF-basic was chosen to be consistent with the TOE environment. The SOF-claim is associated with the authentication mechanism described in Identification and Authentication, which supports FIA_UAU.2.

The list of relevant security functions and security functional requirements includes:

- Identification and Authentication Security Function
    - FIA_UAU.2 – User authentication before any action, security functional requirement

      The password is the only probabilistic or permutational function on which the strength of the authentication mechanism depends.

The system places the following restrictions on the passwords selected by the user:

- The password must be more than eight characters; a minimum of nine characters

Furthermore, the user is told to not use consecutive sequences, or easily guessable passwords

The password space is calculated as follows:

Patterns of human usage are important considerations that can influence the approach to searching a password space, and thus affect SOF. Assuming the worst case scenario and the user chooses a number comprising only nine characters, the number of password permutations is:

52 alpha characters (upper and lower)
10 digits
+ 16 special characters (!, @, #, $, %, ^, &, *, (,), +, =, <, >, :, ;)
78 possible values

78^9 = (78*78*78*78*78*78*78*78*78) = **106,868,920,913,284,608**

A proficient or expert person could create a program to guess passwords approximately 20 times every second without using any specialized equipment. This assumption is based on timing a logon attempt on a 3.4 GHz Pentium. The average total time to guess the correct password can be estimated by:

(53,434,460,456,642,304 passwords) * (.2 seconds / password guess) * (1 hour / 3600 seconds) * (1 day / 24 hours) * (1 year / 365 days) = 338879125 years

In accordance with annex B.3 in the CEM, the elapse time of attack over which the user would try to guess the password is too great to make the TOE vulnerable and thus results in a basic strength of function (SOF-basic) rating,.