National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Marimba, Inc.

Marimba Desktop/Mobile Management
And
Server Change Management

Report Number: CCEVS-VR-05-0103

Dated: 10 June 2005

Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation
Common Criteria Testing Laboratory

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of Marimba Desktop/Mobile Management and Server Change Management (DMM/SCM). It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by Science Applications International Corporation (SAIC), and was completed during May 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by SAIC. The evaluation determined the product to be both **Part 2 conformant** and **Part 3 conformant,** and to meet the requirements of **EAL 3**. The product is not conformant with any published Protection Profiles

The product family provides centralized, automated distribution and maintenance of software applications and content either within a company or across the internet. In particular, the DMM/SCM products provide change management and configuration management tasks such as operating system (O/S) migration, software updates (e.g., O/S patches, anti-virus updates), and IT inventory management.[1]

[1] This evaluation is a follow-on to the one performed on this product family and reported in Validation Report # CCEVS-VR-O4-0066, dated 30 June 2004. The revised product is essentially the same as the one evaluated previously, but incorporates some patches that were necessitated during the original evaluation, encompasses some code consolidation, and includes several small changes.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Marimba Desktop/Mobile Management (DMM) and Server Change Management (SCM) for Windows and Solaris
Protection Profile	None
Security Target	*Marimba Desktop/Mobile Management and Server Change Management*, Version 2.0, 26 May 2005
Evaluation Technical Report	*Evaluation Technical Report for the Marimba Desktop/Mobile Management and Server Change Management,* Part 1 (Non-Proprietary), Version 2.1, May 27 2005
Conformance Result	Part 2 conformant, Part 3 conformant, EAL 3
Sponsor	BMC Software, Inc.
Developer	BMC Software, Inc.
Evaluators	Science Applications International Corporation
Validators	The Aerospace Corporation

3. ARCHITECTURAL INFORMATION

3.1. Software

The DMM/SCM provides administrators with the ability to perform change management of software across an enterprise, e.g., automated distribution of applications and application updates. The product also allows administrators to perform O/S migration as well as hardware and software inventories. The SCM is designed for use with groups of servers, whereas the DMM is designed for use with groups of desktop machines. These products run on Pentium hardware running various versions of Windows and on Sun Microsystems SPARCstation hardware running Solaris 8 or 9.[2]

Both the Desktop/Mobile Management and the Server Change Management packages are implemented as a set of Java applications, and rely on a pair of applications called the *Tuner* and the *Transmitter*, which serves *channels* (i.e., applications or files) over a network.

- The Tuner is the application by which users subscribe to channels that have been published on the Transmitter component. The Tuner downloads the channel files, or updates to the channel files, to the managed server endpoint. Additionally, the Tuner provides a Java execution environment for running all other Marimba products (including the Transmitter).
- The Transmitter component is a data server that delivers channels (i.e., provides content for updated and distributed software packages) to its clients; Tuners. It acts as the server in both the DMM and SCM distributed environments, providing application change management services to the client computer (DMM) and the managed server endpoint (SCM).

The other primary components of the DMM are the *Infrastructure Administrator*, *Subscription Policy Manager*, and the *Report Center*[3]:

- The Infrastructure Administrator provides the administrator with the ability to install, configure and manage the components of the TOE;
- The Subscription Policy Manager provides the capability for assigning channels and for managing the subscription capabilities;
- The Report Center—an administrator tool— 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.

For the SCM, the primary components—other than the Tuner and Transmitter components—are the *Infrastructure Administrator*, *Deployment Manager*, and *Content Replicator*

- The Infrastructure Administrator (see above description)

---

[2] See the Security Target for the details of which software suites host the various components.

[3] These functional elements are incorporated in the Common Management Services (CMS) module of the DMM architecture, that provides an application server on which Marimba applications execute.

- Deployment Manager provides administrators centralized control and monitoring of content distribution.
- Content Replicator performs installation of data and content on managed server endpoints, and also performs roll-back of installations. Content Replicator can be run remotely via the Deployment Manager.

3.2. Hardware and IT Environment

Although not part of the TOE, *per se*, the following hardware and software entities are required as platforms and to provide required support (e.g., data archiving, I&A).

3.2.1. DMM

The managed desktop endpoints require Pentium processors running Windows NT 4.0 (SP6a or higher), Windows 2000, or Windows XP. Pentium processors running either Windows NT 4.0 or Windows 2000 are required for the Marimba Infrastructure and Policy Manager server-side components. The full suite of DMM components requires a Sparc Netra T1 running Solaris 8 or 9, and Common Desktop Environment (CDE)

3.2.2. SCM

The managed server endpoints require Pentium processors running Windows NT 4.0 (SP6a or higher), Windows 2000, or Windows XP. The Marimba Infrastructure and Deployment Manager server-side components require Pentium processors running either Windows NT 4.0 or Windows 2000. The full suite of SCM components also requires a Sparc Netra T1 running Solaris 8 or 9, and Common Desktop Environment (CDE).

In addition, both the SCM and DMM require an external RDBMS for archiving records—including security audit information—as well as an external authentication service, via LDAP or an NT Domain Controller.

4. SECURITY POLICY

The Marimba DMM/SCM product enforces access control, I&A, and auditing policies, and also provides mechanisms for allowing administrators to manage users and their security attributes. However, the mechanisms are not implemented consistently across the elements of the TOE. As an example, the Deployment Manager component of the SCM performs I&A on the users that interface to it. However, for users that access the TOE via other components an external LDAP server or NT Domain Controller (in the IT environment) is used to perform I&A, with the access control policy being enforced on the basis of the identity established by the external entity. Thus, it is imperative that the Security Target be reviewed and understood, as there are important details regarding the distribution of security mechanisms across the elements of the architecture. The level of architectural and implementation detail required to discuss the allocation of security features across system elements is beyond the scope of a validation report.

4.1. Access Control

The product mediates access between user processes (i.e., "subjects") and user data objects (also referred to as "named objects).[4] Access of subjects to user data objects is based on the identity of the user requesting access and/or the group membership, and is determined by access permissions (e.g., read, write, execute, delete, change permissions) that the subject has to the particular object that is being accessed. For the SCM product, the access control policy is implemented via permission bits that are associated with each named object. For the DMM, the implementation is via an Access Control List (ACL) that is associated with each object,[5] and which contains an attribute indicating the user or user group that can access a channel (i.e., a published application or content).

Access checks are performed on each reference to an object.

Each user is associated with one or more groups; adding a user to a group confers all the permissions defined for the group.

4.2. Identification and Authentication

All users must be successfully identified and authenticated prior to being able to obtain data and services. However, I&A is performed differently between the SCM and the DMM, and I&A is also performed differently for the various administrator roles that are defined.

Users accessing DMM, and also SCM components that are common with the DMM, are identified and authenticated via an external authentication server—an LDAP server or NT Domain Controller. For users that access the SCM via the Deployment Manager (i.e., administrators), I&A is performed by the TOE. Prior to any security management functions being performed on the SCM Deployment Manager, users must be successfully identified and authenticated. As noted, this I&A is performed by the Deployment Manager—either via the GUI or the command line interface.

Other than the Deployment Manager, all other SCM components are common with the DMM and thus, users for these components are authenticated via the external authentication server.

Regardless of where I&A takes place, all users must be successfully identified and authenticated prior to being allowed any other TSF-mediated actions on behalf of the user.

4.3. Auditing

Events within the Transmitter are logged, including security events (e.g., startup and shutdown of Transmitter). Audit records include the identity of the user associated with the event, a description of the event, date and time of the event, and the outcome (i.e., success or failure). The Transmitter's audit logs are compiled by a collection agent, and forwarded to the central repository (i.e., external RDBMS).

Audit records are stored both local to the Transmitter (on the file system of the host platform) and also in the central repository. The various administrator roles access audit records on the external

---

[4] The Security Target contains a complete list of the named objects that are subject to the access control policy.

[5] Note that the set of objects that are accessible are not the same between SCM and DMM. See the "TOE Summary Specification" section of the ST for details.

RDMBS using the Report Center component. The Report Center component is also the vehicle via which the logging component is configured. An administrator can specify, among other items, which audit records are to be collected.

4.4. Security Management

The TSF provides the ability to manage the security functions of the TOE, including management of access control to named objects and configuration of the authentication source (e.g., LDAP).

All management functions can be performed through either the GUI or command line interface. Both interfaces require successful identification and authentication of the authorized administrator, as discussed above. All security functions are controlled through the assignment of roles; the TOE supports the following defined roles:[6]

- Primary Administrator;
- Administrator;
- Operator;
- Deployment Manager Administrator;
- Regular Users.

It will be important for administrators to be aware of the administrative guidance provided for the product, as some access authorizations are restrictive by default (e.g., Deployment Manager folders), while others (e.g., access to channels and Transmitter folders) are permissive by default.

5. ASSUMPTIONS

5.1. Usage Assumptions

Administrators are assumed to be trusted (i.e., non-malicious) and competent to carry out their responsibilities. It is further assumed that the TOE has been delivered, installed, and configured in accordance with documented procedures.

Additionally, it is assumed that communications between TOE components will be protected from unauthorized access.

5.2. Environmental Assumptions

The system is expected to be used in what has traditionally been known as "a relatively benign environment." That is, all the information on the system is at the same level of sensitivity, all users are authorized for that level of information (although do not necessarily have permissions for access to all the data). However, users are not expected to be trustworthy; they may make attempts to bypass system security controls or otherwise exceed their authorizations to data and system

[6] For a detailed definition of the capabilities of each role, as well as the component for which they are defined, see the Security Target (Section 6.1.4).

resources. Accordingly, it is assumed that the operational environment is such as to provide physical protection of the TOE and its hardware & software platforms.

6. DEPENDENCIES

As the TOE consists of a set of software (i.e., Java) applications, there are several dependencies on the IT environment. Specifically:

- There is a requirement that there be an external authentication server that provides reliable user identities;
- There is a requirement for an external relational database (RDBMS) for archiving and reviewing audit records;
- The hardware and software platform (i.e., the host O/S) must provide isolation of the TOE software, protect it from tamper, and prevent bypass of the TOE security functions;
- The host platform is relied on for providing a reliable time source (i.e., for accurate timestamps for audit records);
- The Transmitter uses the file system of the host platform for storing and protecting audit records.

7. DOCUMENTATION

The evaluation team made use of a considerable number of Marimba documents during the analysis and testing. Among the documents reviewed were:[7]

- Security Target
- Configuration Management Guide
- Server Management Installation Guide
- Functional Specification
- Server Command Line Interface
- High-Level Design
- Administrator Guides
- Test Plans and Test Cases

[7] For a complete list of documentation available to the evaluators, see the non-proprietary version of the ETR (reference [9].

8. IT PRODUCT TESTING

8.1. Developer Testing

Vendor testing is oriented toward security functional requirements; the documentation includes a test plan describing test approach, test configuration, test procedures, and test coverage. Each test procedure is further broken out into test cases that target specific security behavior associated with a security functional requirement (SFR). The evaluation team found the vendor test suite to be sufficiently broad in scope, addressing each of the security functional requirements in combination with the related external interfaces. However, the vendor test plans were also judged to be spotty relative to depth of testing, with only some of the subsystem interactions being tested.

During the testing of the previous version of the TOE, the evaluation team identified test procedures that were either unnecessary or judged to be ineffective, and created test procedure modifications for improved effectiveness and depth of testing. These modifications, along with test scripts, were provided to the developer who subsequently incorporated them into his test suite; the expanded test suite is currently the basis for the developer's security testing.

8.2. Evaluator Testing

The evaluation team exercised all of the developer's manual test procedures, and reused the team tests from the earlier evaluation effort. Additionally, new tests procedures were developed which concentrated on new features (i.e., the Policy Manager) of the TOE. In particular, the evaluation team significantly extended the developer test suite for Policy Manager, exercising a larger number of the access combinations that are made possible by the increased granularity of access control in the latest version of the TOE.

Problems, including a vulnerability, encountered during the testing of the earlier version of the TOE had been corrected during the earlier evaluation activity, and were no longer present in the current version.

9. EVALUATED CONFIGURATION

The test configuration consisted of two Marimba DMM and SCM instantiations, each configured per the defined evaluated configuration for the suite of Marimba applications. That is, the test configuration consisted of a single test environment, which included two TOE instances:

- One running on Microsoft Windows 2000
- One running on Sun Microsystems Solaris 8.

Additionally, an additional platform is required to host the following server products. These are not part of the TOE, but are in the IT Environment, and are required to execute the test scripts.

- Microsoft SQL Server 2000 (MS SQL), running on Windows 2000
- Sun One Directory Server (LDAP) version 5.1, running on Windows 2000

MS SQL is the central repository for recording and reporting on audit records. The LDAP server provides password authentication services and provides user group functionality for role and ACL support.

10. RESULTS OF THE EVALUATION

The TOE was found to provide the capabilities defined by the Security Target, and to satisfy all the requirements of EAL 3.

11. EVALUATOR COMMENTS

There are no Evaluator Comments.

12. VALIDATOR COMMENTS

Section 4.3 of the Security Target (i.e., Security Objectives for the Non-IT Environment) shows the hardware and software platforms that the vendor presumes will be in place to support the various elements of the TOE. Although there is room for interpretation within the CC guidance relative to the construct of Security Targets, the Validator feels that this material is identified incorrectly. The Validator feels that the set of hardware and software identified in this section is more correctly identified as being part of the TOE logical and physical boundary (Section 2.4) as it represents the hardware and software platforms on which the TOE functions. In fact, the hardware and software identified are the platforms on which the TOE was tested by both the vendor and the evaluators.

Although the Validator has chosen to bring this issue to light here, the reader should understand that there is no criticism of the material *per se*; the substance of the material is correct. The Validator feels, however, that presenting it as Objectives is confusing, and that it should have been presented, as noted, as being part of the logical and physical boundary of the evaluated configuration.

13. SECURITY TARGET

The Security Target, *Marimba Desktop/Mobile Management and Server Change Management;* Version 2.0, 26 May 2005, is included here by reference.

14. INTERPRETATIONS APPLIED

For the evaluation of the Marimba product, the following international interpretations were applied:

- RI-3 Unique identification of configuration items in the configuration list
- RI-4 ACM_SCP.*.1C requirement unclear
- RI-38 Use of "as a minimum" in C & P elements
- RI-43 What does "clearly stated" mean?

- RI-51 Use of documentation without C & P elements
- RI-84 Aspects of objectives in TOE and environment
- RI-85 SOF level is optional, not mandatory
- RI-103 Association of access control attributes with subjects and objects
- RI-201 "Other properties" specified by assignment
- RI-202 Selecting one or more items in a selection operation and using "None" in assignment

15. GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
DMM	Desktop/Mobile Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
SCM	Server Change Management
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

16. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Security Target, Marimba Desktop/Mobile Management and Server Change Management; Version 2.0, 26 May 2005.

[8] Evaluation Team Test Plan/Report for the Marimba Desktop/Mobile Management and Server Change Management, Version 2.0, March 29 2005.

[9] Evaluation Technical Report for the Marimba Desktop/Mobile Management and Server Change Management; Part 1 (Non-Proprietary); Version 2.1, May 27, 2005.

[10] Evaluation Technical Report for the Marimba Desktop/Mobile Management and Server Change Management; Part 2 (SAIC and Marimba Proprietary); Version 2.1, April 18 2005.