National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Oracle Primavera

Primavera® P6™ Enterprise Project Portfolio Management

(Version 6.2.1)

Report Number:	**CCEVS-VR-VID10182-2009**
Dated:	**25 August 2009**
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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Jandria Alexander, Senior Validator
The Aerospace Corporation
Scott Shorter, Lead Validator
Orion Security Solutions

Common Criteria Testing Laboratory

Anthony Apted, Lead Evaluator
Katie Sykes, Evaluation Team Member
Science Applications International Corporation (SAIC)
Columbia, Maryland 21046

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1)[1] product from Oracle Primavera was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in July 2009. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Conformant and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 4. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

Primavera is a project management product that is implemented using client/server architecture with a centralized project database. Primavera can be used to manage projects, resources, and methodologies. Resources can represent either people or materials, depending on how the project is defined. Methodologies are templates for defining new projects and can be used to codify an organization’s best practices.

Primavera provides multiple methods for connecting to and accessing the data (i.e., projects, resources, methodologies) under its control: Windows-based heavy clients; browser-based Web clients; and an API. The evaluated configuration requires an LDAP server in the operational environment to support user identification and authentication. Details of supported components in the operational environment are in Section 5.

Primavera is dependent on the correct operation of the various components in its operational environment, which are not included within the scope of the evaluation. It should also be noted that the access control policies implemented by Primavera are enforced only on access attempts made through the Primavera’s interfaces. Primavera does not and cannot control attempts to access data directly (e.g., via the underlying database system or operating system).

Primavera P6 Version 6.2.1, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1) Security Target.

[1] Hereinafter generally referred to as Primavera P6 Version 6.2.1, or just Primavera.

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1)
Sponsor:	Oracle Primavera Global Business Unit Three Bala Plaza West, Suite 700 Bala Cynwyd, PA 19004
Developer:	Oracle Primavera Global Business Unit Three Bala Plaza West, Suite 700 Bala Cynwyd, PA 19004
CCTL:	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Kickoff Date:	September 18, 2006
Completion Date:	13 August 2009
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1 Revision 2, September 2007.
Evaluation Class:	EAL 4
Description:	Primavera is a project management product that is implemented using client/server architecture with a centralized project database. It can be used to manage projects, resources, and methodologies. It consists of the following components: Project Management Client Module; Methodology Management Client Module; Web Access Application Server; Web Client Module; Timesheet client application; Group Server (Timesheet server); Integration API.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Primavera P6 Version 6.2.1 product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	None

Evaluation Personnel:	Science Applications International Corporation: Anthony J. Apted Katie Sykes
Validation Body:	National Information Assurance Partnership CCEVS
Validation Personnel:	Jandria Alexander, The Aerospace Corporation Scott Shorter, Orion Security Solutions, Inc.

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE is intended to counter.

T.MASQUERADE An unauthorized user, process, or external IT entity may masquerade as an authorized user to gain access to the TOE.

T.TSF_COMPROMISE A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).

T.UNAUTH_ACCESS An authorized user may gain unauthorized access (view, modify, delete) to user data through the TOE.

2 Identification

The evaluated product is **Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1)**.

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the Primavera security policy has been extracted and reworked from the Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1) ST and Final ETR.*

3.1 User Data Protection

Primavera implements three separate access control policies—one controls access to projects, another controls access to resources, and the third controls access to methodology objects. Access control decisions are made differently for each type of object.

3.2 Identification and Authentication

Primavera defines users in terms of security attributes comprising user identity and global profile, which contain authorizations corresponding to functions a role may perform. Primavera requires users to be identified before they can gain access to its capabilities. In the evaluated configuration, authentication of claimed identities is performed by an LDAP server in the IT environment.

3.3 Security Management

Primavera provides administrative users with the ability to manage access controls on projects, resources, and methodologies, and the security attributes associated with users. Administrative capabilities are granted by the privileges allocated to a user via a global profile associated with the user.

4 Assumptions

The following assumptions are identified in the ST:

Table 2 – Assumptions

Assumption Identifier	Assumption Description
A.LOCATE	The TOE will be located within controlled access facilities and connected to networks that are protected from external tampering by a network firewall, which will prevent unauthorized physical access and mitigate unauthorized network access.
A.ADMIN	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

4.1 Clarification of Scope

The Target of Evaluation (TOE) is Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1), henceforth referred to as Primavera.

The TOE is dependent on the correct operation of the components in the operational environment, which are not included within the scope of the evaluation. It should also be noted that the access control policies implemented by the TOE are enforced only on access attempts made through the TOE's interfaces. The TOE does not and cannot control attempts to access data directly (e.g., via the underlying database or operating system).

5 Architectural Information

Primavera is intended to be used to plan and control projects. Project data is stored in a central project management database that is located in the IT environment. The TOE provides the following specific capabilities.

- Project management—allows users to plan and control projects. Project management capabilities include centralized resource management, including resource timesheet approval and the ability to communicate with project resources via web-based timesheet interfaces

- Methodology management—allows users to author and store methodologies, which are also called project plan templates. Methodology management capabilities include providing the ability to define project management methodologies, which are called "best practices", and store them in a central methodology management database
- Timesheets—allows users to enter and track time in a timekeeping system. Team members use timesheets to enter information for assignments across projects, including recording time against a project.

The TOE restricts the ability to access it by requiring users to identify and authenticate themselves (although in the evaluated configuration, the authentication decision is made by an LDAP server in the TOE environment). Furthermore, it provides the capability of controlling access to user data through access control policies. Lastly, it provides administrators with the ability to administer security attributes to manage the security of the TOE.

The TOE comprises the following subsystems:

- Project Management subsystem—used to plan and control the projects, resources and methodologies defined within the TOE
- Timesheet subsystem—allows users to enter and track time in a timekeeping system
- Web Project Management subsystem—provides user interfaces to access project management and timesheet review/approval functions
- Integration subsystem—provides the user with Java language interfaces to the TOE's business rules and underlying database
- Database subsystem—provides an internal interface for interacting with the database in the IT environment, reducing network traffic and easing development effort.

The **Project Management** subsystem comprises the Project Management Client Module and the Methodology Management Client Module. These are "heavy" clients that execute as applications in user space in a Windows operating system environment. They use DbExpress in the IT environment to establish database connections to the centralized database (also in the IT environment). The Project Management Client Module loads all the projects that the user is authorized to access and enforces controls on the operations the user is authorized to perform on specific project data. Similarly, the Methodology Management Client Module loads all the methodologies the user is authorized to access and enforces controls on the operations the user is authorized to perform on specific methodology data. Additionally, both the Project Management and Methodology Management Client Module enforce restrictions on the security management capabilities available to users.

The Project Management and Methodology Management Client Modules are supported on Microsoft Windows XP SP3 and Windows Vista Business Edition, SP1.

The **Timesheet** subsystem comprises the Group Server and the Timesheet Java Application Module. The Group Server executes as a Windows Service on a Windows operating system and provides the server side component of the Timesheet subsystem. It manages resource security, data integrity and business rules. It connects to the centralized database using ActiveX Data Objects (ADO) in combination with Object Linking and Embedding, Database (OLEDB), both of which are in the IT environment. The Timesheet Java Application Module provides the end-user interface to the Timesheet subsystem and is used to enter time worked against particular tasks.

The Group Server is supported on Windows Server 2003 R2 (SP2) with Internet Information Services (IIS) v6.0. The Timesheet Java Application Module is supported on:

- Microsoft Internet Explorer 6 (SP3) on Microsoft Windows XP (SP3), Microsoft Internet Explorer 7 on Microsoft Windows Vista SP1 (Business Edition), or Firefox 3.0.3 on Ubuntu Linux 7.0.4
- Sun Java Runtime Environment (JRE) JRE 1.5.0_18 or JRE 1.6.0_14.

The **Web Project Management** subsystem comprises the P6 Web Access Application Server module and the Web Client module. The P6 Web Access Application Server module is the server-based business rule and security engine for the Web Project Management subsystem, providing browser-based access to project management and time approval functions. It is a Java application that is deployed on an application server (in the IT environment) and uses Java Database Connectivity (JDBC) (also in the IT environment) to connect to the centralized database. The Web Client module is the end-user browser-based interface to the Web Project Management subsystem. It comprises Java applets and HTML pages that are presented to the user in the context of a web browser (which is in the IT environment).

The P6 Web Access Application Server is supported on:

- Operating System / Web Server
    - Microsoft Windows Server 2003 R2 (SP2) with Internet Information Services v 6.0, or
    - Microsoft Windows Server 2008 (SP1) with Internet Information Services v 7.0
- Application Server
    - JBoss 4.0.5 with Sun Java 2 JDK 1.5.0_15, or
    - BEA WebLogic Express (ISV) 10 MP1 with Sun JDK 1.5.0_11, or
    - BEA WebLogic Enterprise Edition 10 MP1 with Sun Java 2 JDK 1.5.0_11, or
    - IBM WebSphere Application Server 6.1 fp17 with IBM Java 2 JDK 1.5.

The Web Client module is supported on Microsoft Internet Explorer 6 (SP3) on Microsoft Windows XP (SP3) or Microsoft Internet Explorer 7 on Microsoft Windows Vista SP1 (Business Edition). It also requires Sun Java Runtime Environment (JRE) JRE 1.5.0_18 or JRE 1.6.0_14.

The **Integration** subsystem comprises a single module, the Java Integration API module, which provides a Java programmatic interface to the objects and business rules exposed in the P6 Web Access Application Server module. The Java Integration API module in turn consists of client side and server side libraries. In the evaluated configuration, the client side modules can be installed on the end user’s local computer, while the server side libraries are to be installed on a remote, physically secure server. In this configuration, the Integration subsystem uses Java Remote Method Invocation (RMI) in the IT environment for communication between the client and server sides. As with the P6 Web Access Application Server module of the Web Project Management subsystem, the server side libraries use JDBC to connect to the centralized database.

The Java Integration API Module requires the Java Development Kit (JDK), version 1.5.x, also known as J2SE 5.0.

The **Database** subsystem comprises a single module, the Primavera Stored Procedures module, which provides mechanisms for automating database tasks, including: stored procedures that aggregate multiple database commands into atomic behaviors; triggers, indexes, and database integrity constraints; views; and relational table data and LOB data.

The Primavera database is supported on the following database servers:

- Microsoft SQL Server 2005 (SP2) on Windows Server 2003 R2 (SP2), or Windows 2008 Server (SP1) with Microsoft sqljdbc.jar driver: version 1.2.2828.100
- Oracle version 10.2.0.3 on Windows Server 2003 R2 (SP2) or Red Hat Enterprise Linux AS 5.0 with Oracle OJDBC5.jar driver: version 11.1.0.6.0
- Oracle version 11.1.0.6 on Windows Server 2003 R2 (SP2), or Windows 2008 Server (SP1), or Red Hat Enterprise Linux AS 5.0 with Oracle OJDBC5.jar driver: version 11.1.0.6.0

The TOE also requires an LDAP server in the operational environment to support user identification and authentication. The following LDAP servers are supported:

- Microsoft Active Directory on Windows Server 2003 R2 (SP2)
- SunOne Directory Server v.5.2 on Windows Server 2003 R2 (SP2)

6 Documentation

The guidance documentation examined during the course of the evaluation and therefore included in the TOE is as follows:

- Primavera P6 Administrator's Guide, Version 6.2.1
- P6 Methodology Management Reference Manual, Version 6.2.1
- Primavera P6 Project Management Reference Manual, Version 6.2.1
- Primavera P6 Integration API Administrator's Guide, Version 6.2.1
- P6 Web Access Help
- Primavera Timesheets Help
- Primavera Integration API Programmer's Reference
- Primavera Integration API Javadoc, Version 6.2.1
- Evaluated Configuration for Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1), Issue 1.0, July 2009.

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for Oracle Primavera Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1).

Evaluation team testing was conducted at the vendor's development site in November 2008, with follow-up testing occurring in February and April 2009.

7.1 Developer Testing

Primavera's approach to testing for Primavera P6 Version 6.2.1 is based on functional requirements testing. The vendor has developed a test suite comprising various automated and manual tests designed to demonstrate that the TSF satisfies the SFRs specified in the ST. The vendor has a comprehensive and highly automated test infrastructure and has specifically developed many new tests to provide a comprehensive demonstration the TOE satisfies its SFRs. These tests are now part of the standard product test suite.

The vendor addressed test depth by analyzing the functionalities addressed in the TOE design and associating test cases that cover the addressed functionalities. The TOE design addressed the general functions of the TOE subsystems and modules, identifying the security functionality of each subsystem and module as appropriate. The vendor test documentation maps specific tests and test steps to TSF subsystems and interfaces.

The vendor ran the TOE test suites in various configurations, consistent with the test environment described in the testing documentation, and provided the evaluation team with the actual results. The test configurations were representative of the components supported in the operational environment and the intended environment and method of use of the TOE. All tests passed.

7.2 Evaluation Team Independent Testing

The evaluation team executed a sample of the vendor test suite for Primavera per the evaluated configuration as described in the vendor's test documentation ("NIAP Test Configurations R3" spreadsheet).

The Test Configurations spreadsheet describes the following three testing configurations:

- "Balcony", comprises:
    - P6 Web Access Application Server running on WebSphere Application Server 6.1, on IBM AIX 5.3
    - Group Server running on Windows 2008 Server with IIS v7
    - Oracle 10.2.0.3, running on Red Hat AS 4.0
    - Heavy clients (PM, MM) running on:
        - Windows XP SP3
        - Windows Vista SP1
    - Timesheets client running JRE 1.6.0_07 and Internet Explorer 7
- "Havasupai", comprises:
    - P6 Web Access Application Server running on WebLogic 10, on Windows 2008
    - Group Server running on Windows 2008 Server with IIS v7
    - Oracle 11, running on Red Hat AS 5.0
    - Heavy clients (PM, MM) running on:
        - Windows XP SP3
        - Windows Vista SP1
    - Timesheets client running JRE 1.6.0_07 and Internet Explorer 7
- "Bright Angel", comprises:
    - P6 Web Access Application Server running on JBoss 4.05, on Windows 2008
    - Group Server running on Windows 2008 Server with IIS v7
    - SQL Server 2005 SP2, running on Windows 2008 Server

- Heavy clients (PM, MM) running on:
  - Windows XP SP3
  - Windows Vista SP1
- Timesheets client running JRE 1.5.0_15 and Internet Explorer 7

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The test environment described above was used with team generated test procedures and team analysis to determine the expected results.

The evaluation team performed the following additional functional tests:

- **Aggregation of Project Privileges**—Section 6.1.1 of the ST states that if a user is assigned, via multiple OBS assignments, to multiple nodes in the EPS hierarchy, an assignment at a lower node aggregates all of the user's permissions from higher nodes in the hierarchy. The evaluation team confirmed the TOE behaves as described in the ST
- **Global Profile**—the TOE documentation indicates a user must be assigned a global profile. The test demonstrated that it is not possible to create a user in either Project Management or Methodology Management without assigning the user a global profile
- **Security Management**—the evaluation team exercised security management capabilities of the TOE using only the operational guidance documentation for guidance. The evaluation team confirmed the security management functions are invoked and behave as described in the guidance documentation.
- **Security Attribute Management**—the evaluation team confirmed the restrictions on which roles can manage the security attributes used to enforce the TOE's access control policies behave as specified in the ST.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE or in components of the operational environment the TOE is reliant on for its security functionality. The evaluation team did not discover any open source vulnerabilities relating to the TOE. The evaluation team determined, through analysis of vulnerability descriptions and consideration of the intended environment and method of use of the TOE, that vulnerabilities reported in components in the operational environment have either had fixes published by the responsible vendor, or are not relevant to the TOE in its evaluated configuration.

In addition to the open source search, the evaluation team devised a set of penetration tests based on a focused search of the evaluation evidence. The evaluation team performed the following penetration tests on the TOE in the test environment:

- **Port Scan**—the evaluation team used a commercial vulnerability scanner to examine open ports on the server machine in the test environment, both before and after the P6 Web Access Application server and the Group Server were initialized. The evaluation team determined the TOE components did not open up any additional ports.
- **Login Bypass**—the evaluation team determined the TOE does not permit users accessing it via the Web Access client to gain access without first identifying and authenticating themselves.
- **LDAP Configuration**—the evaluation team confirmed that when LDAP is configured for authentication, attempting to add a user that is not found in the LDAP store will

result in an error message and the user will not be added. In addition, the evaluation team confirmed the P6 Web Application Server must be configured for the same authentication mode (LDAP in the evaluated configuration) as the Project Management client.

- **Separation of Project and Methodology Management User Spaces**—the evaluation team confirmed the TOE maintains separate user spaces for Project Management and Methodology Management databases and applications.
- **SSL Protection**—the evaluation team confirmed, using a commercial network analysis tool, that the TOE supports configuration of SSL in the IT environment to provide protection of TSF data communicated between separate TOE components.
- **Heavy Client Module Integrity**—the developer, in their design evidence, described various mechanisms that have been implemented to protect the integrity of the Project Management and Methodology Management client applications. The evaluation team confirmed the mechanisms operated as described.
- **User Privileges Granting and Revocation**—the evaluation team determined that changes to the privileges granted to users (which are made using the heavy client applications) are propagated to the user even when the user is currently logged on, though it is not possible to delete a user that has an active session.

The evaluation team, during the course of the evaluation and testing, also observed the measures the developer has taken to address potential cross-site scripting and SQL injection vulnerabilities in the TOE.

8 Evaluated Configuration

The evaluated version of the TOE is Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1).

Primavera is a project management product that is implemented using client/server architecture with a centralized project database. Primavera can be used to manage projects, resources, and methodologies. Resources can represent either people or materials, depending on how the project is defined. Methodologies are templates for defining new projects and can be used to codify an organization’s best practices.

9 Results of the Evaluation

The evaluation was conducted based upon version 3.1 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an EAL4 certificate rating be issued for Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1).

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table:

TOE Security Assurance Requirements

Assurance Component ID	**Assurance Component Name**
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.2	Testing: security enforcing modules
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.3	Focused vulnerability analysis

10 Validator Comments/Recommendations

Primavera is dependent on the correct operation of the TOE environment, which is not included within the scope of the evaluation. This includes the underlying operating system and database management system. It is important that these components be assessed when determining the overall system security posture.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1) Security Target**, Version 1.2.5, dated 6 July 2009.

13 Glossary

The following acronyms beyond those in the CC or CEM are supplied; however, no additional definitions are supplied:

- **JDK –** Java Development Kit
- **LDAP –** Lightweight Directory Access Protocol

14 Bibliography

URLs

- NIAP Common Criteria Evaluation and Validation Scheme (http://www.niap-ccevs.org/cc-scheme/)
- SAIC CCTL (http://www.saic.com/infosec/common-criteria/)
- Oracle Corporation (http://www.oracle.com/primavera/index.html)

NIAP CCEVS Documents:

- *Common Criteria for Information Technology Security Evaluatio*n, version 3.1, Revision 2, September 2007
- *Common Evaluation Methodology for Information Technology Security*, version 3.1, Revision 2, September 2007.

Other Documents:

- *Primavera*$^{®}$ *P6™ Enterprise Project Portfolio Management (Version 6.2.1) Security Target*, Version 1.2.5, 6 July 2009.