Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

HP OpenView Select Access v5.2

Certificate Number: 37/2006

March 2006

Version 1.0

Amendment Record

Version	Date	Description
1.0	17/03/2006	Public release.

Executive Summary

1 This report describes the findings of the IT security evaluation of Hewlett Packard's HP OpenView Select Access v5.2 to the Common Criteria (CC) evaluation assurance level EAL2. The report concludes that the product has met the target assurance level of EAL2 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by LogicaCMG and was completed in February 2006.

2 Select Access is a software package that provides user identity management and allows secure access to network services and enterprise resources through a web interface.

3 The Australasian Certification Authority (ACA) provides recommendations in this report that are specific to the secure use of Select Access. In addition, clarification of the scope of evaluation is provided and readers are informed of how to determine if Select Access is in its evaluated configuration.

4 Recommendations are provided on the following topics:

- Policy Validator cache clearing
- Denial of Service
- File System, and
- Single sign-on configuration.

5 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

6 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target (Ref [1]), and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

7 HP OpenView Select Access v5.2, the Target of Evaluation (TOE), is a software package that provides user identity management and allows secure access to network services and enterprise resources through a web interface. This report documents the Common Criteria (CC) evaluation and subsequent certification of the TOE.

1.2 Purpose

8 The purpose of this Certification Report is to:

a) document the certification of results of the IT security evaluation of the TOE, against the requirements of the CC evaluation assurance level EAL2, and

b) provide a source of detailed security information about the TOE for any interested parties.

9 This report should be read in conjunction with the TOE's Security Target (Ref [1]), which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

10 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.5.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	HP OpenView Select Access v5.2
Software Version	HP OpenView Select Access v5.2 with Engineering Patch G, HP Media Part Number T2593-15002.
Security Target	HP OpenView Select Access Security Target v3.0
Evaluation Level	EAL2
Evaluation Technical Report	HP OpenView Select Access v5.2 Evaluation Technical Report for Australasian Certification Authority. Issue 1.2, February 2006.
Criteria	CC Version 2.1, August 1999, with Final Interpretations to 6 November 2002.
Methodology	CEM-99/045 Version 1.0, August 1999, with Final Interpretations to 6 November 2002.
Conformance	CC Part 2 Conformant CC Part 3 Conformant
Sponsor	Hewlett Packard
Developer	Hewlett Packard
Evaluation Facility	LogicaCMG

Chapter 2 - Target of Evaluation

2.1 Description of the TOE

11 The TOE is an authorisation management solution that facilitates the administration and enforcement of user privileges and transaction entitlements to enterprise resources in a distributed environment; essentially providing a single sign-on capability across web-based applications and Web services.

12 When deployed, the TOE operates in a three-tiered architecture consisting of the directory server (policy store), Validator (policy decision server), and Enforcer (application plug-in). Logs are collected at a Security Audit Server. Administrators connect to the Administration Server using a web browser to run the Policy Builder, a java based GUI.

13 The Administrator and Delegated Administrators manage access and authorisation privileges using the Policy Builder. The Enforcer intercepts requests for access to network resources, querying the Validator to see if a given access or command is authorised. The Validator retrieves the relevant policy data from the directory server, evaluates the logic based on the information passed from the Enforcer, and returns the authorisation decision. The Enforcer then enforces the decision.

14 The TOE integrates with Sun iPlanet 4.1 or Microsoft IIS 5.0 web servers, and J2EE compliant application servers. The TOE policies are stored and accessed directly using LDAP to a range of directory servers.

2.2 TOE Architecture

15 The TOE consists of the following major architectural components:

a) **Policy Builder:** a Java based browser applet that is served by the Administration Server. It is a management GUI that allows administrators to create and manage access and authorisation privileges.

b) **Administration Server:** provides central co-ordination of the TOE, providing the following administrative functionality:

   i) Web server to facilitate access to the Policy Builder,

   ii) Management of SSL connections between Select Access components,

   iii) Management of policy data.

c) **Enforcer:** a plug-in on the web server that manages access to network resources, the enforcer queries (XML query) the Policy Validator with user access requests and enforces the subsequent

validation decision. A network resource is a URL local to the web server or an application server accessed through the web server. The Enforcer also provides an authentication interface to enable users to authenticate when necessary.

d) **Validator:** determines if access to a resource is permitted. It reads policy data from the LDAP policy store in order to make access decisions as requested by the Enforcer component(s).

e) **Secure Audit Server:** provides a consolidated audit trail. All Select Access components send audit entries to the Secure Audit Server, which can output the log data to multiple destinations and audit stores.

2.3 Clarification of Scope

16 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.3.1 Evaluated Functionality

17 The TOE provides the following evaluated security functionality:

a) **Validation of access requests:** The TOE provides a policy validation and authorisation function through the Validator component.

b) **Enforcement of access control:** The TOE provides a policy enforcement function through the Enforcer component.

c) **Authentication of users:** The TOE provides support for authenticating users requesting access to resources using methods including passwords and X.509 certificates.

d) **Native password management:** The TOE provides facilities for the enforcement of password policies based on specified password attributes, changing of password at regular intervals and locking of accounts that have been the subject of suspicious activity.

e) **Policy definition:** The TOE provides a Java-based GUI to define authorisation policies for users and resources.

f) **Delegation of policy-based administrative functions:** The TOE allows the Administrator to delegate administration of authorisation policy to another trusted individual, a Delegated Administrator.

g) **Secure audit collection and storage:** The TOE provides a consolidated security audit trail via the Secure Audit Server. The level of logging can be configured by the Administrator both specifically for each TOE component, as well as at the Secure Audit Server for the whole TOE.

h) **Reporting of audit data:** The TOE provides a Reporting Engine which enables the definition of detailed reporting procedures commensurate with operational and audit policies. Audit data are verified by the Reporting Engine on the bases of the digital signatures of the audit records.

i) **Alerting to audit events:** The TOE provides the ability to set custom audit alert based on authorisation information, level of severity of the alert and the alert handling instruction.

j) **Secure communications between distributed components:** The TOE implements a secure subset of both the SSL v3.0 and TLS v1.0 protocols.

TLS connections between TOE components use Ephemeral Diffie-Hellman key exchange, including RSA keys of at least 1024 bits and AES keys of 256 bits to provide confidentiality of data transmitted between components and authentication of the components.

SSL connections between the Administration Server and administrator browsers use RSA key exchange, including RSA keys and 3DES keys to provide confidentiality of TOE administration data.

2.3.2 Non-evaluated Functionality

18 Potential users of the TOE are advised that a set of functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration. The functions and services that have not been included as part of the evaluation are provided below:

a) The LDAP directory server;

b) The Web server or J2EE application server protected by the Enforcer component;

c) Audit storage device; e.g. NT event log or flat file;

d) Select Access APIs for expanding or further tailoring the product;

e) Application, portal and wireless support;

f) User self-registration;

g) Storage of audit information other than as controlled by the Secure Audit Server;

h) Authentication methods other than passwords and X.509 certificates;

i) Data replication between redundant distributed components;

j) High availability functions;

k) User profile self management;

l) Security Assertion Markup Language (SAML); and

m) Any functions of SSL or TLS other than those implementing SSL v3.0/TLS v1.0 ciphersuites:

i) "SSL_RSA_WITH_3DES_EDE_CBC_SHA" (i.e. algorithms other than 3DES and RSA, or key lengths less than 128 bits); or

ii) "TLS_DHE_RSA_WITH_AES256_CBC_SHA" (i.e. algorithms other than AES and RSA, or key lengths other than 265 bits).

2.4 Security Policy

19 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TSP is defined in the Security Target (Ref [1]). A summary of the TSP is provided below:

a) **Identification and Authentication:** The TOE will provide the means to support authentication of individuals using multiple authentication mechanisms before granting access to IT resources protected by the TOE.

b) **Cryptographic Support:** The TOE will provide the means to protect the confidentiality and integrity of data when transmitted between components of the TOE.

c) **Data Protection:** The TOE will provide the means to grant or deny access to individuals or groups of individuals to IT resources protected by the TOE.

d) **Security Management:** The TOE will provide the means to enable the Administrator to effectively manage the TOE and its security functions. Further, the TOE will enable the delegation of subsets of administrative functions.

e) **Audit:** The TOE will provide the means of recording any security relevant events so as to assist an Administrator in the detection of potential attacks or misconfiguration of the TOE security functions. The TOE shall protect audit records from unauthorised deletion and provide a mechanism to detect modifications to audit records.

f) **Self Protection:** The TOE will provide the means to ensure that access to the IT resources protected by the TOE is not granted in the event of a failure of a Validator or Enforcer.

2.5 Usage

2.5.1 Evaluated Configuration

20 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configuration(s).

21 The TOE is implemented entirely in software, comprised of the following components:

a) **Policy Builder and Administration Server:** This component is only supported on the Windows platform. There can only be one Administration Server in a Select Access system.

b) **Validator:** The Select Access Validator is supported on both the Windows and UNIX platforms. There may be multiple Validators in a Select Access system.

c) **Enforcer:** The Select Access enforcer is a plug-in to the Web server that provides access to protected resources. It is implemented in an Internet Server API (ISAPI) filter for Microsoft IIS 5.0 on the Windows platform and as a Netscape Server API (NSAPI) for the iPlanet Web Server 4.1 on the UNIX platform.

d) **Secure Audit Server:** The Select Access Audit Server is supported on both the Windows and UNIX platforms.

22 None of the components of the TOE are implemented in hardware.

23 The minimum requirements for the Windows platform are:

a) Operating System:

i) Windows 2000 Server with SP2 or higher

b) Hardware:

i) Intel Pentium 4, 1.2 GHz processor

ii) 256 MB RAM

24 The minimum specifications for the UNIX platform are:

a) Operating system:

i) Solaris 8 (2.8) patch 108940-07 or higher

b) Hardware:

i) 440 MHz UltraSPARC-III

ii) 2 MB cache

iii) 512 MB RAM

2.5.2 Determining the Evaluated Configuration

25 An administrator can determine that they are running the evaluated version of the TOE by performing the following steps for the different TOE components:

a) Checking the contents of the version.txt file, which is installed in the base installation directory of a host that the product is installed on. This gives the major version (v5.2) and applies for both Windows and Solaris installations.

b) Checking the properties of the enforcer32.dll and IISPlugin32.dll files (by right clicking on them and selecting "Properties"). On the version tab in the window that appears, the File Version for these files will be 5.2.0.323. These files are only installed on Windows, and as such, there is no equivalent check required for Solaris platforms.

26 The administrator should also confirm that Select Access is configured to use the services and functions included within the scope of evaluation, and should carefully consider the configuration settings related to non-evaluated functionality.

2.5.3 Delivery procedures

27 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated version of Select Access.

28 When the TOE is received, the user should check to ensure that the tamper evident sticker on the CD-ROM slipcover shows no signs of tampering.

29 Users should also confirm that the CR-ROM is labelled with Barcode and Media Part Number and Product Revision: T2593-15002 Rev 5.2.

30 To gain further confidence of the integrity of the delivered TOE, a user may cross reference the contents of the CR-ROM with Appendix A ‘Delivery CD-ROM Contents’ of the Security Target (Ref [1]).

2.5.4 Documentation

31 It is important that the TOE is used in accordance with guidance documentation. The following documentation is available upon request from the developer:

a) HP OpenView Select Access Version 5.2 Installation Guide (Ref [2]),

b) HP OpenView Select Access Version 5.2 Network Integration Guide (Ref [3]),

c) HP OpenView Select Access Version 5.2 Policy Builder Guide (Ref [4]),

d) HP OpenView Select Access Version 5.2 Developer's Guide (Ref [5]),

e) HP OpenView Select Access Version 5.2 Release Notes (Ref [6]).

2.5.5 Secure Usage

32 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

33 The following assumptions were made:

a) The Administrator will follow all policies and procedures described in the TOE system documentation to ensure secure administration of the TOE. Those delegated with administrative functions will follow all policies and procedures in the TOE systems documentation applicable for their delegated responsibilities to ensure secure administration of the TOE.

b) The Administrator, and those delegated with administrative functions, is assumed to be non-hostile and trusted to perform all their duties in a competent manner.

c) The TOE will be used for authorising and authenticating users for granting or denying access to IT resources protected by the TOE, e.g. Web Pages.

d) It is assumed that strong physical security measures will be in place to prevent unauthorised physical access to all components of the TOE.

e) It is assumed that the TOE will be installed in a network that provides appropriate logical protection, against access or modification, to all components of the TOE.

f) It is assumed that there exists an appropriate means of securely generating, distributing and managing good TOE user authentication credentials, for example operating the TOE within a securely managed PKI.

Chapter 3 - Evaluation

3.1 Evaluation Procedures

34 The criteria against which the Target of Evaluation (TOE) has been evaluated are expressed in the Common Criteria for Information Technology Security Evaluation (Ref [7], [8],[9]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [10]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [11], [12]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [13]) were also upheld.

3.2 Functional Testing

35 The developers approach to functional testing of the TOE included both positive and negative tests of the TOE Security Functions. All security functions described in the Security Target (Ref [1]) were tested. The evaluators repeated all of the developer's tests, only having to perform one independent test to investigate the operation of the password policy feature more extensively than done by the developer. All test results were as expected.

36 All testing was performed in a Microsoft Windows environment, using IIS 5.0.

3.3 Penetration Testing

37 The evaluators devised multiple penetration tests based on the developer vulnerability analysis. The vulnerability analysis identified obvious security vulnerabilities and demonstrated that they cannot be exploited in the intended environment for the TOE. The evaluators assessed the vulnerability analysis, performing tests where necessary to ensure that obvious vulnerabilities have been addressed. The evaluators concluded that there are no exploitable vulnerabilities in the TOE, within the context of the intended environment.

38 The evaluators identified multiple residual vulnerabilities in the TOE that are not exploitable in the TOE's intended environment, these are:

a) brute-force attacks on password mechanisms,

b) Enforcer plug-in bypass attacks,

c) brute-force and man-in-the-middle attacks on encrypted channels,

d) public SSL vulnerabilities,

e) LDAP implementation vulnerabilities,

f) start-up file modification,

g) IIS directory traversal with Unicode.

Chapter 4 - Certification

4.1 Certification Result

39 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [14]), the Australasian Certification Authority certifies the evaluation of HP OpenView Select Access v5.2 performed by the Australasian Information Security Evaluation Facility, LogicaCMG.

40 LogicaCMG has found that HP OpenView Select Access v5.2 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria evaluation assurance level EAL2.

41 Certification is not a guarantee of freedom from security vulnerabilities; there is a small probability that exploitable vulnerabilities remain undiscovered.

4.2 Assurance Level Information

42 EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

43 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

44 EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

4.3 Recommendations

4.3.1 Policy Validator Cache

45 Administrators should clear the Policy Validator's data cache subsequent to altering user privileges or performing other security relevant policy changes. This is described in Chapter 14 of the Policy Builder Guide (Ref [4]).

4.3.2 Denial of Service

46 Administrators should note that the Security Target does not claim the ability to counter any external threats to the availability of the TOE; therefore the TOE has not been evaluated with regards to resistance to denial of service attacks. Whilst the developers have made every effort to counter known vulnerabilities which could result in a denial of service to legitimate users, administrators should be aware that vulnerabilities of this nature may still be exploitable in the intended environment for the TOE.

4.3.3 File System

47 It is recommended that the NTFS file system be used where components are installed on Microsoft platforms.

4.3.4 Single Sign-on Configuration

48 When enabling single sign-on with cookies, administrators should ensure sessions are protected by SSL.

Annex A - References and Abbreviations

A.1 References

[1] HP OpenView Select Access Security Target, Version 3.0, BeTrusted, February 2006.

[2] HP OpenView Select Access Version 5.2 Installation Guide, Hewlett Packard, February 2004.

[3] HP OpenView Select Access Version 5.2 Network Integration Guide, Hewlett Packard, October 2003.

[4] HP OpenView Select Access Version 5.2 Policy Builder Guide, Hewlett Packard, February 2004.

[5] HP OpenView Select Access Version 5.2 Developer's Guide, Hewlett Packard, October 2003.

[6] HP OpenView Select Access Version 5.2 Release Notes, Hewlett Packard, October 2003.

[7] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, Incorporated with interpretations as of 2003-12-31

[8] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, Incorporate with interpretations as of 2003-12-31

[9] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, Incorporate with interpretations as of 2003-12-31

[10] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, Incorporated with interpretations as of 2003-12-31

[11] AISEP Publication No. 1 – Description of the AISEP, AP 1, Version 2.0, February 2001, Defence Signals Directorate.

[12] AISEP Publication No. 2 – The Licensing of the AISEFs, AP 2. Version 2.1, February 2001, Defence Signals Directorate.

[13] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[14] HP OpenView Select Access v5.2 Evaluation Technical Report for Australasian Certification Authority. Issue 1.2, February 2006.

A.2 Abbreviations

ACA	Australasian Certification Authority
AES	Advanced Encryption Standard
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HP	Hewlett-Packard
IIS	Microsoft Internet Information Services web server
ISAPI	Internet Server Application Programming Interface
IT	Information Technology
J2EE	Java 2 Platform, Enterprise Edition
LDAP	Lightweight Directory Access Protocol
NSAPI	Netscape Server Application Programming Interface
NT	Microsoft Windows NT operating system
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, and Adelman
SAML	Security Assertions Markup Language
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSP	TOE Security Policy
URL	Uniform Resource Locator
XML	Extensible Markup Language