National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Hewlett-Packard

OpenView Operations™ for UNIX V A.08.10 with patches:

PHSS_32820 (OVO management server on HP-UX 11.11)

ITOSOL_00403 (OVO management server on Solaris 9)

Report Number: CCEVS-VR-05-0114
Dated: 19 August 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

Executive Summary

This report documents the National Information Assurance Partnership (NIAP) Validator's assessment of the Common Criteria Evaluation and Validation Scheme (CCEVS) evaluation of the Hewlett Packard (HP) OpenView Operations for UNIX version A.08.10 with patches: PHSS_32820 (OVO management server on HP-UX 11.11) and ITOSOL_00403 (OVO management server on Solaris 9) (OVO/UNIX or just short OVO).

The evaluation for OVO/UNIX was performed by CygnaCom in the United States and was completed on 19 August 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2, Evaluation Assurance Level 2 (EAL2), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Part 2, Version 2.2.

The Target of Evaluation (TOE) is software-only and includes the OVO/UNIX Management Server, OVO HTTPS Agent, Command Line Interfaces on the OVO/UNIX management server and OVO HTTPS Agent, OVO Motif Admin GUI, and OVO Java GUI.

Components that are outside of this evaluation include: HP Network Node Manager (NNM), OVO Distributed Computing Environment (DCE) server components (the OVO DCE server components will be configured to not be accessible remotely and the OVO DCE Agent components will not be used), the underlying operating system (OS) software and hardware, the third party relational database, the PAM client software and corresponding authentication software, and the third-party encryption software (i.e., OpenSSL) that is used to provide a trusted communication path between users and the TOE. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

OVO/UNIX provides the following six security features for the TOE. These are described in Section 3 of this report:

1. Security Audit
2. Access Control
3. User Identification and Authentication (I&A)
4. System Identification and Authentication
5. Security Management
6. Partial Protection of the TOE Security Functions

CygnaCom is an approved NIAP Common Criteria Testing Laboratory (CCTL). The CCTL concluded that the Common Criteria assurance requirements for Evaluation Assurance Level 2 (EAL2) have been met and that the conclusions in its Evaluation Technical Report are consistent with the evidence produced.

This Validation Report is not an endorsement of the OVO/UNIX by any agency of the US Government and no warranty of the product is either expressed or implied.

Table ES-1 provides the required evaluation identification details.

Table ES-1. Evaluation Details

Item	Description
Evaluation Scheme	US Common Criteria Evaluation and Validation Scheme (CCEVS)
Target of Evaluation	HP OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO management server on HP-UX 11.11) and ITOSOL_00403 (OVO management server on Solaris 9)
EAL	EAL2
Protection Profile	N/A
Security Target	HP OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO management server on HP-UX 11.11) and ITOSOL_00403 (OVO management server on Solaris 9), Security Target v1.10, 18 August 2005.
Developer	Hewlett-Packard Development Company, L.P, Fort Collins, CO
Evaluators	CygnaCom Solutions - Common Criteria Testing Laboratory 7925 Jones Branch Drive, Suite 5200 West McLean, VA 22102-3321
Validator	Catalina M. Gomolka Mitretek Systems, Inc., Falls Church, VA
Dates of Evaluation	June 2004 to 19 August 2005
Conformance Result	Part 2 extended, Part 3 conformant, and EAL2 conformant
Common Criteria (CC) Version	Part 1: Introduction and General Model, Version 2.2, January 2004, CCIMB-2004-01-001 Part 2: Security Functional Requirements, Version 2.2, January 2004, CCIMB-2004-01-002 Part 3: Security Assurance Requirements, Version 2.2, January 2004, CCIMB-2004-01-003
Common Evaluation Methodology (CEM) Version	Part 1: Introduction and general model, CEM-97/017, Version 0.6, 97/01/11 Part 2: Evaluation Methodology, CEM-2004-01-004, Version 2.2, January 2004 Supplement: ALC_FLR - Flaw Remediation, CEM-2001/0015, Version 1.0, August 2001
Evaluation Technical Report	Hewlett - Packard OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO mgmt sv on HP-UX 11.11) ITOSOL_00403 (OVO mgmt sv on Solaris 9) ETR Version 1.0, Date Aug 18, 2005

Table of Contents

Table of Tables and Figures

Table of Figures

1 Identification of the TOE

HP OpenView Operations for UNIX is a distributed client-server software solution designed to help system administrators detect, solve, and prevent problems occurring in networks, systems, and applications in any enterprise. With HP OpenView Operations for UNIX, administrators have the capability to continuously monitor heterogeneous environments (i.e., networks, systems, and applications) providing the ability to increase availability and performance.

In the remainder of this document:

- references to "OVO" or "OVO/UNIX" should be understood as referring to the TOE: HP OVO OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO management server on HP-UX 11.11) and ITOSOL_00403 (OVO management server on Solaris 9)

The OVO management concept is based on communication between a management server and managed nodes. OVO/UNIX management server processes running on the central system communicate with OVO agent processes running on managed nodes throughout the environment. The OVO agent processes collect and process events on the managed nodes, then forward relevant information in the form of OVO messages to the OVO/UNIX management server. The OVO/UNIX management server responds with actions to prevent or correct problems on the managed nodes. The OVO/UNIX management server is the central computer to which all managed nodes forward their messages. Multiple management servers may share management responsibility.

Managed nodes are monitored and controlled by the OVO/UNIX management server. Events are occurrences on the managed nodes. Events trigger messages. The OVO HTTPS agent on the OVO/UNIX management server also serves as the local managed node. Communication between the managed nodes and the OVO/UNIX management servers consists of messages, actions, and configuration changes.

The following are the TOE components that comprise HP OpenView Operations for UNIX:

- OVO/UNIX Management Server,
- OVO HTTPS Agent,
- Command Line Interface on the OVO/UNIX Management Server,
- Command Line Interface on the OVO HTTPS Agent,
- Administrator (OVO Motif Admin GUI) User Interface, and
- Operator (OVO Java GUI) User Interface.

In addition to the above-mentioned components, OVO is also comprised of a set of components that are NOT included in the TOE. These are:

- Third party relational database,

- The Network Node Manager,
- The DCE runtime on the OVO management server and OVO DCE agent components,
- Operational Motif UI,
- Cryptographic Support, and
- Pluggable Authentication Module (PAM).

2 Interpretations

The Evaluation Team performed an analysis of the international and national interpretations of the CC and the CEM and determined that no interpretations applied to this evaluation.

3 Security Policy

The TOE provides the following six security features:

1. Security Audit
2. Access Control
3. User Identification and Authentication
4. System Identification and Authentication
5. Security Management
6. Partial Protection of the TOE Security Functions

3.1 Security Audit

HP OpenView Operations for UNIX provides its own auditing capabilities separate from those of the Operating System. HP OVO relies on the operating system to supply the UNIX User Identification of the TOE user. HP OVO uses the UNIX user's identification, such as the user 'root', to supplement its own audit information to further delineate the subject that causes an auditable event. Audit logs are stored within a relational database, which is not part of the TOE.

3.2 Access Control

HP OpenView Operations for UNIX provides its own access control, separate from the Operating System, for the user login attempts into the OVO Motif Admin GUI and OVO Java GUI. This is covered by the HP OpenView Operations Access Control Policy (ACP). HP OVO/UNIX relies on the underling OS to enforce the operating system's access control policy to restrict execution of the OVO CLIs to the UNIX user root (Windows user a*dministrator*).

Table 3-1 identifies the different roles and their management functions.

Table 3-1. Management Functions per User Role

Roles	Allowed Operations on TSF Data (Management Functions)
OVO Administrator (opc_adm)	The Administrator is allowed all responsibilities of Template Administrator and Operator. In addition the OVO Administrator can: • Review and download the audit logs • Change audit level • Configure the System Settings • Query, add, modify, or delete scheduled actions and applications • Setup notification and trouble ticket services • Grant and revoke certificate requests for OVO HTTPS Agent • Install / update software and configuration on OVO HTTPS Agent • Up- / download the OVO HTTPS agent configuration data • Download the OVO server configuration data • Download the OVO message history • Download and sign the OVO templates • Configure Service hours • Start and stop agent processes • Start and stop server processes • Execute reports • Query, add, modify, and delete templates and template groups; assign and distribute template and template groups to OVO HTTPS agents • Define and implement the message policy • Query, add, modify, copy, and delete conditions • Change the sequence of conditions • Query, add, modify, or delete automatic or operator-initiated action
Template Administrator	The Template Administrator can: • Query, add, modify, and delete templates, template groups, and monitors • Define and implement the message policy • Query, add, modify, copy, and delete conditions • Change the sequence of the conditions • Query, add, modify, or delete automatic or operator-initiated action
Operator	The Operator can: • Start / stop automatic or operator-initiated actions of OVO messages and services • Query and modify message attributes (change severity, message text, or custom message attribute (CMA)) • Query, own/disown, annotate, acknowledge, escalate, and unacknowledged messages • Start and customized start of applications • Unbuffering of pending messages, which have been arrived outside the configured service hours

3.3 User Identification and Authentication

HP OpenView Operations for UNIX provides user identification and authentication of the OVO Motif Admin GUI and OVO Java GUI through the use of user accounts and the enforcement of password policies using the Pluggable Authentication Module (PAM) interfaces. As mentioned in Section 1, PAM is not part of the TOE.

3.4 System Identification and Authentication

HP OpenView Operations for UNIX uses certificates for the OVO/UNIX management server and HTTPS agents to identify and authorize appropriate activities - such as configuration deployment from the OVO/UNIX management server to the OVO HTTPS agent, remote action execution, application launches, etc.

3.5 Security Management

HP OpenView Operations for UNIX provides security management through the use of the OVO Motif Admin GUI and CLIs. The enforcement of the OVO/UNIX ACP restricts the ability to manage various security attributes and TSF data to the OVO Administrator using the administrator interface. On the OVO/UNIX management server, normally a dedicated system to just run the OpenView suite, the Operating System user "*root*" is a privileged user able to perform OVO administrative management tasks, such as policy configuration, certificate management, and start/stop OVO, via CLIs. On the OVO/UNIX agent the Operating System user "*administrator*" is a privileged user able to perform OVO administrative tasks, such as stop/start OVO agent, via CLIs.

3.6 Partial Protection of the TOE Security Functions

HP OpenView Operations for UNIX protects its programs and data from unauthorized access through its own interfaces. For example, the local HTTPS agent configuration has a digital signature, OVO messages sent from the OVO HTTPS agent to the OVO/UNIX management server are encrypted, actions are signed, etc.

4 Assumptions and Clarification of Scope

This section describes the security aspects of the environment in which OVO is expected to operate.

4.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of OVO. Table 4-1 identifies the specific conditions that are assumed to exist in an environment where OVO is employed.

Table 4-1. Assumptions

1	A.AdmTra	Administrators and operators are non-hostile, appropriately trained and follow all administrative guidance, including guidance on setting passwords. However, administrators and operators are capable of error.
2	A.Crypto	The TOE relies upon the IT environment to provide cryptographic functionality.
3	A.Database	The TOE relies upon a database in the IT environment to store TSF data.
4	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the OVO/UNIX management server host.

5	A.OS	The TOE relies upon the OS to provide file protection and OS user authentication.
6	A.Physical	Physical protection is assumed to be provided by the environment. The TOE hardware and software critical to the security policy enforcement will be protected from unauthorized physical modification. This also includes a trusted environment between the OVO Motif UI and the OVO/UNIX management server - assuming the OVO Motif Admin GUI is redirected to another display station using X redirection.
7	A.Time	It is assumed that the underlying operating system provides reliable time stamps.
8	A.Users	It is assumed that users will protect their authentication data.
9	A.Admin	It is assumed that the OVO Administrator is also a *root* system administrator on the OS underlying the OVO/UNIX management server.

4.2 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product. The TOE will counter the threats to security identified in Table 4-2.

Table 4-2. Threats

1	T.Abuse	An undetected compromise of the TOE may occur as a result of an authorized user of the TOE performing actions the individual is authorized to perform.
2	T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF.
3	T.Mismgmt	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
4	T.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
5	T.Tamper	An attacker may attempt to modify TSF programs and data.
6	T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users.
7	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

5 Architectural Information

The TOE components that comprise HP OpenView Operations for UNIX are: the OVO/UNIX Management Server, OVO HTTPS Agent, Administrator User Interface, Operator User Interfaces, and Command Line Interfaces on the OVO/UNIX Management Server and OVO HTTPS Agent.

Figure 5-1 displays a high-level diagram of the physical TOE boundary as described by the TOE components. All shaded objects are part of the TOE (i.e., OVO Data Store is not part of the TOE).

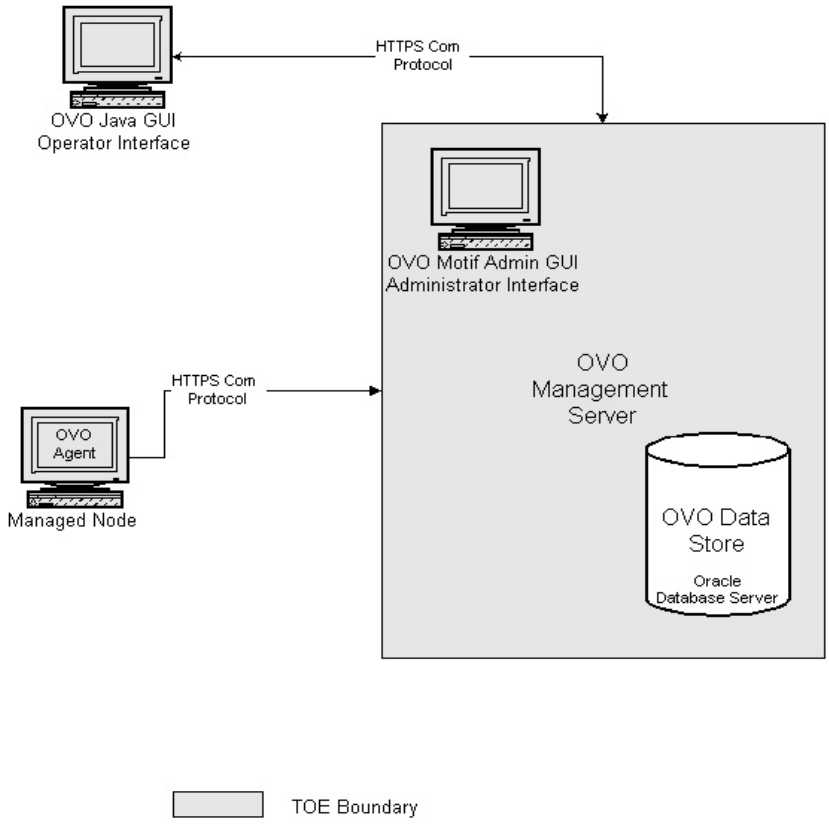

Figure 5-1. HP OpenView Operations for UNIX – Physical TOE Boundary

In addition, OVO is also made up of a set of components that are NOT included in the TOE. These components are:

- The Network Node Manager,
- Third party relational database,
- Pluggable Authentication Module,
- Cryptographic support,
- The DCE runtime on the OVO management server and OVO DCE agent components, and
- Operational Motif UI.

5.1 TOE Components

5.1.1 OVO/UNIX Management Server

The OVO/UNIX management server performs the central processing functions of OVO. The entire software package, including the complete application configuration, is stored on the OVO/UNIX management server. The OVO/UNIX management server does the following:

- **Collects Data:** Collects data from managed nodes, where the OVO agents are installed.
- **Manages Messages:** Manages and groups messages. Managing includes filtering, event correlation, event enrichment, forwarding the messages to trouble ticket systems and/or to notification services, etc.
- **Manages Actions:** Calls the appropriate OVO agent to:

  • *Start actions:* Start remote automatic actions on the managed nodes according to the defined action security setup.
  • *Initiate sessions/Launch Applications:* Initiate sessions on managed nodes (for example, open a virtual console, execute a script or program) triggered by the OVO administrator and/or OVO operator.
- **Manages Audit Trail and History:** Controls the history database for messages and performed actions.
- **Forwards Messages:** Forwards messages to other OVO/UNIX management servers.
- **Deploys OVO Agent Software & Configuration:** Deploys OVO agent software on managed nodes. The OVO/UNIX management server also notifies the managed nodes about configuration changes and initiates any updates. The OVO agent software can also be manually installed directly on the remote managed nodes.
- **Configuring Nodes:** The OVO environment can be composed of different types of managed nodes (e.g., nodes marked controlled, monitored, message-allowed, or disabled). Nodes can be managed by setting a range of IP addresses or hostname patterns. This allows all nodes to become automatically known and be immediately managed by OVO when they become part of a specific network or are added manually.

5.1.2 OVO HTTPS Agent

The OVO Agent is the client software that collects and processes events on the managed nodes, then forwards relevant information in the form of OVO messages to the OVO/UNIX management server. The OVO HTTPS agent uses HTTP with OpenSSL-based encryption for communication with the OVO/UNIX Management Server system. This enables encryption, as well as authentication & authorization. The encryption utilized is outside the TOE Boundary and has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation

5.1.3 OVO Administrator User Interface

HP OpenView Operations for UNIX has a Motif based graphical user interface through which most of the HP OVO/UNIX functions are managed (some management functions are only capable of being executed via the CLIs).

Within the OVO Motif Admin GUI, the OVO Administrator (opc_adm) has many tasks and responsibilities, such as:

- **Configure and maintain the managed environment:** Defines which systems and applications of the IT environment should be monitored by OVO; deploys the OVO agent software and appropriate configuration (templates / policies); and, maintains and fine tunes the monitored environment (e.g., deploying software updates, adding automatic corrective actions for standard problem scenarios, etc).
- **Customizes user environments:** Defines a custom environment for each user and manages all installation, configuration, and customization adaptations. These adaptations to the system add or change operators, template administrators, nodes, retrieved messages, and so on.
- **Delegates responsibility:** Defines responsibility and capability sets and decides which tools the operator needs to maintain the assigned nodes and perform the required tasks.
- **Develops guidelines:** Develops the guidelines template administrators use to implement a message policy. The administrator defines each template administrator's responsibility for templates or template groups.
- **Maintains audit trail and history data:** Maintains and reviews the OVO/UNIX audit trail and OVO/UNIX message history data. This history tracking enables the administrator to intelligently modify or develop automatic and operator-initiated actions, provide specific event instructions, and tracks recurring problems. For example, reviewing history data would reveal which nodes have consistently high disk space use.

5.1.4 Operator User Interface

The OVO operators use the OVO Java GUI to carry out their assigned tasks. Every operator's environment consists of a set of managed nodes. These nodes are the basis for daily operator tasks, such as application startups. The nodes also provide information operators use to solve problems. OVO operators have customized views of their own managed environments. For example, one operator might be responsible for all nodes at a facility. Another operator might be responsible for a subset of nodes at another facility just for the backup purposes. By creating task-orientated

environments, OVO operators see only the information from systems and objects under their control.

5.1.5 Command Line Interface

Command line interfaces are included on the OVO/UNIX management server. These CLIs are only available for the "root" user to perform TOE security management actions. HP OpenView relies on the Operating System to provide identification and authentication of the "root" user before being allowed to manage TOE functions through the CLI. The Operating System's Access Control Policy controls the access that the "root" user has in executing commands. The CLIs are implemented to provide the following functionality:

- **Installation and initial configuration of the OVO/UNIX Management Server:** CLIs are used for the initial installation of the OVO/UNIX Management Server application; including database setup, licensing and fundamental customer environment specific configuration, etc.

- **Customization and ongoing maintenance of managed IT environment:** These adaptations add or change nodes or node groups; assign or de-assign templates or template groups; sync configuration data with other OVO/UNIX management servers; define OVO message forwarding policies to other OVO/UNIX management servers; and define OVO message outage conditions, remote action execution settings, changes of IP addresses / hostnames and so on. Maintenance of remote OVO agents include procedures such as: start and stop of agent processes, query or modification of remote OVO agent configuration, deployment of agent software, etc.

- **Customization of user environment and service navigator configuration:** Used for creating adaptations to the environment for each user. These adaptations to the system add or change the user and user profiles, assign responsibilities (node groups, message groups, applications) and associated capabilities (e.g. acknowledge OVO messages) – using *opccfgupld*. Assigning and de-assigning of Service Views to operators are done by using the *opcservice* CLI.

- **Download and upload of audit trail, history data, and configuration:** Allows uploading and downloading of user OVO/UNIX audit data, OVO/UNIX history messages, and OVO/UNIX configuration data.

- **Certificate management:** Maintenance of the OVO HTTPS Agent certificates like creation of certificates, mapping, and granting of certificate requests. There is a manual and automatic capability of distributing certificates. The automatic distribution capability is NOT included in the TOE.

- **Start/Stop, troubleshooting:** Allows to start/stop the OVO/UNIX management server related processes, tracing of OVO/UNIX processes, runs troubleshooting tools, etc.

5.2 Supporting Environment and Non-TOE Components

It is assumed that there will be no untrusted users or software on the HP OpenView Operations for UNIX management server, since it's normally a dedicated system. The TOE environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

The following subsections describe the principal environmental components that support OVO/UNIX but are NOT included in the TOE boundary.

5.2.1 Operating System

OVO/UNIX relies on the operating system to provide the following:

- Reliable time stamps,
- The UNIX user identification (OS must have I&A) for the use in the OVO/UNIX audit trail,
- Protection of the HP OpenView Operations for UNIX management server from other interference or tampering, and
- Access control to only allow the UNIX system administrator, 'root' user, the ability to execute the OVO command line interface executables to perform TOE security management actions.

The operating systems tested for the server component are: HP-UX 11.11 and Solaris 9. The operating systems tested for the HTTP agent component are: HP-UX 11.11, Solaris 9, Red Hat Linux AS3U4, Windows 2003 server SP1. The operating system tested for the Java UI was Windows XP Pro SP2.

5.2.2 Network Node Manager

The Network Node Manager Version 7.5 product is only required on the OVO/UNIX management server. Neither the OVO agent nor Java UI client systems use the NNM product.

The following are the NNM pieces that are mandatory on the OVO/UNIX Management Server:

- The OVO/UNIX Motif UIs use the NNM Motif libraries and corresponding integration means.
- The OVO/UNIX Motif UI registers itself as NNM, requiring NNM processes to run in order to start up the OVO/UNIX management server (e.g. *ovwdb*, *ovspmd*, *ovdbrun* and *ovtopmd*).

5.2.3 Database

A database serves as the central data repository for all OVO messages and most configuration data on the OVO/UNIX management server (some configuration data that is stored in the directory structure of the TOE). Runtime and historical data can be used to generate reports. HP OVO/UNIX uses Oracle 9.2 for its database. For this TOE, the database software is installed on and its processes

run on the OVO/UNIX management server. However, since the database is outside of the TOE Boundary, database functionality was not tested as part of this evaluation..

5.2.4 Pluggable Authentication Module

Authentication mechanisms are provided for OVO/UNIX through the use of the Pluggable Authentication Module. The OVO PAM interface enables third-party authentication methods (e.g. LDAP) to be used while preserving existing system environments. PAM retrieves and checks user and password information when a user logs into the OVO Motif Admin GUI or OVO Java GUI.

The following two authentication mechanisms for the OVO user login were included in the evaluated configuration:

1) pam_unix: using /etc/passwd
2) pam_ldap: accessing (remote) LDAP

5.2.5 Cryptographic Support

The TOE relies on the IT environment to provide cryptographic support and the cryptographic module. These include:

- The local OVO HTTPS agent configuration is signed with digital signature to protect the OVO HTTPS agent configuration against unauthorized tampering.
- HP OVO uses SSL to provide a trusted path to prevent data disclosure between the OVO/UNIX management server and HTTPS agents as well as between OVO/UNIX management server and the OVO Java GUIs.
- Encryption of sensitive data – HP OVO/UNIX uses encryption to protect sensitive data stored in the file system (e.g. KeyStore that contains the certificates, or if a certificate is "created/exported" for manual installation on a managed node)

5.2.6 Distributed Computing Environment (DCE) Technology

The Remote Procedure Calls (RPC) of the Distributed Computing Environment (DCE) technology is used on the OVO/UNIX management server for some local inter-process communication.

The few OVO/UNIX processes that act as a DCE server process do not need to be accessible remotely. Meaning the endpoint mapper (dced/rpcd) port 135 can/should be blocked for remote access by a firewall. The only exception to this configuration would be when the customer still wants to manage some systems using the older OVO DCE agent technology.

For the purpose of the CC evaluation, the OVO/UNIX process that act like a DCE server will **NOT** be accessible remotely. The DCE server process is considered part of the IT Environment and therefore is **NOT** in the scope of the TOE.

5.2.7 OVO DCE Agent

The OVO DCE agent is the old OVO agent technology and is **NOT** part of this TOE. The OVO DCE agent uses light-weight encrypted remote procedure calls (RPC) for communication with the

OVO/UNIX Management Server system using DCE and/or NCS technology. The configuration for the OVO interceptors (Logfile Encapsulator, SNMP Trap Interceptor, OVO Message Interceptor), Monitoring Agent and Action Agent is stored in so called templates. The configuration updates are pulled from the OVO/UNIX management server.

For the purpose of the CC evaluation, the OVO DCE agent was **NOT** used because it is a remnant of the older technology and therefore outside of this TOE. Product end users who want to maintain operations in compliance with the CC evaluation must not use the OVO DCE Agent.

5.2.8 Operational Motif UI

OVO/UNIX still offers an operational Motif UI, versus the Java UI, where operators can work on the OVO messages and daily operations.

This operational Motif UI is similar to the Motif Admin UI, but it does NOT contain any kind of configuration capabilities. It provides the functionality of the OVO Event Browser, Application Desktop, Managed Node Map and Message Group Map – containing only the objects the logged-in operator is responsible for.

For the purpose of the CC evaluation, the operational Motif UI was **NOT** used because it is a remnant of the older operational UI technology and therefore outside of this TOE. Product end users who want to maintain operations in compliance with the CC evaluation must not use this interface.

6 Documentation

The following is a list of the evaluation evidence used in the evaluation of OVO/UNIX.

6.1 Installation, Generation, and Start-Up Procedures

File Name	Description
AdminRefGuide_Edn_2.pdf	HP OpenView Operations -Administrator's Reference Software Version A.08.10
HTTPSAgentGuide_Edn3.pdf	HP OpenView Operations - HTTPS Agent Manual Software Version A.08.10
RelNotes_OVOU_8.10_HPUX_PA-RISC_Edn_6.pdf	HP OpenView Operations - Release Notes Software Version A08.10 for HP-UX
RelNotes_OVOU_8.10_Solaris_Edn_6.pdf	HP OpenView Operations - Release Notes Software Version A08.10 for Solaris
InstallationGuide_HP_Edn_2.pdf	HP OpenView Operations -Installation Guide Software Version A.08.10 for HP-UX
InstallationGuide_Sol_Edn_2.pdf	HP OpenView Operations -Installation Guide Software Version A.08.10 for Solaris
http://ovweb.external.hp.com/lpe/doc_serv/	External available Documentation for HP OpenView
OVOU-SecurityAdvisory.doc	HP OpenView Operations Security Advisory document

6.2 Configuration Management Documentation

File Name	Description
OVO8.1_Config_Mgmt_v1.0.doc	ClearCase and Build-Factory documentation
OVOU810_Configuration_Item_List.doc	Configuration Item List

6.3 Delivery Procedures

File Name	Description
CC_Delivery_Process	HP software manufacturing process overview
evisTraining.ppt	Slide show on the tracking system used by HP
HP Solution Factory Rev B. cdrom	Movie clips that explain the manufacturing to boxing of product.

6.4 Functional Specification Documentation

File Name	Description
FSP_interfaces_idx.xls	The FSP maps security relevant functionality and OVO commands.
ManPages	HP OpenView Operations Manpages in PDF and text format
Error Output	English error messages of the HP OpenView Operation command line interfaces
AdminRefGuide_Edn_2.pdf	HP OpenView Operations -Administrator's Reference Software Version A.08.10
HTTPSAgentGuide_Edn3.pdf	HP OpenView Operations - HTTPS Agent Manual Software Version A.08.10
http://ovweb.external.hp.com/lpe/doc_serv/	External available Documentation for HP OpenView

6.5 High-Level Design Documentation

File Name	Description
SecurityFeaturesOfOVO8.ppt	High-level documentation of the security features provided by the new HTTPS based Server <-> Agent communication.
Design_Docs/HLDs	MS Visio 2003 High-level Design Papers
ConceptsGuide.pdf	HP OpenView Operations Concepts Guide A.08.10
AdminRefGuide_Edn_2.pdf	HP OpenView Operations -Administrator's Reference Software Version A.08.10
HTTPSAgentGuide_Edn3.pdf	HP OpenView Operations - HTTPS Agent Manual Software Version A.08.10
http://ovweb.external.hp.com/lpe/doc_serv/	External available Documentation for HP OpenView

6.6 Representation Correspondence

File Name	Description
FSP_interfaces_idx.xls	The FSP maps security relevant functionality, OVO commands and test cases.

6.7 Administrative Guidance

File Name	Description
InstallationGuide_HP_Edn_2.pdf	HP OpenView Operations -Installation Guide Software Version A.08.10 for HP-UX
InstallationGuide_Sol_Edn_2.pdf	HP OpenView Operations -Installation Guide Software Version A.08.10 for Solaris
AdminRefGuide_Edn_2.pdf	HP OpenView Operations -Administrator's Reference Software Version A.08.10
HTTPSAgentGuide_Edn3.pdf	HP OpenView Operations - HTTPS Agent Manual Software Version A.08.10
ServiceGuide.pdf	HP OpenView Service Navigator Concepts & Configuration Guide A.08.10
RelNotes_OVOU_8.10_HPUX_PA-RISC_Edn_6.pdf	HP OpenView Operations - Release NotesSoftware Version A08.10 for HP-UX
RelNotes_OVOU_8.10_Solaris_Edn_6.pdf	HP OpenView Operations - Release NotesSoftware Version A08.10 for Solaris
ConceptsGuide.pdf	HP OpenView Operations Concepts Guide A.08.10
Firewall.pdf	HP OpenView Operations Firewall Guide A.08.10
ManPages	HP OpenView Operations Manpages in PDF and text format
OVOU-SecurityAdvisory.doc	HP OpenView Operations Security Advisory document
JavaOperatorGuide.pdf	HP OpenView Operations Java Operator Guide A.08.10
Manuals/ito_op/help/en/ovo/html/index.htm	HP OpenView Operations Java Operator Online Help A.08.10
http://ovweb.external.hp.com/lpe/doc_serv/	External available Documentation for HP OpenView

6.8 User Guidance

File Name	Description
ConceptsGuide.pdf	HP OpenView Operations Concepts Guide A.08.10
ServiceGuide.pdf	HP OpenView Service Navigator Concepts & Configuration Guide A.08.10
JavaOperatorGuide.pdf	HP OpenView Operations Java Operator Guide A.08.10
Manuals/ito_op/help/en/ovo/html/index.htm	HP OpenView Operations Java Operator Online Help A.08.10
http://ovweb.external.hp.com/lpe/doc_serv/	External available Documentation for HP OpenView

6.9 Test Documentation

File Name	Description
Test coverage analysis	
FSP_interfaces_idx.xls	The FSP maps security relevant functionality and test cases.
cc_eal2_testcases.doc	Documentation of the EATE driven command line test cases.
CC_Security Testcases	All manual Administrator GUI, automated EATE, manual and automated XDE (Java Operator UI) Test case sources
Test Documentation	
FSP_interfaces_idx.xls	The FSP maps security relevant functionality and test cases.
cc_eal2_testcases.doc	Documentation of the EATE driven command line test cases.
CC_Security Testcases	All manual Administrator GUI, automated EATE, manual and automated XDE (Java Operator UI) Test case sources
EATE Report: NIAP_ServerCLI_BBN.html	Automated OVO/UNIX Server CLI (EATE Report) *complementary tests in Böblingen*
XDE Report: XP-HPUX11.11-HPUX11.11_JavaGUI.html	Automated OVO/UNIX Java Operator UI Translated Rational Test manager Report (HP-UX 11.11 <-> HP-UX 11.11) *complementary tests in Böblingen*
XDE Report: XP-HPUX11.11-Solaris9_JavaGUI.html	Automated OVO/UNIX Java Operator UI Translated Rational Test manager Report (HP-UX 11.11 <-> Solaris 9) *complementary tests in Böblingen*
XDE Report: XP-HPUX11.11-Win2003_JavaGUI.html	Automated OVO/UNIX Java Operator UI Translated Rational Test manager Report (HP-UX 11.11 <-> MS Win 2003 EE) *complementary tests in Böblingen*
XDE Report: XP-Solaris9-Solaris9_JavaGUI.html	Automated OVO/UNIX Java Operator UI Translated Rational Test manager Report (Solaris 9 <-> Solaris 9) *complementary tests in Böblingen*
XDE Report: XP-Solaris9.0-RedHat_JavaGUI.html	Automated OVO/UNIX Java Operator UI Translated Rational Test manager Report (Solaris 9 <-> RedHat-AS 3.0) *complementary tests in Böblingen*
XDE Report: XP-Solaris9-Win2003_JavaGUI.html	Automated OVO/UNIX Java Operator UI Translated Rational Test manager Report (Solaris 9 <-> MS Win 2003 EE) *complementary tests in Böblingen*

TMS Report: Complementary-BBN_Automated_ServerCLI.html	Automated OVO/UNIX Server CLI (TMS Report) *complementary tests in Böblingen*
TMS Report: Complementary-BBN_Automated_OperatorUI.html	Consolidated Automated OVO/UNIX Java Operator UI tests(TMS Report) *complementary tests in Böblingen*
TMS Report: Complementary-BBN_MotifAdminGui.html	Consolidated manual Motif Administrator GUI tests(TMS Report) *complementary tests in Böblingen*
Independent Testing	
FSP_interfaces_idx.xls	The FSP maps security relevant functionality and test cases.
all_audit_report.txt	Audit output generated during Evaluator Ad-Hoc testing
CC_Security Testcases	All manual Administrator GUI, automated EATE, manual and automated XDE (Java Operator UI) Test case sources
NIAP-Ethereal-Sniffing	Output of Etherreal sniffing session
Versions	Output of manual installed version(s) check on the installed systems
Permissions	HP OpenView Operations Documentation of file access permissions on test systems in Ft. Collins except the Win2003 system. There was no functionality available to entirely list the file access permissions regarding ACL on MS Windows 2003. Checks had to be done manually in Ad-Hoc tests.
Screenshots	Screenshots from Ad-Hoc tests of the evaluator in Ft. Collins
EATE Report: NIAP_ServerCLI.html	Automated OVO/UNIX Server CLI (EATE Report)
EATE Report: NIAP_AgentCLI.html	Automated OVO/UNIX HTTPS Agent CLI (EATE Report)
XDE Report: niap_1-hptest13_6-wtest63.html	Automated OVO/UNIX Java Operator UI Translated Rational Test manager Report (#1 HP-UX 11.11 <-> #6 RedHat-AS 3.0)
XDE Report: niap_2-suntest20_3-hptest65_2nd.html	Automated OVO/UNIX Java Operator UI Translated Rational Test manager Report (#2 Solaris 9 <-> #3 HP-UX 11.11)
TMS Report: FtCollins_Automated_ServerCLI.html	Automated OVO/UNIX Server CLI (TMS Report)
TMS Report: FtCollins_Automated_AgentCLI.html	Automated OVO/UNIX HTTPS Agent CLI (TMS Report)
TMS Report: FtCollins_Automated_OperatorUI.html	Consolidated Automated OVO/UNIX Java Operator UI tests (TMS Report)

6.10 Strength of Function Documentation

File Name	Description
ADV_FSP	FSP Evidence
ADV_HLD	HLD Evidence
ASE	Security Target
The evaluator did not find any probabilistic or permutational mechanisms that required the developer to produce a special analysis.	

6.11 Vulnerability Analysis Documentation

File Name	Description
misc_status.xls	HP OpenView Operations Vulnerability analysis
OVOU-SecurityAdvisory.doc	HP OpenView Operations Security Advisory document
CVE_Assessment	HP OpenView Operations CVE Assessment documents
Permissions	HP OpenView Operations Documentation of file access permissions on test systems in Ft. Collins except the Win2003 system. There was no functionality available to entirely list the file access permissions regarding ACL on MS Windows 2003. Checks had to be done manually in Ad-Hoc tests.
NIAP-Ethereal-Sniffing	Output of Etherreal sniffing session
NIAP-Ethereal-Sniffing Server <-> HTTP Agent	Actions performed between Management Server and HTTPS Agent under inspection of Etherreal
NIAP-Ethereal-Sniffing Server <-> Java UI	Actions performed between Management Server and Java Operator UI under inspection of Etherreal
ov_scan.trc	Tracefile of ov_scan
ov_scan.trc	Second tracefile of ov_scan after fixing remaining issues
GfiLanguard	Logfiles of GfiLanguard scans in Ft. Collins

6.12 Security Target

File Name
HP OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO management server on HP-UX 11.11) and ITOSOL_00403 (OVO management server on Solaris 9); Security Target v1.11, 18 August 2005.

7 IT Product Testing

This section describes the testing efforts of the vendor and the Evaluation Team.

7.1 Vendor Testing

The overall testing approach used by the developer was to test all of the human interfaces that covered the security functions described in the ST. The tests covered the MOTIF Admin UI, JAVA

Operator UI, and Command Line Interfaces for the server and agents. The security functions covered were Access Control, Configuration tasks, Security Management, Audit, and I&A.

The developer used a test tool that allowed the user to develop a test plan, keep track of tests, maintain results (success and failure) for every time the test was run, keep history of the tests, and create final reporting. The tests that were developed were automated and could be run individually or in a suite.

The tests were not intended to be an exhaustive test of the commands. Most of the commands have several input parameters and combinations of parameters that could be used. As a result, the developer used a representative set of parameters for each command that would most often be used by the customer. There is no realistic way the evaluator can assign a percentage of coverage on this particular aspect.

The Security Functions covered were 85-90 percent. Two out of the 19 security functions described in the ST did not have interfaces. These two security functions were tested during the evaluator independent testing.

7.2 Evaluator Testing

The following is an overview of the testing that was performed by the evaluator.

1. Verification of the TOE Installation and configuration
   - The evaluator physically/visually identified and recorded the TOE components and support software (name and version number). The version numbers of the TOE components were then compared to the configuration item list and the description section of the ST.

2. Execution of **ALL** the developer's functional tests
   - The evaluator (or assigned individual) reran **ALL** of the developer test procedures. The test procedures were run against the first test configuration using an HP-UX 11.11 machine as the server. The test was then run against the second configuration using a Solaris 9 machine as the server.

3. Execution of Independent Testing
   - The evaluator selected individual tests (scripts) from the set of Developer Functional Tests and modified input parameters to ensure full functionality of the interface. The classifications of tests mainly included, but were not limited to, access control, identification and authentication, and security management. Tests covered both the GUIs and CLI interfaces.
   - The evaluator selected tests from each security function categorization and then used the Onsite Notes section to fully describe the changes implemented along with expected results.

4. Vulnerability Testing

- The evaluator took the security target, developer design documents, vulnerability analysis, and guidance documentation into consideration for development the vulnerability tests.
- Building on the developer's vulnerability analysis the evaluator felt that the following should be considered for penetration testing:
    - Test #1: Run a vulnerability scan against each of the machines in the configuration prior to conducting any further testing. This will provide a reasonable assurance that the developers did in fact search publicly available information about obvious known vulnerabilities.
    - Test #2: Check to see if an attacker gains access through guest, maintenance, or default account [Misuse; GUI / CLI]
    - Test #3: Check to see if an attacker gains access because security-relevant files are not secured properly [Tampering; GUI / CLI, application]. Physically check the directory and file permissions on the server to ensure that they indeed are restricted to 'root' user.
    - Test #4: Check to see if the I&A mechanism incorrectly handles user input and allows inappropriate access [Bypass; GUI / command line interface (CLI)]
        - Special characters (e.g. CTRL-C, ALT-0010, !, space)
        - Encoded characters (e.g. %20,)
        - Null input
        - Huge input.
    - Test #5: Check to see if an attacker bypasses validity checking in an HTTP form by constructing GET / POST request directly. [Bypass; HTTP]
    - Test #6: Check to ensure that the HTTP Agent will not load a policy file that has been altered. [Tampering; CLI, Agent]
    - Test #7: Check the TOEs response to dependent software, such as the Oracle database, being crashed or disabled

5. Installation of the TOE in its evaluation configuration

- The evaluator used the newest version of the installation instructions and CC installation supplement. The evaluator (or designated person) followed the instructions step-by-step to install the TOE on the HP UX OS platform.
- The evaluator then physically/visually identified and recorded the TOE components and support software (name and version number).
- The evaluator then conducted a vulnerability scan, as in Test #1 of the Vulnerability Test, against the server. The results were compared against the Test #1 results against the HP UX server and the OVO HTTP Agent. This provided a reasonable assurance that

the developers did in fact cover all aspects in the Installation Guidance and CC supplemental instructions.

8 Evaluated Configuration

The developer test configuration included the use of seven machines. This section describes the set up of each of these machines.

Physical machine #1 (HP-UX Server) and Physical machine #2 (Solaris Server) included the following:

- TOE Components in Scope
  - HP OVO/UNIX Management Server, OVO Motif admin GUI, OVO administrative command line interfaces (CLI) on the same physical machine.
- Other Components out of Scope
  - Network Node Manager 7.5 which includes the required Apache web services GUI engine. (Only mandatory portions of the NNM as described in the ST will be configured to operate.)
  - Oracle 9.2.0.2, and its interface, for data management.
  - PAM client for local /etc/password access (pam_unix)
  - PAM client for remote Active Directory Service access running on MS Windows 2003 or other open remote LDAP server (pam_ldap) [HP only]
  - OpenSSL 0.9.6m (statically linked)
  - DCE Components (Provided for Solaris by OVO/UNIX, Included in HP UX. Both will be configured to not work remotely)
  - Operational MOTIF UI (configured to not be used)

Physical machines #3 (HP-UX agent), #4#7 (Solaris agent), #5 (MS Window 2003 sp1 agent), #6 (Red Hat Linux 3.0 AE agent)

- TOE Components in Scope
  - HP OVO HTTPS Agent, OVO agent administrative CLIs
- Other Components out of Scope
  - OpenSSL 0.9.6m (statically linked) Oracle 9.2.0.2, and its interface, for data management.
  - ADS for Windows 2003 [MS Windows]

Physical machine #7 (Windows XP SP2: Java Operator User Interface)

- TOE Components in Scope
  - OVO Java User Interface

- Other Components out of Scope
  - OpenSSL 0.9.6m (statically linked) Oracle 9.2.0.2, and its interface, for data management.
  - Internet Explorer 6.0
  - JRE 1.4.2

Additional machines include the DNS server and firewall to isolate from corporate LAN. It should also be noted that the cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

9 Results of the Evaluation

The HP OVO/UNIX satisfies all of the EAL2 assurance requirements against which it was evaluated. The EAL2 assurance requirements include the following:

Table 9-1. EAL2 Assurance Components

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.2 Configuration items
Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Tests (ATE)	ATE_COV.1 Evidence of Coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

The Security Target provides a detailed description of how HP OVO/UNIX meets each of the listed components.

10 Validation Comments/Recommendations

The OVO/UNIX, in its evaluated configuration, performed as expected and should meet the expectations of the customer. The installation guidance provided contains the necessary information for a proper installation of the TOE. In addition, a Security Advisory Guide is provided by HP to be used to ensure that the TOE is installed in its CC compliant state without any of the obvious vulnerabilities. Following the procedures within the Security Advisory Guide reduce any possible vulnerability that may be present in either the TOE or the IT environment. The latest version of the Security Advisory Guide can be found at the following location:

http://ovweb.external.hp.com/lpe/doc_serv/

Select "Operations for UNIX" and version 8.10.

As noted in the installation guidance information, the customer should be aware that after installing HP OVO/UNIX version 8.10, they must ensure that they apply the following security patches in order to have a version that is CC compliant: for the OVO management server HP-UX 11.11, patch PHSS_32820; and, for the Solaris 9 OVO management server ITOSOL_00403.

As seen in the ST, security requirements have been defined for both the TOE and its IT environment. The need for a large portion of the IT Environment security requirements results from the use of command line interfaces. Although a portion of the CLIs have corresponding Admin UI commands that can be used, there are still several commands that are only available through the CLIs. These CLIs are executed by the "root" user to perform TOE security management functions. As a result, OVO/UNIX relies on the operating system to provide identification and authenticate of the "root" user before being allowed to manage TOE functions through the CLI.

In addition, it shall be noted that the cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, the CEM and CCEVS practices. She agrees that the CCTL presented appropriate rationales to support the Results of the Evaluation presented in Section 4 of the ETR Part I and the Conclusions presented in Section 5 of the ETR Part II. Therefore, the Validator concludes that the evaluation and the Pass results for the TOE identified below are complete and correct:

Hewlett-Packard OpenView Operations for UNIX V A.8.10 with patch PHSS_32820 (OVO mgmt sv on HP-UX 11.11)

Hewlett-Packard OpenView Operations for UNIX V A.8.10 with patch ITOSOL_00403 (OVO mgmt sv on Solaris 9)

Including:

- Hewlett-Packard OpenView Operations for UNIX Agents that operate on the host OS of HP-UX 11.11, Solaris 9, MS Windows 2003 Server SP1, and Red Hat Linux AS3U4.

- Hewlett-Packard OpenView Operations for UNIX Java UI that operates on Windows XP SP2.

11 Security Target

HP OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO management server on HP-UX 11.11) and ITOSOL_00403 (OVO management server on Solaris 9), Security Target v1.11, 18 August 2005.

12 Acronyms

ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
API	Application Programming Interface
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
CCTL	Common Criteria Testing Laboratory
CLI	Command Line Interface
DCE	Distributed Computing Environment
EAL	Evaluation Assurance Level
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
FTP	Trusted Channels/Path
GUI	Graphical User Interface
HP	Hewlett Packard
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP over SSL
I&A	Identification & Authentication
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MS	Microsoft
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NNM	Network Node Manager
OS	Operating System
OVO	HP OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO management server on HP-UX 11.11) and ITOSOL_00403 (OVO management server on Solaris 9)
OVO/UNIX	HP OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO management server on HP-UX 11.11) and ITOSOL_00403 (OVO management server on Solaris 9)
PAM	Pluggable Authentication Module
PC	Personal Computer
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SP	Service Pack
SSL	Secure Sockets Layer
ST	Security Target

TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
US	United States

13 Bibliography

The following documents were used in compiling this Validation Report:

- Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004:
  - Part 1: Introduction and general model, CCIMB-2004-01-001, Version 2.2, January 2004
  - Part 2: Security functional requirements, CCIMB-2004-01-002, Version 2.2, January 2004
  - Part 3: Security assurance requirements, CCIMB-2004-01-003, Version 2.2, January 2004
- Common Evaluation Methodology for Information Technology Security:
  - Part 1: Introduction and general model, CEM-97/017, Version 0.6, 97/01/11
  - Part 2: Evaluation Methodology, CEM-2004-01-004, Version 2.2, January 2004
  - Supplement: ALC_FLR - Flaw Remediation, CEM-2001/0015, Version 1.0, August 2001
- Hewlett - Packard OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO mgmt sv on HP-UX 11.11) ITOSOL_00403 (OVO mgmt sv on Solaris 9), TR Version 1.0, Date Aug 18, 2005
- HP OpenView Operations for UNIX V A.08.10 with patches: PHSS_32820 (OVO management server on HP-UX 11.11) and ITOSOL_00403 (OVO management server on Solaris 9), Security Target v1.11, 18 August 2005.
- HP OpenView Operations for UNIX V A.8.10 Test Plan, version 1.2, May 27, 2005.