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)

Security Target V 1.11

Debra Baker

August 18, 2005

CYGNACOM SOLUTIONS

Suite 5200 West♦7925 Jones Branch Drive♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

Revision History:

Date:	Version:	Author:	Description
3/9/2004	0.1	Debra Baker	First Draft
3/15/2004	0.2	Debra Baker	Second Draft
3/24/2004	0.3	Debra Baker	Third Draft
3/26/2004	0.4	Debra Baker	Fourth Draft
4/8/04	0.5	Debra Baker	Fifth Draft
4/23/04	0.6	Debra Baker	Sixth Draft
4/30/04	0.7	Debra Baker	Seventh Draft
5/10/04	0.8	Debra Baker	Eighth Draft
5/27/04	1.0	Patrik Batsching	Ready for NIAP containing input also from Dave Trout
7/20/04	1.1	Debra Baker	Updates to ST introduction, TOE Description, and Environment based on Evaluator comments
8/30/04	1.2	Marco Stiegeler, Patrik Batsching	Some minor changes – especially wrt auditing coverage (table 5-2, 5-3, 5-4) and table “Security Function: Configuration Tasks of OVO Administrator”
11/11/04	1.3	Debra Baker	Updated section 6 TSS
12/2/04	1.4	Debra Baker	Updated section 6 TSS
12/3/04	1.5	Debra Baker	Added developer comments to section 6 and 8.
12/16/04	1.6	Debra Baker Marco Stiegeler	Updates throughout including figures 2-4 and 2-5
01/17/05	1.7	Steffen Walter, Debra Baker	Update related to Herb’s comments
03/04/05	1.7.1	Debra Baker	Update related to Herb’s comments
03/24/05	1.8	Debra Baker	Update related to Herb’s comments including HP’s comments
05/01/05	1.9	Debra Baker	Update related to Herb’s comments including HP’s comments
7/15/05	1.10	Debra Baker	Update related to Herb’s comments to fix FIA_UAU problems
8/18/05	1.11	Debra Baker	Update related to Validator and Evaluator comments

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification: HP 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)

ST Title: HP OpenView Operations for Unix V A.08.10 plus with patches:
PHSS_32820 (OVO management server on HP-UX 11.11)
ITOSOL_00403 (OVO management server on Solaris 9)

ST Version: Version 1.11

ST Authors: Debra Baker

ST Date: Aug 18, 2005

Assurance Level: EAL2

Registration: <To be filled in upon registration>

Keywords: Access Control, Identification, Authentication, Security Management, Security Target, OVO/UNIX management server, Administrator Motif Admin GUI, OVO Java GUI, and OVO HTTPS Agent

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for HP OpenView Operations for Unix version A.08.10 with patches PHSS_32820 (OVO mgmt sv on HP-UX 11.11) and HP OpenView Operations for Unix version A.08.10 with patches ITOSOL_00403 (OVO mgmt sv on Solaris 9) here on in will be referred to as version 8.10 for short. HP OpenView Operations for UNIX (OVO/UNIX) is a network and system management system that enables HP OVO authorized administrators and operators to manage a multi-vendor network via the HP OVO Administrator and User Interfaces. OVO 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.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.2.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Sections 9 and 10 provide acronym definitions and references.

2 TOE Description

2.1 Product Type

HP OpenView Operations for UNIX (OVO/UNIX or just short OVO) 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. 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.

A relational 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. 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.

For more details about the HP OpenView Operations for UNIX concepts, please refer to the “OVO Concepts” guide. The complete OVO/UNIX 8.10 end user documentation set can be downloaded from http://ovweb.external.hp.com/lpe/doc_serv/".

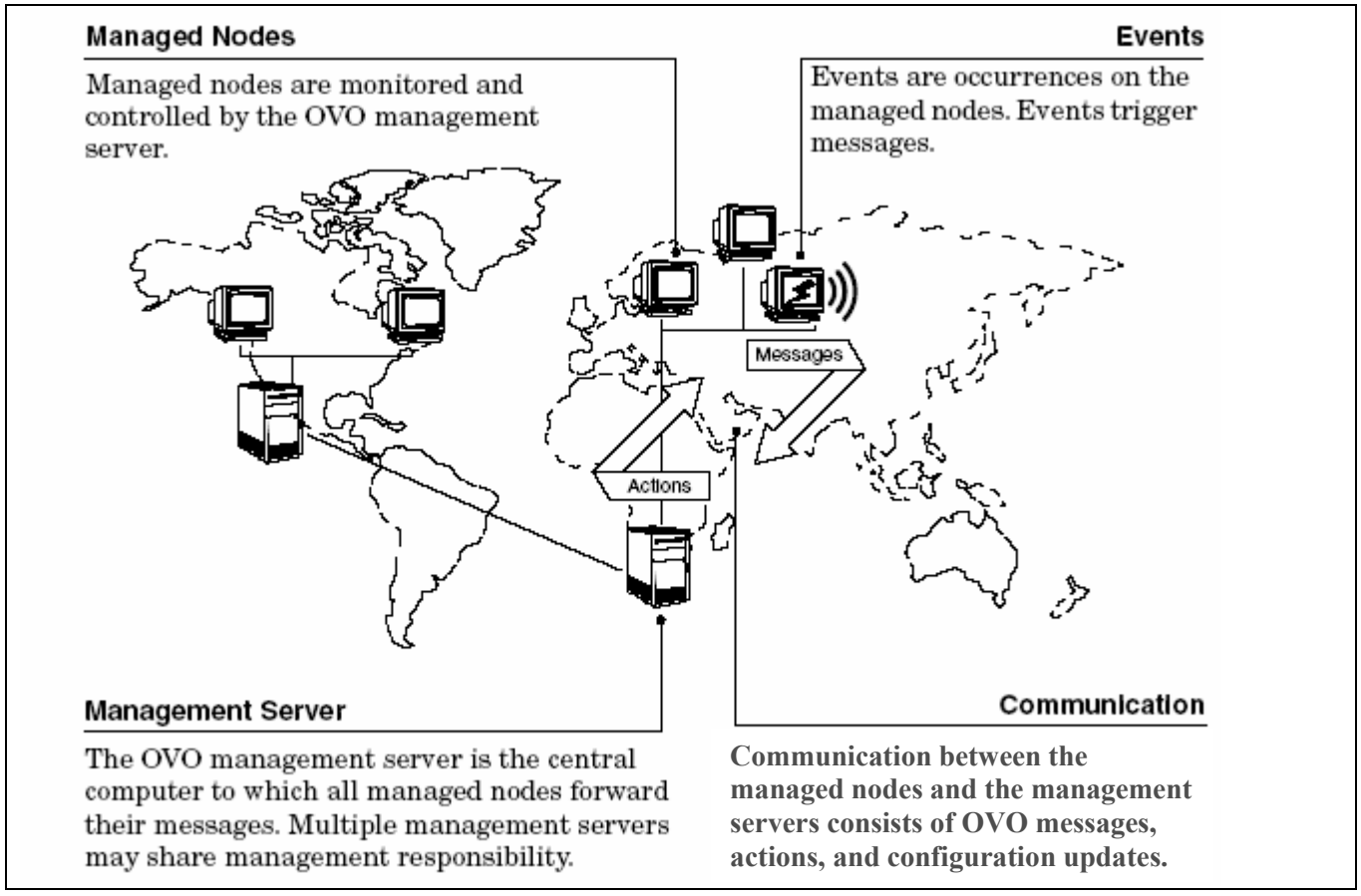

Figure 2-1 OVO Client – Server Concept

2.2 HP OpenView Operations for UNIX Components

The TOE components that comprise HP OpenView Operations for UNIX, are the OVO/UNIX Management Server, OVO HTTPS Agent, Command Line Interfaces on the OVO/UNIX Management Server and OVO HTTPS Agent, Administrator (OVO Motif Admin GUI) and Operator (OVO Java GUI) User Interfaces.

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 (NNM) [Section 2.2.1.3],
- The DCE runtime on the OVO management server and OVO DCE agent components [Sections 2.2.1.2 and 2.2.3.2],
- Pluggable Authentication Module (PAM) [Section 2.2.2],
- Operational Motif GUI [Section 2.2.6.2], and
- Cryptographic Support [Section 2.5].

2.2.1 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 (for example, 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.

2.2.1.1 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:

- Allow batch processing for mass updates, nightly backup runs, etc.

- Provide management capabilities that are not included in the Motif Admin GUI (see section 2.2.4), such as upload of audit, configuring GUI login banner, configuring the OVO Service Navigator, manually update certificates, and recovery.
- Provide an alternative way for the OVO Administrator while acting as the system administrator (root) to perform the security management duties instead of using the OVO Motif Admin GUI.

2.2.1.2 OVO-internal Communication on the OVO/UNIX Management Server

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 outside the scope of the TOE.

2.2.1.3 Network Node Manager

OVO/UNIX only partially uses the Network Node Manager (NNM) functionality. Some functionality is mandatory for the OVO/UNIX use cases.

The NNM product is ONLY required on the OVO/UNIX management server. Neither the OVO agent nor Java GUI client systems use the NNM product.

NNM contains some overlapping functionality – such as an Event Browser (xnmevents) – and a simple action mechanism; therefore these parts are normally switched-off / unused in the OVO/UNIX use case.

Mandatory NNM pieces on the OVO/UNIX Management Server:

- The OVO/UNIX Motif GUIs use the NNM Motif libraries and corresponding integration means.
- The OVO/UNIX Motif GUI registers itself as NNM, requiring NNM processes to run in order to start up the OVO/UNIX management server.
  For example ovwdb, ovspmd, ovdbrun and ovtopmd.
- OVO/UNIX uses the Apache web server that ships with NNM for:
  - downloading the signed Java GUI share file
  - downloading the ServiceNavigator icons
  - serving the online help of the Java GUI.

For the purpose of the CC evaluation, the NNM product as a whole is considered in the IT Environment and therefore is outside the scope of the TOE. However, only the mandatory NNM functions, as described above, by default will be operational.

2.2.2 PAM

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

By default, OVO stores the user name & password information internally in its database. Activating the appropriate PAM client interface requires configuring the OVO/UNIX Management server. To be

compliant with the CC tested configuration the end user must activate the PAM client interface as defined below and NOT use the default OVO setting.

There are standard Authentication Modules such as pam_unix (which uses /etc/passwd) and pam_ldap. Customers can implement their own method, since the PAM APIs are standardized.

For the purpose of the CC evaluation the PAM will be considered part of the IT Environment and therefore is outside the scope of the TOE. The PAM will however be configured to operate with the standard Authentication Modules: pam_unix using /etc/passwd and pam_ldap.

2.2.3 OVO 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 Agent does the following:

- **Intercepting Messages (OVO Interceptors)**

Once installed and running, the OVO agent software monitors log files, monitors MIB values and intercepts SNMP traps. Also the OVO message interceptor can intercept messages from any OVO instrumented script/application running locally on the managed node using the OVO message interface (opcmsg).

- **Monitoring Performance (OVO Monitoring Agent)**

Performance values are monitored at configurable intervals, and messages can be generated when performance varies from limits. Using the OVO monitoring interface (opcmon), custom variables can be monitored and validated against the configured min/max threshold.

- **Comparing Messages**

The OVO agent compares all messages with conditions in preconfigured policies / templates and then forwards unexpected or important messages to the OVO/UNIX management server while ignoring unimportant messages. If so configured, the OVO agent even suppresses duplicate or similar events. The message filtering can be customized either by modifying existing policies / templates or by configuring a customized set of policies / templates and conditions.

- **Logging Messages**

All messages (including the suppressed messages) can be logged locally on the managed node or written directly into the history database on the OVO/UNIX management server. This history function enables all messages to be examined, even if the system has been configured to disregard the message as unimportant.

- **Buffering Messages**

If the OVO/UNIX management server is not reachable, messages are retained in a storage buffer until the OVO/UNIX management server can receive them again.

- **Correcting Problems (Action Agent)**

Corrective actions can be immediately started locally on the managed node in response to a message, and can be stopped and restarted, if necessary. Corrective actions can be also triggered by the OVO/UNIX management server or by other managed nodes, in case they are authorized.

The Action Agent is also used to start operator-initiated actions (pre-defined actions for OVO messages) and pre-configured applications & tools assigned to the operators.

- **Self Monitoring**

OVO can also monitor its own health status. The OVO/UNIX management server performs regular heartbeat monitoring of the OVO agent software. The OVO agent itself checks the health status of the different processes and can pro-actively send alive messages to the OVO/UNIX management server. The heartbeat monitoring type and interval can be configured for each managed node individually.

- **Flexible Alarming**

The OVO agent can send the OVO messages depending on date/time and OVO message attributes to different OVO/UNIX management servers. This allows different kind of multiple OVO/UNIX management server setups – such as:

  - Follow-the-sun: OVO message are sent only to the OVO/UNIX management server, where the operations staff currently runs its day-light shift.
  - Competency Center: Operations staff on different OVO/UNIX management server have different skills and knowledge areas – e.g. database, security, performance. The OVO messages are sent correspondingly.
  - Regional vs. central/hierarchical OVO/UNIX management servers: Depending on the date/time and/or OVO message attributes, the OVO message is sent to the regional or central OVO/UNIX management server.
  - Any kind of combination from above.

- **Minimal Command Line Interface**

The OVO agent comes with a small set of command line interfaces (CLIs) to start/stop/status the agent processes, enable and disable the policies / templates and housekeeping functions.

2.2.3.1 OVO HTTPS Agent

In the following, the areas are listed, where the OVO HTTPS agent differs from the OVO DCE agent. The HTTPS agent contains several new standardized OpenView software components (the so called Common Management Environment) – such as common CLIs to start/stop the OpenView software, access local configuration, consistent file tree layout, common tracing, etc.

- **Agent – Server Communication**

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

NOTE: 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

.

- **Local Configuration**

  The OVO HTTPS agent accesses its local configuration using the ovconfget and ovconfchg CLIs and corresponding API functions.

  The configuration for the OVO interceptors (Logfile Encapsulator, SNMP Trap Interceptor, OVO Message Interceptor), Monitoring Agent and Action Agent is stored in so called policies. These policies are stored on the management server in the relational database and transferred to the OVO HTTPS agent using OVO's internal distributions mechanism – based on HTTPS. Locally on the HTTPS agent these policies are stored in two separate files policy header file and policy data file in the HTTPS Agent filesystem. The policy header file contains a signature of the policy data file and a certificate. OpenSSL API is used to verify if the certificate is valid, the issuer of the certificate is authorized properly and if the provided signature is the correct one for the policy data file. Only policies signed by authorized Management Server systems are accepted. Any modification of signature, certificate or policy data file will be detected and the policy won't be processed by the corresponding interceptor.

  The configuration updates are pushed from the OVO/UNIX management server to the OVO HTTPS agent.

  Multiple OVO/UNIX management servers can configure the same OVO HTTPS agent provided they are authorized, which is determined by a valid certificate and the policy ownership flag.

2.2.3.2 OVO DCE Agent

In the following, the areas are listed, where the OVO DCE agent differs from the OVO HTTPS agent. The OVO DCE agent is the old OVO agent technology and is NOT part of this TOE.

- **Agent – Server Communication**

  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.

  As communication broker the standard dced/rpcd/llbd process is used.

- **Local Configuration**

  The OVO DCE agent accesses its local configuration using proprietary API functions.
  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. These templates are stored on the management server in the relational database and transferred to the OVO DCE agent using OVO's internal distributions mechanism – based on remote procedure calls. Locally on the DCE agent these templates are stored with a light-weight proprietary encryption to prohibit unauthorized changes.

  The configuration updates are pulled from the OVO/UNIX management server.

  Only the primary OVO/UNIX management server is allowed to configure the OVO DCE agent.

For the purpose of the CC evaluation, the OVO DCE agent was NOT used because it is a remnant of the older operational GUI 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.

2.2.4 OVO Administrator User Interface (OVO Motif Admin GUI)

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).

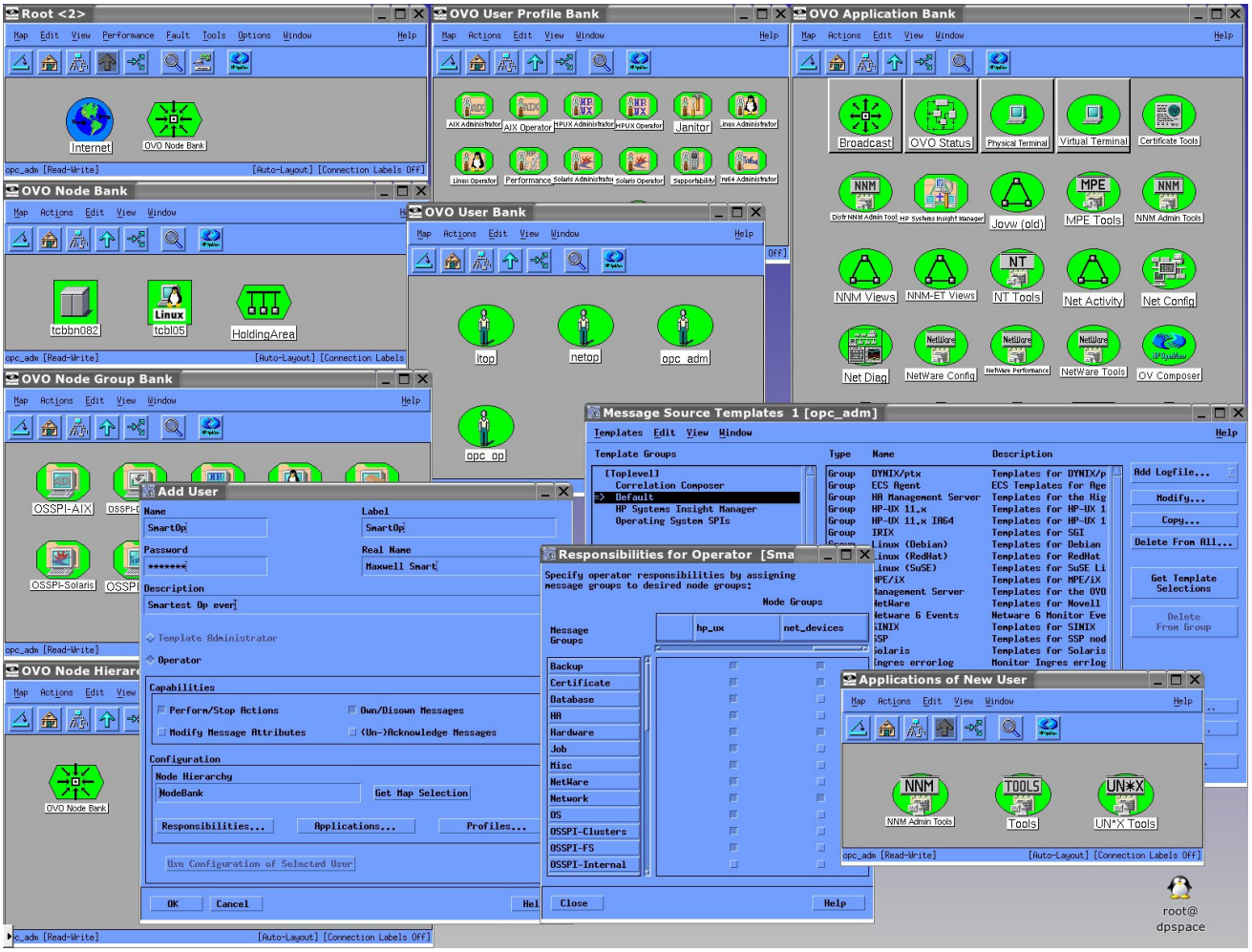

Figure 2-2 OVO Motif Administrator GUI

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

- **Configures & Maintains 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) .

  Maintains and fine tunes the monitored environment – for example deploying software updates, adding automatic corrective actions for standard problem scenarios, etc.

- **Customizes User Environments**

Defines a custom environment for each user. 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.

Depending on the OVO/UNIX management server configuration, the user login into the OVO Motif Admin GUI is validated via the PAM integration or checking the username / password combination stored in the OVO database. There is only ONE dedicated user who can log into the OVO Motif Admin GUI as OVO administrator at a time using the dedicated user name "opc_adm".

There are special user roles for so called "OVO Template Administrators", who can only administer template / policy configuration.

Application Note: OVO/Unix is migrating away from the term template, which is used for the OVO DCE Agent technology to, policy which is used for the OVO HTTP Agent. As of this evaluation, the server application continues to identify audit events and the special administrators in terms of template. Therefore, consider the terms template and policy as interchangeable.

2.2.5 Administrative Command Line Interface on the OVO/UNIX Management Server

The administrative Command Line Interfaces (CLIs) on the OVO/UNIX management server can be grouped into following categories:

- **Installation and initial Configuration of the OVO/UNIX Management Server**
  CLIs are used for the initial installation of the OVO/UNIX Management Server application. This includes database setup, licensing and fundamental customer environment specific configuration and so on.

- **Customization and ongoing Maintenance of Managed IT Environment**
  These adaptations add or change nodes or nodegroups; 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, including procedures such as; start and stop of agent processes, query or modifification 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, assigned responsibilities (nodegroups, message groups, applications) and associated capabilities (e.g. acknowledge OVO messages) – using opccfgupld(1m). Assigning and de-assigning of Service Views to operators are done by using the opcservice(1m) CLI.

- **Down- and upload of Audit Trail, History Data, and Configuration**
  Allows to up- and download 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, run troubleshooting tools, etc.

2.2.6 Operator User Interface

The OVO operators use either the OVO Motif GUI or 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.

2.2.6.1 Java GUI

The Java GUI is the modern operational user interface of OVO/UNIX and provides several additional features, which are NOT offered in the operational Motif GUI – for example customizable Message Browser, Workspace, Service Navigator, operate on a remote system, and officially MS Windows certified for various versions.

The main components in the OVO Java GUI are:

- **User Login**

The user login for operators in the OVO Java GUI is validated via the PAM integration. In case the OVO administrator (opc_adm) logs into the Java GUI, he has almost the same privileges as any other operator - with a few exceptions - e.g. he can disown OVO messages currently owned by another operator.

- **Message Browser**

Displays all incoming messages from the OVO operator's managed environment. The Severity column is colored to reflect the current status of the message. Or, if so configured, OVO colors the entire line in the message browser to reflect the severity of the message. Different filter browsers can be configured to run in parallel to allow easy & quick context switches – for example to monitor events from different mission-critical applications, monitoring of alarms from different facility sites or customers, etc. Message related actions can be easily started via the right-click pop-up menu.

- **Object Pane**
  - **Managed Nodes**

    Displays the operator's managed environment. Each node (or group of nodes) is represented by an icon and the node name. OVO changes the color of these icons to reflect the current status of the node.
  - **Message Groups**

    Displays the operator's message groups. Messages are grouped by function, location, application, or any other logical classification. OVO changes the color of these icons to reflect the current status of the message group.
  - **Applications**

    Displays pre-configured application the operator can start to perform his/her daily duties. The OVO operator starts these tasks by double-clicking the corresponding item. The application will then be started on the selected node or multiple nodes
- **Workspace Pane**

The workspace pane contains information about the OVO message statistics, displays the output of the launched applications, service views, etc. Multiple workspaces can be setup to enable a quick context switch.

- **Service Navigator**

In case the Service Navigator component is configured (using opcservice), the operator can also have service health information presented in appropriate service views enabling the management by service level objectives.

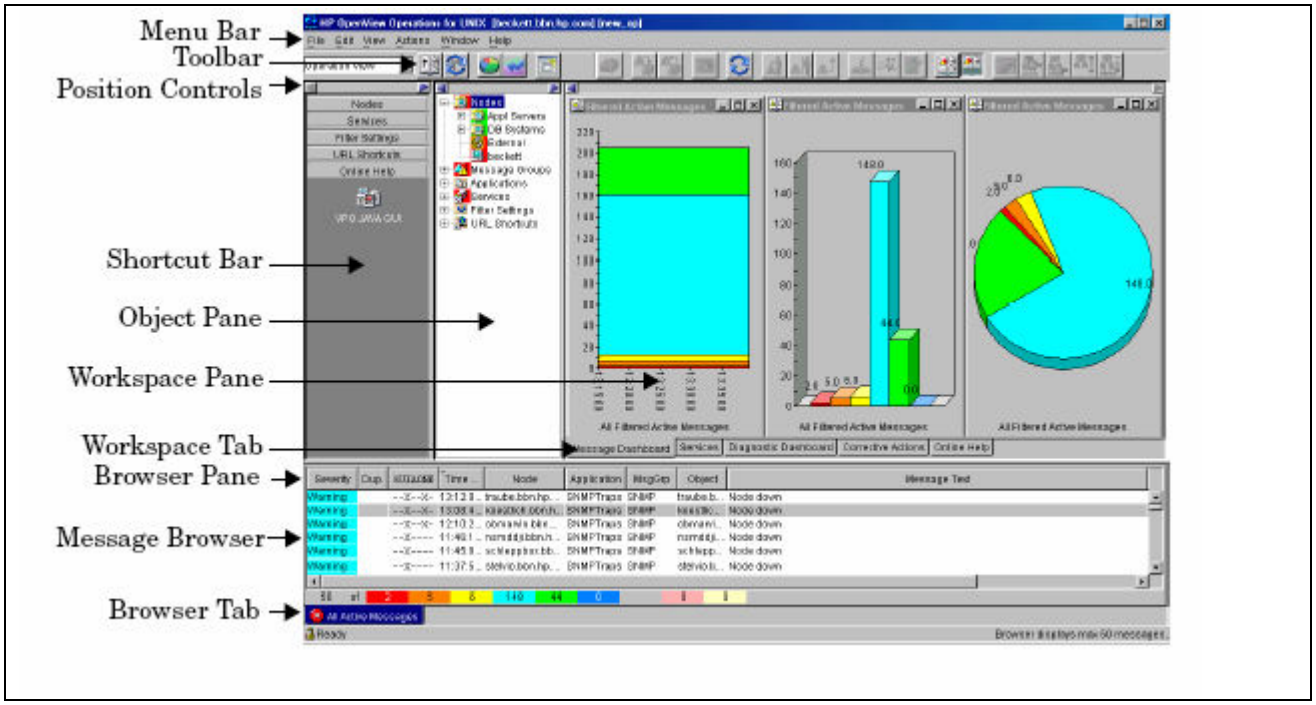

Figure 2-3 OVO Java GUI

2.2.6.2 Operational Motif GUI

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

This operational Motif GUI is similar to the Motif Admin GUI, 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.

The operational Motif GUI processes are running on the OVO/UNIX management server and the display can be redirected using standard X redirection means.

For the purpose of the CC evaluation, the operational Motif GUI was NOT used because it is a remnant of the older operational GUI 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.

2.3 TSF Physical Boundary and Scope of the Evaluation

The evaluated configuration includes the following:

Table 2-1 TOE Physical Boundary and Scope

TOE Component	**Not included in the TOE**		
		Run on the following OSs	**Other Software on same machine**
OVO/UNIX Management Server A.08.10 – Section 2.2.1 HP Server: PHSS_32820 Solaris Server: ITOSOL _00403	Physical Machine #1 Physical Machine #2	HP-UX 11.11 Solaris 9 OS	• Oracle 9.2.0.2 (HP-UX)/ 9.2.0.6 (Solaris) • HP OpenView Network Node Manager 7.5 (including the Apache web server and only the mandatory portions of the NNM will be configured to operate.) • PAM client for local /etc/passwd access (pam_unix) • PAM client for remote remote ldap server. (pam_ldap) • 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 GUI (NOT USED)
OVO Motif Administrator Interface (Motif Admin GUI) – Section 2.2.4			
OVO Administrative Command Line Interfaces – Section 2.2.5			

TOE Component	Not included in the TOE		
		Run on the following OSs	**Other Software on same machine**
OVO HTTPS Agent V A.08.11 – Section 2.2.3	Physical Machine #3-#6	HP-UX 11.11 (same as #1) Solaris 9 OS (same as #2) MS Windows 2003 SP1 Red Hat Enterprise Linux 3.0 – Advanced Edition	• OpenSSL 0.9.6m (statically linked)
OVO Agent Administrative Command Line Interfaces – Section 2.2.3			
OVO Java User Interface A.08.13 – Section 2.2.6.1	Physical Machine #7	Windows XP SP2 Java GUI will be running as Java application using JRE 1.4.2 or as applet in Internet Explorer	• JSSE 1.4.2 • Internet Explorer 6.0 • JRE 1.4.2

The TOE 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.

The HP Network Node Manager is not included in the TOE boundary. However, only the mandatory NNM functions, as described in Section 2.2.1.3, will be configured to operate.

The DCE runtime on the OVO management server is not included in the TOE boundary. The OVO DCE server components will be configured to NOT be accessible remotely, as described in Section 2.2.1.2. Nor will the OVO DCE Agent components be used.

In addition, the underlying operating system (OS) software and hardware are not part of the TOE.

The third party relational database (Oracle 9.2) is not included in the TOE. The interface of the third party database in not included as part of the TOE.

The TOE also does not include the third-party encryption software that is used to provide a trusted communication path between users and the TOE. OVO ships an OpenSSL component to authenticate and encrypt the OVO/UNIX communication between OVO/UNIX management server and OVO HTTPS agent as well as between the OVO/UNIX management server and the OVO Java GUI. Since OpenSSL is an open source component, it's not further assessed as part of this TOE.

The TOE does not include the PAM client software and corresponding authentication software – such as LDAP.

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

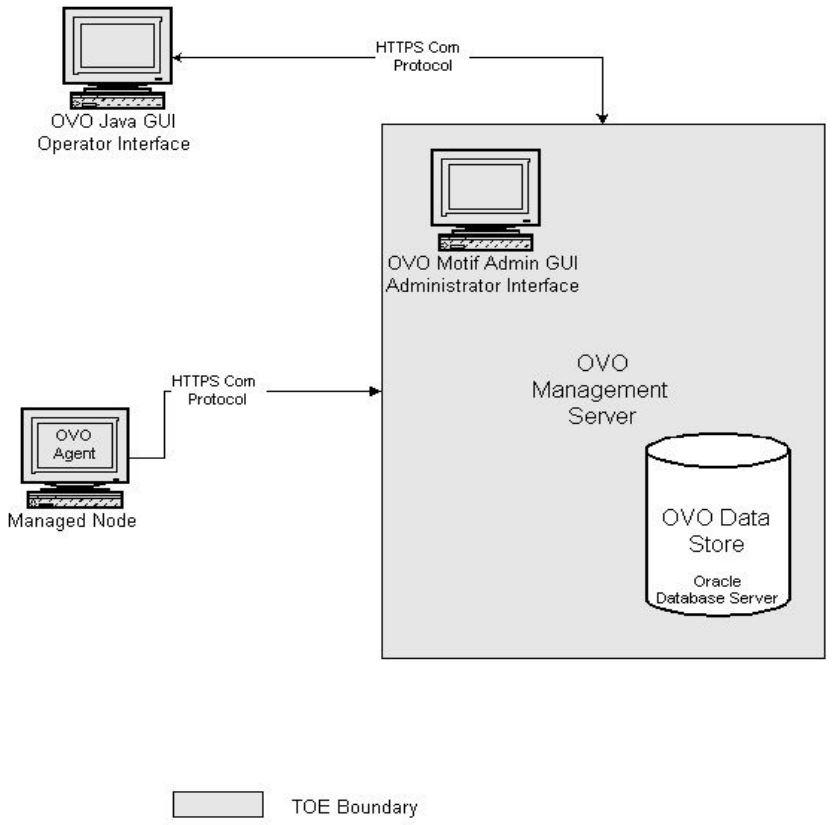

Figure 2-4 HP OpenView Operations for UNIX - Physical TOE Boundary

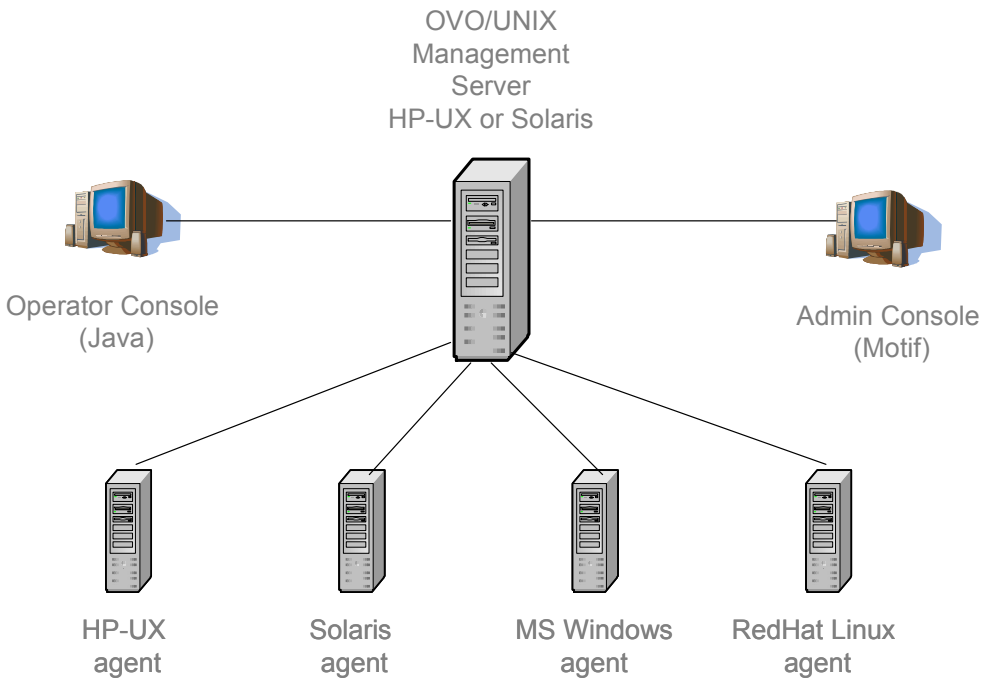

Figure 2-5 OVO/UNIX Infrastructure Test Configuration

2.4 Logical Boundary

The TOE provides the following security features:

- **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.

- **Access Control** - HP OpenView Operations for UNIX provides its own access control (authorization) 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.

  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 *administrator*).

- **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. PAM is outside of the TOE boundary.

  HP OVO/UNIX relies on the underling OS to require identification and authentication prior to allowing access to the OVO CLIs to the Unix user *root* (Windows user *administrator*).

- **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..

- **Security Management** - HP OpenView Operations for UNIX provides security management through the use of the OVO Motif Admin GUI and CLIs. Through the enforcement of the HP OpenView Operations Access Control Policy, the ability to manage various security attributes is controlled 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.

- **Partial Protection of TSF** - 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. (Note: 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).

2.5 TOE Security Environment

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.

HP OpenView Operations for UNIX relies upon the underlying operating system and platform to:

- provide reliable time stamps,
- provide the Unix user identification (OS must have I&A) for the use in the OVO/UNIX audit trail,
- protect 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.

HP OpenView Operations for UNIX provides generic interfaces to third party notification (paging) services and trouble ticket applications – such as HP OpenView Service Desk.

The TOE environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE security environment can be categorized as follows:

- **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)
- **Partial Protection of TSF** - HP OpenView Operations for UNIX relies on the underlying OS to provide security capabilities for the TOE's protection. For the TOE's own protection the OS includes requirements that relate to the integrity of the TSF. These include SFP domain separation, user data protection (access control), and a reliable time-stamp.
- **Trusted Path** - The TOE relies on the IT environment to provide encrypted communications over a trusted path. Trusted path refers to the encrypted connection that prevents disclosure and detects modification of data transmitted between the OVO HTTPS Agent and OVO/UNIX management server and data transmitted between the OVO Java GUI and OVO/UNIX management server.
  - The path from the OVO Java GUI to the OVO/UNIX management server relies on a trusted path provided by the IT environment.
  - The path initiated by the TOE from the OVO HTTPS Agent and OVO/UNIX management server relies on the trusted path provided by the IT environment.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 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 GUI 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.

3.2 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 following threats to security:

Table 3-2 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.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 Security Objectives for TOE

1	O.Access	The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OVO access control SFP.
2	O.Admin	The TOE will provide the functionality to enable authorized administrator(s) to effectively manage the TOE and its security functions.
3	O.Attributes	The TOE will be able to store and maintain attributes.
4	O.Audit	The TOE will record audit records for data accesses and use of the TOE functions.
5	O.AuditProtect	The TOE will ensure the protection of the audit storage.
6	O.Banner	The TOE will provide the capability of displaying an advisory warning about unauthorized use of the TOE.
7	O.IDAuth	The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data.
8	O.NonBypass	The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.
9	O.PartSelfProt	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.
10	O.ProtectData	The TSF will protect TSF data when transmitted between separate parts of the TOE and while being stored.
11	O.Roles	The TOE will support multiple roles.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 Security Objectives for IT Environment

1E	OE.AuditProtect	The IT environment will ensure the protection of the audit storage.
2E	OE.PartSelfProt	The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
3E	OE.ProtectComm	The IT environment will protect communications between the TOE and its users.
4E	OE.ProtectData	The IT environment will protect TSF data when transferred between TOE Components.
5E	OE.Time	The underlying operating system will provide reliable time stamps.
6E	OE.NonBypass	The IT environment will ensure that its protection mechanisms cannot be bypassed.
7E	OE.Access	The IT environment will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OS access control SFP.
8E	OE.Admin	The IT Environment will provide the functionality to enable authorized administrator(s) to effectively manage the TOE and its security functions.

9E	OE.IDAuth	The IT Environment will be able to identify and authenticate users prior to allowing access to TOE functions and data.

4.2.2 Security Objectives for Non-IT Security Environment

The Non-IT security objectives are as follows:

Table 4-3 Security Objectives for Non-IT Environment

1N	ON.Install	Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security.
2N	ON.NoUntrusted	The administrator will ensure that there are no untrusted users and no untrusted software on the HP OpenView Operations for UNIX management server.
3N	ON.Operations	The TOE will be managed and operated in a secure manner as outlined in the supplied guidance.
4N	ON.ProtectAuth	Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.
5N	ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
6N	ON.Physical	Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, explicitly stated requirements based on Part 2 of the CC, assurance components from Part 3 of the CC, and CCIMB Final Interpretations.

5.1 Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.2 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 2 and paragraph 2.1.4 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified with a dash number "**-#**". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.
- *Explicitly Stated Requirements* will be noted with a "_EXP" added to the component name.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *NIAP and CCIMB Interpretations* have been reviewed. Relevant Interpretations are included and are noted in Interpretation Notes. Interpretation Notes are denoted by *italicized text.* The original CC text modified by the interpretation is not denoted nor explained.
- *Comments* are provided as an aid to the ST author and evaluation team. These items will be deleted in the final version of the ST.

5.2 TOE Security Functional Requirements

The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC, explicitly stated requirements based on components from Part 2 of the CC, and CCIMB Final Interpretations summarized in the Table 5-1 below.

Table 5-1 Functional Components

Item	Component	Component Name

Item	Component	Component Name
1.	FAU_GEN.1	Audit data generation
2.	FAU_SAR.1	Audit review
3.	FAU_SAR.2	Restricted audit review
4.	FAU_STG_EXP.1-1	Protected audit trail storage
5.	FDP_ACC_EXP.1-1	Subset access control
6.	FDP_ACF_EXP.1-1	Security attribute based access control
7.	FDP_ITT_EXP.1-1	Basic internal transfer protection
8.	FIA_ATD.1	User attribute definition
9.	FIA_UAU_EXP.2-1	User authentication before any action
10.	FIA_UID_EXP.2-1	User identification before any action
11.	FMT_MOF_EXP.1-1	Management of security functions behavior
12.	FMT_MSA_EXP.1-1	Management of security attributes
13.	FMT_MSA_EXP.3-1	Static attribute initialisation
14.	FMT_MTD_EXP.1-1	Management of TSF data
15.	FMT_SMF_EXP.1-1	Specification of management functions
16.	FMT_SMR_EXP.1-1	Security roles
17.	FPT_ITT_EXP.1-1	Basic internal TSF data transfer protection
18.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP
19.	FPT_SEP_EXP.1-1	TSF domain separation
20.	FTA_TAB.1	Default TOE access banners

5.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **[*not specified*]** level of audit; and

c) **[*the following auditable events (See Tables 5-2 and 5-3):***

Table 5-2 Auditable GUI and API Events

Subject	Audit Area	GUI Audit Event	API Audit Event
Operator	Logon, Logoff, Operator Action, Application	• Logon, including attempted logins (Note: Administrator and Template Administrator Logins are also audited on the Operator Level) • Logoff • Changes to the OVO user passwords (Note: There is no audit entry if the OVO admin changes an OVO user password) • OVO message-related operator initiated actions started from the browsers and application launches (incl. customized startup) *(Application Note: there is no audit event for startup or customized startup of applications of type 'Start URL on Local WEB Browser')*	
Administrator	Logon, Logoff	• Logon, including attempted logins • Logoff • Change password (Note! with PAM there is no way to change the password in the OVO GUI, but you need to change it directly in the plugged in user authentication system)	• Logon, including attempted logins • Logoff • Change password (Note! not possible with PAM in the OVO GUI)
	Operator Action, Application,	• Start Operator Action • Add, modify, or delete Application	• Start • Add, modify, or delete Application
	Template	• Add, modify, delete condition - within condition you can add automatic or operator-initiated action - forward to MSI (Message Stream Interface) Add, modify, copy, delete template	
	Node	• Add, modify, delete nodes • Distribute (templates, actions, monitors, or commands – not explicitely listed) • Assign template • Node certificate requests, grants, and denial	• Add, modify, delete nodes • Distribute (templates, actions, monitors, or commands – not explicitely listed) • Assign template • Node certificate requests, grants, and denial

Subject	Audit Area	GUI Audit Event	API Audit Event
	NodeGroup	• Add, modify, or delete • Assign managed node to node groups • Deassign managed node from node groups	• Add, modify, or delete • Assign managed node to node groups • Deassign managed node from node groups
	User	• Add, modify, or delete User or Profile - assign applications - assign profiles - assign nodes (via set up responsibility matrix sub (node groups X Message Groups)) - modify capabilities (Perform/Stop Actions only)	Add, modify, or delete - assign applications - assign profiles - set up responsibility matrix sub (node groups X Message Groups) - modify capabilities (Perform/Stop Actions only)
Template Administrator	Logon/Logoff	• Logon, including attempted logins • Logoff • Change password (Note! not possible with PAM in the OVO GUI)	• Logon, including attempted logins • Logoff • Change password (Note! not possible with PAM in the OVO GUI)
	Template	• Add, modify, delete condition - within condition you can add automatic or operator-initiated action - forward to MSI (Message Stream Interface) • Add, modify, copy, delete template	

Table 5-3 Auditable Events CLI Features Only

Level	Audit Area	Audit Event
Operator	Logon, Logoff	• Logon, including attempted logins • Logoff
Administrator	Logon, Logoff	• Logon, including attempted logins • Logoff
	Node	• Add, modify, delete nodes • Assign templates to nodes • Deassign templates from nodes • Remotely administer agent processes • Node certificate requests, grants, and denial • Change node address • Switch heartbeat polling on/off

Level	Audit Area	Audit Event
Administrator	NodeGroup	• Add, modify, delete node groups • Assign managed node to node group • Remove managed node from node group • Assign templates to node groups • Deassign templates from node groups
	Template	• Assign templates to nodes or node groups
	Audit Upload, Audit Download	• Upload audit logs into the database • Download audit logs
	Config Upload, Initialize DB,	• Upload configuration data • (Re-)Initialization of the database • Enable, disable, modify the customized start-up message
	History Upload, History Download	• Download acknowledged messages • Upload acknowledged messages
	OVO Services	• Upload service status logs

Application Note: In regards to the GUI audit events, OVO creates an audit entry when the action is carried out using the GUI.

In regards to the API audit events, OVO creates an audit entry when the action is carried out using an API. No entry in this column indicates only that no audit information is collected. It does not indicate that no APIs are available.

In regards to the CLI audit events, OVO creates an audit entry when the action is carried out using a command-line interface (CLI). No entry in this column indicates only that no audit information is collected. It does not indicate that no command line interfaces are available.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: **[*no other information*]**

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*the OVO administrator*]** with the capability to read **[*all audit information*]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: Audit information can be written to a report for future review, and can be displayed in the OVO Reports window. You can view these reports on your screen, write them to a file, or print them. The audit log is stored in the relational database which is outside of the TOE..

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

FAU_STG_EXP.1-1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG_EXP.1.1-1 The TSF shall protect the stored audit records from unauthorised deletion initiated through its own TSFI.

FAU_STG_EXP.1.2-1 The TSF shall be able to prevent unauthorised modifications to the audit records in the audit trail initiated through its own TSFI.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: The log files are stored encrypted within the relational database which is outside of the TOE.

5.2.2 Class FDP: User Data Protection

FDP_ACC_EXP.1-1 Subset access control

Hierarchical to: No other components.

FDP_ACC_EXP.1.1-1 The TSF shall enforce the HP OVO Access Control SFP on

Subjects: (OVO Administrators, Template Administrators, and Operators)

Objects: source node, messages, services, and templates

Operations:

- On Source Nodes:
  - Start and stop applications
  - Start and stop agent
- On messages:
  - Start and stop actions,
  - Acknowledge and un-acknowledge messages
  - Own and disown messages
  - Modify message attributes
  - Execute applications
- On services:
  - Start services action
- On templates:
  - Add and modify templates
  - Define and implement message policies
  - Download and sign templates.

Dependencies: FDP_ACF_EXP.1-1 Security attribute based access control

Application Note: Root is another subject (user role) that has the ability to affect the objects defined above through the use of CLIs. Root is required by HP OVO but is NOT within the TOE's Scope of Control. See FDP_ACC_EXP.1-2 Subset access control

FDP_ACF_EXP.1-1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF_EXP.1.1-1 The TSF shall enforce the HP OVO Access Control SFP to objects based on the following:

Subjects (OVO Administrators, Template Administrator, and Operators):

Capabilities

Responsibilities

Assigned Node Groups

Assigned Messages Groups

Assigned Services

Assigned Applications

Profiles

Objects (source nodes, messages, services, and templates):

Source Nodes (Influences amount and type of messages an operator can see and work on)

Message Groups (Influences amount and type of messages an operator can see and work on)

Services (Triggers amount and type of messages an operator can see and work on)

Templates (Influences message handling through policies and filtering conditions) .

FDP_ACF_EXP.1.2-1 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. Subjects (see FDP_ACF_EXP.1.1-1) may perform actions associated with the capabilities assigned to his/her role
2. Subjects are responsible for all messages belonging to the assigned message groups on their assigned nodes and for all messages that belong to assigned services.
   FYI, multiple operators may share the SAME responsibilities.
3. If a subject is granted an application, the application is available for the subject's use
4. If a subject is assigned a profile, the subject has the capabilities, responsibilities, applications, and profiles associated with that profile
5. A Subject can work on services that have been assigned to him/her.

Application Note: User profiles may be hierarchical.

FDP_ACF_EXP.1.3-1 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: no additional rules.

FDP_ACF_EXP.1.4-1 The TSF shall explicitly deny access of subjects to objects based on the following rules: no additional explicit deny rules.

Dependencies: FDP_ACC_EXP.1-1 Subset access control

FMT_MSA_EXP.3-1 Static attribute initialisation

Application Note: FDP_ACF_EXP.1-1 and FDP_ACF_EXP.1-2 (IT Environment) security attribute based access control policies are mutually exclusive. Both must be implemented in order to provide proper access control for the TOE's objects: FDP_ACF_EXP.1-1defines the enforcement for subjects accessing TSF objects using the administrative and operator GUI and FDP_ACF_EXP.1-2 defines the enforcement for root using OVO CLIs to access TSF objects.

FDP_ITT_EXP.1-1 Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT_EXP.1.1-1 The TSF shall enforce the HP OVO Access Control SFP to prevent the disclosure and modification of user data when it is transmitted between physically-separated parts of the TOE.

Dependencies: [FDP_ACC_EXP.1-1 Subset access control, or

FDP_IFC.1 Subset information flow control]

Application Note: Messages sent from OVO HTTPS Agent to OVO/UNIX management server are protected from disclosure and modification. The TOE relies on the IT Environment to secure the network path between TOE Components. The TSF calls the cryptographic modules which provide the cryptographic functions.

5.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **[*User Identity;***
- ***Roles user can assume (OVO Administrators, Template Administrator, Operator);***
- ***Assigned Profile(s);***
- ***Assigned Applications;***
- ***Assigned Message Groups;***
- ***Assigned Node Groups;***
- ***Assigned Services.***
- ***Assigned Capabilities***
  - ***Perform/Stop Actions,***
  - ***Modify Message Attributes,***
  - ***Own/Disown Messages,***
  - ***(Un-)Acknowledge Messages***
  - ***Execute applications.***
- ***Assigned Responsibilities***

]

Dependencies: No dependencies.

Application Note: Password is a user security attribute, but is controlled by the PAM which is outside the scope of the TOE.

FIA_UAU_EXP.2-1 User authentication before any action

Hierarchical to: No other components.

FIA_UAU_EXP.2.1-1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID_EXP.2-1 Timing of identification

Application Note: The TOE collects the authentication data via a login window, passes that information to the PAM, receives an allow/deny access response from the PAM, and then enforces the response. The PAM is external to the TOE. See FIA_UAU.5 in the IT Environment for more details.

FIA_UID_EXP.2-1 User identification before any action

Hierarchical to: No other components.

FIA_UID_EXP.2.1-1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.2.4 Class FMT: Security Management

FMT_MOF_EXP.1-1 Management of Security Functions Behavior

Hierarchical to: No other components.

FMT_MOF_EXP.1.1-1 The TSF shall restrict the ability to determine the behavior of, disable, enable, and modify the behavior of the functions audit (see FAU_GEN.1.1) to the OVO Administrator.

Dependencies: FMT_SMR_EXP.1-1 Security roles

FMT_SMF_EXP.1-1 Specification of Management Functions

FMT_MOF_EXP.1-2.

Application Note: FMT_MOF_EXP.1-1 and FMT_MOF_EXP.1-2 (IT Environment) management of security functions behaviour SFRs are required for a complete implementation of this function. Both must be implemented in order to provide proper restriction to the same TSF function: FMT_MOF_EXP.1-1defines the restriction for subjects accessing TSF functions using the administrative GUI and FMT_MOF_EXP.1-2 defines the restriction for root using OVO CLIs to access TSF functions. Since it is a stated requirement that the OVO administrator must have root privilege and has use of both interfaces (GUI and CLI) to access the same function, there is an added dependency of FMT_MOF_EXP.1-2.

FMT_MSA_EXP.1-1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA_EXP.1.1-1 The TSF shall enforce the **[*HP OVO Access Control SFP*]** to restrict the ability to **[*query, modify, delete,* [*see operations specified in Table 5-4*]]** the security attributes **[*as specified in Table 5-4*]** to **[*the role as specified in Table 5-4*]**.

Dependencies: [FDP_ACC_EXP.1-1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR_EXP.1-1 Security roles

FMT_SMF_EXP.1-1 Specification of Management Functions

FMT_MSA_EXP.1-2 Management of security attributes

Application Note: FMT_MSA_EXP.1-1 and FMT_ MSA _EXP.1-2 (IT Environment) management of security attributes SFRs are required for a complete implementation of this function. Both must be implemented in order to provide proper restriction to the same TSF data: FMT_ MSA _EXP.1-1defines the restriction for subjects accessing TSF data using the administrative GUI and FMT_ MSA _EXP.1-2 defines the restriction for root using OVO CLIs to access TSF data. Since it is a stated requirement that the OVO administrator must have root privilege and has use of both interfaces (GUI and CLI) to access the same TSF data, there is an added dependency of FMT_ MSA _EXP.1-2.

Table 5-4 Management of Security Attributes

Subjects with roles of the following:	Allowed Action on Specified Security Attributes
OVO Administrator (opc_adm)	• Query and modify roles (template administrator or operator); assign users to roles • Create, query, modify, and delete user identity • Create, query, modify, and delete profiles; assign users to profiles • Query, add, modify, or delete applications; assign applications to users or profiles • Query, add, modify, or delete nodes, node groups and message groups; assign node groups and message groups to users or profiles • Query, add, modify, or delete services; assign services to operators • Query, add, modify, or delete capabilities; assign capabilities to users or profiles • Query, add, modify, or delete responsibilities; assign responsibilities to users or profiles

FMT_MSA_EXP.3-1 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA_EXP.3.1-1 The TSF shall enforce the **[*OVO Access control SFP*]** to provide **[*permissive*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA_EXP.3.2-1 The TSF shall allow the **[*OVO Administrator*]** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA_EXP.1-1 Management of security attributes

FMT_SMR_EXP.1-1 Security roles

FMT_MSA_EXP.3-1 Static attribute initialisation

Application Note: FMT_MSA_EXP.3-1 and FMT_ MSA _EXP.3-2 (IT Environment) static attribute initialization SFRs are required for a complete implementation of this function. Both must be implemented in order to provide proper restriction to the same TSF data: FMT_ MSA _EXP.3-1defines the restriction for subjects accessing TSF data using the administrative GUI and FMT_ MSA _EXP.3-2 defines the restriction for root using OVO CLIs to access TSF data. Since it is a stated requirement that the OVO administrator must have root privilege and has use of both interfaces (GUI and CLI) to access the same TSF data, there is an added dependency of FMT_ MSA _EXP.3-2.

FMT_MTD_EXP.1-1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD_EXP.1.1-1 The TSF shall restrict the ability to **[*change_default*, *query, modify, delete,* [*see operations specified in Table 5-5*]]** the **[*TSF Data as specified in Table 5-5*]** to **[*the role as specified in Table 5-5*].**

Dependencies: FMT_SMR_EXP.1-1 Security roles

FMT_SMF_EXP.1-1 Specification of Management Functions

FMT_MTD_EXP.1-2.

Application Note: FMT_ MTD _EXP.1-1 and FMT_ MTD _EXP.1-2 (IT Environment) management of TSF data SFRs are required for a complete implementation of this function. Both must be implemented in order to provide proper restriction to the same TSF data: FMT_ MTD _EXP.1-1defines the restriction for subjects accessing TSF data using the administrative GUI and FMT_ MTD _EXP.1-2 defines the restriction for root using OVO CLIs to access TSF data. Since it is a stated requirement that the OVO administrator must have root privilege and has use of both interfaces (GUI and CLI) to access the same TSF data, there is an added dependency of FMT_ MTD _EXP.1-2.

Table 5-5 Management of TSF Data

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 unacknowledge messages • Start and customized start of applications • Unbuffering of pending messages, which have been arrived outside the configured service hours

FMT_SMF_EXP.1-1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF_EXP.1.1-1 The TSF shall be capable of performing the following security management functions: **[**

- ***determine the behavior of, disable, enable, and modify the behavior of the functions audit (see FAU_GEN.1.1) (see FMT_MOF_EXP.1-1),***
- ***query, modify, delete, and create the security attributes as specified in Table 5-4 (see FMT_MSA_EXP.1-1),***
- ***change_default, query, modify, delete, and create as specified in Table 5-5 and the TSF Data as specified in Table 5-5 (See FMT_MTD_EXP.1-1)*****].**

Dependencies: FMT_SMF_EXP.1-2.

Application Note: FMT_ SMF _EXP.1-1 and FMT_ SMF _EXP.1-2 (IT Environment) specification of management functions SFRs are required for a complete implementation of this function. Both must be implemented in order to provide proper restriction to the same TSF function: FMT_ SMF _EXP.1-1 defines the capabilities for TSF functions using the administrative GUI and FMT_ SMF _EXP.1-2 defines the defines the capabilities for TSF functions using OVO CLIs. Since it is a stated requirement that the OVO administrator must have root privilege and has use of both interfaces (GUI and CLI) to access the same TSF data, there is an added dependency of FMT_ SMF _EXP.1-2.

FMT_SMR_EXP.1-1 Security roles

Hierarchical to: No other components.

FMT_SMR_EXP.1.1-1 The TSF shall maintain the roles **[*OVO Administrator, Template Administrator, Operator*].**

FMT_SMR_EXP.1.2-1 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID_EXP.2-1 Timing of identification

Application Note: Root is another subject (user role) that has the ability to affect the TOE and TSF Data through the use of CLIs. Root is required by HP OVO but is NOT within the TOE's Scope of Control. See FMT_SMR_EXP.1-2 Security Roles

5.2.5 Class FPT: Protection of the TOE Security Functions

FPT_ITT_EXP.1-1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT_EXP.1.1-1 The TSF shall protect the OVO HTTPS Agent's Configuration Policy from modification when it is transmitted between the separate parts of the TOE and while stored on the OVO HTTPS Agent machine.

Dependencies: No dependencies.

FPT_RVM_EXP.1-1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP.1-1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP_1.1-1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP_1.2-1 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2.6 Class FTA: TOE access

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

Dependencies: No dependencies.

5.2.7 Strength of Function

There is an overall strength of function claim of SOF-Basic. The strength of function requirement does not apply to a specific SFR since FIA_SOS.1 is not included in this ST.

5.3 IT Environment Security Requirements

HP OpenView Operations for UNIX requires:

- The operating system platform provide reliable time stamps.
- The operating system to provide file storage and protection for the TOE audit trail.
- Cooperation of the operating system to provide TSF domain separation and Non-bypassability of the TSP.
- The operating system to have identification and authentication for access to system.
- The operating system is configured to have a role of *root* and has an access control policy that restricts the use of the OVO command line interfaces of the TOE to *root*.
- All cryptographic functions are part of the IT environment, not part of the TOE.

Table 5-6 Functional Components for the IT environment

Item	Component	Component Name
21.	FAU_STG_EXP.1-2	Protected audit trail storage
22.	FCS_CKM.1*	Cryptographic key generation
23.	FCS_CKM.4	Cryptographic key destruction
24.	FCS_COP.1*	Cryptographic operation
25.	FDP_ACC_EXP.1-2	Subset access control
26.	FDP_ACF_EXP.1-2	Security attribute based access control

Item	Component	Component Name
27.	FDP_ITT_EXP.1-2	Basic internal transfer protection
28.	FIA_UAU_EXP.2-2	User authentication before any action
29.	FIA_UID_EXP.2-2	User identification before any action
30.	FMT_MOF_EXP.1-2	Management of security functions behavior
31.	FMT_MSA_EXP.1-2	Management of security attributes
32.	FMT_MSA.2	Secure security attributes
33.	FMT_MSA_EXP.3-2	Static attribute initialisation
34.	FMT_MTD_EXP.1-2	Management of TSF data
35.	FMT_SMF_EXP.1-2	Specification of management functions
36.	FMT_SMR_EXP.1-2	Security roles
37.	FPT_ITT_EXP.1-2	Basic internal TSF data transfer protection
38.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
39.	FPT_SEP_EXP.1-2	TSF domain separation
40.	FPT_STM.1	Reliable time stamps
41.	FIA_UAU.5	Multiple authentication mechanisms

5.3.2 Class FAU: Security Audit

FAU_STG_EXP.1-2 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG_EXP.1.1-2 The IT Environment shall protect the stored audit records in the TSF audit trail from unauthorised deletion initiated through the IT Environment's Interfaces.

FAU_STG_EXP.1.2-2 The IT Environment shall be able to prevent unauthorised modifications to the audit records in the TSF audit trail initiated through the IT Environment's Interfaces.

Dependencies: FAU_GEN.1 Audit data generation

5.3.3 Class FCS: Cryptographic Functions -

FCS_CKM.1-1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1-1 **Refinement:** The ***IT environment*** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*Triple-DES*]** and specified cryptographic key sizes **[*168 bit*]** that meet the following: **[*Data Encryption Standard (DES), FIPS PUB 46-3*]**.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.1-2 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1-2 **Refinement:** The ***IT environment*** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*Blowfish*]** and specified cryptographic key sizes **[*128 bit*]** that meet the following: **[*Vendor Affirmed*]**.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.1-3 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1-3 **Refinement:** The ***IT environment*** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*RSA*]** and specified cryptographic key sizes **[*1024 bits*]** that meet the following: **[*ANSI X9.31*; *Digital Signature Standard (DSS), FIPS PUB 186-2*]**.

Dependencies: [FCS_CKM.2 Cryptographic key distribution
or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 **Refinement:** The ***IT environment*** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[*which zeroizes all plaintext cryptographic keys*]** that meets the following: **[*none*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

FCS_COP.1-1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1-1**Refinement:** The ***IT environment*** shall perform **[*symmetric key encryption and decryption*]** in accordance with a specified cryptographic algorithm **[*Triple-DES*]** and cryptographic key sizes **[*168 bit*]** that meet the following: **[*Data Encryption Standard (DES), FIPS PUB 46-3*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1-2 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.2-2 **Refinement:** The ***IT environment*** shall perform **[*symmetric key encryption and decryption*]** in accordance with a specified cryptographic algorithm **[*Blowfish*]** and cryptographic key sizes **[*128 bit*]** that meet the following: **[*Vendor Affirmed*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1-3 Cryptographic operation

FCS_COP.1.1-3 **Refinement:** The ***IT environment*** shall perform **[*authentication with public key encryption and decryption*]** in accordance with a specified cryptographic algorithm **[*RSA*]** and cryptographic key sizes **[*1024 bit*]** that meet the following: **[*ANSI X9.31*;*Digital Signature Standard (DSS), FIPS PUB 186-2*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1-4 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1-4 **Refinement:** The ***IT environment*** shall perform **[*hashing functions of the OVO HTTPS Agent's Configuration Policy*]** in accordance with a specified cryptographic algorithm **[*SHA-1*]** and cryptographic key sizes **[*160 bit*]** that meet the following: **[*Secure Hash Standard (SHS), FIPS PUB 180-2*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.3.4 Class FDP: User Data Protection

FDP_ACC_EXP.1-2 Subset access control

Hierarchical to: No other components.

FDP_ACC_EXP.1.1-2 The IT environment shall enforce the OS Access Control SFP on

Subjects: (root)

Objects: OVO command line interface executables

Operations: execute

Dependencies: FDP_ACF_EXP.1-2 Security attribute based access control

FDP_ACF_EXP.1-2 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF_EXP.1.1-2 The IT environment shall enforce the OS Access Control SFP to objects based on the following:

Subjects (root):

Assigned Administration Group

Objects (OVO command line interface executable):

OVO command line interface executable (Influences configuration and operation of the TOE.)

FDP_ACF_EXP.1.2-2 The IT environment shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. Subjects included in the administration group have root privilege.

2. Subjects may execute OVO command line interface executables if the subject belongs to the administration group.

FDP_ACF_EXP.1.3-2 The IT environment shall explicitly authorise access of subjects to objects based on the following additional rules: no additional rules.

FDP_ACF_EXP.1.4-2 The IT environment shall explicitly deny access of subjects to objects based on the following rules: no additional explicit deny rules.

Dependencies: FDP_ACC_EXP.1-2 Subset access control

FMT_MSA_EXP.3-2 Static attribute initialization

FDP_ITT_EXP.1-2 Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT_EXP.1.1-2 The IT environment shall enforce the HP OVO Access Control SFP to prevent the disclosure and modification of user data when it is transmitted between physically-separated parts of the TOE.

Dependencies: [FDP_ACC_EXP.1-2 Subset access control, or

FDP_IFC.1 Subset information flow control]

Application Note: The TOE relies on the IT Environment to secure the network path between TOE Components.

5.3.5 Class FIA: Identification and Authentication

FIA_UAU_EXP.2-2 User authentication before any action

Hierarchical to: No other components.

FIA_UAU_EXP.2.1-2 The IT environment shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID_EXP.2-2 Timing of identification

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 **Refinement:** The IT Environment shall provide **[*the following multiple authentication mechanisms:***

1. **Password authentication for OS Users**
2. **Password authentication for TOE Users]**

to support user authentication.

FIA_UAU.5.2 **Refinement:** The IT Environment shall authenticate any user's claimed identity according to the **[rules:**

1. If a user accesses the TOE from the OS command line interface, then the OS User password mechanism shall be used.

2. If a user accesses the TOE from the Java GUI or OVO Motif Admin GUI, then the TOE User password mechanism shall be used.]

Dependencies: No dependencies.

Application Note: TOE user password mechanism is the PAM. PAM enables multiple authentication technologies to be added without changing any of the login services, thereby preserving existing system environments. It is possible that the configured authorization file/db is the same storage location for both the OS and the TOE.

FIA_UID_EXP.2-2 User identification before any action

Hierarchical to: No other components.

FIA_UID_EXP.2.1-2 The IT environment shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.3.6 Class FMT: Security Management

FMT_MOF_EXP.1-2 Management of Security Functions Behavior

Hierarchical to: No other components.

FMT_MOF_EXP.1.1-2 The IT environment shall restrict the ability to determine the behavior of, disable, enable, and modify the behavior of the functions audit (see FAU_GEN.1.1) to root.

Dependencies: FMT_SMR_EXP.1-2 Security roles

FMT_SMF_EXP.1-2 Specification of Management Functions

FMT_MSA_EXP.1-2 Management of security attributes

Hierarchical to: No other components.

FMT_MSA_EXP.1.1-2 The IT environment shall enforce the OS Access Control SFP to restrict the ability to query, modify, delete, see operations specified in Table 5-7 the security attributes as specified in Table 5-7 to the role as specified in Table 5-7.

Dependencies: [FDP_ACC_EXP.1-2 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR_EXP.1-2 Security roles

FMT_SMF_EXP.1-2 Specification of Management Functions

Table 5-7 Management of Security Attributes

Application Note: The root user on the OVO/UNIX management server has the same access to perform administrative commands as the OVO Administrator.

Subjects with roles of the following:	Allowed Action on Specified Security Attributes
root	• Query and modify roles (template administrator or operator); assign users to roles • Create, query, modify, and delete user identity • Create, query, modify, and delete profiles; assign users to profiles • Query, add, modify, or delete applications; assign applications to users or profiles • Query, add, modify, or delete nodes, node groups and message groups; assign node groups and message groups to users or profiles • Query, add, modify, or delete services; assign services to operators • Query, add, modify, or delete capabilities; assign capabilities to users or profiles • Query, add, modify, or delete responsibilities; assign responsibilities to users or profiles

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 **Refinement:** The ***IT environment*** shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC_EXP.1-2 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA_EXP.1-2 Management of security attributes
FMT_SMR_EXP.1-2 Security roles

FMT_MSA_EXP.3-2 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA_EXP.3.1-2 The IT environment shall enforce the OS Access control SFP to provide permissive default values for security attributes that are used to enforce the OVO Access control SFP.

FMT_MSA_EXP.3.2-2 The IT environment shall allow the root to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA_EXP.1-2 Management of security attributes

FMT_SMR_EXP.1-2 Security roles

FMT_MTD_EXP.1-2 Management of TSF data

Hierarchical to: No other components.

FMT_MTD_EXP.1.1-2 The IT environment shall restrict the ability to change_default, query, modify, delete, see operations specified in Table 5-8 the TSF Data as specified in Table 5-8 to the role as specified in Table 5-8.

Dependencies: FMT_SMR_EXP.1-2 Security roles

FMT_SMF_EXP.1-2 Specification of Management Functions

Table 5-8 Management of TSF Data

Roles	Allowed Operations on TSF Data (Management Functions)
root	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

FMT_SMF_EXP.1-2 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF_EXP.1.1-2 The IT environment shall be capable of performing the following security management functions:

- determine the behavior of, disable, enable, and modify the behavior of the functions audit (see FAU_GEN.1.1) (see FMT_MOF_EXP.1-2),
- query, modify, delete, and create the security attributes as specified in Table 5-7 (see FMT_MSA_EXP.1-2),
- change_default, query, modify, delete, and create as specified in Table 5-8 and the TSF Data as specified in Table 5-8 (See FMT_MTD_EXP.1-2).

Dependencies: No Dependencies

FMT_SMR_EXP.1-2 Security roles

Hierarchical to: No other components.

FMT_SMR_EXP.1.1-2 The IT environment shall maintain the roles root.

FMT_SMR_EXP.1.2-2 The IT environment shall be able to associate users with roles.

Dependencies: FIA_UID_EXP.2-2 Timing of identification

5.3.7 Class FPT: Protection of the TOE Security Functions

FPT_ITT_EXP.1-2 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT_EXP.1.1-2 The IT environment shall protect TSF data from **[*disclosure and modification*]** when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies.

Application Note: The TOE relies on the IT Environment to secure the network path between TOE Components.

FPT_RVM_EXP.1-2 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-2 The IT environment shall ensure that Operating System Security Policy enforcement functions are invoked and succeed before each function within the Operating System's Scope of Control is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP.1-2 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP1.1-2 The IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface.

FPT_SEP_EXP.1.2-2 The IT environment shall enforce separation between the security domains of subjects in the Operating System's Scope of Control.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.4 TOE Security Functional Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed below.

Table 5-9 EAL2 Assurance Components

Item	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

5.2.2 Overview

The following sections describe the IT Security Functions of the OVO/UNIX management server Interface, the Administrator and Operator Interfaces. Together these interfaces provide the security functions which satisfy the TOE security functional requirements. This section includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met. In section 6.1.2, the OVO/UNIX management server Interface, the Administrator and Operator Interfaces, and CLIs will be mutually referred to as HP OpenView Operations for UNIX. The OVO HTTPS Agent interface will be referred to as the OVO HTTPS Agent.

Table 6-1 Security Functional Requirements mapped to Security Functions

SFRs	Security Class	Security Functions	Sub-functions
FAU_GEN.1	Security audit	Audit Capability	OA-1
FAU_SAR.1	Security audit	Audit Capability	OA-2
FAU_SAR.2	Security audit	Audit Capability	OA-3
FAU_STG_EXP.1-1	Security audit	Audit Capability	OA-4
FDP_ACC_EXP.1-1	User data protection	Access Control	OAC-1
FDP_ACF_EXP.1-1	User data protection	Access Control	OAC-1
FDP_ITT_EXP.1-1	User data protection	Access Control	OAC-5
FIA_ATD.1	Identification and authentication	Security management	SM-1
FIA_UAU_EXP.2-1	Identification and authentication	Identification and Authentication	OIA-1
FIA_UID_EXP.2-1	Identification and authentication	Identification and Authentication	OIA-2
FMT_MOF_EXP.1-1	Security management	Security management	SM-2
FMT_MSA_EXP.1-1	Security management	Security management	SM-3
FMT_MSA_EXP.3-1	Security management	Security management	SM-4
FMT_MTD_EXP.1-1	Security management	Security management	SM-5
FMT_SMF_EXP.1-1	Security management	Security management	SM-6
FMT_SMR_EXP.1-1	Security management	Security management	SM-7
FPT_ITT_EXP.1-1	Protection of the TSF	Access Control	OAC-2
FPT_RVM_EXP.1-1	Protection of the TSF	Access Control	OAC-3
FPT_SEP_EXP.1-1	Protection of the TSF	Access Control	OAC-4
FTA_TAB.1	TOE access	Identification and Authentication	OIA-3

5.2.3 Audit Capability

OA-1 Audit data generation (FAU_GEN.1)

HP OpenView Operations for UNIX provides an audit trail function. OVO maintains audit information about user logins and logouts, including attempted logins and changes to OVO user passwords. In addition, OVO creates audit entries when actions are started from the message browsers, and when the configuration of OVO users, managed nodes, node groups, or templates changes.

The TSF shall be able to generate an audit record of the specified auditable events: see Table 5-2 in section 5.2.

The following information is recorded for all events:

- Date and time of event,
- Type of event,
- Subject identity,
- Success or failure of event.

OA-2 Audit review (FAU_SAR.1)

HP OpenView Operations for UNIX provides the OVO administrator with the capability to read all audit information from the audit records. The audit records are provided in a manner suitable for the user to interpret the information. Audit information can be written to a report for future review, and can be displayed in the OVO Reports window. An authorized administrator can view these reports on the screen, write them to a file, or print them. The audit log is stored in the relational database which is outside of the TOE.

OA-3 Restricted audit review (FAU_SAR.2)

The TSF prohibits all users read access to the audit records, except those users that have been granted explicit read-access.

OA-4 Protected audit trail storage (FAU_STG_EXP.1-1)

The TSF protects the stored audit records in the audit trail from unauthorised deletion via the OVO Admin GUI and by offering CLIs, only available to the *root* user on the OVO/UNIX management server, to support the upload and download of the audit records. The TSF is able to prevent unauthorised modifications to the audit records in the audit trail, because no corresponding APIs/CLIs are offered. The TSF logs each audit up/download activities again as new audit entries. The log files are stored within the relational database which is outside of the TOE..

5.2.4 Access Control

The OVO Access Control Security Functional Policy is based on the following subjects, objects, and operations:

OAC-1 Access control function (FDP_ACC_EXP.1-1) (FDP_ACF_EXP.1-1)

HP OpenView Operations for UNIX enforces the HP OVO Access Control SFP on the specified subjects objects and operations among subjects and objects covered by the SFP:

Subjects: (OVO Administrators, Template Administrators, and Operators)

Objects: source node, messages, services, and templates

Operations:

On Source Nodes:

Start and stop applications

Start and stop agent

On messages:

Start and stop actions,

Acknowledge and un-acknowledge messages

Own and disown messages

Modify message attributes

Execute applications

On services:

Start services action

On templates:

Add and modify templates

Define and implement message policies

Download and sign templates.

HP OVO enforces the HP OVO Access Control SFP to objects based on the following security attributes:

Subjects (OVO Administrators, Template Administrator, and Operators):

Capabilities

Responsibilities

Assigned Nodes

Assigned Messages Groups

Assigned Services

Assigned Applications

Profiles

Objects (source nodes, messages, services, and templates):

Source Nodes (Influences amount and type of messages an operator can see and work on)

Message Groups (Influences amount and type of messages an operator can see and work on)

Services (Triggers amount and type of messages an operator can see and work on)

Templates (Influences message handling through policies and filtering conditions) .

HP OVO will enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. The operator may perform actions associated with the capabilities assigned to his/her role
2. The operator is responsible for all messages belonging to the assigned message groups on their assigned nodes and for all messages that belong to assigned services.
   FYI, multiple operators may share the SAME responsibilities.
3. If an operator is granted an application, the application is available for the operator's use
4. If an operator is assigned a profile, the user has the capabilities, responsibilities, applications, and profiles associated with that profile
5. Operator can work on services that have been assigned to him/her].

Application Note: User profiles may be hierarchical.

Operators are assigned varying responsibilities and capabilities. 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. By creating task-orientated environments, OVO operators see only the information from systems and objects under their control. Operators are assigned nodes or group of nodes, messages groups, services, applications, and profiles.

When configuring an operator's access control the following items are set:

- **Capabilities -** These are permissions to start and stop actions, to acknowledge and unacknowledge, to own and disown messages, and to modify message attributes.
- **Responsibilities -** The operator is responsible for all events belonging to the assigned message groups on their assigned nodes.
- **Applications -** These are the applications and tools available to the operators in their particular Application Desktop window.
- **Profiles -** These are preconfigured user profiles that define the configuration of abstract OVO users.

The Operating System's Access Control Policy controls the access that the *root* user has in executing OVO CLIs.

OAC-2 Basic internal TSF data transfer protection (FPT_ITT_EXP.1-1)

The TSF shall protect the OVO HTTPS Agent's Configuration Policy from modification when it is transmitted between the separate parts of the TOE and while stored on the OVO HTTPS Agent machine. The OVO/UNIX management server digitally signs the OVO HTTPS Agent's Configuration Policy file for the protection of the file from modification during transmission. The digital signature is verified by the HTTPS Agent prior to installing the policy. If the file has been modified in any way, the hash will detect the modification and the policy will not be installed by the OVO HTTPS Agent. The TOE calls the cryptographic module that provides hashing function.

OAC-3 Non-bypassability of the TSP (FPT_RVM_EXP.1-1)

The TSF after being invoked by the OS ensures that TOE security functions are non-bypassable. HP OVO ensures that security protection enforcement functions are invoked and succeed before each function within HP OVO's scope of control is allowed to proceed. All management user operations are conducted in the context of an associated management session. This management session is allocated only after successful authentication into the TOE. User operations are checked for conformance to the granted level of access, and rejected if not conformant. The management session is destroyed when the corresponding user logs out of that session.

OAC-4 TSF domain separation (FPT_SEP_EXP.1-1)

HP OpenView Operations for UNIX maintains a security domain for its own execution and enforces separation between the security domains of users initiating actions through its own Administrator and Operator Interfaces.

The TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. OVO/UNIX management server is a passive device in that it indirectly connects to networks via other devices' e.g. network interface.

HP OVO's protected domain includes the HP OVO software and all of its software components.

The TSF enforces separation between the security domains of subjects in the TSC. HP OVO maintains separation between data from different input interfaces.

In addition to the HP OVO-specific software, other software files such as configuration files are also stored on disk. HP OVO relies partially on the Operating System to provide file access permissions and identification and authentication of users at the OS level. In addition, HP OVO relies on the OS for file process separation. These configuration files can be modified by an authorized administrator

accessing them through the HP OVO GUI interface, or by *root* using CLIs, or by *root* using file editor. The HP OVO Access Control Policy is providing protection to accessing these files. The underlying assumption regarding the operation of HP OVO is that it is maintained in a physically secure environment.

OAC-5 Basic internal transfer protection (FDP_ITT_EXP.1-1)

Messages sent from the OVO HTTPS Agent to the OVO/UNIX management server are protected from disclosure and modification. The TOE relies on the IT Environment to secure the network path between TOE Components. The TSF calls the cryptographic modules of OpenSSL which provide the cryptographic functions.

The OVO HTTPS Agent uses bind two-way certificate-based SSL without password (client and server authentication; also known as mutual authentication) to support OVO HTTPS Agent authentication. The OVO/UNIX management server shall authenticate any OVO HTTPS Agent's claimed identity according to the industry standard X.509 certificate based authentication.

5.2.5 Identification and Authentication

OIA-1 User authentication before any action (FIA_UAU_EXP.2-1)

HP OpenView Operations for UNIX requires each user to successfully authenticate with a password before being allowed any other actions. HP Openview relies on the Operating System to provide authentication of the *root* user before being allowed to manage TOE functions through the CLI.

HP OpenView Operations for UNIX provides Pluggable Authentication Module (PAM) for users during the Java GUI or OVO Motif Admin GUI login sequences to support user authentication. HP OpenView Operations for UNIX shall authenticate any user's claimed identity by collecting the authentication data through a login window. After checking to see if the identity is registered as an approved user of OVO/UNIX, this information is then passed to the PAM. If the PAM is configured for /etc/passwd, then the user must enter the correct password that corresponds with the /etc/passwd file to be authenticated. If the PAM is configured for LDAP authentication, then the user must enter the correct password to be authenticated by the LDAP Server. The PAM will then send a Allow/Deny back to the TOE. The TOE then enforces the authentication decision.

Application Note: PAM enables multiple authentication technologies to be added without changing any of the login services, thereby preserving existing system environments.

OIA-2 User identification before any action (FIA_UID_EXP.2-1)

The HP OpenView Operations for UNIX requires each user to identify himself/herself before being allowed to perform any other actions. HP Openview relies on the Operating System to provide identification of the *root* user before being allowed to manage TOE functions through the CLI.

OIA-3 Default TOE access banners (FTA_TAB.1)

The HP OpenView Operations for UNIX displays an advisory warning message regarding unauthorized use of the TOE before a user session is established.

According to the NIST 800-37 standard, usage and criticality of any application should be acknowledged before its startup, as well as allowance for its usage. This is achieved with a warning message displayed before the application is started. By default, the OVO GUI startup message does not exist. An authorized administrator can create it by writing the text in the text editor and storing the message into the database. An authorized administrator can also set and change its status (enabled or disabled). The OVO GUI startup message appears, if it is enabled, after the login window. If the agreement defined in this message is accepted, OVO starts. Otherwise, the login sequence is stopped immediately. If the OVO GUI startup message is disabled, OVO starts right after the login

window. An authorized administrator can create the OVO startup message both for the Java and Motif GUI.

5.2.6 Security Management

SM-1 User attribute definition (FIA_ATD.1)

HP OpenView Operations for UNIX maintains the following information for each user:

- User Identity;
- Roles user can assume (OVO Administrator, Template Administrator, and Operator);
- Assigned Profile(s);
- Assigned Applications;
- Assigned Message Groups;
- Assigned Node Groups;
- Assigned Services
- Assigned Capabilities
    - Perform/Stop Actions,
    - Modify Message Attributes,
    - Own/Disown Messages,
    - (Un-)Acknowledge Messages.

Application Note: Password is a user security attribute, but is controlled by the PAM which is outside the scope of the TOE.

SM-2 Management of Security Functions Behavior (FMT_MOF_EXP.1-1)

HP OpenView Operations for UNIX restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and the audit function (see FAU_GEN.1.1) to the OVO Administrator. Management of the audit function is also allowed through the CLI to the *root* user.

SM-3 Management of security attributes (FMT_MSA_EXP.1-1)

HP OpenView Operations for UNIX restricts the ability to query, modify, delete, and create the specified security attributes (see Table 5-4) to the specified users (see Table 5-4). The management of security attributes is allowed through the CLI to the *root* user (see Table 5-7).

SM-4 Static attribute initialisation (FMT_MSA_EXP.3-1)

HP OpenView Operations for UNIX provides permissive default values for security attributes as specified in the HP OVO Access Control SFP and allows the OVO administrator to specify alternative initial values. Through the CLI, the Operating System provides permissive default values for security attributes as specified in the HP OVO Access Control SFP and allows the *root* user to specify alternative initial values.

Table 6-2 Default security attributes

Security Attributes	Defaults
roles	Fixed: Administrator, Template Administrator, Operator
user identity	opc_adm, opc_op, netop, itop
profiles	None
applications	Many

Security Attributes	Defaults
message groups	Many
nodes	Dynamic: <MGMT_SERVER>
services	SVCDISC:Applications SVCDISC:System
capabilities	Perform/Stop Actions Own / Disown Messages Modify Message Attributes (Un-) Acknowledg Messages
operator roles	opc_op, netop, itop
administrator roles	opc_adm
template administrator roles	None

SM-5 Management of TSF data (FMT_MTD_EXP.1-1)

HP OpenView Operations for UNIX restricts the ability to access data as specified in Table 5-5. Through the CLI interface, the Operating System restricts the ability to access TSF data as specified in Table 5-8.

SM-6 Specification of Management Functions (FMT_SMF_EXP.1-1)

HP OpenView Operations for UNIX provides the following security management functions through the OVO Administrator Interface and via the CLI:

- determine the behavior of, disable, enable, and modify the behavior of the functions audit (see FAU_GEN.1.1) (see FMT_MOF_EXP.1-1),
- query, modify, delete, and create the security attributes as specified in Table 5-4 (see FMT_MSA_EXP.1-1),
- change_default, query, modify, delete, and create as specified in Table 5-5 and the TSF Data as specified in Table 5-5 (See FMT_MTD_EXP.1-1).

SM-7 Security roles (FMT_SMR_EXP.1-1)

HP OpenView Operations for UNIX maintains the following trusted roles:

- OVO Administrator,
- Template Administrator, and
- Operator.

The Operating System maintains the role of *root*.

5.2.7 SOF Claims

There is an overall SOF Claim of SOF-Basic. There is no specific SOF Claims, since FIA_SOS.1 is not included in this ST.

5.3 Assurance Measures

The HP OpenView Operations for UNIX satisfies the assurance requirements for Evaluation Assurance Level EAL2. The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-3 Assurance Measures and How Satisfied

Configuration Managment ACM_CAP.2

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

Delivery Procedures ADO_DEL.1

Related Files	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.

Installation, Generation, and Start-Up procedures ADO_IGS.1

Related Files	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 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
InstallationGuide_HP_Edn_2.pdf	HP OpenView Operations -Installation GuideSoftware Version A.08.10 for HP-UX
InstallationGuide_Sol_Edn_2.pdf	HP OpenView Operations -Installation GuideSoftware 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

Functional Specification ADV_FSP.1

Related Files	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

High Level Design ADV_HLD.1

Related Files	Description
SecurityFeaturesOfOVO8.ppt	Highlevel documentation of the security features provided by the new HTTPS based Server <-> Agent communication.
Design_Docs/HLDs	MS Visio 2003 Highlevel 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

Representation Correspondence ADV_RCR.1

Related Files	Description
FSP_interfaces_idx.xls	The FSP maps security relevant functionality, OVO commands and testcasesr.

Administrator Guidance AGD_ADM.1

Related Files	Description
InstallationGuide_HP_Edn_2.pdf	HP OpenView Operations -Installation GuideSoftware Version A.08.10 for HP-UX
InstallationGuide_Sol_Edn_2.pdf	HP OpenView Operations -Installation GuideSoftware 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 OnlineHelp A.08.10
http://ovweb.external.hp.com/lpe/doc_serv/	External available Documentation for HP OpenView

User Guidance ADG_USR.1

Related Files	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 OnlineHelp A.08.10
http://ovweb.external.hp.com/lpe/doc_serv/	External available Documentation for HP OpenView

Test Coverage Analysis ATE_COV.1

Related Files	Description
FSP_interfaces_idx.xls	The FSP maps security relevant functionality and testcases.
cc_eal2_testcases.doc	Documentation of the EATE driven command line testcases.
CC_Security Testcases	All manual Adminstrator GUI, automated EATE, manual and automated XDE (Java Operator GUI) Testcase sources

Test Documentation ATE_FUN.1

Related Files	Description
FSP_interfaces_idx.xls	The FSP maps security relevant functionality and testcases.
cc_eal2_testcases.doc	Documentation of the EATE driven command line testcases.
CC_Security Testcases	All manual Adminstrator GUI, automated EATE, manual and automated XDE (Java Operator GUI) Testcase 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 GUI Translated Rational Testmanager 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 GUI Translated Rational Testmanager Report (HP-UX 11.11 <-> Solaris 9) *complementary tests in Böblingen*
XDE Report: XP-HPUX11.11-Win2003_JavaGUI.html	Automated OVO/Unix Java Operator GUI Translated Rational Testmanager 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 GUI Translated Rational Testmanager Report (Solaris 9 <-> Solaris 9) *complementary tests in Böblingen*
XDE Report: XP-Solaris9.0-RedHat_JavaGUI.html	Automated OVO/Unix Java Operator GUI Translated Rational Testmanager Report (Solaris 9 <-> RedHat-AS 3.0) *complementary tests in Böblingen*
XDE Report: XP-Solaris9-Win2003_JavaGUI.html	Automated OVO/Unix Java Operator GUI Translated Rational Testmanager 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 GUI 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*

All Tests in Ft. Collins are executed in a separated sub network (see NIAP-Testing_052605) consisting of the following systems

Ref	System	Role	OS
#1	hptest13	OVO/Unix Server	HP-UX 11.11
#2	suntest20	OVO/Unix Server	Solaris 9
#3	hptest65/a	HTTPS Agent	HP-UX 11.11
#4	suntest20	HTTPS Agent	Solaris 9
#5	wtest59	HTTPS Agent	MS Win 2003 EE
#6	wtest63	HTTPS Agent	RedHat -AS 3.0
#7	ramsiam	Java Operator GUI	MS Win XP
#8	hptest65/s	OVO/Unix Server - scratch Installation	HP-UX 11.11

Related Files	Description
FSP_interfaces_idx.xls	The FSP maps security relevant functionality and testcases.
all_audit_report.txt	Audit output generated during Evaluator Ad-Hoc testing
CC_Security Testcases	All manual Adminstrator GUI, automated EATE, manual and automated XDE (Java Operator GUI) Testcase 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-	Automated OVO/Unix Java Operator GUI

wtest63.html	Translated Rational Testmanager 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 GUI Translated Rational Testmanager 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 GUI tests (TMS Report)

Strength of Function AVA_SOF.1

Related Files	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 an special analysis.	

Vulnerability Analysis AVA_VLA.1

Related Files	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 GUI	Actions performed between Management Server and Java Operator GUI 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 PP Claims

The HP OpenView Operations for UNIX Security Target was not written to address any existing Protection Profile.

7 Rationale

7.1 Security Objectives Rationale

7.1.1 Threats to Security

Table 7-1 shows that all the identified threats to security are countered by Security Objectives for the TOE. Rationale is provided for each threat below the table.

Table 7-1 All Threats to Security Countered

Item	Threat Name	Threat Description	Security Objective
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.	O.Access OE.Access O.Attributes O.Audit O.IDAuth OE.IDAuth O.AuditProtect OE.AuditProtect OE.Time
2	T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF.	O.NonBypass OE.NonBypass
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.	O.Admin OE.Admin O.Roles
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.	O.Access OE.Access O.Banner O.Attributes O.PartSelfProt OE.PartSelfProt O.IDAuth OE.IDAuth
5	T.Tamper	An attacker may attempt to modify TSF programs and data.	O.PartSelfProt OE.PartSelfProt O.ProtectData OE.ProtectData
6	T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users.	OE.ProtectComm
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.	O.Audit O.AuditProtect OE.AuditProtect OE.Time

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. T.Abuse is countered by:

- O.Access: The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OVO access control SFP. This objective counters this threat by providing access controls that limit the actions an individual is authorized to perform.
- OE.Access: The IT environment will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OS access control SFP. This objective counters this threat by providing access controls that limit the actions an individual is authorized to perform.
- O.Attributes: The TOE will be able to store and maintain attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with user accounts and privileges that the HP OpenView Operations Access Control Policy is based on.
- O.Audit: The TOE will record audit records for data accesses and use of the TOE functions. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
- O.IDAuth: The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.
- OE.IDAuth: The IT Environment will be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.
- O.AuditProtect: The TOE will ensure the protection of the audit storage. This objective counters this threat by requiring the TOE to provide partial protection of the audit storage.
- OE.AuditProtect: The IT environment will ensure the protection of the audit storage. This objective counters this threat by requiring the IT Environment to provide partial protection of the audit storage.
- OE.Time: The underlying operating system will provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

T.Bypass: An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF. T.Bypass is countered by:

- O.NonBypass: The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. This objective counters this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.
- OE.NonBypass: The IT environment will ensure that its protection mechanisms cannot be bypassed. This objective for the IT environment counters this threat by ensuring the security functions of the Operating System that support the TSF are not compromised.

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. T.Mismgmt is countered by:

- O.Admin: The TOE will provide the functionality to enable authorized administrator(s) to effectively manage the TOE and its security functions. This objective provides for administrative tools make it easier for administrators to correctly manage the TOE.
- OE.Admin: The IT Environment will provide the functionality to enable the *root* user to effectively manage the TOE and its security functions. This objective provides for a command line interface that aids the *root* user in managing the TOE.
- O.Roles: The TOE will support multiple roles. This objective provides for multiple roles that can be used to enforce separation of duty, so that one administrator can catch errors made by another administrator.

T.Privil: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. T.Privil is countered by:

- O.Access: The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OVO access control SFP. This objective builds upon the O.IDAuth objective by only permitting authorized users to access TOE functions.
- OE.Access: The IT environment will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OS access control SFP. This objective counters this threat by providing access controls that limit the actions an individual is authorized to perform. This objective builds upon the OE.IDAuth objective by only permitting authorized users to access TOE functions.
- O.Banner: The TOE will provide the capability of displaying an advisory warning about unauthorized use of the TOE. This objective counters this threat by requiring the TOE to provide an advisory warning before the login of any users.
- O.Attributes: The TOE will be able to store and maintain attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with user accounts and privileges that the HP OpenView Operations Access Control Policy is based on.
- O.PartSelfProt: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. The TOE will maintain separation between code executing on behalf of different users. This objective addresses this threat by providing TOE self-protection and separation between users.
- OE.PartSelfProt: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by protecting the TOE and its data.
- O.IDAuth: The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE function access.
- OE.IDAuth: The IT Environment will be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.

T.Tamper: An attacker may attempt to modify TSF programs and data. T.Tamper is countered by:

- O.PartSelfProt: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing separation between code executing on behalf of different users. In addition, this objective addresses this threat by providing TOE self-protection and separation between users.
- OE.PartSelfProt: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by protecting the TOE and its data.
- O.ProtectData: The TSF will protect TSF data when transmitted between separate parts of the TOE and while being stored. This objective addresses this threat by calling the hashing function that digitally signs the OVO HTTPS Agent's Configuration Policy. This protects the Configuration Policy from modification. The IT environment provides the hashing function.
- OE.ProtectData: The IT environment will protect TSF data when transferred between TOE Components. This objective provides for the protection of TSF data when transferred between TOE Components.

T.Transmit: TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users. T.Transmit is countered by:

- OE.ProtectComm: The IT environment will protect communications between the TOE and its users. This objective prevents data from being disclosed or modified when it is being transmitted between client and server components.

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. T.Undetect is countered by:

- O.Audit: The TOE will record audit records for data accesses and use of the TOE functions. This objective records attempts to violate the security policy.
- O.AuditProtect: The TOE will ensure the protection of the audit storage. This objective counters this threat by requiring the TOE to provide partial protection of the audit storage.
- OE.AuditProtect: The IT environment will ensure the protection of the audit storage. This objective counters this threat by requiring the IT Environment to provide partial protection of the audit storage.
- OE.Time: The underlying operating system will provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

7.1.2 Assumptions

Table 7-2 shows that all of the secure usage assumptions are addressed by either security objectives for the IT environment or Non-IT security objectives. Rationale for each assumption is provided below the table.

Table 7-2 All Assumptions Addressed

Item	Name	Assumption	Objective
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.	ON.Install ON.Operations ON.Person
2	A.Crypto	The TOE relies upon the IT environment to provide cryptographic functionality.	OE.ProtectComm OE.ProtectData
3	A.Database	The TOE relies upon a database in the IT environment to store TSF data.	ON.Install
4	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the Management Server host.	ON.NoUntrusted
5	A.OS	The TOE relies upon the OS to provide file protection and OS user authentication.	ON.Install
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 Admin GUI and the OVO/UNIX management server.	ON.Physical
7	A.Time	It is assumed that the underlying operating system provides reliable time stamps.	OE.Time
8	A.Users	It is assumed that users will protect their authentication data.	ON.ProtectAuth
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.	ON.Operations

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. A.AdmTra is covered by:

- ON.Install: Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes correctly configuring the TOE. This objective provides for secure installation and configuration of the TOE.
- ON.Operations: The TOE will be managed and operated in a secure manner as outlined in the supplied guidance. This objective provides for operation procedures to be in place.
- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system. This objective provides for competent personnel to administer the TOE.

A.Crypto: The TOE relies upon the IT environment to provide cryptographic functionality. A.Crypto is covered by:

- OE.ProtectComm: The IT environment will protect communications between the TOE and its users. This objective provides for a trusted path.
- OE.ProtectData: The IT environment will protect TSF data when transferred between TOE Components. This objective provides for the protection of TSF data when transferred between TOE Components.

A.Database: The TOE relies upon a database in the IT environment to store TSF data. A.Database is covered by:

- ON.Install: Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes installing the HP OpenView Operations for UNIX server according to the product's installation requirements. This includes installing the relational database according to the Guidance documentation. This objective provides for secure installation of the TOE.

A.NoUntrusted: It is assumed that there will be no untrusted users and no untrusted software on the OVO/UNIX management server host. A.NoUntrusted is covered by:

- ON.NoUntrusted: The administrator will ensure that there are no untrusted users and no untrusted software on the HP OpenView Operations for UNIX server host. This objective provides for the protection of the TOE from untrusted software and users.

A.OS: The TOE relies upon the OS to provide file protection and OS user authentication. A.OS is covered by:

- ON.Install: Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes installing the HP OpenView Operations for UNIX Management Server and OVO HTTPS Agents on recommended Operating Systems according to the product's installation requirements and Guidance documentation. This objective provides for secure installation of the TOE.

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 GUI and the OVO/UNIX management server - assuming the OVO Motif Admin GUI is redirected to another display station using X redirection. A.Physical is covered by:

- ON.Physical: Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective provides for the physical protection of the TOE hardware and software.

A.Time: It is assumed that the underlying the operating system provides reliable time stamps. A.Time is covered by:

- OE.Time: The underlying operating system will provide reliable time stamps. This objective provides for reliable time stamps.

A.Users: It is assumed that users will protect their authentication data. A.Users is covered by:

- ON.ProtectAuth: The users must ensure that their authentication data is held securely and not disclosed to unauthorised persons. This objective provides for users to protect their authentication data.

A.Admin: It is assumed that the OVO Administrator is also a *root* system administrator on the OS underlying the OVO/UNIX management server. A.Admin is covered by:

- ON.Operations: The TOE will be managed and operated in a secure manner as outlined in the supplied guidance. This objective provides for operation procedures to be in place. As part of the operation procedures, the OVO Administrator is also a *root* system administrator on the OS of the underlying OVO/UNIX management server.

7.2 Security Requirements Rationale

7.2.1 Functional Requirements

Table 7-3 shows that all of the security objectives of the TOE are satisfied. Rationale for each objective is included below the table.

Table 7-3 All Objectives Met by Functional Components

Item	Objective	Objective Description	Security Functional Requirement
1	O.Access	The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OVO access control SFP.	FAU_SAR.2 Restricted audit review FDP_ACC_EXP.1-1 Subset access control FDP_ACF_EXP.1-1 Security attribute based access control FDP_ITT_EXP.1-1 Basic internal transfer protection FIA_UAU_EXP.2-1 User authentication before any action FIA_UID_EXP.2-1 User identification before any action FMT_MOF_EXP.1-1 Management of security functions behavior FMT_MTD_EXP.1-1 Management of TSF data
2	O.Admin	The TOE will provide the functionality to enable authorized administrator(s) to effectively manage the TOE and its security functions.	FAU_SAR.1 Audit review FAU_STG_EXP.1-1 Protected audit trail storage FMT_MOF_EXP.1-1 Management of security functions behavior FMT_MSA_EXP.1-1 Management of security attributes FMT_MSA_EXP.3-1 Static attribute initialisation FMT_MTD_EXP.1-1 Management of TSF data FMT_SMF_EXP.1-1 Specification of management functions

Item	Objective	Objective Description	Security Functional Requirement
3	O.Attributes	The TOE will be able to store and maintain attributes.	FIA_ATD.1 User attribute definition
4	O.Audit	The TOE will record audit records for data accesses and use of the TOE functions.	FAU_GEN.1 Audit data generation
5	O.AuditProtect	The TOE will ensure the protection of the audit storage.	FAU_STG_EXP.1-1 Protected audit trail storage
6	O.Banner	The TOE will provide the capability of displaying an advisory warning about unauthorized use of the TOE.	FTA_TAB.1 Default TOE access banners
7	O.IDAuth	The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data.	FIA_UAU_EXP.2-1 User authentication before any action FIA_UID_EXP.2-1 User identification before any action
8	O.NonBypass	The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.	FPT_RVM_EXP.1-1 Non-bypassability of the TSP
9	O.PartSelfProt	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.	FPT_SEP_EXP.1-1 Domain separation
10	O.ProtectData	The TSF will protect TSF data when transmitted between separate parts of the TOE and while being stored.	FPT_ITT_EXP.1-1 Basic internal TSF data transfer protection
11	O.Roles	The TOE will support multiple roles.	FMT_SMR_EXP.1-1 Security roles

O.Access: The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OVO access control SFP. O.Access is addressed by:

- FAU_SAR.2 Restricted audit review, which requires that access to audit data be restricted to authorized users.
- FDP_ACC_EXP.1-1 Subset access control, which requires that the TSF enforce access controls on all operations between any subject in the TSC and any object within the TSC.
- FDP_ACF_EXP.1-1 Security attribute based access control, which requires the TSF enforce access controls based on specified security attributes. In addition, the TSF can explicitly authorize and deny access to specified subjects.
- FDP_ITT_EXP.1-1 Basic internal transfer protection, which requires the TSF enforce access controls to prevent the disclosure and modification of user data when it is transmitted between physically-separated parts of the TOE.
- FIA_UAU_EXP.2-1 User authentication before any action, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID_EXP.2-1 User identification before any action, which requires that users be successfully identified before allowing access to the TOE.

- FMT_MOF_EXP.1-1 Management of security functions behavior, which restricts the ability to disable, enable, and modify functions to authorized users.
- FMT_MTD_EXP.1-1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.

O.Admin: The TOE will provide the functionality to enable authorized administrator(s) to effectively manage the TOE and its security functions. O.Admin is addressed by:

- FAU_SAR.1 Audit review, which requires that the authorized administrator be able to read all audit records.
- FAU_STG_EXP.1-1 Protected audit trail storage, which requires the audit log be protected from unauthorized deletion and modifications to the audit log will be prevented.
- FMT_MOF_EXP.1-1 Management of security functions behaviour, which requires that the OVO administrator is able to manage the behavior of the audit tools.
- FMT_MSA_EXP.1-1 Management of security attributes, which enforces the Table 5-4 Management of Security Attributes to restrict the ability to create, query, modify, and delete the specified security attributes to the authorized account types.
- FMT_MSA_EXP.3-1 Static attribute initialisation, which requires the TSF enforce access control for specified default values of security attributes.
- FMT_MTD_EXP.1-1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FMT_SMF_EXP.1-1 Specification of management functions, which requires the TSF be capable of performing the specified security management functions.

O.Attributes: The TOE will be able to store and maintain attributes. O.Attributes is addressed by:

- FIA_ATD.1 User attribute definition, which requires that the TSF maintain security attributes of users.

O.Audit: The TOE will record audit records for data accesses and use of the TOE functions. O.Audit is addressed by:

- FAU_GEN.1 Audit data generation, which requires the ability to audit specified events.

O.AuditProtect: The TOE will ensure the protection of the audit storage. O.AuditProtect is addressed by:

- FAU_STG_EXP.1-1 Protected audit trail storage, which requires the audit log be protected from unauthorized deletion and modifications to the audit log will be prevented.

O.Banner: The TOE will provide the capability of displaying an advisory warning about unauthorized use of the TOE.

- FTA_TAB.1 Default TOE access banners, which requires that before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

O.IDAuth: The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data. O.IDAuth is addressed by:

- FIA_UAU_EXP.2-1 User authentication before any action, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID_EXP.2-1 User identification before any action, which requires that users be successfully identified before allowing access to the TOE.

O.NonBypass: The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. O.NonBypass is addressed by:

- FPT_RVM_EXP.1-1 Non-bypassability of the TSP, which requires that TSP enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.

O.PartSelfProt: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. O.PartSelfProt is addressed by:

- FPT_SEP_EXP.1-1 TSF domain separation which requires the TSF provides a domain that protects itself from interference and tampering by untrusted users. This requires that the TOE maintain separation between code executing on behalf of different users.

O.ProtectData: The TSF will protect TSF data when transmitted between separate parts of the TOE and while being stored. O.ProtectData is addressed by:

- FPT_ITT_EXP.1-1 Basic internal TSF data transfer protection, which requires the TSF to protect TSF data from disclosure and modification when being transmitted to separate parts of the TOE. This requires the TOE to protect TSF data during transmission and while being stored on the OVO HTTPS Agent machine.

O.Roles: The TOE will support multiple roles. O.Roles is addressed by:

- FMT_SMR_EXP.1-1 Security roles, which requires that the TSF maintain multiple roles.

7.2.2 Dependencies

Table 7-4 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. If the TOE dependency is met by an SFR in the IT environment an "E" will be next to the reference number.

Table 7-4 TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1.	FAU_GEN.1	Audit data generation	FPT_STM.1	41 E
2.	FAU_SAR.1	Audit review	FAU_GEN.1	1
3.	FAU_SAR.2	Restricted audit review	FAU_SAR.1	2
4.	FAU_STG_EXP.1-1	Protected audit trail storage	FAU_GEN.1	1
5.	FDP_ACC_EXP.1-1	Subset access control	FDP_ACF_EXP.1-1	6
6.	FDP_ACF_EXP.1-1	Security attribute based access control	FDP_ACC_EXP.1-1	5
			FMT_MSA_EXP.3-1	14
7.	FDP_ITT_EXP.1-1	Basic internal transfer protection	FDP_ACC_EXP.1-1	5
8.	FIA_ATD.1	User attribute definition	None	None
9.	FIA_UAU_EXP.2-1	User authentication before any action	FIA_UID_EXP.2-1	11
10.	FIA_UID_EXP.2-1	User identification before any action	None	None
11.	FMT_MOF_EXP.1-1	Management of security functions behavior	FMT_SMR_EXP.1-1	17
			FMT_SMF_EXP.1-1	16
			FMT_MOF_EXP.1-2	31 E
12.	FMT_MSA_EXP.1-1	Management of security attributes	FDP_ACC_EXP.1-1	5
			FMT_SMR_EXP.1-1	17
			FMT_SMF_EXP.1-1	16
			FMT_MSA_EXP.1-2	32 E
13.	FMT_MSA_EXP.3-1	Static attribute initialisation	FMT_MSA_EXP.1-1	13
			FMT_SMR_EXP.1-1	17
			FMT_MSA_EXP.3-2	34 E
14.	FMT_MTD_EXP.1-1	Management of TSF data	FMT_SMR_EXP.1-1	17
			FMT_SMF_EXP.1-1	16
			FMT_MTD_EXP.1-2	35 E
15.	FMT_SMF_EXP.1-1	Specification of management functions	FMT_SMF_EXP.1-2	36 E
16.	FMT_SMR_EXP.1-1	Security roles	FIA_UID_EXP.2-1	11
17.	FPT_ITT_EXP.1-1	Basic internal TSF data transfer protection	None	None
18.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	None	None
19.	FPT_SEP_EXP.1-1	TSF domain separation	None	None
20.	FTA_TAB.1	Default TOE access banners	None	None

Table 7-5 IT Environment Dependencies are Satisfied

No.	Component	Component Name	Dependencies	Reference
21.	FAU_STG_EXP.1-2	Protected audit trail storage	FAU_GEN.1	1
22.	FCS_CKM.1*	Cryptographic key generation	FCS_COP.1	25 E
			FCS_CKM.4	24 E
			FMT_MSA.2	33 E
23.	FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1	23 E
			FMT_MSA.2	33 E
24.	FCS_COP.1*	Cryptographic operation	FCS_CKM.1	23 E
			FCS_CKM.4	24 E
			FMT_MSA.2	33 E
25.	FDP_ACC_EXP.1-2	Subset access control	FDP_ACF_EXP.1-2	27 E
26.	FDP_ACF_EXP.1-2	Security attribute based access control	FDP_ACC_EXP.1-2	26 E
			FMT_MSA_EXP.3-2	34 E
27.	FDP_ITT_EXP.1-2	Basic internal transfer protection	FDP_ACC_EXP.1-2	26 E
28.	FIA_UAU_EXP.2-2	User authentication before any action	FIA_UID_EXP.2-2	30 E
29.	FIA_UID_EXP.2-2	User identification before any action	None	None
30.	FMT_MOF_EXP.1-2	Management of security functions behavior	FMT_SMR_EXP.1-2	37 E
			FMT_SMF_EXP.1-2	36 E
31.	FMT_MSA_EXP.1-2	Management of security attributes	FDP_ACC_EXP.1-2	26 E
			FMT_SMR_EXP.1-2	37 E
			FMT_SMF_EXP.1-2	36 E
32.	FMT_MSA.2	Secure security attributes	ADV_SPM.1	See section 8.2.3
			FDP_ACC_EXP.1-2	26 E
			FMT_MSA_EXP.1-2	32 E
			FMT_SMR_EXP.1-2	37 E
33.	FMT_MSA_EXP.3-2	Static attribute initialisation	FMT_MSA_EXP.1-2	32 E
			FMT_SMR_EXP.1-2	37 E
34.	FMT_MTD_EXP.1-2	Management of TSF data	FMT_SMR_EXP.1-2	37 E
			FMT_SMF_EXP.1-2	36 E
35.	FMT_SMF_EXP.1-2	Specification of management functions	None	None
36.	FMT_SMR_EXP.1-2	Security roles	FIA_UID_EXP.2-2	30 E
37.	FPT_ITT_EXP.1-2	Basic internal TSF data transfer protection	None	None
38.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP	None	None
39.	FPT_SEP_EXP.1-2	TSF domain separation	None	None
40.	FPT_STM.1	Reliable time stamps	None	None
41.	FIA_UAU.5	Multiple authentication mechanisms	None	None

7.2.3 Rationale why dependencies are not met

For FMT_MSA.2, ADV_SPM.1 is not included because FMT_MSA.2 is levied on the IT environment. As a result, ADV_SPM.1 is also levied on the IT environment. According to Annex H.2, the dependency relates to the definition of what “secure” means for these attributes. Since the attributes

in question are not under the control of the TOE, but rather the IT environment, the TOE should not be responsible for providing this definition. Determination whether and how secure values are accepted by the IT environment for these attributes is not relevant to evaluation of the TOE. What is required in this case is that the TOE depends upon the values provided by the IT environment.

7.2.4 Strength of Function Rationale

A strength of function level of SOF-basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product. There is an overall SOF claim of SOF_Basic. There are no specific SOF Claims since FIA_SOS.1 is not included in this ST.

7.2.5 Assurance Rationale

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

7.2.6 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, each of the SFRs builds on the others. For example, FAU_GEN.1 details the auditable events generated by the TSF. FAU_SAR.1 states that the TSF shall provide the authorized administrator with the capability to read all audit information within the authorized administrator's scope of control from the audit records. FAU_SAR.2 builds on FAU_SAR.1 by stating the TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_STG_EXP.1-1 provides for protected storage of the audit data. Audit records are generated for many events where other requirements are coming to bear, such as login, policy check failures, and management functions.

Together FDP_ACC_EXP.1-1 and FDP_ACF_EXP.1-1 provide User Data Protection. FDP_ACC_EXP.1 defines the HP OVO Access Control SFP. FDP_ACF_EXP.1-1 specifies that the TSF enforces access based upon security attributes. The subjects with roles of the following listed in Table 5-5 Management of TSF data (FMT_MTD_EXP.1-1) are also defined in FMT_SMR_EXP.1-1. FDP_ITT_EXP.1-1 specifies that the TSF will enforce the HP OVO Access Control SFP to prevent the disclosure and modification of user data when it is transmitted between physically-separated parts of the TOE.

Login processing brings in elements of many requirements, but all in a complementary way. FIA_UID_EXP.2-1 wants the user identified before allowing any other operations and FIA_UAU_EXP.2-1 wants the user authenticated before allowing any other operations. FIA_ATD.1 specifies the security attributes belonging to individual users. FTA_TAB.1 provides a default access banner displays an advisory warning to users regarding unauthorized use.

The management requirements (FMT_) are related to many of the other requirements. FMT_MOF_EXP.1-1 provides for the management of the audit functions (FAU_GEN.1). FMT_MSA_EXP.1-1 enforces the HP OpenView Operations Access Control Policy (FDP_ACC_EXP.1-1). FMT_MSA_EXP.3-1 enforces the HP OpenView Operations Access Control Policy to provide permissive default values for security attributes. FMT_MTD_EXP.1-1 specifies the management of TSF Data according to assigned roles. FMT_SMF_EXP.1-1 which specifies the security management functions of the TSF. In many cases, the other functions will enforce the settings made through the management functions. Installation functions (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM) documents the management functions.

FPT_ITT_EXP.1-1 makes sure the OVO HTTPS Agent's Configuration Policy from modification when it is transmitted between the separate parts of the TOE and while stored on the OVO HTTPS Agent machine. FPT_RVM_EXP.1-1 makes certain the HP OpenView Operations Access Control Policy (FDP_ACC_EXP.1-1) is invoked and succeeds before any other functions within the TOE's Scope of Control are allowed to proceed. FPT_SEP_EXP.1-1 relies partly on FDP_ACC_EXP.1-1 to provide protection against unauthorized subjects from gaining access to the TOE's administrative interface.

7.2.7 Explicitly Stated Requirements Rationale

FPT_ITT_EXP.1* had to be explicitly stated because a refinement adds additional detail and narrows the scope, but has to be iterated to meet the original scope of the SFR. In addition, in cases where a refined requirement is iterated, it is permissible that each iteration address only a subset of the scope of the requirement; however, the sum of the iterations must together meet the entire scope of the original requirement. A refinement of FPT_ITT.1 would not allow for the broadening of scope of the SFR. I broadened the scope of FPT_ITT_EXP.1-1 by adding "and while stored on the OVO HTTPS Agent machine. " A refinement of the FPT_ITT.1* would not correctly describe the functionality of the TSF protect the OVO HTTPS Agent's Configuration Policy from modification.

FPT_SEP_EXP.1* had to be explicitly stated because in the Basic Robustness Guide, it is recommended to explicitly state FPT_SEP_EXP.1* in this manner. FPT_RVM_EXP.1*, FPT_SEP_EXP.1*, FAU_STG_EXP.1*, and FDP_ITT_EXP.1* had to be explicitly stated because they all provide partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. According to CCIMB RI#19, which states the following: "Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. " Since the iterations of the following SFRs span both the TOE requirements and IT Environment, they must be explicitly stated following the same guidance as above:

- FDP_ACC_EXP.1*
- FDP_ACF_EXP.1*
- FIA_UAU_EXP.2*
- FIA_UID_EXP.2*
- FMT_MOF_EXP.1*
- FMT_MSA_EXP.1*
- FMT_MSA_EXP.3*
- FMT_MTD_EXP.1*
- FMT_SMF_EXP.1*
- FMT_SMR_EXP.1*

7.2.8 Requirements for the IT Environment

Table 7-6 shows that all of the security objectives for the IT environment are satisfied. Rationale for each objective is included below the table.

Table 7-6 All Objectives for the IT Environment map to Requirements in the IT environment

Item	Objective	Objective Description	Requirement for the IT Environment	Component Title
1E	OE.AuditProtect	The IT environment will ensure the protection of the audit storage.	FAU_STG_EXP.1-2	Protected audit trail storage
2E	OE.PartSelfProt	The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.	FMT_MSA.2	Secure security attributes
			FPT_SEP_EXP.1-2	TSF domain separation
3E	OE.ProtectComm	The IT environment will protect communications between the TOE and its users.	FCS_CKM.1*	Cryptographic key generation
			FCS_CKM.4	Cryptographic key destruction
			FCS_COP.1*	Cryptographic operation
			FDP_ITT_EXP.1-2	Basic internal transfer protection
4E	OE.ProtectData	The IT environment will protect TSF data when transferred between TOE Components.	FPT_ITT_EXP.1-2	Basic internal TSF data transfer protection
5E	OE.Time	The underlying operating system will provide reliable time stamps.	FPT_STM.1	Reliable time stamps
6E	OE.NonBypass	The IT environment will ensure that its protection mechanisms cannot be bypassed.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
7E	OE.Access	The IT environment will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OS access control SFP.	FDP_ACC_EXP.1-2	Subset access control
			FDP_ACF_EXP.1-2	Security attribute based access control
			FIA_UAU_EXP.2-2	User authentication before any action
			FIA_UAU.5	Multiple Authentication mechanisms
			FIA_UID_EXP.2-2	User identification before any action
			FMT_MOF_EXP.1-2	Management of security functions behavior
			FMT_MTD_EXP.1-2	Management of TSF data

Item	Objective	Objective Description	Requirement for the IT Environment	Component Title
8E	OE.Admin	The IT Environment will provide the functionality to enable authorized administrator(s) to effectively manage the TOE and its security functions.	FMT_MOF_EXP.1-2	Management of security functions behavior
			FMT_MSA_EXP.1-2	Management of security attributes
			FMT_MSA_EXP.3-2	Static attribute initialisation
			FMT_MTD_EXP.1-2	Management of TSF data
			FMT_SMF_EXP.1-2	Specification of management functions
			FMT_SMR_EXP.1-2	Security roles
9E	OE.IDAuth	The IT Environment will be able to identify and authenticate users prior to allowing access to TOE functions and data.	FIA_UAU_EXP.2-2	User authentication before any action
			FIA_UID_EXP.2-2	User identification before any action

OE.AuditProtect: The IT environment will ensure the protection of the audit storage. OE.AuditProtect is addressed by:

- FAU_STG_EXP.1-2 Protected audit trail storage, which requires the IT environment to protect the stored audit records in the audit trail from unauthorized deletion and can prevent unauthorized modifications to the audit records in the audit trail. The TOE relies on the underlying OS, DBMS, and hardware to protect the audit trail storage.

OE.PartSelfProt: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. OE.PartSelfProt is addressed by:

- FMT_MSA.2 Secure security attributes, which requires the IT environment to ensure only secure values are accepted for security attributes. This relates to the cryptographic functions and requires that only secure algorithms and key sizes can be configured.
- FPT_SEP_EXP.1-2 TSF domain separation, which requires the Operating System to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface. The IT environment will enforce separation between security domains of subjects in the Operating System's Scope of Control.

OE.ProtectComm: The IT environment will protect communications between the TOE and its users. OE.ProtectComm is addressed by:

- FCS_CKM.1* Cryptographic key generation, which requires the IT environment generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet a specified standard.
- FCS_CKM.4 Cryptographic key destruction, which requires the IT environment, shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method.

- FCS_COP.1* Cryptographic operation, which requires that the IT environment perform cryptographic operations in accordance with a specified cryptographic algorithm and cryptographic key sizes that meet a specified standard.
- FDP_ITT_EXP.1-2 Basic internal transfer protection, which requires that the IT environment enforce the HP OVO Access Control SFP to prevent the disclosure and modification of user data when being transmitted.

OE.Time The underlying operating system will provide reliable time stamps. OE.Time is addressed by:

- FPT_STM.1 Reliable time stamps, which require that time stamps be provided by the IT environment.

OE.NonBypass: The IT environment will ensure that its protection mechanisms cannot be bypassed. OE.NonBypass is addressed by:

- FPT_RVM_EXP.1-2: Non-bypassability of the TSP, which requires that the Operating Systems's Security Policy is invoked and succeeds before a security-relevant function is allowed to proceed.

OE.ProtectData: The IT environment will protect TSF data when transferred between TOE Components.

- FPT_ITT_EXP.1-2 Basic internal TSF data transfer protection, which requires the IT environment to protect TSF data from disclosure and modification when being transmitted to separate parts of the TOE.

OE.Access: The IT environment will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the OS access control SFP. OE.Access is addressed by:

- FDP_ACC_EXP.1-2 Subset access control, which requires that the OS enforce access controls on the *root* subject user and the OVO command line interface executables.
- FDP_ACF_EXP.1-2 Security attribute based access control, which requires the TSF enforce access controls based on specified security attributes.
- FIA_UAU_EXP.2-2 User authentication before any action, which requires each user to be successfully authenticated by the Operating System before allowing access to the TOE CLI interfaces.
- FIA_UAU.5-1 Multiple authentication mechanisms, which requires that the TSF be able to authenticate a user using the PAM.
- FIA_UID_EXP.2 User identification before any action, which requires that users be successfully identified by the Operating System before allowing access to the TOE CLI interfaces.
- FMT_MOF_EXP.1-2 Management of security functions behavior, which restricts the ability to disable, enable, and modify the audit function to the *root* user.
- FMT_MTD_EXP.1-2 Management of TSF data, which specifies the management of TSF Data according to assigned roles.

OE.Admin: The IT Environment will provide the functionality to enable the *root* user to effectively manage the TOE and its security functions. O.Admin is addressed by:

- FMT_MOF_EXP.1-2 Management of security functions behaviour, which requires that the *root* user is able to manage the behavior of audit.
- FMT_MSA_EXP.1-2 Management of security attributes, which enforces the Table 5-7 Management of Security Attributes to restrict the ability to create, query, modify, and delete the specified security attributes to the *root* user.
- FMT_MSA_EXP.3-2 Static attribute initialisation, which requires the OS enforce access control for specified default values of security attributes.
- FMT_MTD_EXP.1-2 Management of TSF data, which specifies the management of TSF Data according to assigned roles.

- FMT_SMF_EXP.1-2 Specification of management functions, which requires the IT Environment be capable of performing the specified security management functions.
- FMT_SMR_EXP.1-2 Security roles, which requires that the TSF maintain user role(s).

OE.IDAuth: The IT Environment will be able to identify and authenticate users prior to allowing access to TOE functions and data. OE.IDAuth is addressed by:

- FIA_UAU_EXP.2-2 User authentication before any action, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID_EXP.2-2 User identification before any action, which requires that users be successfully identified before allowing access to the TOE.

Table 8-7 is included as a consistency check that all security requirements for the IT environment map to corresponding threats and assumptions.

Table 7-7 Reverse Mapping of Security Requirements for the Environment to Security Objectives of the Environment

No.	IT Environment SFR	IT Environment Security Objective
21	FAU_STG_EXP.1-2	OE.AuditProtect
22	FCS_CKM.1*	OE.ProtectComm
23	FCS_CKM.4	OE.ProtectComm
24	FCS_COP.1*	OE.ProtectComm
25	FDP_ACC_EXP.1-2	OE.Access
26	FDP_ACF_EXP.1-2	OE.Access
27	FDP_ITT_EXP.1-2	OE.ProtectData
28	FIA_UAU_EXP.2-2	OE.Access
29	FIA_UID_EXP.2-2	OE.Access
30	FMT_MOF_EXP.1-2	OE.Access
31	FMT_MSA_EXP.1-2	OE.Access
32	FMT_MSA.2	OE.PartSelfProt
33	FMT_MSA_EXP.3-2	OE.Admin
34	FMT_MTD_EXP.1-2	OE.Admin
35	FMT_SMF_EXP.1-2	OE.Admin
36	FMT_SMR_EXP.1-2	OE.Admin
37	FPT_ITT_EXP.1-2	OE.ProtectData
38	FPT_RVM_EXP.1-2	OE.NonBypass
39	FPT_SEP_EXP.1-2	OE.PartSelfProt
40	FPT_STM.1	OE.Time
41	FIA_UAU.5	OE.Access

7.3 TOE Summary Specification Rationale

7.3.1 IT Security Functions

Table 7-8 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 7-8 Mapping of Functional Requirements to TOE Summary Specification

Item	Functional Requirement		Requirement is met by:	
			Security Function Ref. No	Rationale
1.	FAU_GEN.1	Audit data generation	OA-1	Specifies the types of events to be audited by the management sever and specifies the information to be recorded in an audit record. Specifies the information to be recorded in an audit record. .
2.	FAU_SAR.1	Audit review	OA-2	Specifies who has the capability to read information from the audit records.
3.	FAU_SAR.2	Restricted audit review	OA-3	Specifies that NO users have read access to the audit records – except the users defined in OA-3.
4.	FAU_STG_EXP.1-1	Protected audit trail storage	OA-4	Specifies that HP OpenView Operations for UNIX is able to protect the stored audit records from unauthorized deletion. Audit up/download activities are recorded as audit entries as well.
5.	FDP_ACC_EXP.1-1	Subset access control	OAC-1	Specifies the HP OpenView Operations Access Control Policy.
6.	FDP_ACF_EXP.1-1	Security attribute based access control	OAC-1	Specifies the subjects and objects controlled under the HP OpenView Operations Access Control Policy.
7.	FDP_ITT_EXP.1-1	Basic internal transfer protection	OAC-5	Specifies that messages sent from the OVO HTTPS Agent to the OVO/UNIX management server are protected from disclosure and modification. Specifies the OVO HTTPS Agent uses bind two-way certificate-based SSL without password (client and server authentication; also known as mutual authentication) to support OVO HTTPS Agent authentication.
8.	FIA_ATD.1	User attribute definition	SM-1	Specifies the security attributes maintained for each user.
9.	FIA_UAU_EXP.2-1	User authentication before any action	OIA-1	Specifies that the HP OpenView Operations for UNIX requires each user to successfully authenticate with a password before being allowed any other actions. Specifies that the HP OpenView Operations for UNIX provides Pluggable Authentication Module (PAM) for users during the OVO Java GUI or OVO Motif Admin GUI login sequences to support user authentication.

Item	Functional Requirement		Requirement is met by:	
			Security Function Ref. No	Rationale
10.	FIA_UID_EXP.2-1	User identification before any action	OIA-2	Specifies the HP OpenView Operations for UNIX requires each user to identify himself/herself before being allowed to perform any other actions.
11.	FMT_MOF_EXP.1-1	Management of security functions behavior	SM-2	Specifies that HP OpenView Operations for UNIX restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the functions related to the audit function (see FAU_GEN.1.1) to the OVO Administrator.
12.	FMT_MSA_EXP.1-1	Management of security attributes	SM-3	Specifies that HP OpenView Operations for UNIX restricts the ability to query, modify, delete, create, and change the specified security attributes see Table 5-4 to the specified users see Table 5-4. The management of security attributes is allowed through the CLI to the *root* user (see Table 5-7).
13.	FMT_MSA_EXP.3-1	Static attribute initialisation	SM-4	Specifies that HP OpenView Operations for UNIX provides permissive default values for security attributes and the OVO Administrator can specify alternative initial values.
14.	FMT_MTD_EXP.1	Management of TSF data	SM-5	Specifies that HP OpenView Operations for UNIX restricts the ability to access data.
15.	FMT_SMF_EXP.1-1	Specification of management functions	SM-6	Specifies the security management functions provided by HP OpenView Operations for UNIX.
16.	FMT_SMR_EXP.1-1	Security roles	SM-7	Specifies the roles maintained in the HP OpenView Operations for UNIX.
17.	FPT_ITT_EXP.1-1	Basic internal TSF data transfer protection	OAC-2	Specifies the TSF protects the OVO HTTPS Agent's Configuration Policy from modification when it is transmitted between the separate parts of the TOE and while stored on the OVO HTTPS Agent machine.
18.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	OAC-3	Specifies that HP OpenView Operations for UNIX ensures that the HP OVO Access Control SFP is invoked and succeeds before each function is allowed to proceed.
19.	FPT_SEP_EXP.1-1	Domain separation	OAC-4	Specifies that HP OpenView Operations for UNIX maintains a security domain for its own execution and enforces separation between security domains of users. The HP OVO Access Control SFPI is used to protect TSF data from tampering.
20.	FTA_TAB.1	Default TOE access banners	OIA-3	Specifies HP OpenView Operations for UNIX displays an advisory warning message regarding unauthorized use of the TOE.

7.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 7-9.

Table 7-9 Assurance Measures Rationale

Configuration Managment ACM_CAP.2	
Related Files	Description
OVO8.1_Config_Mgmt_v1.0.doc	ClearCase and Build-Factory documentation
OVOU810_Configuration_Item_List.doc	Configuration Item List

- CM Proof
  - Shows the CM system is being used.
- Configuration Item List(s)
  - is comprised of a list of the source code files and version numbers
  - is comprised of a list of design documents with version numbers
  - is comprised of test documents with version numbers
  - user and administrator documentation with version numbers

Delivery Procedures ADO_DEL.1	
Related Files	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.

Provides a description of all the procedures that are necessary to maintain security when distributing HP OpenView Operations for UNIX software to the user's site.

- Applicable across all phases of delivery from packaging, storage, distribution

Installation, Generation, and Start-Up procedures ADO_IGS.1	
Related Files	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 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
InstallationGuide_HP_Edn_2.pdf	HP OpenView Operations -Installation GuideSoftware Version A.08.10 for HP-UX
InstallationGuide_Sol_Edn_2.pdf	HP OpenView Operations -Installation GuideSoftware 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

Provides detailed instructions on how to install HP OpenView Operations for UNIX software.

Functional Specification ADV_FSP.1

Related Files	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

Provides rationale that TSF is fully represented. Describes the TSF interfaces and TOE functionality.

High Level Design ADV_HLD.1

Related Files	Description

SecurityFeaturesOfOVO8.ppt	Highlevel documentation of the security features provided by the new HTTPS based Server <-> Agent communication.
Design_Docs/HLDs	MS Visio 2003 Highlevel 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

Describes the TOE subsystems and their associated security functionality

Representation Correspondence ADV_RCR.1

Related Files	Description
FSP_interfaces_idx.xls	The FSP maps security relevant functionality, OVO commands and testcases.

Provides the following two dimensional mappings:
1. TSS and functional specification;
2. Functional specification and high-level design.

Administrator Guidance AGD_ADM.1

Related Files	Description
InstallationGuide_HP_Edn_2.pdf	HP OpenView Operations -Installation GuideSoftware Version A.08.10 for HP-UX
InstallationGuide_Sol_Edn_2.pdf	HP OpenView Operations -Installation GuideSoftware 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 OnlineHelp A.08.10
http://ovweb.external.hp.com/lpe/doc_serv/	External available Documentation for HP OpenView

Describes how to administer the TOE securely.

User Guidance ADG_USR.1

Related Files	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 OnlineHelp A.08.10
http://ovweb.external.hp.com/lpe/doc_serv/	External available Documentation for HP OpenView

Describes the secure use of the TOE.

Test Coverage Analysis ATE_COV.1

Related Files	Description

FSP_interfaces_idx.xls	The FSP maps security relevant functionality and testcases.
cc_eal2_testcases.doc	Documentation of the EATE driven command line testcases.
CC_Security Testcases	All manual Adminstrator GUI, automated EATE, manual and automated XDE (Java Operator GUI) Testcase sources

Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Test Documentation ATE_FUN.1

Related Files	Description
FSP_interfaces_idx.xls	The FSP maps security relevant functionality and testcases.
cc_eal2_testcases.doc	Documentation of the EATE driven command line testcases.
CC_Security Testcases	All manual Adminstrator GUI, automated EATE, manual and automated XDE (Java Operator GUI) Testcase 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 GUI Translated Rational Testmanager 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 GUI Translated Rational Testmanager Report (HP-UX 11.11 <-> Solaris 9) *complementary tests in Böblingen*
XDE Report: XP-HPUX11.11-Win2003_JavaGUI.html	Automated OVO/Unix Java Operator GUI Translated Rational Testmanager 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 GUI Translated Rational Testmanager Report (Solaris 9 <-> Solaris 9) *complementary tests in Böblingen*
XDE Report: XP-Solaris9.0-RedHat_JavaGUI.html	Automated OVO/Unix Java Operator GUI Translated Rational Testmanager Report (Solaris 9 <-> RedHat-AS 3.0) *complementary tests in Böblingen*
XDE Report: XP-Solaris9-Win2003_JavaGUI.html	Automated OVO/Unix Java Operator GUI Translated Rational Testmanager 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 GUI 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*

Test documentation includes test plans and procedures and expected and actual results.

Independent Testing ATE_IND.2

All Tests in Ft. Collins are executed in a separated sub network (see NIAP-Testing_052605) consisting of the following systems

Ref	System	Role	OS
#1	hptest13	OVO/Unix Server	HP-UX 11.11
#2	suntest20	OVO/Unix Server	Solaris 9
#3	hptest65/a	HTTPS Agent	HP-UX 11.11
#4	suntest20	HTTPS Agent	Solaris 9
#5	wtest59	HTTPS Agent	MS Win 2003 EE
#6	wtest63	HTTPS Agent	RedHat -AS 3.0
#7	ramsiam	Java Operator GUI	MS Win XP
#8	hptest65/s	OVO/Unix Server - scratch Installation	HP-UX 11.11

Related Files	Description
FSP_interfaces_idx.xls	The FSP maps security relevant functionality and testcases.
all_audit_report.txt	Audit output generated during Evaluator Ad-Hoc testing
CC_Security Testcases	All manual Adminstrator GUI, automated EATE, manual and automated XDE (Java Operator GUI)

	Testcase 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. Co9llins
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 GUI Translated Rational Testmanager 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 GUI Translated Rational Testmanager 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 GUI tests (TMS Report)

The TOE will be provided for testing. Conclusions are based Test Results.

Strength of Function AVA_SOF.1

Related Files	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 document.

Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.

Vulnerability Analysis AVA_VLA.1

Related Files	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 GUI	Actions performed between Management Server and Java Operator GUI 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

Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

7.4 PP Claims Rationale

Not applicable. There are no PP claims.

8 Acronyms

Table 8-1 Acronyms

ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
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
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
I&A	Identification & Authentication
IT	Information Technology
Java GUI	Java Graphical User Interface
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
OVO	OpenView Operations
PAM	Pluggable Authentication Module
PC	Personal Computer
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SP	Service Pack
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

9 References

Table 9-1 References

Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-002, Version 2.2, January 2004.
HP OpenView Operations Administrator's Reference Software Version A.08.10
HP OpenView Operations HTTPS Agent Concepts and Configuration Guide Software Version A.08.10
HP OpenView Operations Concepts Guide Software Version A.08.10
HP OpenView Operations Java GUI Operator's Guide Software Version A.08.10
HP OpenView Operations Installation Guide for HP-UX/Solaris Software Version A.08.10
HP OpenView Operations Release Notes for HP-UX/Solaris Software Version A.08.10
HP OpenView Service Navigator Concepts & Configuration Guide Software Version A.08.10