

## Software Product Description

### HP OpenVMS Enterprise Directory V5.6 and HP Administrator for Enterprise Directory V2.2

SPD 81.03.05

#### Description

The HP OpenVMS Enterprise Directory V5.6 is the fourth release of Enterprise Directory available on the HP Integrity Server Family of Intel® Itanium® based systems, sharing a common code base with the OpenVMS AlphaServer version.

V5.6 adds support for:

- The Draft Behera password policy to ensure secure read and update access to directory information throughout the network. User password hashing is also incorporated, where 'user' is any LDAP client application that has an identity in the directory.
- SAMBA Schema 3.0
- Memory tracing facility for faster diagnostics of the DSA.

The product continues to conform to the ITU-T X.500 Recommendations. These recommendations split the functions of the directory between one or more Directory System Agents (DSA), where all information is held and one or more Directory User Agents (DUA), from which all enquiries and other directory actions are made.

Using the X.500 model, departments and organizations may adopt an incremental independent approach to the establishment of a directory service using, if required, conforming products from multiple vendors. These separate implementations may then be connected together to provide a single logical directory service that spans the department, the organization, the region or the world, as appropriate. The Directory may contain information on anything of interest, typically people, authentication credentials and certificates (such as PKI) systems, network resources and may be accessed both by individual users and applications.

V5.6 includes an extended management client known as the hp Administrator for Enterprise Directory (HP AED) V2.2, which is described within this document.

The OpenVMS Enterprise Directory product set includes:

- OpenVMS Enterprise Directory Server - a Directory System Agent
- Lightweight Directory Access Protocol version 3 (LDAPv3) support
- Full management of the DSA from the hp Administrator for Enterprise Directory (HP AED) for Windows clients, eliminating the need for NCL commands
- An NCL emulator for those customers that must continue using NCL commands, perhaps in NCL scripts, but no longer wishing to configure DECnet-Plus
- Use of an LDAP port number for operation with an RFC1006 Presentation Address over a TCP/IP network without DECnet-Plus being present
- IPv6 Internet Protocol Version 6 (IPv6) to a distributed network directory service over a pure TCP/IP environment without DECnet-Plus. For those customers that wish to continue to deploy over an OSI transport, this capability is fully retained
- SAMBA Schema V3.0: Applications that require Samba Schema support can create entries in the directory using these schema elements

AE-PX3PS-TF

- Schema extensions to support the storage of OpenVMS Authentication information
- OpenVMS Cluster support
- OpenVMS Enterprise Directory Administration Facility - a Directory User Agent

Other HP messaging and networking products such as all versions of Office Server and ALL-IN-1 V3.2, also provide the directory user agent function in order to access information in the Enterprise Directory Server.

The OpenVMS Enterprise Directory products are based on the 1993 edition of ISO/IEC 9594 and the ITU-T X.500 series of recommendations.

### Abstract Services

The OpenVMS Enterprise Directory components provide and support all of the X.500 Abstract Services, including:

- Read  
Read attributes from a named entry
- Compare  
Test an attribute value without reading it
- Abandon  
Abandon an outstanding operation
- List  
List names of subordinate entries
- Search  
Find entries matching a search expression
- Add  
Create a new entry
- Remove  
Delete an entry
- Modify Entry  
Add or remove attributes or values
- Modify RDN  
Rename an entry

The following operations are supported via the LDAPv3 protocol:

- Bind – with simple password
- Unbind
- Search – no extensibleMatch option
- Modify
- Add
- Delete
- Modify Distinguished Name – no newSuperior option
- Compare
- Abandon

- Backwards compatibility with LDAPv2 clients and directories

The following LDAP string syntaxes are supported:

AttributeTypeDescription (not in v2)

- Binary
- BitString
- Boolean
- Distinguished Name
- DirectoryString
- FacsimileTelephoneNumber
- GeneralisedTime (not in v2)
- IA5String
- Integer
- Jpeg
- MHS-OR-Address
- Octet String
- UTC Time
- Telex Number
- NumericString
- ObjectClassDescription
- OID
- PostalAddress
- PrintableString
- TelephoneNumber
- Delivery Method
- Printable or Numeric String

In addition the LDAP extension ManageDSAIT is included.

### Schema

The OpenVMS Enterprise Directory uses a highly configurable schema allowing customer definition of attributes, object classes, structure rules, and name forms. The schema is installed individually at each DSA.

V5.6 supports extensions to the schema object classes and attributes to support the OpenVMS LDAP SYSSACM Authentication Agent, as the first step in enabling network authentication across an OpenVMS environment.

A default schema that implements the schema in X.520 and X.521 (1995 edition) as well as other useful definitions such as inetOrgPerson ObjectClass as defined in RFC2798 are included.

### Security

To ensure the secure read and update access to directory information throughout the network, the Draft Behera password policy is supported.

User password hashing is also incorporated, where 'user' is any LDAP client application that has an identity in the directory.

The OpenVMS Enterprise Directory supports a subset of the Simplified Access Control scheme from the 1993 edition of the standard. This allows administrators to define policies that control access rights (such as read, browse, modify, remove) to entries and individual attributes within a particular part of the directory (naming context).

The OpenVMS Enterprise Directory allows for the authentication of users by name and password. It also allows access to be restricted based on network address and for chained operations.

### **Distributed Operations**

The DSA supports standard X.500 distributed operations including chaining and referrals. Knowledge management of superior and subordinate references allows an OpenVMS Enterprise Directory DSA to participate as a first-level DSA or a subordinate DSA in a multi-vendor distributed Directory Information Base (DIB).

### **Replication**

The OpenVMS Enterprise Directory supports shadowing of data between DSAs, allowing data to be replicated in the network for high availability and performance. Shadowing also allows replication of knowledge information for distributed operation, access control policies and authentication information, thus reducing the amount of management required.

### **Selective Shadowing**

Selective Shadowing offers the ability to specify which attributes can and cannot be shadowed to a consumer DSA.

The shadowing filter is controlled by the shadowingAttributeSelection attribute in the shadow agreement subentry. Thus there is a specific filter for every shadowing agreement.

Shadowed information is represented using the DSA Information Model defined in the 1993 edition of the standard. OpenVMS Enterprise Directory supports the shadowing service defined in X.525, including supplier initiated and consumer-initiated agreements, both scheduled and on change replication providing full or incremental updates.

### **Protocols**

The Directory Service is based on the client-server model. The DSA server supports the directorySystemAC application context (DSP protocol) to communicate with other DSAs. Communications between server DSAs and client DUAs are supported by the directoryAccessAC application context (DAP protocol). DAP enables DUAs in other X.500 implementations to access the OpenVMS Enterprise Directory DSA and vice-versa. DSP enables full inter-working with DSAs in other implementations.

The X.500 DSA server supports LDAPv2 and LDAPv3 protocols.

For shadowing, the DSA supports shadowSupplierInitiatedAC and shadowConsumerInitiatedAC application contexts in both the synchronous and asynchronous variants (DISP protocol) and the directoryOperationalBindingManagementAC application context (DOP protocol).

The OpenVMS Enterprise Directory V5.6 runs on the OpenVMS Integrity and Alpha operating systems. It provides integrated, multi-protocol support allowing concurrent DAP and DSP access over OSI (using transport classes TP0, TP2, TP4) and RFC1006 over TCP/IP.

### **Security – SSL/TLS Support**

Secure Socket Layer/Transport Layer Security support is provided utilising the SSL shareable library in OpenVMS V7.3-2 and above.

The Directory can receive commands over a secure line using LDAPv3. The following protocols are non-simultaneously supported:

- SSLv23
- SSLv3
- TLSv1

The Directory does not provide a default or private key. These may be obtained from <http://www.openssl.org>

The Directory can be placed in one of three management selectable security states – no security, selectable security and mandatory security.

### **Database**

The OpenVMS Enterprise Directory provides a Directory Information Base based on the

1993 edition of Extended Information Models. This indexed database supports high-performance searching and sophisticated matching including approximate (Soundex) match. The database is held in main memory to ensure optimal response times.

### Support for NCL Service Management

The OpenVMS Enterprise Directory provides DSA management conforming to the Enterprise Management Architecture (EMA), integrated with DECnet-Plus. This provides remote management facilities to configure and control DSAs, and to log significant events.

### Programming Interface

Application access to the OpenVMS Enterprise Directory is provided through the X/Open™ Company Limited's OSI-Abstract-Data Manipulation API and API to Directory Services, also known as the XDS/XOM Application Program Interface.

Documentation, useful libraries and supporting files for the API are included with the OpenVMS Enterprise Directory.

The OpenVMS Enterprise Directory includes a base component that contains the DUA libraries and other supporting files necessary to support applications written to the directory API. This base component, therefore, provides run-time client access to the API libraries; it is distributed with the OpenVMS Enterprise Directory product.

### HP Administrator for Enterprise Directory V2.2

#### Description

The HP Administrator for Enterprise Directory (HP AED) is a Graphical User Interface designed to enable system managers and administrators to easily manage multiple Enterprise Directory servers using LDAPv3 commands. The HP AED provides multiple views of a directory network, visually depicting associations and dependencies.

The HP AED provides full DSA Management, replacing NCL commands when an OSI Transport is not present and can be configured to run over pure TCP/IP even when an OSI transport is present.

The HP AED is written as a Java™ application designed to run on any platform that supports the Java2 Runtime Environment (JRE) V1.5 or later. JRE V1.5 is supplied with the kit.

The “Look-and-Feel” of the HP AED is that of the Sun *Metal* look and feel chosen because of its multi-platform support and minimal software dependency on the host platforms.

All communication with Enterprise Directory servers is via LDAP over an IP network allowing management of multiple directories from a single HP AED. The HP AED takes full advantage of features within the Enterprise Directory V5.6 to maximize manageability.

All management operations performed by the HP AED are subject to checking by Enterprise Directory, that prevents the user inadvertently modifying a DSA in such a way that it is left in an inconsistent state.

### Functionality Supported

The HP AED allows an administrator to connect simultaneously to an arbitrary number of Enterprise Directories - subject to suitable authentication - and provide a view of the DSA that highlights and allows manipulation of the following entities:

- Naming Contexts
  - Display and highlight existing naming contexts
  - Create new naming contexts
  - Remove existing naming contexts
- Superior References
  - Display an existing Superior Reference
  - Create a new Superior Reference
  - Modify or delete an existing Superior Reference
- Subordinate References
  - Display existing subordinate references
  - Create new subordinate references
  - Modify or delete existing subordinate references
- Replication
  - Display existing replication information
  - Create new replication agreements

- Modify or delete existing replication agreements

### HP AED Utility Functions

For the following operations the GUI relies on the HP AED Utility:

- Displaying a list of the available schema files
- Creating a new schema file
- Editing an existing schema file
- Recompiling the schema
- Restarting the DSA
- Editing the DSA Characteristics

The system manager can decide whether or not the HP AED Utility should be enabled on any given server. The GUI only requires that the HP AED Utility be available in order to carry out the functions listed above. Other administrative operations - such as viewing and updating the contents of the DSA - do not require the HP AED Utility to be running.

Use of the HP AED Utility is dependant upon a management password that is specific and should be made unique to the Utility.

Communication between the HP AED and the Utility may utilize SSL connections over default port 907, which can be overridden within the configuration file.

### Security and Authentication

An authentication mechanism is available to ensure security and integrity of the DSAs and Schema.

For DSA Management operations the HP AED communicates with a Utility program that runs on the same node as the target DSA. Access to this utility is restricted by password that will be supplied by the system manager to trusted administrators etc.

For operations that involve multiple DSAs e.g. setting up a subordinate reference, the HP AED makes checks on all DSAs involved before proceeding, and will issue appropriate diagnostic information in the case of inconsistency.

### Internet Protocol V6 Support

Client and server modules in the HP Enterprise Directory product have been enabled to support IPv6 in a pure IPv4, pure IPv6 or dual IPv4/v6 environment.

The supported servers in the DSA discover the configured protocols (IPv4, IPv6) on the

system. In a DECnet-less environment, if IPv6 is configured on a particular system, the servers initialize to 'listen' on IPv6, else they fall back to 'listening' on IPv4.

Similarly the supported clients (and client APIs) in the DSA have been modified to connect to the server making use of the user provided or stored address of the server host. If this attempt fails, then all the configured addresses of the server host are locally resolved. Then an attempt is made to establish a connection on each of the resolved address (IPv4, IPv6) successively, till either a successful connection is established or the resolved addresses are exhausted.

### Supported Platforms

The HP AED has been tested and certified with the following platforms:

- Windows 2000 SP4  
or
- Windows XP SP2  
with
- Java2 Runtime Environment V1.5  
and
- Connection to an IPv4 and IPv6 network

### Minimum Disk Space Requirements

75 MB

### Memory Requirements

32 MB

### DISTRIBUTION MEDIA

This product is supplied with the OpenVMS Enterprise Directory V5.6 and is downloadable from the Web.

The on-line documentation for this product is included in the supplied kits.

### Directory User Agents

The OpenVMS Enterprise Directory Administration Facility provides a Directory User Agent. The Information Management Utility (DXIM) allows users to search and browse the directory and to maintain the data stored in it. Operations include the addition, modification, and deletion of entries. DXIM supports both DECwindows Motif® and command line interfaces. It can be used on a

DSA node or remotely from any other node in the network.

DXIM is configurable, based on the schema definitions, to support customer defined attributes and classes.

Access to the OpenVMS Enterprise Directory may also be obtained through other HP software products that contain the Directory User Agent function. For example, Office Server will allow users of TeamLinks, Microsoft Outlook, IMAP4, POP3 and Web clients access to information in the Enterprise Directory.

Inclusion of the LDAP interface enables the following clients to obtain directory information:

- Internet Explorer
- Netscape Web Client
- Outlook 2000 Client

And any client accessing from Office Server V6.0 and V6.1, all of which include LDAPv3 support.

## STANDARDS SUPPORTED

The OpenVMS Enterprise Directory products are implemented according to the 1993 edition of ISO/IEC 9594 and the ITU-T X.500 series of Recommendations. The products have successfully completed testing to the Open Systems Testing Consortium (OSTC) 1988 X.500 conformance tests. The conformance testing was carried out by the United Kingdom National Computer Centre, an accredited OSTC testing centre, which produced OSTC test reports valid in all European Community states. The products have been registered by the U.S. National Institute of Standards and Technology (NIST) as conformant to U.S. GOSIP.

The products are designed and implemented to conform, with some minor exceptions, to the following European and US profiles:

NIST OIW Stable Implementor's Agreements - Version 5 edition 1

- ENV 41210
- ENV 41212
- ENV 41215
- ENV 41512

The product also supports, where applicable, the following Internet standards:

- RFC 1006
- RFC 1274
- RFC 1277 (as it applies to TCP/IP networks)
- RFC 1278

The LDAP functionality will conform to the following standards. For LDAP V2:

- RFC 1777 Lightweight Directory Access Protocol
- RFC 1558 A String Representation of LDAP Search Filters
- RFC 1778 The String Representation of Standard Attribute Syntaxes

For LDAP V3:

- RFC 2251 Lightweight Directory Access Protocol (v3)
- RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
- RFC 2253 Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names
- RFC 2254 The String Representation of LDAP Search Filters
- RFC 2255 The LDAP URL Format
- RFC 2256 A Summary of the X.500 (96) User Schema for use with LDAP V3
- RFC 2798 A general purpose object class that holds attributes about people including inetOrgPerson
- RFC 2830 Start TLS extension to LDAP for us with SSL
- RFC 3296 ManageDSAIT Control

## Character Set Support

LDAPv3 strings are based on the UTF-8 character set and are restricted to characters that can be mapped to the T.61 character set. Input characters will be substituted by their base character wherever possible, if they can't be mapped to T.61.

## HARDWARE REQUIREMENTS

### Processors Supported

OpenVMS Enterprise Directory V5.6 is supported on all HP Integrity server and AlphaServer systems that can support the memory and disk requirements.

For deployments utilising DECnet-Plus, refer to the DECnet-Plus for OpenVMS Software Product Description (SPD 50.45.xx) for further information on supported hardware configurations.

**Disk Space Requirements**

The counts below refer to the disk space required on the system disk or specified file systems. The sizes are approximate; actual sizes may vary depending on the user's system environment, configuration, and software options selected.

The values refer to the space required to install the Directory Server, Administration and Application Programming components. The Base component is a mandatory component for all installations. Permanent disk space requirements for the components are cumulative. Directory data files are not included and will require additional space that can be on a non-system disk.

Disk space required for installation on HP Integrity servers:

<i>Component</i>	<i>Blocks</i>	<i>Kbytes</i>
All:	654000	327000

Disk space required for use (permanent):

<i>Component</i>	<i>Blocks</i>	<i>Kbytes</i>
Base:	80178	40089
Server:	256738	128369
Administration:	309082	154541
Application Programming:	1024	512
Look-up client	7168	3584

OpenVMS AlphaServer systems require 30% less space for the Base and Server components.

If the HP AED is installed this will require an additional 125,000 blocks and the HP AED Utility will require a further 105,000 blocks.

**Memory Requirements**

The performance of this product is dependent on the amount of system memory. The memory size suggested for most typical hardware configurations is at least one Gigabyte for systems running the Directory Server. On these server systems, memory usage increases in proportion to the amount of data stored in the database.

**CLUSTER ENVIRONMENT**

This layered product is fully supported when installed on any valid and licensed VMSccluster\* configuration without restrictions. The HARDWARE REQUIREMENTS section of this document details any special hardware required by this product.

\* VMSccluster configurations are fully described in the VMSccluster Software Product Description (29.78.xx) and include CI, Ethernet and Mixed Interconnect configurations.

**SOFTWARE REQUIREMENTS**

For OpenVMS Integrity servers:

OpenVMS Integrity Operating System V8.2 and later

For OpenVMS AlphaServer systems:

OpenVMS Alpha Operating System V7.3-2 and later

and optionally, for pure TCP/IP deployments:

HP TCP/IP Services V5.6 or later for OpenVMS V8.2 or later.

HP TCP/IP Services V5.4 ECO 5 or later for OpenVMS V7.3-2.

Note this is a pre-requisite if the HP AED is deployed.

and optionally, for deployments utilising OSI Transport:

DECnet-Plus for OpenVMS Integrity V8.2 or later

DECnet-Plus for OpenVMS Alpha V7.3-2 or later.

Additionally the OSI Applications Kernel (OSAK) needs to be installed, instructions for which are in the DECnet-Plus for OpenVMS Applications Installation and Advanced Configuration manual. If you have installed DECnet-Plus then you must also install OSAK.

Note if it is intended to utilise RFC1006, then a TCP/IP network must also be deployed.

For LDAPv3 over SSL, HP SSL Version 1.1 for OpenVMS or later is required.

For all OpenVMS Systems:

This product may run in either of the following ways:

Standalone Execution - Running the X11 display server and the client application on the same machine.

Remote Execution - Running the X11 display server and the client application on different machines.

### OpenVMS Tailoring:

The following OpenVMS classes are required for full functionality of this layered product:

OpenVMS Required Saveset  
Network Support  
Programming Support  
VMS Workstation Support

### GROWTH CONSIDERATIONS

The minimum hardware/software requirements for any future version of this product may be different from the requirements for the current version.

### DISTRIBUTION MEDIA

This product is available:

- with OpenVMS V8.2 and later distributions of OpenVMS
- the OpenVMS Alpha Layered Products CD-ROM distribution's Software Product Library, formerly known as CONDIST
- the OpenVMS e-Business CD V2.0 and later

The on-line documentation for this product is available on the Integrity and Alpha Online Documentation CD-ROM distributions.

### ORDERING INFORMATION

In this section, an asterisk (\*) denotes variant fields. For additional information on available

licenses, services, and media, refer to the appropriate price book.

*Software Product Services:*

- QT-2NZA\*-.\*\*

### HP OpenVMS Enterprise Directory Administration Facility:

*Software Licenses on the OpenVMS Integrity and Alpha Software Products Library:*

QL-2P0A\*-.\*\*

*Software Product Services:*

QT-2P0A\*-.\*\*

### Documentation for all products:

*OpenVMS Printed Documentation:*

QA-0P4AA-GZ

SOFTWARE LICENSING

This software is furnished under the licensing provisions of HP Computer Limited Standard Terms and Conditions. For more information about HP's licensing terms and policies, contact your local HP office or Partner.

### License Management Facility Support

There are no LMF license checks.

In a messaging environment with mail user agents, a MAILbus 400 MTA and gateways, a 5,000 entry DSA may be sufficient to support a user population of around 1000 people. For further details of this mechanism, consult the product documentation.

The OpenVMS Enterprise Directory includes a base component that contains the DUA libraries and other supporting files necessary to support applications written to the directory API. This base component, therefore, provides run-time client access to the API libraries; it is distributed with the OpenVMS Enterprise Directory product.

## SOFTWARE PRODUCT SERVICES

Software Product Services is based on Service level SPL3 when the product is first activated on every system.

## SOFTWARE WARRANTY

This software is provided by HP, with a warranty in accordance with the HP OpenVMS operating system warranty that it is installed upon.

© Copyright 2007 Hewlett-Packard  
Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

MOTIF is a registered trademark of The Open Group.

Printed in the US