

HP-UX AAA Server A.06.01.02 Release Notes

HP-UX 11.00 and 11i Version 1

www.docs.hp.com



**Manufacturing Part Number : T1428-90038
E0903**

U.S.A.

© Copyright 2001 - 2003 © Hewlett-Packard Development Company, L.P.

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD DEVELOPMENT COMPANY L.P.
20555 S.H. 249
Houston, Texas 77070

Use of this document and any supporting software media supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Copyright Notice

Copyright © 1997-2003 Hewlett-Packard Development Company L.P. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Trademark Notices

ProLDAP™ is a trademark of Interlink Networks, Inc.

Internet Explorer ® is a registered trademark of Microsoft Corporation.

HP-UX AAA Server A.06.01.02

The information in this document is for the HP-UX AAA Server A.06.01.02 only.

Product Overview

The HP-UX AAA Server utilizes the industry standard Remote Authentication Dial-In User Service (RADIUS) protocol to provide user-based authentication, authorization and accounting of network access. At the network entry point, the HP-UX AAA Server provides:

- authentication for network access devices
- authorization of user access
- accounting (access) log files of that can be utilized by billing and accounting applications

The HP-UX AAA Server supports RADIUS and EAP (Extensible Authentication Protocol) over RADIUS compliant devices including:

- Network Access Servers (NAS)
- LAN switches *
- LAN hubs *
- Wireless LAN (WLAN) access points *

** Note: device must be RADIUS/EAP enabled*

Merit (default) and Livingston accounting style formats are supported to ensure interoperability with a wide variety of billing and mediation applications. Store account information in any of the following repositories for users accessing the network through the HP-UX AAA Server:

- local AAA server configuration files
- LDAP version 3 compliant directories **
- Oracle 8.1.7 databases **

*** AAA server offers support for authentication request load balancing and failover*

The HP-UX AAA Server also includes the following features:

- DHCP support for centralized administration of IP Address assignment
- SNMP support for effective management
- web-based administration with Server Manager graphic user interface
- session management capabilities
- full set of support utilities

Product Documentation

In addition to these Release Notes, HP provides the following two guides to support the HP-UX AAA Server A.06.01.02:

- *HP-UX AAA Server A.06.01 Getting Started Guide* (MPN #T1428-900XX)
 - Product and Technology Overview
 - Installation
 - Task Introductions
- *HP-UX AAA Server A.06.01 Administrator's Guide* (MPN #T1428-900XX)
 - Administering HP-UX AAA Servers
 - Managing and Authenticating Users
 - Troubleshooting
 - Reference

NOTE The Getting Started Guide is to guide you through the initial set-up and configuration. Start with this introductory guide to install and become familiar with the product. The Administrator's Guide contains complete product documentation. Refer to this guide after using the Getting Started Guide to install and become familiar with the product.

You can find the Getting Started Guide, Administrator's Guide, and HP-UX AAA Server documentation at the following locations:

- the product directories in `/opt/aaa/share/doc/`
- the Server Manager interface Help system
- the HP Technical Documentation website on the Internet and Security Solutions page at: <http://www.docs.hp.com>

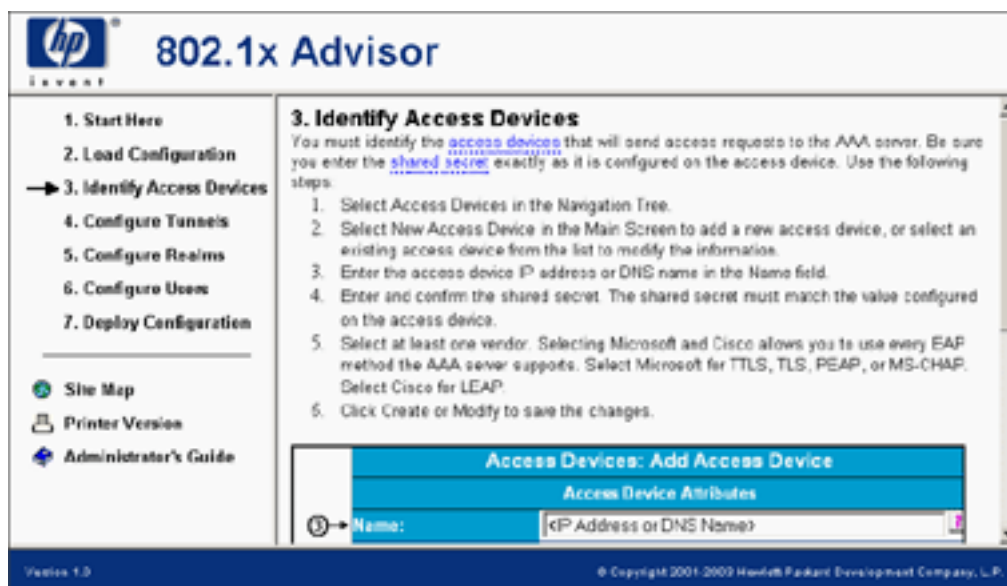
IMPORTANT Monitor <http://www.docs.hp.com> for the most recently released product documentation.

Wireless-LAN Documentation—The 802.1x Advisor

The 802.1x Advisor is an HTML tutorial/help system in the Server Manager GUI that walks-you-through the tasks and Server Manager screens for securing WLANs with the HP-UX AAA Server. The 802.1x Advisor provides information only—it does not edit configuration files. Follow the 802.1x Advisor and use Server Manager to create and deploy basic AAA configurations for securing WLANs. Refer to the HP-UX AAA Server Administrator's Guide for complete HP-UX AAA Server documentation.

The following graphic shows the 802.1x Advisor used to quickly secure WLANs with the HP-UX AAA Server:

Figure 1 **The 802.1x Advisor For Securing WLANs**



Compatibility Information and Installation Requirements

The information in this section lists the requirements needed to install and run the HP-UX AAA Server A.06.01.02, including the following:

- Hardware Requirements
- Operating System Requirements
- Product Dependencies
- Patch Dependencies
- Web Browser Requirements
- LDAP Compatibility

Hardware Requirements

- HP 9000 Computers
- minimum of 128 MB memory
- 5 GB disk space

Operating System Requirements

- HP-UX 11.0 (32 or 64 bit)
- HP-UX 11i version 1 (32 or 64 bit)

Product Dependencies

You must have the following product dependencies installed on your system to use the HP-UX AAA Server:

- HP-UX SDK for Java version 1.4.1.x or higher (product #T1456AA)
- HP-UX Tomcat-based Serverlet Engine version 1.0.03.x or higher (product # HPUXWSSUITE)
- HP-UX Apache-based Web Server version 1.0.03.x or higher (product # HPUXWSSUITE)

The Tomcat and Apache dependencies are both components of the HP-UX Web Server Suite (product # HPUXWSSUITE). You do not need the Webmin-based Admin component of the Web Server Suite for the HP-UX AAA Server.

You can get the HP-UX SDK for Java version 1.4.1.x at:

<http://www.hp.com/products1/unix/java/index.html>

You can get the Tomcat and Apache components of the Web Server Suite version 1.0.03.x on the *Security and Manageability* page at: <http://software.hp.com/>

Patch Dependencies

You must have the following patch dependencies installed on your system to use the HP-UX AAA Server A.06.01.02. Both patches are available at:

ftp://us-ffs.external.hp.com/hp-ux_patches/s700_800/11.X/

Table 1 Patch Dependencies for HP-UX AAA Server A.06.01.02

HP-UX 11.00	HP-UX 11i Version 1
PHSS_26945	PHSS_26946

NOTE HP strongly recommends installing Hardware Enablement Patch B.11.00.0209.5 or higher for HP-UX 11.00. You can get this patch at http://www.software.hp.com/SUPPORT_PLUS/hwe.html

Web Browser Requirements

You must have access to a web browser to use the Server Manager interface to administer and configure the HP-UX AAA Servers. Use only the following web browsers with the HP-UX AAA Server A.06.01.02—known interoperability issues exist in other web browser versions:

- Netscape Navigator 4.76 or higher
- Internet Explorer 5.05 or higher

LDAP Compatibility

The HP-UX AAA Server A.06.01.02 is designed to interoperate with LDAP version 3 compliant directories. HP certified the HP-UX AAA Server A.06.01.02 with Netscape Directory Server version 6.

Availability in Native Languages

The HP-UX AAA Server A.06.01.02 is currently available in English only.

What's New in the HP-UX AAA Server A.06.01.02

Features

The following is a list of the new features in the HP-UX AAA Server A.06.01.02:

- Support for EAP-TLS, EAP-TTLS, PEAP, EAP-MSCHAP, and EAP-GTC
- DHCP Interface for IP Address Management
- 8021.x Advisor help system in Server Manager interface to facilitate WLAN configuration
- "Self-signed" AAA server digital certificates created during installation for deploying a secured EAP-TTLS and PEAP environment without having to generate your own digital certificates.

NOTE The `sesstab` and `radrecord` command line utilities are no longer supported from the command line, however, the functionality is still available through the Server Manager interface.

Fixes

The following is a list of defects discovered in previous versions and fixed in the A.06.01.02:

- When an accounting request for a user without a realm arrives, an inaccurate logfile message ("user realm not configured") is logged.
- AAA server performs highest level of debug logging when it receives a non-RADIUS (vendor-specific) packet type.
- Server Manager deletes Tokenpool names in `/etc/opt/aaa/authfile` when modifying realm entries.

Known Problems and Limitations in Version A.06.01.02

The following information describes known problems and limitations in the HP-UX AAA Server A.06.01.02.

Known Problems

- Server Manager incorrectly hashes user password when MD5 hashing is the file storage.
- Local realms configured for default user file storage do not support aliases.
- Single PEAP session does multiple lookup in user repository to authenticate user.
- Server Manager cannot modify manually added BIN/CIS options for realm entries in `/etc/opt/aaa/authfile`.

Known Limitations

- Server Manager interface does not manage previous version of AAA server software.
 - **Workaround:** Follow the steps in “Migrating to Version A.06.01.02” on page 13 to migrate your configuration.
- The AAA server loads all shared libraries in the `/opt/aaa/aatv/` directory when starting. Libraries with unresolved external references will cause the startup to fail. User-created libraries for previous versions of the product may also fail during execution. Updating your installation replaces only the libraries originally installed with the product—any user-created libraries will remain.
 - **Workaround:** Remove any user-created shared libraries from the `/opt/aaa/aatv` directory before starting the HP-UX AAA Server.
- Server Manager interface does not load configuration applets in some network environments when using your browser's autocomplete or “Remember My Password” feature for the Server Manager password.
 - **Workaround:** Disable autocomplete for passwords, or remove the Server Manager password from the autocomplete list in your browser.

Supplicants Support and Interoperability

The information in this section lists the supplicants and EAP methods (for each supplicant) certified with the HP-UX AAA Server A.06.01.02.

Funk Odyssey version 1

The following is a list of EAP methods this supplicant and the HP-UX AAA Server A.06.01.02 support:

- EAP-TTLS with PAP, CHAP, MS-CHAP, or MD5
- LEAP
- EAP-TLS
- EAP-MD5

Funk Odyssey version 2

The following is a list of EAP methods this supplicant and the HP-UX AAA Server A.06.01.02 support:

- EAP-TTLS with PAP, CHAP, MS-CHAP, or MD5
- PEAP with EAP-MD5 or EAP-GTC
- LEAP
- EAP-TLS
- EAP-MD5

Microsoft for Windows 2000 (SP4 or higher) and XP (SP1 or higher)

The following is a list of EAP methods this supplicant and the HP-UX AAA Server A.06.01.02 support:

- PEAP with EAP-MS-CHAP v2
- EAP-TLS

Cisco Aironet Client Utility version 6.1

The following is a list of EAP methods this supplicant and the HP-UX AAA Server A.06.01.02 support:

- PEAP with EAP-GTC
- LEAP

NOTE

After installing and selecting the AAA Server CA certificate on some Cisco supplicants, you may encounter the following condition:

```
"PEAP validation failed, status=-16"
```

You will still be able to authenticate by deselecting the AAA Server CA certificate in the supplicant. You will be prompted to inspect and accept the certificate during authentication.

Migrating to Version A.06.01.02

There are significant structure and feature differences between the HP-UX AAA Server A.06.01.02 and previous versions of the product that affect the configuration files. The information in this chapter explains the steps you must perform to migrate to A.06.01.02 from previous versions.

NOTE Contact your HP Support representative if you need assistance with your migration.

Steps for Migrating

The following is a list of the directories you will use when migrating to the HP-UX AAA Server A.06.01.02 from legacy versions:

- `/etc/opt/aaa/`: A.06.01.02 working directories.
- `/etc/opt/aaa.old/`: configuration files from your legacy AAA server installation.
- `/opt/aaa/newconfig/etc/opt/aaa/`: backup of the default A.06.01.02 files for reference.

Use the following steps to migrate to the HP-UX AAA Server A.06.01.02 from legacy versions:

- Step 1.** Backup your existing AAA server configuration.
- Step 2.** Install the HP-UX AAA Server A.06.01.02 without removing your existing HP-UX AAA Server software.
- Step 3.** Copy the following files from `/etc/opt/aaa.old/` to `/etc/opt/aaa/`. You do not need to modify these files when migrating to A.06.01.02:
 - `clients`
 - `las.conf`
 - `iaaaAgent.conf`
 - `db_srv.opt`
 - `engine.config`
 - `DAC.grp` and additional decision/policy files

Step 4. Update the following A.06.01.02 files in `/etc/opt/aaa/` to include any modifications you made for your legacy configuration. Perform this step to include your legacy configuration in the new A.06.01.02 file format. Refer to the copy of your legacy files in `/etc/opt/aaa.old/` and update the corresponding A.06.01.02 files listed below:

- `vendors`
- `log.config`
- `radius.fsm`
- `dictionary`
- `aaa.config`

Step 5. Copy your legacy users files from `/etc/opt/aaa.old/` to `/etc/opt/aaa/` (including the default `users` file and all files with the `.users` extension). Update the users files as follows:

- Remove all `DEFAULT`, `dumbuser`, `pppuser`, and `slipuser` entries. The following shows example entries for each:

DEFAULT

```
DEFAULT Authentication-Type = Realm
Filter-Id = "unlim"
```

dumbuser

```
dumbuser Authentication-Type = None
Service-Type = Login,
Login-Service = Telnet,
Login-IP-Host = 255.255.255.255
```

pppuser

```
pppuser Authentication-Type = None
Service-Type = Framed,
Framed-Protocol = PPP,
Framed-IP-Netmask = 255.255.255.0,
Framed-Routing = None,
Framed-MTU = 1500,
Framed-Compression = Van-Jacobson-TCP-IP
```

slipuser

```
slipuser Authentication-Type = None
        Service-Type = Framed,
        Framed-Protocol = SLIP,
        Framed-IP-Netmask = 255.255.255.0,
        Framed-Routing = None,
        Framed-MTU = 1500,
        Framed-Compression = Van-Jacobson-TCP-IP
```

- **Remove all Authentication-Type=Realm and Authentication-Type=File strings from the remaining user entries. The following is a sample sed command you can modify to remove these entries:**

```
$ sed -e 's/Authentication-Type[ ]*=[ ]*Realm[ ,]*//g'-e 's/Authentication-Type[ ]*=[ ]*File[ ,]*//g' <users or *.users file name>
```

Step 6. Use Server Manager to re-configure all of your legacy realm and outbound proxy entries on A.06.01.02. Refer to your legacy authfile at `/etc/opt/aaa.old/authfile`:

- Use Server Manager's [Proxies](#) link to re-configure entries in `/etc/opt/aaa.old/authfile` with the following syntax:

```
realm.com    RADIUS    <Realm_host_name>
```

- Use Server Manager's [Local Realms](#) link to re-configure the realm entries as they appear in `/etc/opt/aaa.old/authfile`.

Step 7. If you are using a Netscape Directory server, update the RADIUS schema file for the directory server. Copy `/opt/aaa/examples/proldap/55iaaa-radius.ldif` to the Netscape Directory server. Stop and restart `slapd` after copying the schema file to the Netscape server.

Step 8. If you are using an OpenLDAP server, update the RADIUS schema file for the directory server. Copy `/opt/aaa/examples/proldap/iaaa-radius.ldif` to the OpenLDAP server. Stop and restart `slapd` after copying the schema file to the OpenLDAP server.

NOTE After completing the migration to the HP-UX AAA Server A.06.01.02, the configuration secrets in `/opt/aaa/remotecontrol/rmiserver.properties` and `/opt/hpws/tomcat/webapps/aaa/WEB-INF/gui.properties` will be the default values. Refer to "Changing the Default RMI Objects Secret" in the Administrator's Guide for information on changing these secrets.
