

HP-UX AAA Server A.07.00 Release Notes

HP-UX 11i v1, HP-UX 11i v2, and HP-UX 11i v3

Documentation Web Site: <http://www.docs.hp.com>



Manufacturing Part Number: T1428-90065

September 2007

Legal Notices

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

Confidential computer software. Valid license required from HP 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 additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

UNIX is a registered trademark of The Open Group.

HP-UX AAA Server A.07.00 Release Notes

This document discusses the most recent product information on HP-UX AAA Server A.07.00. HP-UX AAA Server A.07.00 is supported on HP-UX 11i v1 (B.11.11), HP-UX 11i v2 (B.11.23), and HP-UX 11i v3 (B.11.31).

This document addresses the following topics:

- “Product Overview” on page 5
- “What is New in this Version” on page 8
- “Fixes Included in the HP-UX AAA Server A.07.00” on page 12
- “Known Problems and Limitations in HP-UX AAA Server A.07.00” on page 14
- “Supplicant Support and Interoperability” on page 16
- “Product Documentation” on page 18
- “Installation Requirements” on page 20
- “Availability in Native Languages” on page 24

Product Overview

The HP-UX AAA Server utilizes the industry standard Remote Authentication Dial-In User Service (RADIUS) protocol and Extensible Authentication Protocol (EAP) to provide standards-based user authentication, authorization, and accounting services to network devices and software applications.

The HP-UX AAA Server can be utilized for securing wired and wireless LAN access, provide authentication and accounting for Virtual Private Network (VPN) gateways, firewalls and other network devices, and to enhance the security of RADIUS enabled software applications in Enterprise and Service Provider environments.

Product Features

The HP-UX AAA Server includes the following features:

- **Common Database Interface:** Supports HP-UX AAA Server interaction with supported databases via the SQL Access AATV and database client connector libraries.
- **EAP Support for Authenticated LAN Access:** Secure wired and wireless LANs using Extensible Authentication Protocol (EAP) to support 802.1x enabled network access devices. EAP methods supported include PEAP, TTLS, TLS, LEAP, GTC, MSCHAPv2, and MD5.
- **Multi-Server Session Management:** Supports user, group, or custom limits on concurrent logins to limit simultaneous sessions. Customizable shared session management for multiple HP-UX AAA Servers is supported via the SQL Access feature.
- **IP Address Management:** DHCP interface for centralized administration of IP Address assignment.
- **IPv6 Support:** Supports RADIUS IPv6 attributes with HP-UX 11i v1 (and subsequent releases). Also supports RADIUS communication over IPv6 transports with HP-UX 11i v2 (and subsequent releases).
- **SNMP Support:** Effectively integrate and manage HP-UX AAA Servers with SNMP compliant network management tools.

- **LDAP Integration:** Supports user profile storage and authentication using LDAP Version 3 compliant directories with request load balancing and failover.
- **Web-based Administration:** The Server Manager web-based administration utility provides management and configuration of multiple HP-UX AAA Servers sharing a common configuration set.
- **Secure LAN Advisor:** Utility inside the Server Manager administration tool to help plan, configure, and deploy authenticated LAN access via 802.1x and EAP.
- **Flexible Policy Management:** Quickly and easily configure a variety a dynamic access control policies, including combinations of time, date, password expiration, or other user defined attributes.
- **Robust RADIUS Proxy Capabilities:** Forwards authentication and accounting requests to other RADIUS servers by DNS, realm, or custom criteria with configurable retry and time-out periods.
- **Multi-vendor RADIUS Client Support:** Includes pre-defined attribute mappings for leading network access vendors and a customizable vendor dictionary to support a wide range of RADIUS clients.
- **Flexible and Customized Session Logging:** Customize session logs to capture the desired volume of session and accounting information. Session logging formats for Merit (default) and Livingston CDR Standard are included. Logging directly to the database, including shared accounting for multiple HP-UX AAA Servers is also supported via the SQL Access feature.
- **RADIUS Server Plug-in SDK:** Server Plug-in Software Developer's Kit for customizing and extending the features of the AAA Server. For more information, email aaainfo@cup.hp.com.
- **IETF RADIUS RFC Standards:** Supports the following IETF RFCs:

Table 1 Supported IEF T RFCs

RFC#	RFC Title
2284	PPP Extensible Authentication Protocol (EAP)
2619	RADIUS Authentication Server MIB

Table 1 Supported IEFT RFCs (Continued)

RFC#	RFC Title
2621	RADIUS Accounting Server MIB
2716	PPP EAP-TLS Authentication Protocol
2865	Remote Authentication Dial-In User Service (RADIUS)
2866	RADIUS Accounting
2867	RADIUS Accounting Modifications for Tunnel Protocol Support
2868	RADIUS Attributes for Tunnel Protocol Support
2869	RADIUS Extensions
3162	RADIUS and IPv6

What is New in this Version

HP-UX AAA Server version A.07.00 includes the following new and changed features:

- SQL Access Support for Oracle OCI and ODBC
- Wi-Fi Protected Access 2 (WPA2) Support
- Server Manager Enhancements for Realm Configuration
- Detailed Error Logging for Improved Troubleshooting
- Manual Rollover of the Server Log File and Accounting Stream
- Improved Performance for EAP-TLS
- Improved Support for Multiple CRLs
- Deprecation of Oracle and LDAP Policy

SQL Access Support for Oracle OCI and ODBC

HP-UX AAA Server A.07.00 now supports SQL Access for Oracle OCI and Open Database Connectivity (ODBC) compliant database client libraries.

SQL Access provides a highly flexible interface to customize the functionality of the AAA Server to meet your business requirements. SQL Access enables the execution of user-defined SQL statements that are mapped to RADIUS transactions. In addition, pre-defined and/or customized functions enable the extension the HP-UX AAA Server functionality and additional control over the HP-UX AAA Server operation.

The ability to integrate the HP-UX AAA Server with an SQL compliant database offers the following benefits:

- Scalability across multiple HP-UX AAA Servers by using a database as a central repository for user, account, and session information
- Extension of HP-UX AAA Server functionality by introducing customized behaviors using SQL
- Session state tracking and session limit enforcement across multiple HP-UX AAA Servers for greater scalability and availability

- Integration of HP-UX AAA Servers with existing Oracle OCI and ODBC compliant databases for authentication, accounting, and session management

The SQL Access feature consists of the SQL Access AATV, client connector libraries for supported database clients, and a set of reference implementation files that provide a quick and easy way to set up a working environment that provides fully functional reference implementations. These reference implementations can be used as-is, or customized to meet your deployment requirements.

The reference implementation uses SQL statements to retrieve user entries and optionally perform accounting and session management (with or without DHCP) in a multi-server environment.

See the following README files based on your implementation requirements:

- `/opt/aaa/examples/sqlaccess/oracle-1/`: to implement SQL Access using the Oracle database server and OCI client
- `opt/aaa/examples/sqlaccess/mysql-1/`: to implement SQL Access using the MySQL database server and MySQL Unix ODBC client

See the SQL Access Chapter in the [HP-UX AAA Server A.07.00 Administrator's Guide](#) for more details on the SQL Access feature.

NOTE

The new SQL Access feature provides database connectivity via customer supplied database client or driver libraries. HP provides connectors for specific database client vendors and versions.

Refer to SQL Access Requirements in the Installation Requirements section of this document for the list of currently provided connectors.

The database server and client libraries are not provided with the HP-UX AAA Server.

Wi-Fi Protected Access 2 (WPA2) Support

HP-UX AAA Server A.07.00 supports Wi-Fi Protected Access 2 (WPA2) enabled RADIUS clients. WPA2 is the official IEEE 802.11i standard that enhances security with Advanced Encryption Standard (AES) for data encryption.

Server Manager Enhancements for Realm Configuration

The Server Manager **Add/Modify Local Realms** screen includes the following enhancements:

Modified EAP Options

EAP options are now modified to clearly state the EAP method used. For example, MD5 is now listed as EAP-MD5.

Inner and Outer TTLS Realm Support

The Server Manager **Add/Modify Local Realms** screen enables the creation of the same inner and outer realm by specifying a combination of the following new options:

- TTLS (EAP-MD5)
- TTLS (EAP-MSCHAPv2)
- TTLS (EAP-PAP/CHAP/MSCHAP/MSCHAPv2)

The following rules of mutual exclusivity apply:

- TTLS options may only be selected with other TTLS options
- PEAP options may only be selected with other PEAP options

Authentication Method Specification

You can now specify the authentication method for a realm as follows:

- Enable EAP: for authentication via EAP
- Enable RADIUS Standard: use standard RADIUS authentication methods (PAP, CHAP, MSCHAP, and MSCHAPv2)

See the [HP-UX AAA Server A.07.00 Administrator's Guide](#) and the Secure LAN Advisor in the Server Manager for more details on the **Add/Modify Local Realms** screen.

Detailed Error Logging for Improved Troubleshooting

HP-UX AAA Server A.07.00 logs detailed error messages in the server log file. The error messages contain information on the symptom, description, and corrective action for common errors.

Manual Rollover of the Server Log File and Accounting Stream

HP-UX AAA Server A.07.00 log files and accounting stream can be rolled over using the new `radsignal` command. See the `radsignal` manpage for more information.

Improved Performance for EAP-TLS

HP-UX AAA Server A.07.00 optimizes Certification Revocation List (CRL) processing. This results in improved performance with EAP-TLS. The performance improvement is more noticeable as the number of entries in the CRL file increases.

Improved Support for Multiple CRLs

HP-UX AAA Server A.07.00 now supports multiple Certificate Revocation Lists (CRLs) in a single CRL file.

Deprecation of Oracle and LDAP Policy

Oracle access via the `db_srv` daemon is deprecated for this release and may not be supported in future releases. It is recommended to use the SQL Access feature for Oracle database access.

Advanced Policy support via LDAP is deprecated on this release and may not be supported in future releases. It is recommended to use policy configuration via local configuration files.

Fixes Included in the HP-UX AAA Server A.07.00

The following defect fixes are included in the A.07.00 release:

SR Number	Description
8606329329	<p>The Server Manager now generates valid MD5 password hashes when creating local user profiles.</p> <p>Prior to the A.07.00 release, the Server Manager generated incorrect MD5 hashes, leading to Access-Rejects for locally configured users with MD5 hashed passwords.</p>
8606396481	<p>The Server Manager now excludes upload of files in the <code>/etc/opt/aaa/security</code> directory.</p> <p>Prior to the A.07.00 release, the Server Manager uploaded files in the <code>/etc/opt/aaa/security</code> directory, which contains digital certificates and key files. These files would then be downloaded to all managed HP-UX AAA Servers. This would result in the overwriting of individual server certificates and key files.</p> <p>If you have a need to propagate any of these files, copy to the <code>/etc/opt/aaa</code> directory, and modify the file location in the Server Manager Certificate Properties screen.</p>
8606426587	<p>Accounting message forwarding and session tracking are now configured independently for proxy realms.</p> <p>Prior to the A.07.00 release, if account message forwarding to the home HP-UX AAA Server was disabled, local session tracking was automatically enabled.</p>

- 8606429881** **Proxy realms with wildcard names are now supported.**
- Prior to A.07.00, wildcard proxy realms were ignored when processing inbound requests.
- 8606448711** **The default local session clear time (the length of time to hold AAA server acquired IP addresses associated with a terminated session) is now configured as five minutes.**
- Prior to the A.07.00 release, the default value was 48 hours.

Known Problems and Limitations in HP-UX AAA Server A.07.00

This section lists the known problems and limitation of the HP-UX AAA Server A.07.00.

Known Problems

- Decreased RADIUS response time under heavy load due to increased CPU consumption.

NOTE: This problem occurs with the HP-UX AAA Server A.07.00 on HP-UX 11i v2 PA-RISC systems only. HP-UX 11i v1 and HP-UX 11i v2 Integrity systems are not affected.

Workaround: Utilize the `pthread` environment variable that minimizes `pthread` overhead for the HP-UX AAA Server in the environment where the `radiusd` daemon is launched:

```
$export PTHREAD_FORCE_SCOPE_SYSTEM=ON
```

- The HP-UX AAA Server leaks memory when the SQL Access feature uses the MySQL Unix ODBC/MySQL client to interact with a MySQL database.

NOTE: This problem occurs with the HP-UX AAA Server A.07.00 on HP-UX 11i v2 PA-RISC systems with the PHSS_31849 (or later) patch only. HP-UX 11i v1 and HP-UX 11i v2 Integrity systems are not affected.

Workaround: Install PHSS_34858 (linker + fdp cumulative patch) on the system where the `radiusd` daemon is launched.

Known Limitations

- Using stored procedure output parameters with MySQL databases will result in `NULL` values for SQL Access output mappings. Input mappings can be processed normally with MySQL stored procedures.

Workaround: Utilize direct SQL statements for SQL Actions requiring output data from MySQL databases.

- The HP-UX AAA Server does not recognize realm aliases for local realms configured with local user file storage.

Workaround: Configure separate realms for each alias.

- The HP-UX AAA Server A.07.00 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.

- Unsupported browsers, including Netscape Navigator 7.0 and Mozilla 1.2.X periodically display various Server Manager icons, buttons, and default values incorrectly.

Workaround: Use a supported browser version with Server Manager.

Supplicant Support and Interoperability

This section lists the supplicants and EAP methods (for each supplicant) certified with the HP-UX AAA Server A.07.00.

Cisco Aironet Client Utility Version 6.6

The following EAP methods are certified for the Cisco Aironet Client Utility Version 6.6 supplicant with the HP-UX AAA Server A.07.00:

- PEAP (EAP-MSCHAPv2, EAP-GTC)
- LEAP
- EAP-TLS

NOTE

After installing and selecting the HP-UX AAA Server CA certificate on some Cisco supplicants, you may encounter the following condition:
"PEAP validation failed, status=-16"

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

Cisco Aironet Desktop Utility Version 3.0

The following EAP methods are certified for the Cisco Aironet Desktop Utility Version 3.0 supplicant with the HP-UX AAA Server A.07.00:

- PEAP (EAP-MSCHAPv2, EAP-GTC)
- LEAP
- EAP-TLS

Cisco Secure Services Client Version 4.0

The following EAP methods are certified for the Cisco Secure Services Client (formerly, Meetinghouse AEGIS SecureConnect) Version 4 supplicant with HP-UX AAA Server A.07.00:

- EAP-TTLS (PAP, CHAP, MSCHAP, MSCHAPv2, EAP-MD5, EAP-MSCHAPv2)
- LEAP
- EAP-TLS
- EAP-MD5
- PEAP (EAP-GTC, EAP-MSCHAPv2)

Juniper Networks Odyssey Access Client Version 4.5

The following EAP methods are certified for the Juniper Networks Odyssey (formerly, Funk Software Odyssey) Access Client Version 4.5 supplicant with the HP-UX AAA Server A.07.00:

- EAP-TTLS (PAP, CHAP, MSCHAP, MSCHAPv2, EAP-MD5, EAP-MSCHAPv2)
- LEAP
- EAP-TLS
- EAP-MD5
- PEAP (EAP-GTC, EAP-MSCHAPv2)

Microsoft for Windows 2000 (with SP4) and Windows XP (SP1 or SP2)

The following EAP methods are certified for the Microsoft Windows 2000 (with SP4) and Windows XP (SP1 or SP2) supplicants with the HP-UX AAA Server A.07.00:

- PEAP (EAP-MSCHAPv2)
- EAP-TLS

Product Documentation

HP-UX AAA Server documentation is available on <http://www.docs.hp.com>.

The documents listed in Table 2 are also installed with the HP-UX AAA Server.

Table 2 **Documentation Installed with the HP-UX AAA Server**

Document	Location
Text Release Notes	/opt/aaa/README
Administrator's Guide	/opt/aaa/share/doc/admin.pdf
Man pages	/opt/aaa/share/man/
Secure LAN Advisor Help System	Server Manager administration utility

NOTE The Administrator's Guide may also be accessed via the Server Manager administration utility

IMPORTANT Monitor the HP-UX AAA Server documentation for the most recent product documentation.

The Secure LAN Advisor

The Secure LAN Advisor is an HTML help system in the Server Manager administration utility that walks you through the Server Manager screens and tasks for securing LANs and WLANs with the HP-UX AAA Server.

The Secure LAN Advisor provides information only, it does not edit configuration files. Follow the Secure LAN Advisor and use the Server Manager to create and deploy basic AAA configurations for securing LANs and WLANs. See the HP-UX AAA Server A.07.00 Administrator's Guide on <http://docs.hp.com> for more information.

Installation Requirements

This section lists the HP-UX AAA Server A.07.00 requirements:

Hardware and Operating Systems Requirements

Following are the hardware and operating systems requirements for installing HP-UX AAA Server A.07.00:

- Hardware: HP 9000 and HP Integrity Servers
- Operating Systems: HP-UX 11i v1, HP-UX 11i v2, or HP-UX 11i v3
- Minimum of 128 MB memory
- 5 GB disk space

System Resource Requirements

Following are the minimum system resources required to install and run HP-UX AAA Server A.07.00:

- Disk Space: 5 GB
- Memory: 128 MB

Product Requirements

Table 3 lists the product requirements for the HP-UX AAA Server A.07.00 on HP-UX 11i v1, HP-UX 11i v2, and HP-UX 11i v3:

Table 3 **Product Requirements**

Product Requirements	HP-UX 11i v1	HP-UX 11i v2	HP-UX 11i v3
	Version	Version	Version
HP-UX SDK for Java	1.4.2.x or higher	1.4.2.x or higher	1.4.2.x or higher
HP-UX Tomcat-based Servlet Engine	1.0.03.x or higher	1.0.10.01 or higher	B.5.5.9.04 or higher

Table 3 Product Requirements (Continued)

Product Requirements	HP-UX 11i v1	HP-UX 11i v2	HP-UX 11i v3
	Version	Version	Version
OpenSSL	A.00.09.07e or higher	A.00.09.07e or higher	A.00.09.08d or higher

You can download all the product requirements at the HP Software Depot (<http://software.hp.com>) using the following links:

- [HP-UX SDK for Java](#)
- [HP-UX Tomcat-based Servlet Engine](#)
- [OpenSSL from HP](#)

NOTE

HP-UX Tomcat-based Servlet Engine is a component of HPUXWSSUITE on HP-UX 11i v1 and HP-UX 11i v2. On HP-UX 11i v3, HP-UX Tomcat-based Servlet Engine is version B.5.5.9.04 is available as part of the core operating environment.

Patch Requirements

Table 4 lists the patch requirements for the HP-UX AAA Server A.07.00 on HP-UX 11i v1, HP-UX 11i v2, and HP-UX 11i v3.

Table 4 Patch Requirements

Patch Requirements	HP-UX 11i v1	HP-UX 11i v2	HP-UX 11i v3
	Version	Version	Version
BUNDLE11i	Required (February 2001 or later)	Required (Sep. 2004 or later)	Not applicable
PHSS_26946 or later	Required	Not applicable	Not applicable
PHCO_31903 or later	Required	Not applicable	Not applicable

Installation Requirements

Download the patch dependencies from the Patch/Firmware Database in the [maintenance and support for HP products](#) section of HP's IT Resource Center at <http://www.itrc.hp.com>.

Web Browser Requirements

You must have a Web browser to use the Server Manager interface to administer and configure the HP-UX AAA Servers. Following are the Web browser requirements for HP-UX AAA Server A.07.00:

- Use only the following web browsers with the HP-UX AAA Server A.07.00—known interoperability issues exist with other web browser versions:
 - Internet Explorer 6.0 or higher with Java 1.4.2.09 or higher
 - Mozilla 1.7.12 or higher with Java 1.4.x or higher
- Set the browser preferences (Internet options) to “always compare loaded pages to cached pages”.

NOTE

Download Mozilla free of charge from HP at:

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

LDAP Compatibility

The HP-UX AAA Server A.07.00 is designed to interoperate with LDAP version 3 compliant directories. HP has certified the HP-UX AAA Server A.07.00 with the Red Hat Directory Server version 7.0, Netscape Directory Server version 6.2, and OpenLDAP version 2.3.24.001.

NOTE

HP recommends the Netscape/Red Hat Directory Server for environments requiring high performance and availability.

SQL Access Requirements

The HP-UX AAA Server A.07.00 is designed to interoperate with the Oracle OCI and ODBC compliant database clients/drivers. The database client/driver products are not included with the HP-UX AAA server, and must be acquired and installed separately.

In addition, the HP-UX AAA Server provides connectors for the client/driver products. Connectors for the following database clients/drivers are included with this release:

Table 5

SQL Access Requirements for HP-UX AAA Server A.07.00

Vendor	Client
Oracle - OCI	Oracle Instant Client Version 10.2.0.2
MySQL - ODBC	MySQL Unix ODBC Client Version 2.2.11/MySQL Client 5.0.22

For information on obtaining additional connectors for other database clients or drivers, email aaainfo@cup.hp.com.

Availability in Native Languages

The HP-UX AAA Server A.07.00 is currently available in English only.