

# HP-UX PAM RADIUS A.01.00 Release Notes

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

HP Part Number: 5992-3382  
Published: March 2008  
Edition: 1.0



© Copyright 2008 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.

UNIX is a registered trademark of The Open Group.

---

## HP-UX PAM RADIUS A.01.00 Release Notes

This document provides the most recent product information on HP-UX PAM RADIUS A.01.00 software that is supported on a system running an HP-UX 11i v2 (B.11.23) or HP-UX 11i v3 (B.11.31) operating system. This document addresses the following topics:

- “HP-UX PAM RADIUS Software Overview.”
- “HP-UX PAM RADIUS A.01.00 Features and Benefits.”
- “PAM Modules Supported by HP-UX PAM RADIUS A.01.00”
- “Known Problems and Limitations” (page 8)
- “HP-UX PAM RADIUS Resources” (page 9)
- “HP-UX PAM RADIUS Software Availability” (page 9)
- “Installing HP-UX PAM RADIUS” (page 9)
- “Software Availability in Native Languages” (page 10)

### HP-UX PAM RADIUS Software Overview

The HP-UX PAM RADIUS A.01.00 software enables users to use RADIUS authentication for system entry services, such as `login` and `ftp`. Using this software, you can enable RADIUS authentication by configuring the options in the `/etc/pam.conf` file. The HP-UX PAM RADIUS A.01.00 software also enables PAM-capable systems to function as RADIUS clients for authentication and accounting requests. The HP-UX implementation of PAM RADIUS is based on the PAM Authentication and Accounting module v1.3.17 from FreeRADIUS.

### HP-UX PAM RADIUS A.01.00 Features and Benefits

The HP-UX PAM RADIUS A.01.00 software offers the following features and benefits:

- Performs RADIUS authentication (PAP based) and accounting with RADIUS servers that are compliant with RFCs 2865 and RFC 2866.
- Supports OTP based authentication. This feature makes the HP-UX PAM RADIUS software compatible with RADIUS servers that support OTP based authentication, such as the HP-UX AAA Server A.07.01 and later versions. Typically, OTP is used to provide two-factor authentication.
- Supports IPv6 communication with RADIUS servers that support IPv6.
- Supports controlled access of a service to the users based on realm.

### PAM Modules Supported by HP-UX PAM RADIUS A.01.00

The HP-UX PAM RADIUS A.01.00 software supports the following modules:

- “Authentication Module” (page 4)
- “Account Management Module” (page 8)
- “Session Management Module” (page 8)

The following sections discuss these modules in detail.

## Authentication Module

The HP-UX PAM RADIUS authentication module provides the following functions:

- The `pam_sm_authenticate()` function, which verifies the identity of a user against the RADIUS server
- The `pam_sm_setcred()` function, which sets user credentials

The following options to the HP-UX PAM RADIUS authentication module can be set in the `/etc/pam.conf` file.

`debug`

This option enables `syslog(3C)` to log debugging information at `LOG_DEBUG` level.

`use_first_pass`

This option allows the initial password (entered when the user is authenticated to the first authentication module in the stack) to authenticate with the RADIUS server. If the user cannot be authenticated, or if this is the first authentication module in the stack, HP-UX PAM RADIUS quits without prompting the user for a password. HP recommends that this option be used only if the authentication module is designated as `optional` in the `/etc/pam.conf` configuration file.

`try_first_pass`

This option allows the initial password (entered when the user is authenticated to the first authentication module in the PAM stack) to authenticate with the RADIUS server. If the user cannot be authenticated, or if this is the first authentication module in the stack, HP-UX PAM RADIUS prompts the user for a password.

`default_realm=<realm name>`

This option enables sending a configured realm name along with `<user name>` to the RADIUS server. The `<user name>` and configured `<realm name>` are combined as `<user name>@<realm name>` and sent in the `User-Name` RADIUS attribute to the RADIUS server.

`skip_passwd`

This option enables HP-UX PAM RADIUS to authenticate users without prompting for a password, even if no password is retrieved from a previous module. HP-UX PAM RADIUS sends a previous password if it exists. If the previous password does not exist, it sends a `NULL` password. If authentication fails, the authentication module exits with `PAM_ERROR`.

If an Access-Challenge message is returned, HP-UX PAM RADIUS displays the Access-Challenge message, and prompts the user for a response and returns success or failure as appropriate.

The password sent to the next authentication module is not the response to the challenge. If a password from a previous authentication module exists, it is passed to the next authentication module. Otherwise, no password is sent to the next module.

`conf=<filename>`

This option enables configuring a different filename for the RADIUS server configuration file. The default configuration file is `/etc/raddb/server`. For information on the syntax of the configuration file, see the `/etc/raddb/server.sample` sample configuration file.

`client_id=<clientID>`

This option enables configuring a `NAS-Identifier` RADIUS attribute with the `<clientID>` string instead of the standard PAM service name (such as `login` and `su`). You can disable this option by using a blank value for `client_id`, for example `'client_id='`.

`retry=<retrycount>`

This option allows `<retrycount>` number of authentication attempts before continuing to the next configured RADIUS server.

`ruser`

This option uses the value of `PAM_RUSER` instead of `PAM_USER`, to determine the user name to authenticate using RADIUS. This option is valid only if `PAM_USER` is root.

`localifdown`

This option prompts HP-UX PAM RADIUS to return `PAM_IGNORE` instead of `PAM_AUTHINFO_UNAVAIL`, if RADIUS authentication fails because of network unavailability. `PAM_IGNORE` prompts the PAM engine to continue down the stack regardless of the control option used.

The following options have been added to support OTP authentication:

`recv_authtok=<tokentype>`

This option informs the module about the authentication token that was set as `PAM_AUTHTOK item_type` in the PAM handle

by the previous module. Following are the valid values for *<tokentype>*:

Password	The previous module had set password as the authentication token. This is the default value, if this option is not set, or if an invalid value is set.
Otp	The previous module had set OTP as the authentication token.
PasswordOtp	The previous module had set password appended with OTP as the authentication token.

**Usage when use\_first\_pass is set:**

- If the option set here (for example, Password) is not consistent with rad\_authtok (for example, Otp), then the module fails to authenticate the user.
- If rad\_authtok=PasswordOtp, and rcv\_authtok=Password (or OTP), the module picks the Password (or Otp) from the PAM handle and prompts the user for the missing token (either Otp or Password).

**Usage when try\_first\_pass is set:**

If try\_first\_pass is set, then the module attempts to use the previous value if possible; if not it prompts the user for the required authentication tokens.



---

**NOTE:** This option is used only when try\_first\_pass or use\_first\_pass is set.

---

rad\_authtok=*<tokentype>*

This option informs the module about the nature of the validation that must be performed. Based on the value of the rad\_authtok option and the authentication token received from the previous module, HP-UX PAM RADIUS prompts the user for the missing authentication tokens and performs the authentication. Following are the valid values for *<tokentype>*:

Password	Perform only password validation. This is the default value, if this option is not set, or if an invalid value is set.
Otp	Perform only OTP validation. When this option is set, the module prompts the user for OTP information (if required). Once the module receives the OTP, it sends it as a password to the RADIUS server for validation. Set this option when using RADIUS servers that support OTP based authentication (such as the HP-UX AAA Server A.07.01 and later versions).
PasswordOtp	Perform both Password and OTP validation. During this operation the module appends the OTP value to the password and sends it to the RADIUS server for authentication. Set this option when using RADIUS servers that support OTP based authentication (such as HP-UX AAA Server A.07.01 and later versions).
<code>set_authtok=&lt;tokentype&gt;</code>	This option allows you to configure the authentication token that must be set as <code>PAM_AUTHTOK item_type</code> in the PAM handle. Following are the valid values for <code>&lt;tokentype&gt;</code> :
Password	Set the password as the authentication token. This is the default value, if this option is not set, or if an invalid value is set.
Otp	Set the OTP as the authentication token.
PasswordOtp	Set the password appended with OTP as the authentication token.

If the authentication token that must be set as `PAM_AUTHTOK` in the PAM handle is not available, then the module ignores this option.

## Account Management Module

The HP-UX PAM RADIUS account management module provides functions to manage user accounts.



**NOTE:** Account management (tasks such as user's password and account verification by checking the password and account expiration, and log-in time validation) is not defined under RADIUS protocol standard. Therefore, this module returns `PAM_SUCCESS`. The functions in this module are supported only for the naming convention as per the PAM framework.

You can set the debug option in the `/etc/pam.conf` file. The debug option is passed to the HP-UX PAM RADIUS account management module. For more information on the debug option, see the option information listed in “Authentication Module” (page 4).

## Session Management Module

The HP-UX PAM RADIUS session management module provides the following functions:

- The `pam_sm_open_session()` function, which initiates sessions
- The `pam_sm_close_session()` function, which terminates sessions

A RADIUS Accounting-Start message is sent to the RADIUS server when the session is opened and an Accounting-Stop message is sent to the RADIUS server when the session is terminated.

The following options can be set to the session management module through the `/etc/pam.conf` file:

- `debug`
- `default_realm=<realm name>`
- `conf=<filename>`
- `clientid=<clientID>`
- `retry=<retrycount>`
- `localifdown`

For more information on these options, see “Authentication Module” (page 4).

## Known Problems and Limitations

There are no known problems and limitations in the HP-UX PAM RADIUS A.01.00 software.

## HP-UX PAM RADIUS Resources

For more information about the HP-UX PAM RADIUS A.01.00 software, see the following documents:

- The *pam\_radius*(5) manpage that is bundled with the HP-UX PAM RADIUS software
- The FreeRADIUS website at:  
<http://www.freeradius.org/>
- The PAM RFC - 86.0 available at the following web address:  
<http://www.opengroup.org/tech/rfc/rfc86.0.html>



**NOTE:** Documentation for the HP-UX AAA Server A.07.01 is available at:  
<http://www.docs.hp.com/en/internet.html#AAA%20Server%20%28RADIUS%29>

## HP-UX PAM RADIUS Software Availability

The HP-UX PAM RADIUS A.01.00 software is available on the HP Software Depot at the following web address:

<http://software.hp.com>.

## Installing HP-UX PAM RADIUS

This section describes how to install the HP-UX PAM RADIUS A.01.00 software. It also discusses the system and patch requirements for installing the HP-UX PAM RADIUS A.01.00 software.

### System Requirements

Table 1 lists the system requirements for installing the HP-UX PAM RADIUS A.01.00 software.

**Table 1 System Requirements for Installing the HP-UX PAM RADIUS A.01.00 Software**

Component	Requirement
Operating System	<ul style="list-style-type: none"><li>• HP-UX 11i v2</li><li>or</li><li>• HP-UX 11i v3</li></ul>
Hardware	<ul style="list-style-type: none"><li>• HP 9000 servers</li><li>or</li><li>• HP Integrity servers</li></ul>
Disk space	Approximately 32 MB of disk space

## Patch Requirements

You need not install any patches before installing the HP-UX PAM RADIUS A.01.00 software.

## Installation Procedure

To install the HP-UX PAM RADIUS A.01.00 software, complete the following steps:

1. Log in as superuser.
2. Download the HP-UX PAM RADIUS depot file from the following web address:  
<http://software.hp.com> .
3. Move the depot to the /tmp directory.
4. Verify that the depot is downloaded correctly by entering the `swlist` command.



**NOTE:** The `swlist` and `swinstall` commands require that the full path name to the source depot be specified. For example:

```
swlist -d @ /tmp/<depot_name>
# Initializing...
# Contacting target "localhost"...
#
# Target:  localhost:/tmp/PAMRADIUS.depot
#
#
# Bundle(s) :
#
HP-UX-PAM-RADIUS  A.01.00.00  HP-UX PAM RADIUS
```

5. To install the HP-UX PAM RADIUS software, enter the `swinstall` command, as follows:

```
swinstall -s /tmp/<depot_name> \*
```

6. To configure the HP-UX PAM RADIUS A.01.00 software, edit the `/etc/pam.conf` and `/etc/raddb/server` files.

For more information on configuring the HP-UX PAM RADIUS A.01.00 software, see `/etc/raddb/quickstart.txt`.

## Software Availability in Native Languages

The HP-UX PAM RADIUS A.01.00 software is available in English only.